(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2024-0043267
(43) 공개일자 2024년04월03일

(51) 국제특허분류(Int. Cl.)
G06F 21/75 (2013.01) *G01C 17/28* (2006.01)
G01C 19/02 (2006.01) *G06T 17/10* (2006.01)
(52) CPC특허분류
G06F 21/75 (2020.05)
G01C 17/28 (2013.01)
(21) 출원번호 10-2022-0122131
(22) 출원일자 2022년09월27일
심사청구일자 2022년09월27일

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
이선우
서울특별시 서초구 남부순환로309길 38, 5동 522호
이동훈
서울특별시 종로구 사직로8길 34, 1404호(내수동, 경희궁의아침3단지아파트)
(74) 대리인
김등용

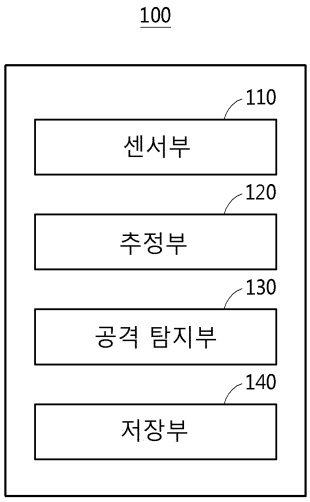
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 **자이로스코프와 자력계의 관계를 이용한 신호 주입 공격 탐지 장치 및 그 방법**

(57) 요 약

자이로스코프와 자력계의 관계를 이용한 신호 주입 공격 탐지 장치 및 방법이 개시된다. 상기 신호 주입 탐지 장치는 제1 센서와 제2 센서를 포함하는 센서부, 상기 제1 센서와 상기 제2 센서 중 어느 하나 센서에 의해 측정된 데이터로부터 상기 제1 센서와 상기 제2 센서 중 다른 하나의 센서의 출력을 추정하는 추정부, 및 상기 측정된 데이터와 추정된 데이터를 비교하여 신호 주입 공격(signal injection attack)을 탐지하는 공격 탐지부를 포함한다.

대 표 도 - 도7



(52) CPC특허분류
G01C 19/02 (2023.08)
G06T 17/10 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711152468
과제번호	2020-0-00374-003
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	정보보호핵심원천기술개발(정진기금)
연구과제명	무인이동체 공통핵심 보안기술 개발 연구
기 여 율	1/1
과제수행기관명	고려대학교산학협력단
연구기간	2022.01.01 ~ 2022.12.31

명 세 서

청구범위

청구항 1

제1 센서와 제2 센서를 포함하는 센서부;

상기 제1 센서와 상기 제2 센서 중 어느 하나 센서에 의해 측정된 데이터로부터 상기 제1 센서와 상기 제2 센서 중 다른 하나의 센서의 출력을 추정하는 추정부; 및

상기 측정된 데이터와 추정된 데이터를 비교하여 신호 주입 공격(signal injection attack)을 탐지하는 공격 탐지부를 포함하는 신호 주입 공격 탐지 장치.

청구항 2

제1항에 있어서,

상기 제1 센서는 자이로스코프이고,

상기 제2 센서는 자력계인,

신호 주입 공격 탐지 장치.

청구항 3

제1항에 있어서,

상기 공격 탐지부는, 상기 측정된 데이터와 상기 추정된 데이터 사이의 오차가 임계치를 초과하는 경우 상기 신호 주입 공격이 발생한 것으로 판단하는,

신호 주입 공격 탐지 장치.

청구항 4

제3항에 있어서,

상기 신호 주입 공격 탐지 장치는 스마트폰(smart phone), HMD(Head Mounted Device), SBV(Self-Balancing Vehicle), 무인 비행체, 및 자율주행차 중 어느 하나이고,

상기 공격 탐지부는, 상기 신호 주입 공격이 발생한 것으로 판단되는 경우, 상기 측정된 데이터가 아닌 상기 추정된 데이터를 이용하여 상기 신호 주입 공격 탐지 장치의 위치나 자세를 추정하는,

신호 주입 공격 탐지 장치.

