



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0064005
(43) 공개일자 2020년06월05일

(51) 국제특허분류(Int. Cl.)
G05B 23/02 (2006.01) G05D 1/02 (2020.01)
(52) CPC특허분류
G05B 23/0289 (2013.01)
G05B 23/0221 (2013.01)
(21) 출원번호 10-2019-0154532
(22) 출원일자 2019년11월27일
심사청구일자 2019년11월27일
(30) 우선권주장
1020180149758 2018년11월28일 대한민국(KR)

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
이동훈
서울특별시 종로구 사직로8길 34, 1404호(내수동, 경희궁의아침3단지아파트)
이세영
서울특별시 동대문구 망우로18가길 61-10, 4층
(74) 대리인
김홍석

전체 청구항 수 : 총 10 항

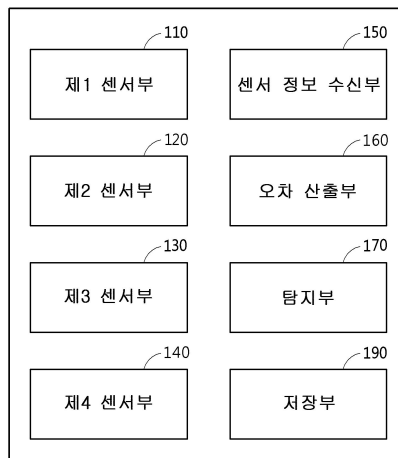
(54) 발명의 명칭 차량의 센서 정보 간 오차를 이용한 센서 공격 탐지 장치 및 방법

(57) 요약

차량에 탑재된 센서 또는 센서로부터 출력되는 센서 정보를 대상으로 하는 공격을 탐지하는 장치와 방법이 개시된다. 공격 탐지 장치는 복수의 센서부들 각각으로부터 센서 정보를 수신하는 센서 정보 수신부, 센서부 별로 수신된 센서 정보의 오차를 계산하는 오차 산출부, 및 센서부 별 오차에 기초하여 센서부 또는 센서 정보를 대상으로 하는 공격을 탐지하는 탐지부를 포함한다.

대 표 도 - 도1

10



(52) CPC특허분류

G05B 23/0262 (2013.01)

G05D 1/0231 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호 20160001390031001

부처명 과학기술정보통신부

연구관리전문기관 정보통신기술진흥센터

연구사업명 정보통신방송연구개발사업

연구과제명 자율주행 스마트자동차용 이상징후 탐지 핵심기술개발

기 여 율 1/1

주관기관 고려대학교산학협력단

연구기간 2018.01.01 ~ 2018.12.31

명세서

청구범위

청구항 1

복수의 센서부들 각각으로부터 센서 정보를 수신하는 센서 정보 수신부;

센서부 별로 수신된 센서 정보의 오차를 계산하는 오차 산출부; 및

센서부 별 오차에 기초하여 센서부 또는 센서 정보를 대상으로 하는 공격을 탐지하는 탐지부를 포함하는 공격 탐지 장치.

청구항 2

제1항에 있어서,

상기 복수의 센서부들 각각은 물체와 상기 공격 탐지 장치가 탑재된 차량 간의 거리 정보를 감지하여, 상기 거리 정보를 상기 센서 정보로 출력하는,

공격 탐지 장치.

청구항 3

제2항에 있어서,

상기 복수의 센서부들 각각은 초음파 센서, 라이다(LiDAR), 레이더(RaDAR), 및 카메라 센서 중 어느 하나로 구현되고,

상기 공격 탐지 장치는 상기 차량에 탑재된 ECU(Electronic Control Unit)로 구현되는,

공격 탐지 장치.

청구항 4

제1항에 있어서,

상기 오차 산출부는,

센서부 별로 센서 정보와 상기 복수의 센서부들 중 적어도 일부로부터 수신되는 센서 정보의 평균 사이의 차이를 오차로 산출하는,

공격 탐지 장치.

