



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2021-0043053
(43) 공개일자 2021년04월21일

(51) 국제특허분류(Int. Cl.)
H04L 12/26 (2006.01) H04L 12/24 (2006.01)
H04L 12/40 (2006.01)
(52) CPC특허분류
H04L 43/0823 (2013.01)
H04L 12/40071 (2013.01)
(21) 출원번호 10-2019-0125549
(22) 출원일자 2019년10월10일
심사청구일자 2019년10월10일

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
김휘강
서울특별시 서초구 태봉로2길 65 404동 302호 (우면동, 테이처힐4단지)
송현민
서울특별시 성북구 안암로9가길 87-6 (안암동5가)
(74) 대리인
김홍석

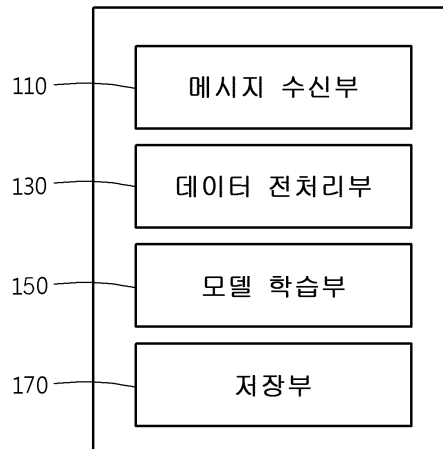
전체 청구항 수 : 총 12 항

(54) 발명의 명칭 오토인코더를 이용한 CAN 트래픽 모델링 장치 및 방법과 이상징후 탐지 장치 및 방법

(57) 요약

CAN 트래픽 모델링 장치가 개시된다. 상기 CAN 트래픽 모델링 장치는 복수의 CAN(Controller Area Network) 메시지들 각각으로부터 CAN ID를 추출하고, 추출된 CAN ID를 전처리하여 학습 데이터를 생성하는 데이터 전처리부 및 상기 학습 데이터를 입력 데이터로 이용하여 오토인코더(autoencoder) 모델을 학습시켜 CAN 트래픽 모델을 생성하는 모델 학습부를 포함한다.

대표도 - 도1



10

(52) CPC특허분류

H04L 41/145 (2013.01)

H04L 43/04 (2013.01)

H04L 2012/40215 (2013.01)

H04L 2012/40273 (2013.01)

명세서

청구범위

청구항 1

복수의 CAN(Controller Area Network) 메시지들 각각으로부터 CAN ID를 추출하고, 추출된 CAN ID를 전처리하여 학습 데이터를 생성하는 데이터 전처리부; 및

상기 학습 데이터를 입력 데이터로 이용하여 오토인코더(autoencoder) 모델을 학습시켜 CAN 트래픽 모델을 생성하는 모델 학습부를 포함하는 CAN 트래픽 모델링 장치.

청구항 2

제1항에 있어서,

상기 데이터 전처리부는 상기 CAN ID를 비트 스트림으로 변환하여 상기 학습 데이터를 생성하는, CAN 트래픽 모델링 장치.

청구항 3

제2항에 있어서,

상기 데이터 전처리부는 3자리의 16진수로 표현되는 상기 CAN ID를 길이가 11인 비트 스트림(bit stream)으로 변환하는, CAN 트래픽 모델링 장치.

청구항 4

제1항에 있어서,

상기 모델 학습부는,

복수 개의 전처리된 CAN ID를 상기 오토인코더 모델의 입력으로 이용하고,

상기 오토인코더 모델의 손실 함수의 출력값인 손실(loss)이 감소하는 방향으로 상기 오토인코더 모델의 가중치들을 갱신하는 동작을 반복적으로 수행하는,

CAN 트래픽 모델링 장치.

청구항 5

제4항에 있어서,

상기 손실 함수는 유클리디안 거리(Euclidean distance)인,

CAN 트래픽 모델링 장치.

청구항 6

적어도 프로세서를 포함하는 CAN 트래픽 모델링 장치에 의해 수행되는 CAN 트래픽 모델링 방법에 있어서,

복수의 CAN 메시지들 각각으로부터 CAN ID를 추출하는 단계;

상기 CAN ID를 미리 정해진 크기를 갖는 비트 스트림으로 변환하는 단계; 및

상기 비트 스트림으로 구성된 학습 데이터를 이용하여 오토인코더 모델을 학습시키켜 CAN 트래픽 모델을 생성하는 단계를 포함하는 CAN 트래픽 모델링 방법.

청구항 7

CAN 버스 상에서 브로드캐스트되는 복수의 CAN 메시지들 각각으로부터 CAN ID를 추출하고, 상기 CAN ID를 비트 스트림으로 변환하는 데이터 전처리부; 및

복수의 CAN ID로부터 생성된 비트 스트림을 제6항에 기재된 방법에 의해 생성된 CAN 트래픽 모델에 입력하고 상기 CAN 트래픽 모델의 손실에 기초하여 차량의 이상징후 유무를 판단하는 이상징후 판단부를 포함하는 이상징후 탐지 장치.

청구항 8

제7항에 있어서,

상기 데이터 전처리부는 3자리의 16진수로 표현되는 상기 CAN ID를 길이가 11인 비트 스트림으로 변환하는, 이상징후 탐지 장치.