청구항 5

제2항에 있어서,

상기 추정부는, 수학식 1 내지 수학식 3을 이용하여, 상기 자력계로부터 측정된 데이터인 자력계 데이터($M_x^b(t)$, $M_y^b(t)$, 및 $M_z^b(t)$)로부터 상기 자이로스코프의 출력($\widehat{\omega}_x^b(t)$, $\widehat{\omega}_y^b(t)$, 및 $\widehat{\omega}_z^b(t)$)을 추정하고,

상기 수학식 1은 $$\widehat{\omega}_x^b(t) = \frac{\frac{d}{dt}M_y^b(t) \cdot M_z^b(t) - M_y^b(t) \cdot \frac{d}{dt}M_z^b(t)}{(M_y^b(t))^2 + (M_z^b(t))^2}$$ 이고,

상기 수학식 2는 $$\widehat{\omega}_y^b(t) = \frac{M_x^b(t) \cdot \frac{d}{dt}M_z^b(t) - \frac{d}{dt}M_x^b(t) \cdot M_z^b(t)}{(M_x^b(t))^2 + (M_z^b(t))^2}$$ 이고,

사기 수학식 3은 $$\widehat{\omega}_z^b(t) = \frac{\frac{d}{dt}M_x^b(t) \cdot M_y^b(t) - M_x^b(t) \cdot \frac{d}{dt}M_y^b(t)}{(M_x^b(t))^2 + (M_y^b(t))^2}$$ 인,

신호 주입 공격 탐지 장치.

청구항 6

제5항에 있어서,

상기 추정부는, 수학식 4를 이용하여, 근사화된(approximated) 상기 자이로스코프의 출력을 추정하고,

상기 수학식 4는 $$\frac{d}{dt}M^b(t) = \frac{f}{2} \cdot (M^b(t+1) - M^b(t-1))$$ 이고,

상기 $M^b(t)$는 상기 $M_x^b(t)$, 상기 $M_y^b(t)$, 및 상기 $M_z^b(t)$ 중 어느 하나이고,

상기 f는 상기 자력계의 샘플링 주파수(sampling frequency)인,

신호 주입 공격 탐지 장치.

청구항 7

제2항에 있어서,

상기 추정부는, 수학식 5 내지 수학식 7을 이용하여, 상기 자이로스코프로부터 측정된 데이터인 자이로스코프 데이터(ω_x^b, ω_y^b, 및 ω_z^b)로부터 상기 자력계의 출력($\widehat{M}_x^b(t)$, $\widehat{M}_y^b(t)$, 및 $\widehat{M}_z^b(t)$)을 추정하고,

상기 수학식 5는 $$\widehat{M}_x^b(t) = M_x^b(t-1) + \frac{1}{f} \cdot (-\omega_y^b(t-1)M_z^b(t-1) + \omega_z^b(t-1)M_y^b(t-1))$$ 이고,

상기 수학식 6은 $$\widehat{M}_y^b(t) = M_y^b(t-1) + \frac{1}{f} \cdot (\omega_x^b(t-1)M_z^b(t-1) - \omega_z^b(t-1)M_x^b(t-1))$$ 이고,

상기 수학식 7은 $$\widehat{M}_z^b(t) = M_z^b(t-1) + \frac{1}{f} \cdot (-\omega_x^b(t-1)M_y^b(t-1) + \omega_y^b(t-1)M_x^b(t-1))$$ 이고,

상기 f는 상기 자이로스코프의 샘플링 주파수이고,

상기 $M_x^b(t-1)$, 상기 $M_y^b(t-1)$, 및 상기 $M_z^b(t-1)$는 t-1 시점에서 상기 자력계에 의해 측정된 자력계 데이터인,

신호 주입 공격 탐지 장치.