청구항 5

제1항에 있어서,

상기 탐지부는,

센서부 별로 미리 정해진 시간 구간 동안에 산출된 오차가 미리 정해진 임계치를 초과하는 횟수가 미리 정해진 임계 횟수에 도달한 경우를 해당 센서부 또는 해당 센서부의 센서 정보를 대상으로 하는 공격으로 판단하는,

공격 탐지 장치.

청구항 6

제5항에 있어서,

산출된 오차가 미리 정해진 임계치를 초과하는 횟수는 상기 미리 정해진 시간 구간 동안에 연속적으로 오차가 임계치를 초과하는 횟수를 의미하는,

공격 탐지 장치.

청구항 7

공격 탐지 장치에 의해 수행되는 공격 탐지 방법에 있어서,

복수의 센서부들 각각으로부터 센서 정보를 수신하는 단계;

센서부 별로 수신된 센서 정보의 오차를 계산하는 단계; 및

센서부 별 오차에 기초하여 센서부 또는 센서 정보를 대상으로 하는 공격을 탐지하는 단계를 포함하는 공격 탐지 방법.

청구항 8

제7항에 있어서,

상기 복수의 센서부들 각각은 물체와 상기 공격 탐지 장치가 탑재된 차량 간의 거리 정보를 감지하여 상기 거리 정보를 상기 센서 정보로 출력하는 초음파 센서, 라이다(LiDAR), 레이더(RaDAR), 및 카메라 센서 중 어느 하나로 구현되는,

공격 탐지 방법.

청구항 9

제8항에 있어서,

상기 센서 정보의 오차를 계산하는 단계는, 센서부 별로 센서 정보와 상기 복수의 센서부들 중 적어도 일부로부터 수신되는 센서 정보의 평균 사이의 차이를 오차로 산출하는,

공격 탐지 방법.

청구항 10

제9항에 있어서,

상기 공격을 탐지하는 단계는, 센서부 별로 미리 정해진 시간 구간 동안에 산출된 오차가 미리 정해진 임계치를 초과하는 횟수가 미리 정해진 임계 횟수에 도달한 경우를 해당 센서부 또는 해당 센서부의 센서 정보를 대상으로 하는 공격으로 판단하는,

공격 탐지 방법.

발명의 설명

기술 분야

본 발명은 차량의 센서로부터 출력되는 센서 정보 간의 오차를 이용하여 센서를 대상으로 하는 공격을 탐지하는 장치 및 방법에 관한 것이다.

[0001]

배경 기술

- [0003] 차량, 특히 자율주행차량에는 차량이 스스로 주변 상황을 인식하고 주행을 판단하기 위해 다양한 센서가 장착되어 있다. 대표적으로 초음파, 라이다(LiDAR), 레이더(RaDAR), 카메라 센서 등이 차량의 전후방에 장착되어 다양한 물리적 신호를 활용하여 차량 주위를 인식한다. 대표적인 자율주행차량의 핵심 기능인 적응형 크루즈 컨트롤(Adaptive Cruise Control, ACC)은 차량에 장착되어 있는 레이더 또는 라이다 센서를 활용하여 전방 차량의 속도 및 거리를 인식하여 차간 거리 유지 및 속도 제어를 제어한다. 또한, 자동주차(Automated Parking) 기능은 차량의 전후방, 측면에 장착되어 있는 초음파 센서 또는 라이다를 이용하여 주변 물체와 공간을 인지하여 속도 및 방향을 조절한다.
- [0004] 적응형 크루즈 컨트롤, 자동주차 등과 같은 자율주행차량 기능이 운전자의 편의성과 안전을 제공하기 위해 가장 중요시되는 정보는 다양한 센서로부터 받은 차량과 물체 사이의 정확한 거리 정보이다. 다양한 센서로부터 전달 받은 거리 정보는 차량 내부에 탑재되어 있는 ECU(Electronic Control Unit)로 전달되고 이 ECU가 안전한 자율주행기능을 수행한다. 그러나, 최근 해외 유명 학회에서 센서 정보(또는 센서)를 타겟으로 한 다양한 공격이 발표되고 있다. 자율주행차량에 탑재된 센서의 정보가 다양한 취약점을 바탕으로 위/변조되어 잘못된 정보를 ECU에 전달할 시, 운전자 및 주변 차량의 안전에 치명적인 위협이 될 수 있다. 예를 들어, 정상 자율주행 중인 차량에 탑재되어 있는 센서 정보를 위/변조시켜 주변에 물체가 존재하지 않지만 물체가 존재한다고 판단하게 하거나, 반대로 물체가 주변에 존재함에도 물체가 없다고 판단하게 하는 등 다양한 오작동을 유발할 수 있다.
- [0005] 본 발명은 이와 같이 자율주행차량에 탑재된 여러 센서로부터 전달받은 거리 정보 중 적어도 일부가 공격자에 의해 위/변조된 정보인지 탐지하는 방법을 제안한다.