청구항 9

제7항에 있어서,

상기 이상징후 탐지 장치는 상기 차량에 설치된 ECU(Electronic Control Unit)인, 이상징후 탐지 장치.

청구항 10

제6항에 기재된 방법에 의하여 생성된 CAN 트래픽 모델이 설치된 이상징후 탐지 장치에 의해 수행되는 이상징후 탐지 방법에 있어서,

CAN 버스 상에서 브로드캐스트되는 복수의 CAN 메시지들 각각으로부터 CAN ID를 추출하는 단계;

상기 CAN ID를 비트 스트림으로 변환하는 단계;

복수의 CAN ID로부터 생성된 비트 스트림을 상기 CAN 트래픽 모델에 입력하고 상기 CAN 트래픽 모델의 손실을 계산하는 단계; 및

상기 손실에 기초하여 차량의 이상징후 유무를 판단하는 단계를 포함하는 이상징후 탐지 방법.

청구항 11

제10항에 있어서,

상기 이상징후 유무를 판단하는 단계는 상기 손실이 미리 정해진 임계값보다 큰 경우 상기 차량에 이상징후가 있는 것으로 판단하는,

이상징후 탐지 방법.

청구항 12

복수의 CAN(Controller Area Network) 메시지들 각각으로부터 CAN ID를 추출하고, 추출된 CAN ID를 전처리하여 학습 데이터를 생성하는 데이터 전처리부; 및

상기 학습 데이터를 입력 데이터로 이용하여 오토인코더 모델을 학습시켜 CAN 트래픽 모델을 생성하는 모델 학습부를 포함하고,

상기 오토인코더 모델은 컨벌루션널 오토인코더(Convolutional Autoencoder, CAE)와 오토인코더의 결합으로 구성되는,

CAN 트래픽 모델링 장치.

발명의 설명

기술 분야

[0001] 본 발명은 자동차의 보안성 향상을 위해 오토인코더를 이용하여 차량 내에서 발생하는 CAN(Controller Area Network) 트래픽을 모델링하고, 이를 이용하여 CAN 버스 상에서 발생하는 이상 징후를 탐지하는 장치 및 방법에 관한 것이다.

배경 기술

[0003] 자동차 제어 시스템이 전통적인 기계식 제어 시스템에서 전자식 제어 시스템으로 전환되고 있다. 전자식 제어 시스템을 사용함으로써, 컴퓨터 네트워크와 유사하게 DoS(Denial of Service) 공격, 위조 메시지 전송 등의 사이버 공격으로부터 위협이 발생하게 되었다.

[0004] 자동차의 CAN 네트워크는 OBD-II(On-Board Diagnosis-II) 단자를 통해 접근하거나 CAN 네트워크에 연결된 텔레매틱스 장비의 취약점을 이용한 접근이 가능하다. CAN은 차량 네트워크에 사용하기 위해 개발된 네트워크 프로토콜로 여러 개의 ECU(Electronic Control Unit)가 서로 통신할 수 있도록 경제적이며 안정적인 네트워크를 제공하는 기술이다. ECU는 CAN 버스에 브로드캐스팅되는 모든 CAN 메시지를 확인하여 자신과 관련된 CAN 메시지만을 필터링하여 제어를 수행하게 된다.

[0005] 하지만, CAN은 모든 ECU에 메시지를 전달하는 브로드캐스팅 프로토콜임에도 불구하고 데이터 암호화나 인증 기능을 대부분 제공하지 않기 때문에 메시지 주입 등의 공격에 취약하다. 본 발명에서는 차량 내부 네트워크 중 CAN 네트워크에서 발생하는 트래픽을 분석하여 이상 징후를 탐지하는 기법을 제안한다.

[0006] 또한, 기존의 기계학습(machine learning) 기반의 CAN 이상징후 탐지 기술은 탐지 모델을 생성하기 위한 학습 데이터로 정상적인 CAN 트래픽과 실제 공격 트래픽이 포함된 CAN 트래픽을 모두 필요로 한다. 특히, 이러한 방식으로 생성된 이상징후 탐지 모델은 학습 데이터에 포함된 이상징후 패턴은 잘 포착하는 반면에 학습 데이터에 포함되지 않은 새로운 유형의 이상징후는 탐지하지 못하는 한계점이 있다.

[0007] 이에, 본 발명은 이상징후가 포함되지 않은 정상 상태에서의 차량 CAN 트래픽 패턴을 오토인코더(autoencoder)를 이용하여 모델링함으로써, 이상징후 발생 시 발생하는 트래픽 패턴의 변화를 감지하여 이상징후를 탐지하는 기술을 제안한다.

선행기술문헌

특허문헌

[0009] (특허문헌 0001) 대한민국 공개특허 제2019-0063209호 (2019.06.07. 공개)

(특허문헌 0002) 대한민국 공개특허 제2018-0109642호 (2018.10.08. 공개)

발명의 내용

해결하려는 과제

- [0010] 본 발명이 이루고자 하는 기술적인 과제는 이상징후가 포함되지 않은 정상 상태에서의 차량 CAN 트래픽 패턴을 오토인코더를 이용하여 모델링함으로써, 이상징후 발생 시 발생하는 트래픽 패턴의 변화를 감지하여 이상징후를 탐지하는 모델의 생성 장치 및 방법과 생성된 모델을 이용하여 이상징후를 탐지하는 장치 및 방법을 제공하는 것이다.