청구항 8

자이로스코프와 자력계를 포함하고 측정된 자이로스코프 데이터와 측정된 자력계 데이터를 출력하는 센서부;

상기 측정된 자이로스코프 데이터로부터 추정된 자력계 데이터를 생성하고, 상기 자력계 데이터로부터 추정된 자이로스코프 데이터를 생성하는 추정부; 및

상기 측정된 자이로스코프 데이터와 상기 추정된 자이로스코프 데이터를 비교하여 상기 자이로스코프를 타겟으로 하는 신호 주입 공격을 탐지라고, 상기 측정된 자력계 데이터와 상기 추정된 자력계 데이터를 비교하여 상기 자력계를 타겟으로 하는 신호 주입 공격을 탐지하는 공격 탐지부를 포함하는 신호 주입 공격 탐지 장치.

청구항 9

제8항에 있어서,

상기 공격 탐지부는, 상기 측정된 자이로스코프 데이터와 상기 추정된 자이로스코프 데이터의 오차가 제1 임계치를 초과하는 경우 상기 자이로스코프를 타겟으로 하는 신호 주입 공격이 발생한 것으로 판단하고,

상기 측정된 자력계 데이터와 상기 추정된 자력계 게이터의 오차가 제2 임계치를 초과하는 경우 상기 자력계를 타겟으로 하는 신호 주입 공격이 발생한 것으로 판단하는,

신호 주입 공격 탐지 장치.

청구항 10

신호 주입 공격 탐지 장치에 의해 수행되는 신호 주입 공격 탐지 방법에 있어서,

자이로스코프에 의해 측정된 자이로스코프 데이터와 자력계에 의해 측정된 자력계 데이터를 획득하는 단계;

상기 측정된 자이로스코프 데이터로부터 추정된 자력계 데이터를 생성하고, 상기 측정된 자력계 데이터로부터 추정된 자이로스코프 데이터를 생성하는 단계;

상기 측정된 자이로스코프 데이터와 상기 추정된 자이로스코프 데이터를 비교하고, 상기 측정된 자력계 데이터와 상기 추정된 자력계 데이터를 비교하는 단계; 및

비교 결과에 기초하여, 상기 자이로스코프 또는 상기 자력계를 타겟으로 하는 신호 주입 공격을 탐지하는 단계를 포함하는 신호 주입 공격 탐지 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 센서에 대한 신호 주입 공격(signal injection attack)에 대한 탐지 및 복원력 제공 방법에 관한 것으로, 특히 자이로스코프와 자력계의 관계를 기반으로 한 수학적 모델을 통해 추정된 데이터를 기반으로 공격을 탐지하고 장기적인 복원력을 제공할 수 있는 방법 및 장치에 관한 것이다.

배 경 기 술

[0002] 센서(Sensor)는 빛, 소리, 또는 움직임과 같은 환경의 변화를 감지하도록 설계된 전자 장치이다. 이러한 센서를 통해 임베디드 장치는 실제 세계의 물리량과 상호 작용할 수 있다.

[0003] 특히, IMU(Inertial Measurement Unit, 관성 측정장치) 센서는 동적 움직임을 측정할 수 있다. IMU 센서는 특정 방향의 선형 가속도를 측정하는 가속도계, 비틀림 또는 회전 운동을 측정하는 자이로스코프, 및 공기 중의 자속 밀도를 감지하여 지구의 자기장을 측정하는 자력계로 구성된다. 따라서, IMU 센서는 산업용 및 일반 가정용 기기에 탑재되어 많은 서비스를 제공할 수 있다. 예를 들어, IMU 센서는 스마트폰, 비디오 게임 리모콘, 및 로봇 청소기 등을 포함한 가전제품의 동작을 추적하는 데 사용될 수 있다. 또한, 증강 현실(Augumented Reality, AR) 및 가상 현실(Virtual Reality, VR) 시스템에서 사용자의 움직임, 예컨대 머리 움직임을 추적할 수 있다. IMU 센서는 인간 조종사가 없는 무인 항공기나 인간 조종사가 있는 유인 항공기를 조정하거나 제어하는 데에도 사용된다.