선행기술문헌

특허문헌

- [0007] (특허문헌 0001) 대한민국 공개특허 제2018-0056391호 (2018.05.28. 공개)
- (특허문헌 0002) 대한민국 등록특허 제1829672호 (2018.02.19. 공고)
- (특허문헌 0003) 대한민국 등록특허 제1857554호 (2018.05.14. 공고)

발명의 내용

해결하려는 과제

- [0008] 본 발명이 이루고자 하는 기술적인 과제는 차량의 센서 또는 센서 정보를 타겟으로 하는 공격을 탐지하는 방법 및 장치를 제공하는 것이다.

과제의 해결 수단

- [0010] 본 발명의 실시예에 따른 공격 탐지 장치는 복수의 센서부들 각각으로부터 센서 정보를 수신하는 센서 정보 수신부, 센서부 별로 수신된 센서 정보의 오차를 계산하는 오차 산출부, 센서부 별 오차에 기초하여 센서부 또는 센서 정보를 대상으로 하는 공격을 탐지하는 탐지부를 포함한다.
- [0011] 또한, 본 발명의 실시예에 따른 공격 탐지 방법은 상술한 공격 탐지 장치에 의해 수행되고, 복수의 센서부들 각각으로부터 센서 정보를 수신하는 단계, 센서부 별로 수신된 센서 정보의 오차를 계산하는 단계, 센서부 별 오차에 기초하여 센서부 또는 센서 정보를 대상으로 하는 공격을 탐지하는 단계를 포함한다.

발명의 효과

- [0013] 본 발명의 실시예에 따른 공격 탐지 장치 및 방법에 의할 경우, 차량의 센서 또는 센서 정보를 대상으로 하는 공격을 탐지할 수 있다.
- [0014] 또한, 공격을 탐지함으로써 운전자, 주변 차량 및 보행자의 안전을 보장할 수 있는 효과가 있다.

도면의 간단한 설명

- [0016] 본 발명의 상세한 설명에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 상세한 설명이 제공된다.
- 도 1은 본 발명의 일 실시예에 따른 공격 탐지 장치의 기능 블록도이다.
- 도 2는 도 1에 도시된 공격 탐지 장치에 의해 수행되는 공격 탐지 방법을 설명하기 위한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

- [0017] 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.
- [0018] 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.
- [0019] 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.
- [0020] 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.
- [0021] 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.
- [0022] 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.
- [0023] 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.