과제의 해결 수단

- [0012] 본 발명의 실시예에 따른 CAN 트래픽 모델링 장치는 복수의 CAN(Controller Area Network) 메시지들 각각으로부터 CAN ID를 추출하고, 추출된 CAN ID를 전처리하여 학습 데이터를 생성하는 데이터 전처리부 및 상기 학습 데이터를 입력 데이터로 이용하여 오토인코더(autoencoder) 모델을 학습시켜 CAN 트래픽 모델을 생성하는 모델 학습부를 포함한다.
- [0013] 또한, 본 발명의 실시예에 따른 CAN 트래픽 모델링 방법은 적어도 프로세서를 포함하는 CAN 트래픽 모델링 장치에 의해 수행되고, 복수의 CAN 메시지들 각각으로부터 CAN ID를 추출하는 단계, 상기 CAN ID를 미리 정해진 크기를 갖는 비트 스트림으로 변환하는 단계, 상기 비트 스트림으로 구성된 학습 데이터를 이용하여 오토인코더 모델을 학습시켜 CAN 트래픽 모델을 생성하는 단계를 포함한다.
- [0014] 또한, 본 발명의 실시예에 따른 이상징후 탐지 장치는 CAN 버스 상에서 브로드캐스트되는 복수의 CAN 메시지들 각각으로부터 CAN ID를 추출하고, 상기 CAN ID를 비트 스트림으로 변환하는 데이터 전처리부 및 복수의 CAN ID로부터 생성된 비트 스트림을 상술한 방법에 의해 생성된 CAN 트래픽 모델에 입력하고 상기 CAN 트래픽 모델의 손실에 기초하여 차량의 이상징후 유무를 판단하는 이상징후 판단부를 포함한다.
- [0015] 또한, 본 발명의 실시예에 따른 이상징후 탐지 방법은 상술한 방법에 의하여 생성된 CAN 트래픽 모델이 설치된 이상징후 탐지 장치에 의해 수행되고, CAN 버스 상에서 브로드캐스트되는 복수의 CAN 메시지들 각각으로부터 CAN ID를 추출하는 단계, 상기 CAN ID를 비트 스트림으로 변환하는 단계, 복수의 CAN ID로부터 생성된 비트 스트림을 상기 CAN 트래픽 모델에 입력하고 상기 CAN 트래픽 모델의 손실을 계산하는 단계, 및 상기 손실에 기초하여 차량의 이상징후 유무를 판단하는 단계를 포함한다.
- [0016] 또한, 본 발명의 다른 실시예에 따른 CAN 트래픽 모델링 장치는 복수의 CAN(Controller Area Network) 메시지들 각각으로부터 CAN ID를 추출하고, 추출된 CAN ID를 전처리하여 학습 데이터를 생성하는 데이터 전처리부 및 상기 학습 데이터를 입력 데이터로 이용하여 오토인코더 모델을 학습시켜 CAN 트래픽 모델을 생성하는 모델 학습부를 포함하고, 상기 오토인코더 모델은 컨벌루션널 오토인코더(Convolutional Autoencoder, CAE)와 오토인코더의 결합으로 구성된다.

발명의 효과

- [0018] 본 발명의 실시예에 따른 이상징후 탐지 모델은 정상 상태에서의 CAN 트래픽만으로 모델을 학습하고, 이를 통해 학습 데이터에 포함되지 않은 새로운 유형의 이상징후를 탐지할 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 실시예에 따른 CAN 트래픽 모델링 장치의 기능 블록도이다.
- 도 2는 도 1에 도시된 데이터 전처리부에 의한 전처리 동작을 설명하기 위한 도면이다.
- 도 3은 도 1에 도시된 모델 학습부에 의해 학습되는 오토인코더 모델의 일 실시예를 도시한다.
- 도 4는 본 발명의 일 실시예에 따른 이상징후 탐지 장치의 기능 블록도이다.

도 5는 도 1에 도시된 모델 학습부에 의해 학습되는 오토인코더 모델의 다른 실시예를 도시한다.