- [0025] 도 1은 본 발명의 일 실시예에 따른 공격 탐지 장치의 기능 블록도이다.
- [0026] 도 1을 참조하면, 공격 탐지 장치(10)는 복수의 센서부들(110 내지 140), 센서 정보 수신부(150), 오차 산출부(160) 및 탐지부(170)를 포함한다. 실시예에 따라, 공격 탐지 장치(10)는 저장부(190)를 더 포함할 수도 있다.
- [0027] 공격 탐지 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. 여기서, 프로세서는 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.
- [0028] 공격 탐지 장치(10)는 저장부(190)와 데이터 송수신이 가능하도록 직접 또는 간접적으로 연결되어 있을 수 있다. 저장부(190)는 센서 정보 수신부(150)에 의해 수신된 센서 정보들, 오차 산출부(160)에 의해 산출된 간 센서 정보의 오차들, 탐지부(170)에 의한 탐지 결과 및/또는 공격 탐지 장치(10)의 제어, 연산 또는 처리 과정에서 생성된 적어도 하나의 데이터를 일시적으로 또는 비일시적으로 저장할 수 있다. 저장부(190)는 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.
- [0029] 공격 탐지 장치(10)는 저장부(190)에 저장된 애플리케이션을 구동시켜, 센서 정보의 수신, 오차 정보 산출, 탐지 동작 등을 수행할 수도 있다. 여기서, 애플리케이션은, 설계자에 의해 직접 작성되어 저장부(190)에 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.
- [0030] 실시예에 따라, 공격 탐지 장치(10)의 적어도 일부만이 컴퓨팅 장치, 예컨대 ECU로 구현될 수도 있다. 예컨대, 공격 탐지 장치(10)는 센서 정보 수신부(150), 오차 산출부(160) 및 탐지부(170)만을 포함하는 EUC로 구현되고, 차량에 탑재된 복수의 센서부들(110 내지 140)로부터 센서 정보를 수신할 수도 있다. 이 경우에도, 공격 탐지 장치(10)는 저장부(190)를 추가적으로 포함할 수도 있다.
- [0032] 복수의 센서부들(110 내지 140)은 제1 센서부(110), 제2 센서부(120), 제3 센서부(130), 및 제4 센서부(140)를 포함한다. 도 1에 도시된 공격 탐지 장치(10)는 4 개의 센서부들을 포함하는 것으로 도시되어 있으나, 복수의 센서부들에 포함되는 센서 또는 센서부의 개수는 가변할 수 있다.
- [0033] 복수의 센서부들 각각은 동종의 센서를 포함하거나 이종의 센서를 포함할 수 있다. 예컨대, 제1 센서부(110) 내지 제4 센서부(140)는 초음파 센서, 라이다(LiDAR), 레이더(RaDAR), 및 카메라 센서 중 어느 하나의 센서를 포함하거나 어느 하나의 센서로 구현될 수 있다. 다른 예로, 제1 센서부(110) 내지 제4 센서부(140) 중 적어도 일부는 다른 센서부와는 다른 센서를 포함하거나 다른 센서로 구현될 수 있다. 구체적으로, 제1 센서부(110)는 초음파 센서를 포함하거나 초음파 센서로 구현되고, 제2 센서부(120)는 라이다(LiDAR)를 포함하거나 라이다(LiDAR)로 구현되고, 제3 센서부(130)는 레이더(RaDAR)를 포함하거나 레이더(RaDAR)로 구현되고, 제4 센서부(140)는 카메라 센서를 포함하거나 카메라 센서로 구현될 수 있다.
- [0034] 복수의 센서부들 각각은 동일한 종류의 센서 정보, 예컨대, 온도 정보, 습도 정보, 거리 정보, 및 속도 정보 중 어느 하나를 출력할 수 있다. 이와는 다르게, 복수의 센서부들 각각으로부터 소정의 센서 정보가 출력되고, 센서 정보 수신부(150)는 각각의 센서부로부터 출력되는 소정의 센서 정보에 기초하여 온도 정보, 습도 정보, 거리 정보, 및 속도 정보 중 어느 하나를 계산할 수도 있다.
- [0035] 실시예에 따라, 복수의 센서들 각각은 소정 물체(예컨대, 장애물, 보행자, 주위 차량, 전방 차량 등)로부터 차량과의 거리를 감지하는(또는 거리를 산출하기 위한 기초 정보를 출력하는 센서를 포함하거나 센서로 구현될 수 있다. 거리 측정을 위한 센서로는 초음파 센서, 라이다(LiDAR), 레이더(RaDAR), 카메라 센서 등이 있다. 이때, 카메라 센서는 깊이 센서(depth sensor)를 포함하여 물체(객체)와의 거리 정보 또는 거리 정보를 산출하기 위한 기초 정보를 출력할 수 있다.