발명을 실시하기 위한 구체적인 내용

- [0021] 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.
- [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 명명될 수 있고 유사하게 제2 구성 요소는 제1 구성 요소로도 명명될 수 있다.
- [0024] 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.
- [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. 그러나, 특허출원의 범위가 이러한 실시 예들에 의해 제한되거나 한정되는 것은 아니다. 각 도면에 제시된 동일한 참조 부호는 동일한 부재를 나타낸다.
- [0029] 도 1은 본 발명의 일 실시예에 따른 CAN 트래픽 모델링 장치의 기능 블록도이다.
- [0030] 도 1을 참조하면, 이상징후 탐지 모델 생성 장치, 트래픽 모델 생성 장치, 모델링 장치 등으로 명명될 수도 있는 CAN 트래픽 모델링 장치(10)는 CAN 네트워크 상에서 브로드캐스트되는 CAN 메시지들의 흐름, 즉 CAN 트래픽을 모델링함으로써 이상 징후 탐지 모델, 트래픽 모델, 탐지 모델 등으로 명명될 수도 있는 CAN(Controller Area Network) 트래픽 모델을 생성할 수 있다.
- [0031] CAN 트래픽 모델링 장치(10)는 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. 또한, 프로세서는 중앙 처리 장치(Central Processing Unit, CPU), 마이크로 컨트롤러 유닛(Micro Controller Unit, MCU), 마이콤(Micro Processor, Micom), 애플리케이션 프로세서(Application Processor, AP), 전자 제어 유닛(Electronic Control Unit, ECU), 그래픽 처리 장치(Graphic Processing Unit, GPU) 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. 또한, 컴퓨팅 장치는 데스크톱 컴퓨터, 랩톱 컴퓨터, 서버용 컴퓨터 및/또는 이외 정보 처리 기능을 수행할 수 있는 적어도 하나의 전자 장치를 포함할 수 있다.

[0032] 도 1을 참조하면, CAN 트래픽 모델링 장치(10)는 데이터 전처리부(130)와 모델 학습부(150)를 포함한다. 실시예에 따라, CAN 트래픽 모델링 장치(10)는 메시지 수신부(110) 및/또는 저장부(170)를 더 포함할 수 있다.

[0033] 메시지 수신부(110)는 CAN 네트워크 상에서 발생하는 CAN 메시지들, 즉 CAN 버스 상에서 브로드캐스트되는 CAN 메시지들을 수신할 수 있다. 실시예에 따르면, 메시지 수신부(110)는 CAN 버스에 직접 접속되어 CAN 버스 상에서 브로드캐스트되는 CAN 메시지들을 직접 수신할 수 있다. 다른 예로, 메시지 수신부(110)는 차량에 설치된 OBD-II 단자로부터 CAN 메시지들을 수신할 수도 있다. 메시지 수신부(110)에 의해 수신된 CAN 메시지들은 저장부(170)에 저장될 수 있다. 또한, 본 발명에서 사용하는 학습 데이터(training data)는 차량이 정상 상태일 때 발생하는 CAN 메시지들로부터 생성되기 때문에, 메시지 수신부(110)에 의해 수신되는 CAN 메시지들은 정상 주행 중에 발생하는 CAN 메시지들일 수 있다.

[0034] 데이터 전처리부(130)는 CAN 메시지들을 전처리할 수 있다. CAN 트래픽 모델링 장치(10)에 메시지 수신부(110)가 포함되는 경우, 데이터 전처리부(130)는 메시지 수신부(110)로부터 상기 CAN 메시지들을 수신하거나 메시지 수신부(110)에 의해 CAN 메시지들이 저장된 저장부(170)로부터 상기 CAN 메시지들을 수신할 수 있다. 실시예에 따라, 데이터 전처리부(130)는 소정의 입력 장치를 통하여 입력된 CAN 메시지들을 수신하거나 상기 소정의 입력 장치를 통하여 입력되고 저장부(170)에 저장되어 있는 상기 CAN 메시지들을 수신할 수도 있다. 데이터 전처리부(130)에 의한 CAN 메시지들에 대한 구체적인 전처리 동작은 후술하기로 한다.

[0035] 모델 학습부(150)는 데이터 전처리부(130)에 의해 전처리된 CAN 메시지들을 이용하여 인공 신경망(Artificial Neural Network, ANN), 예컨대 오토인코더(autoencoder, 오토인코더 신경망이라고도 함)를 학습시킴으로써 CAN 트래픽 모델을 생성할 수 있다. 오토인코더는 딥러닝 모델의 한 가지 유형으로 모델의 입력으로 주어진 고차원의 입력 벡터(input vector)를 저차원의 벡터로 압축하는 인코더(encoder)와 압축된 저차원 벡터를 다시 입력 벡터와 동일한 크기의 출력 벡터로 복원하는 디코더(decoder)로 구성된다. 학습된 모델의 출력 값과 입력 값의 차이가 최소가 되도록 모델을 학습함으로써, 학습에 이용된 데이터의 패턴을 모델링할 수 있다. 즉, 모델 학습부(150)는 데이터 전처리부(130)에 의해 전처리된 학습 데이터를 이용하여 모델을 학습시키는 과정에서 손실을 계산하고, 손실을 감소시키는 방향으로 가중치를 갱신하는 동작을 반복 수행함으로써 CAN 트래픽 모델을 생성(또는 학습)할 수 있다. 모델 학습부(150)에 의한 CAN 트래픽 모델의 구체적인 생성 동작에 관하여는 후술하기로 한다.

[0036] 모델 학습부(150)는 트래픽 모델링 과정에서 유클리디안 거리(Euclidean distance)를 모델의 학습에 사용되는 손실 함수로 이용할 수 있다. 그러나, 본 발명의 권리범위가 이에 제한되는 것은 아니며, 실시예에 따라 다양한 손실 함수의 사용이 가능하다. 손실 함수의 입력값은 모델의 입력 벡터(X)와 모델의 출력 벡터(Y)이다. 모델의 학습은 아래 수학적 식 1로 정의될 수 있는 손실 함수의 출력 값, 즉 손실(loss)을 감소시키는 방향으로 모델의 가중치들을 갱신하는 과정이다.

수학적 식 1

$$loss = \sqrt{(Y-X)^2} = \sqrt{\sum_{i=1}^{11}(y_i - x_i)^2}$$

[0037]

[0038] 저장부(170)에는 메시지 수신부(110)에 의해 수신된 CAN 메시지들, 데이터 전처리부(130)에 의해 전처리된 CAN 메시지들, 모델 학습부(150)에 의해 생성되는 CAN 트래픽 모델 및/또는 CAN 트래픽 모델 생성 과정 중에 생성되는 데이터 등이 저장될 수 있다.

[0040] 도 2는 도 1에 도시된 데이터 전처리부에 의한 전처리 동작을 설명하기 위한 도면이다.

[0041] 도 1과 도 2를 참조하면, 데이터 전처리부(130)는 CAN 메시지에서부터 CAN ID를 추출하고, 추출된 CAN ID의 적어도 일부를 비트 스트림(bit stream)으로 변환할 수 있다(또는 복수의 차원을 가진 벡터로 변환할 수 있다. 즉, 데이터 전처리부(130)는 추출된 CAN ID를 벡터로 변환할 수 있다.

- [0042] 구체적으로, CAN ID는 3자리의 16진수로 표기되어 있는데, 데이터 전처리부(130)는 이를 한 자리씩 이진수로 표현하여 길이가 11인 비트 스트림으로 변환할 수 있다. 이때, 첫번째 16진수 수(도 2에서 '2')는 4 보다 같거나 작은 수의 자리(예컨대, 3 자리)의 이진수로 변환될 수 있다. 이는, 차량 내에 존재하는 CAN ID의 종류 및/또는 개수를 고려한 것이므로, 실시예에 따라서는 4 자리의 이진수로 변환될 수도 있다. 구체적인 예로써, 도 2의 '0x2B0'으로 표시된 16진수 CAN ID는 01010110000의 값을 갖는 비트 스트림 또는 (0,1,0,1,0,1,1,0,0,0,0)의 값을 갖는 벡터로 표현(또는 변환)될 수 있다. '0x2B0'에서 첫번째 16진수 수인 '2'는 '010'으로, 두번째 16진수 수인 'B'는 '1011'로, 마지막 16진수 수인 '0'은 '0000'으로 변환될 수 있다.
- [0043] 요컨대, 데이터 전처리부(130)는 k (k 는 2이상의 자연수, 예컨대 $k=3$)자리의 2^m 진수(m 은 2이상의 자연수, 예컨대 $m=4$)로 표현되는 CAN ID의 적어도 일부를 2진수로 변환하여 크기가 $k \times m$ 과 같거나 작은 비트 스트림(예컨대, 크기가 11인 비트 스트림) 또는 $k \times m$ 차원과 같거나 작은 차원을 갖는 벡터(예컨대, 11차원을 갖는 벡터)를 생성할 수 있다.
- [0044] 전처리된 CAN ID, 즉 비트 스트림(또는 벡터)은 오토인코더의 입력, 즉 학습 데이터로 이용될 수 있다.
- [0046] 도 3은 도 1에 도시된 모델 학습부에 의해 학습되는 오토인코더 모델의 일 실시예를 도시한다.
- [0047] 오토인코더 모델의 구조는 도 3에 도시된 바와 같이, 1개의 입력층(input layer), 복수 개의 은닉층(hidden layer) 및 1개의 출력층(output layer)으로 구성되어 있다. 도 3에 도시된 오토인코더 모델은 5개의 은닉층을 갖는 것으로 도시되어 있으나, 본 발명의 권리범위가 이에 제한되는 것은 아니며, 은닉층의 개수는 실시예에 따라 변화할 수 있다.
- [0048] 또한, 오토인코더 모델의 각 층(layer)의 크기는 121, 60, 30, 15, 30, 60, 121로 설정될 수 있으나, 이 또한 본 발명의 권리범위를 제한하는 것은 아니다. 실시예에 따라, 각 층(layer)의 크기는 변화할 수 있다. 이때, 입력 벡터는 3개의 층(121-60-30)으로 구성된 인코더를 통해 길이(또는 차원) 15의 벡터로 압축되고, 3개의 층(30-60-121)으로 구성된 디코더를 통해 길이(또는 차원) 121의 출력 벡터(Y)가 생성된다.
- [0049] 오토인코더 모델의 입력인 입력 벡터(X)와 출력인 출력 벡터(Y)는 동일한 크기를 갖는다. 예컨대, 전처리된 CAN ID의 크기가 p (p 는 2이상의 자연수) 비트일 때, 입력 벡터(X)와 출력 벡터(Y)는 $p \times q$ (q 는 동시에 또는 연속하여 입력되는 전처리된 CAN ID의 개수로써, 2 이상의 자연수임)의 크기를 갖는 비트 스트림(또는 $p \times q$ 의 차원을 갖는 벡터)일 수 있다. 일 예로, 입력층의 크기가 121인 경우, 각각의 길이가 11 비트인 전처리된 ID 11개가 입력 벡터를 구성할 수 있다.
- [0051] 도 4는 본 발명의 일 실시예에 따른 이상징후 탐지 장치의 기능 블록도이다.
- [0052] 도 4를 참조하면, 이상징후 탐지 장치(30)는 도 1에 도시된 CAN 트래픽 모델링 장치(10)에 의해 생성된 CAN 트래픽 모델을 이용하여 차량의 CAN 네트워크 상에서 브로드캐스트되는 CAN 메시지에 기초하여 차량의 이상징후 유무를 판단할 수 있다.
- [0053] 이상징후 탐지 장치(30)는 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. 또한, 프로세서는 중앙 처리 장치(Central Processing Unit, CPU), 마이크로 컨트롤러 유닛(Micro Controller Unit, MCU), 마이컴(Micro Processor, Micom), 애플리케이션 프로세서(Application Processor, AP), 전자 제어 유닛(Electronic Control Unit, ECU), 그래픽 처리 장치(Graphic Processing Unit, GPU) 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. 또한, 컴퓨팅 장치는 데스크톱 컴퓨터, 랩톱 컴퓨터, 서버용 컴퓨터 및/또는 이의 정보 처리 기능을 수행할 수 있는 적어도 하나의 전자 장치를 포함할 수 있다.
- [0054] 이상징후 탐지 장치(30)는 데이터 전처리부(330, 도 1에 도시된 데이터 전처리부(130)과 구분하기 위하여 제2 데이터 전처리부라 명명될 수도 있음)와 이상징후 판단부(150)를 포함한다. 실시예에 따라, 이상징후 탐지 장치(30)는 메시지 수신부(310, 도 1에 도시된 메시지 수신부(110)과 구분하기 위하여 제2 메시지 수신부라 명명될 수도 있음), 저장부(370, 도 1에 도시된 저장부(170)과 구분하기 위하여 제2 저장부라 명명될 수도 있음) 및 출력부(390) 중 적어도 하나를 더 포함할 수도 있다.