- [0037] 센서 정보 수신부(150)는 복수의 센서부들 각각으로부터 센서 정보를 수신하고, 수신된 센서 정보를 저장부(190)에 저장할 수 있다. 수신된 센서 정보는 온도 정보, 습도 정보, 거리 정보, 속도 정보 중 어느 하나를 의미할 수 있다. 또한, 센서 정보 수신부(150)는 복수의 센서부들 각각으로부터 수신되는 정보를 이용하여 센서 정보를 생성하고, 생성된 센서 정보를 저장부(190)에 저장할 수도 있다. 예컨대, 센서 정보 수신부(150)는 초음파 센서를 포함하는 제1 센서부(110)로부터 물체와 차량 간의 거리 정보를 수신할 수 있지만, 물체를 향해 방사된 초음파 신호의 방사 시점과 물체에 반사되어 되돌아 오는 에코 초음파 신호의 수신 시점(또는 방사 시점과 수신 시점 간의 차이)을 수신하고 이에 기초하여 센서 정보, 즉 물체와 차량 간의 거리 정보를 산출할 수 있다.
- [0039] 오차 산출부(160)는 복수의 센서부들 각각에 의한 감지 결과의 오차를 산출할 수 있다. 일 예로, 복수의 센서부들 중 어느 하나의 센서부에 의한 감지 결과의 오차는 복수의 센서부들 중 적어도 일부의 센서들(예컨대, 상기 어느 하나의 센서부를 제외한 센서부들) 또는 상기 복수의 센서부들에 의한 감지 결과의 평균과 상기 어느 하나의 센서부에 의한 감지 결과의 차이를 의미할 수 있다. 구체적인 예로, 제1 센서부(110) 내지 제4 센서부(140) 각각에 의한 감지 결과를 d_1 , d_2 , d_3 , 및 d_4 라 할 때, 제1 센서부(110)에 의한 감지 결과 d_1 의 오차는 d_1 내지 d_4 의 평균($(d_1+d_2+d_3+d_4)/4$) 또는 d_2 내지 d_4 의 평균($(d_2+d_3+d_4)/3$)과 d_1 의 차이를 의미할 수 있다. 마찬가지로, d_2 의 오차는 d_1 내지 d_4 의 평균($(d_1+d_2+d_3+d_4)/4$) 또는 d_1 , d_3 , 및 d_4 의 평균($(d_1+d_3+d_4)/3$)과 d_2 의 차이를 의미하고, d_3 의 오차는 d_1 내지 d_4 의 평균($(d_1+d_2+d_3+d_4)/4$) 또는 d_1 , d_2 , 및 d_4 의 평균($(d_1+d_2+d_4)/3$)과 d_3 의 차이를 의미하고, d_4 의 오차는 d_1 내지 d_4 의 평균($(d_1+d_2+d_3+d_4)/4$) 또는 d_1 내지 d_3 의 평균($(d_1+d_2+d_3)/3$)과 d_4 의 차이를 의미할 수 있다. 실시예에 따라, 사용되는 평균의 종류는 산술평균, 기하평균, 조화평균, 절사평균, 멱평균, 중앙값(중위값), 최빈값 등 중 어느 하나를 의미할 수 있다.
- [0040] 또한, 오차 산출부(160)에 의한 각 센서부 별 오차의 산출 동작은 연속적으로 수행될 수 있다. 이를 통하여, 오차 산출부(160)는 각 센서부 별로 연속되는 오차를 출력할 수 있다.
- [0042] 탐지부(170)는 오차 산출부(160)에 의해 산출된 복수의 센서부들 각각의 오차에 기초하여 각 센서부를 대상으로 하는 공격을 탐지할 수 있다. 복수의 센서부들 각각에 대하여, 탐지부(170)에 의한 공격 탐지 동작은 다음과 같다.
- [0043] 우선, 탐지부(170)는 감지 결과의 오차를 미리 정해진 임계치와 비교한다. 오차가 임계치를 초과하지 않는 경우에는, 새로이 산출된 오차(즉, 다음 시점에 측정된 감지 결과의 오차)를 상기 임계치와 비교하는 동작을 반복적으로 수행한다.
- [0044] 오차가 상기 임계치를 초과하는 경우, 탐지부(170)는 미리 정해진 (타임) 윈도우 구간 중 오차가 연속적으로 임계치를 벗어나는 횟수를 카운트할 수 있다. 또한, 탐지부(170)는 연속적으로 임계치를 벗어나는 횟수가 임계 횟수에 도달하는 경우를 대응하는 센서부 또는 대응하는 센서부의 센서 정보를 대상으로 하는 공격이 발생한 것으로 결정하고, 공격을 탐지할 수 있다. 실시예에 따라, 탐지부(170)는 미리 정해진 (타임) 윈도우 구간 중 오차가 임계치를 벗어나는 횟수를 카운트할 수 있다. 또한, 탐지부(170)는 임계치를 벗어나는 횟수가 임계 횟수에 도달하는 경우를 대응하는 센서부 또는 대응하는 센서부의 센서 정보를 대상으로 하는 공격이 발생한 것으로 결정하고, 공격을 탐지할 수 있다. 특히, 비교의 대상인 오차가 발생한 센서부, 센서, 또는 센서 정보를 대상으로 하는 공격이 발생한 것으로 판단될 수 있다.
- [0045] 상기 임계치, (타임) 윈도우의 크기, 및/또는 임계 횟수 등은 미리 정해질 수 있다. 즉, 상술한 수치들은 차량의 정상 주행중에 발생하는 감지 결과에 기초하여 미리 결정될 수 있다. 예컨대, 상기 임계치는 차량의 정상 주행중에 산출된 센서 정보 간의 최대 오차를 의미할 수 있으며, 각 센서부 별로 상이한 값을 가질 수도 있다. 또한, 상기 (타임) 윈도우의 크기(즉, 미리 정해진 시간 구간 또는 미리 정해진 감지 횟수) 및/또는 상기 임계 횟수 또한 미리 결정될 수 있다.
- [0046] 이와 같이, 연속되어 임계치를 초과하는 오차가 임계 횟수만큼 발생하는 경우 또는 미리 정해진 시간 구간에 임계치를 초과하는 오차가 임계 횟수만큼 발생하는 경우를 공격으로 탐지함으로써, 오탐지를 예방할 수 있다. 즉, 실제 자율주행 중 정상상황임에도 센서 정보가 임계값을 벗어나 위/변조된 센서 정보로 판단되는 경우를 감소시킬 수 있다.