- [0055] 메시지 수신부(310)는 CAN 네트워크 상에서 발생하는 CAN 메시지들, 즉 CAN 버스 상에서 브로드캐스트되는 CAN 메시지들을 수신할 수 있다. 실시예에 따라, 메시지 수신부(310)는 CAN 버스에 직접 접속되어 CAN 버스 상에서 브로드캐스트되는 CAN 메시지들을 직접 수신할 수 있다. 다른 예로, 메시지 수신부(310)는 차량에 설치된 OBD-II 단자로부터 CAN 메시지들을 수신할 수도 있다. 메시지 수신부(310)에 의해 수신된 CAN 메시지들은 저장부(370)에 저장될 수 있다. 이와 같이, 메시지 수신부(310)가 CAN 네트워크 상에서 발생하는 CAN 메시지들을 실시간으로 수신함으로써, 이상징후 탐지 장치(30)는 차량의 현재 상태(즉, 이상징후의 유무)를 판단할 수 있다.
- [0056] 데이터 전처리부(330)는 CAN 메시지들을 전처리할 수 있다. 데이터 전처리부(330)는 메시지 수신부(310)로부터 상기 CAN 메시지들을 수신하거나 메시지 수신부(310)에 의해 CAN 메시지들이 저장된 저장부(370)로부터 상기 CAN 메시지들을 수신할 수 있다. 데이터 전처리부(330)에 의한 전처리 동작은 도 1에 도시된 데이터 전처리부(130)의 전처리 동작과 동일하므로 이에 대한 상세한 설명은 생략하기로 한다.
- [0057] 이상징후 판단부(350)는 도 1에 도시된 CAN 트래픽 모델링 장치(10)에 의해 생성된 CAN 트래픽 모델을 이용하여 차량의 이상징후 유무를 판단할 수 있다. 즉, 이상징후 판단부(350)는 데이터 전처리부(330)에 의해 전처리된 CAN 메시지들을 상기 CAN 트래픽 모델의 입력으로 이용하여 차량의 이상징후 유무를 판단할 수 있다. 예컨대, 이상징후 판단부(350)는 CAN 트래픽 모델의 입력층의 크기에 대응하는 크기를 갖는 비트 스트림 또는 CAN 트래픽 모델의 입력층의 크기에 대응하는 차원을 갖는 벡터를 상기 CAN 트래픽 모델에 입력한 후 손실(loss)을 계산할 수 있다. 이때, 계산된 손실이 미리 정해진 임계값(threshold, 예시적인 임계값은 0.088일 수 있음)보다 큰 경우(또는 크거나 같은 경우), 이상징후 판단부(350)는 차량에 이상이 발생한 것으로 판단할 수 있다. 정상적인 주행 중에 발생한 CAN 메시지들을 이용하여 학습을 마친 모델은 정상 데이터에 대하여 매우 낮은 손실 값을 갖는다. 반면에, 학습되지 않은 패턴의 데이터(이상징후가 포함된 CAN 메시지들)에 대해서는 상대적으로 높은 손실 값을 갖게 된다. 이를 이용하여, 학습된 모델의 손실 값이 임계값보다 높은 경우(또는 크거나 같은 경우), CAN 트래픽에 이상징후가 포함된 것으로 판단할 수 있다.
- [0058] 저장부(370)에는 메시지 수신부(310)에 의해 수신된 CAN 메시지들, 데이터 전처리부(330)에 의해 전처리된 CAN 메시지들, 도 1에 도시된 CAN 트래픽 모델링 장치(10)에 의해 생성된 CAN 트래픽 모델, 이상징후 유무를 판단하는 과정 중에서 생성되는 데이터 등이 저장될 수 있다.
- [0059] 출력부(390)는 이상징후 판단부(350)의 판단 결과에 따라 미리 정해진 동작을 수행할 수 있다. 예컨대, 차량에 이상이 발생하지 않았다고 판단되는 경우 아무런 동작을 수행하지 않을 수 있으며, 차량에 이상이 발생했다고 판단되는 경우에는 소정의 출력 장치(예컨대, 차량에 설치된 디스플레이 장치, 이상징후 탐지 장치(30)에 포함될 수 있는 별도의 디스플레이 장치, 차량 사용자의 단말기, 또는 차량의 이상징후 정보를 수집하기 위한 목적을 갖는 소정의 서버 등)으로 알림 메시지를 송신할 수 있다.
- [0061] 도 5는 도 1에 도시된 모델 학습부에 의해 학습되는 오토인코더 모델의 다른 실시예를 도시한다.
- [0062] 도 5에 도시된 바와 같이, 오토인코더 모델은 복수의 오토인코더가 결합된 구조를 가질 수 있다. 예컨대, 오토인코더 모델은 컨벌루션얼 오토인코더(Convolutional Autoencoder, CAE), 예컨대 1차원 컨벌루션얼 오토인코더(1D Convolutional Autoencoder)와 오토인코더의 결합으로 구성될 수 있다. 도 5에 도시된 오토인코더 모델에 포함된 오토인코더의 구조는 도 3에 도시된 오토인코더의 구조와 동일하게 1개의 입력층, 복수 개의 은닉층 및 1개의 출력층으로 구성되어 있고, 컨벌루션얼 오토인코더 역시 1개의 입력층, 복수 개의 은닉층 및 1개의 출력층으로 구성되어 있다. 다만, 본 발명의 권리범위가 상술한 입력층, 은닉층 및 출력층의 크기 및 구성에 제한되는 것은 아니다. 다만, 컨벌루션얼 오토인코더에 포함되는 인코더의 출력과 오토인코더에 포함되는 인코더의 출력의 크기는 동일할 수 있다. 이는, 두 가지의 오토인코더의 인코더로부터 출력되는 벡터를 결합하기 위함이다.
- [0063] 컨벌루션얼 오토인코더의 각 층(layer)의 크기는 11×11 , 11×5 , 11×3 , 11×1 , 11×3 , 11×5 , 11×11 로 설정될 수 있다. 그러나, 이 또한 본 발명의 권리범위를 제한하는 것은 아니며, 실시예에 따라 컨벌루션얼 오토인코더의 각 층의 구조와 크기는 변화할 수 있다. 컨벌루션얼 오토인코더 역시 입력 벡터는 3개의 층(11×11 , 11×5 , 11×3)으로 구성된 인코더를 통해 11×1 의 행렬(또는 벡터)로 압축되고, 3개의 층(11×3 , 11×5 , 11×11)으로 구성된 디코더를 통해 11×11 의 행렬의 출력이 생성될 수 있다.
- [0064] 또한, 컨벌루션얼 오토인코더의 입력 데이터와 오토인코더의 입력 데이터는 동일한 데이터(즉, 오토인코더 모델의 입력 벡터인 X)일 수 있다. 다만, 오토인코더의 입력 데이터는 비트 스트림(또는 다차원의 벡터)인 반면에, 컨벌루션얼 오토인코더의 입력 데이터는 입력 데이터(X)를 이용하여 생성된 행렬일 수 있다.

- [0065] 또한, 두 오토인코더(컨벌루션 오토인코더와 오토인코더)를 결합하기 위한 레이텐트 벡터(latent vector, 잠복 벡터로 명명되기도 함)는 컨벌루션 오토인코더에 포함되는 인코더의 출력과 오토인코더에 포함되는 인코더의 출력을 합산함으로써 생성할 수 있으며, 다시 레이텐트 벡터(또는 레이텐트 벡터를 2로 나눈 값)는 컨벌루션 오토인코더에 포함되는 디코더와 오토인코더에 포함되는 디코더의 입력으로 사용될 수 있다. 또한, 최종적인 모델의 출력(즉, 출력 벡터 Y)은 컨벌루션 오토인코더의 출력을 비트 스트림(또는 다차원의 벡터)으로 변환하고, 이를 오토인코더의 출력과 합산함으로써 계산될 수 있다. 실시예에 따라, 최종적인 모델의 출력(즉, 출력 벡터 Y)은 상술한 합산 결과를 2로 나눈 값이 될 수도 있다.
- [0066] 모델 학습부(150)가 도 5의 모델을 이용하여 학습하는 동작 및/또는 이상징후 판단부(350)가 도 5의 모델을 이용하여 이상징후 유무를 판단하는 동작은 도 3의 모델을 이용한 학습 동작 및/또는 이상징후 유무 판단 동작과 동일하므로, 이에 관한 상세한 설명은 생략하기로 한다.
- [0068] 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), 마이크로컴퓨터, 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.
- [0069] 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.
- [0070] 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 설계되고 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.
- [0072] 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 등록청구범

위의 기술적 사상에 의해 정해져야 할 것이다.