- [0048] 도 2는 도 1에 도시된 공격 탐지 장치에 의해 수행되는 공격 탐지 방법을 설명하기 위한 흐름도이다. 공격 탐지 방법을 설명함에 있어, 앞선 기재와 중복되는 내용에 관하여는 그 기재를 생략하기로 한다.
- [0049] 도 1과 도 2를 참조하면, 복수의 센서부들 각각은 임의의 센서 정보, 예컨대, 대상 물체와 차량 간의 거리 정보를 생성하고, 감지된(또는 생성된 센서 정보)를 출력한다. 센서 정보 수신부(150)는 상기 복수의 센서부들 각각으로부터 감지 결과(센서 정보)를 수신한다(S110).
- [0050] 오차 산출부(160)는 센서부 별로 감지 결과의 오차를 산출할 수 있다(S120). 오차 산출부(160)에 의한 오차 산출 동작은 매 감지 시점마다(또는 센서 정보를 수신할 때마다) 반복적으로 수행될 수 있으며, 오차의 산출 방법에 관한 구체적인 설명은 생략하기로 한다.
- [0051] 탐지부(170)는 오차 산출부(160)에 의해 산출된 오차가 임계치를 초과하는지 여부를 결정한다(S130). S130 단계에서, 오차가 임계치를 초과하지 않는 경우에는, 오차 산출 동작이 다시 수행될 수 있다. S130 단계에서, 오차가 임계치를 초과하는 경우, 탐지부(170)는 임계치를 벗어나는 횟수가 임계 횟수에 도달하는지 여부를 판단한다(S140). S140 단계에서 임계치를 벗어나는 횟수가 임계 횟수에 도달하지 않는 경우, 오차 산출 동작이 재차 수행되고, 임계치를 벗어나는 횟수가 임계 횟수에 도달한 경우, 탐지부(170)는 오차에 대응하는 센서부, 센서 또는 센서 정보를 대상으로 하는 공격이 발생한 것으로 판단할 수 있다(S150).
- [0053] 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.
- [0054] 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.
- [0055] 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.