부호의 설명

[0074]

10 : CAN 트래픽 모델링 장치

30 : 이상징후 탐지 장치

110 : 메시지 수신부

130 : 데이터 전처리부

150 : 모델 학습부

170 : 저장부

310 : 메시지 수신부

330 : 데이터 전처리부

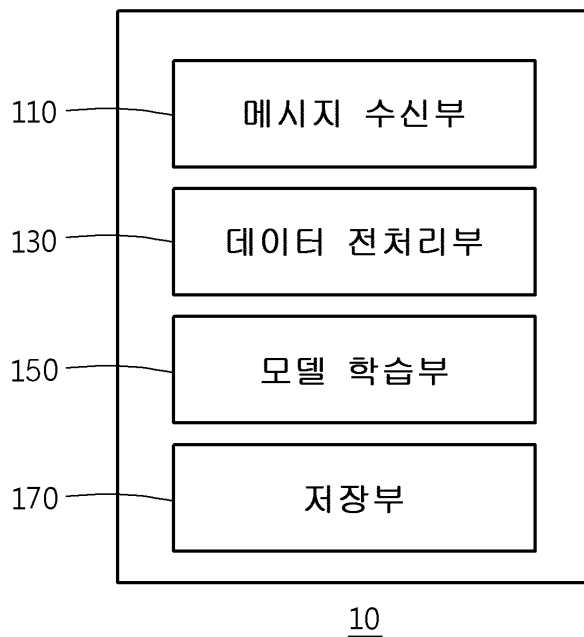
350 : 이상징후 판단부

370 : 저장부

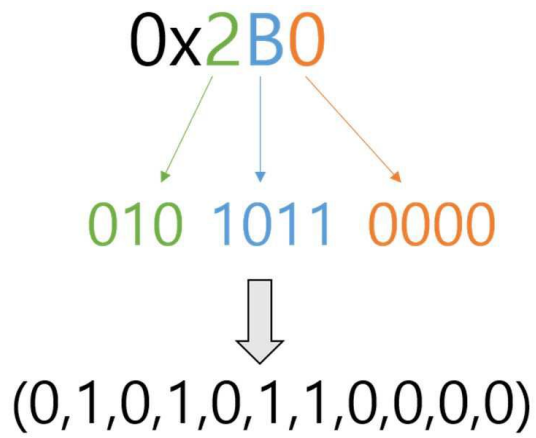
390 : 출력부

도면

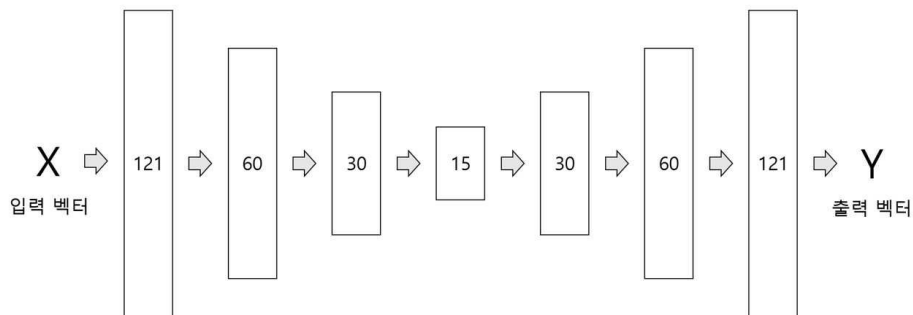
도면1



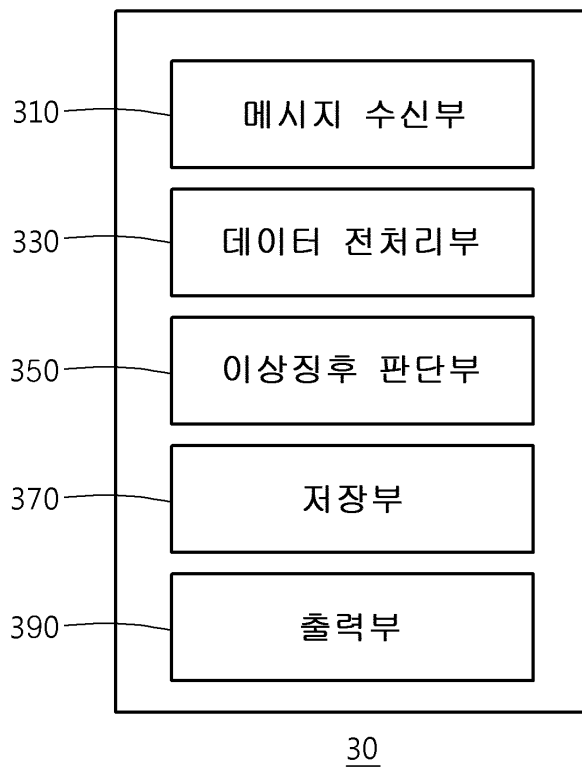
도면2



도면3



도면4



도면5