[0057] 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.

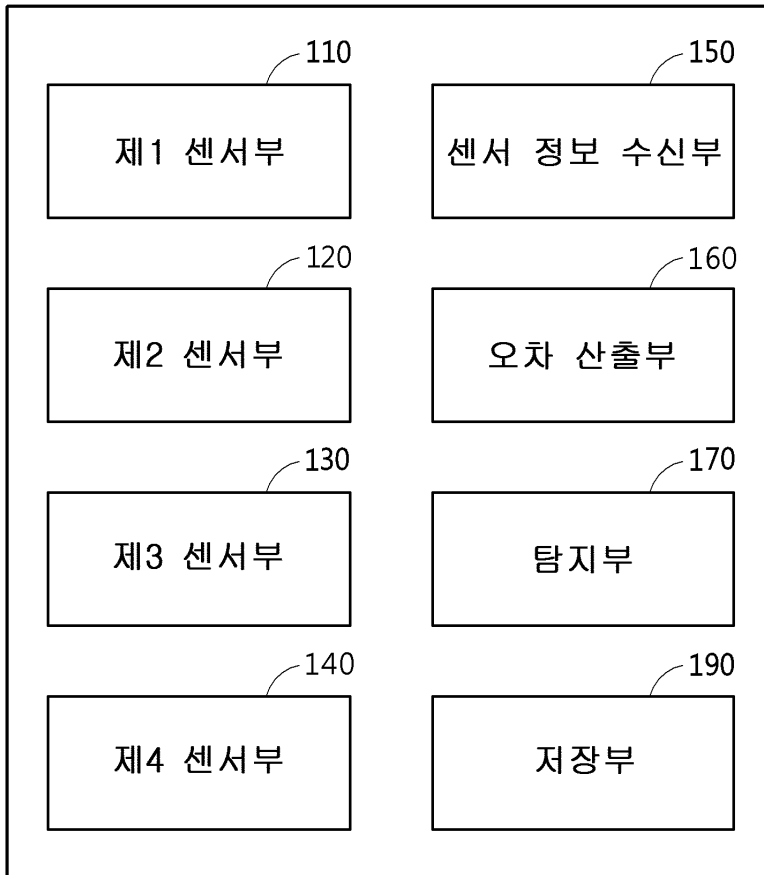
부호의 설명

[0059] 10 : 공격 탐지 장치
 110 : 제1 센서부
 120 : 제2 센서부
 130 : 제3 센서부
 140 : 제4 센서부
 150 : 센서 정보 수신부
 160 : 오차 산출부
 170 : 탐지부
 190 : 저장부

도면

도면1

10



도면2