[0004] 이러한 IMU 센서는 낮은 전력 소비와 비용은 물론 높은 신뢰성과 견고성을 제공한다. 이러한 이유로 최근 몇년 동안 IMU 센서에 대한 수요가 급격히 증가하였다. Mordor Intelligence는 세계 시장이 2020년 109억 2000만 달러에서 2026년 188억 8000만 달러에 이를 것으로 예상하였고, 2021년 부터 2026년 까지의 예측 기간 동안 8.71%의 복합 성장률을 기록할 것이라고 예측하였다.

[0005] 그러나, 최근의 몇몇 연구에서 악성 신호를 물리적으로 센서에 주입함으로써 공격자가 센서의 정상적인 기능을 방해하거나 센서 측정을 완전히 제어할 수 있음을 보여주었다. Son et al.은 먼저 드론에 내장된 자이로스코프에 음향 신호를 주입하여 움직임을 제어할 수 없게 만드는 간단한 공격을 수행하였으며(Yunmok Son, Hocheol Shin, Dongkwan Kim, Youngseok Park, Juhwan Noh, Kibum Choi, Jungwoo Choi, and Yongdae Kim. Rocking drones with intentional sound noise on gyroscopic sensors. In 24th USENIX Security Symposium (USENIX Security 15), pages 881-896, 2015.), Wang et al.은 가상 현실 헤드셋 및 자체 균형 차량(self balancing vehicle, SBV)에서 자이로스코프를 타겟으로 공격을 시도하였다(Zhengbo Wang, Kang Wang, Bo Yang, Shangyuan Li, and Aimin Pan. Sonic gunto smart devices: Your devices lose control under ultrasound/sound. BlackHatUSA, 2017.). 또한, Tu et al.은 자이로스코프가 훨씬 더 세분화된 방식으로 제어될 수 있음을 보여주었으며(Yazhou Tu, Zhiqiang Lin, Insup Lee, and Xiali Hei. Injected and delivered:Fabricating implicit control over actuation systems by spoofing inertial sensors.In 27th USENIX Security Symposium (USENIX

Security 18), pages 1545-1562, 2018.), 특히 7.8m 거리에서 최대 1분 동안 지속되는 신호 주입 공격을 수행할 수 있음을 보여주었다. 그리고, 또 다른 연구에서는 ABS(Anti-lock Braking System) 시스템(Yasser Shoukry, Paul Martin, Paulo Tabuada, and Mani Srivastava. Non-invasivespoofing attacks for anti-lock braking systems. In International Conference onCryptographic Hardware and Embedded Systems, pages 55-72. Springer, 2013.), 자기 인코더(Yasser Shoukry, Paul Martin, Yair Yona, Suhas Diggavi, and Mani Srivastava.Pycra: Physical challenge-response authentication for active sensors under spoofing attacks. In Proceedings of the 22nd ACM SIGSAC Conference on Computer andCommunications Security, pages 1004-1015, 2015.), 또는 자력계 자체(Shoei Nashimoto, Daisuke Suzuki, Takeshi Sugawara, and Kazuo Sakiyama. Sensor con-fusion: Defeating kalman filter in signal injection attack. In Proceedingsof the 2018 on Asia Conference on Computer and Communications Security, pages511-524, 2018., Kevin Sam Tharayil, Benyamin Farshteindiker, Shaked Eyal, Nir Hasidim, RoyHershkovitz, Shani Houri, Ilia Yoffe, Michal Oren, and Yossi Oren. Sensor defense in-software (sdi): Practical software based detection of spoofing attackson position sensors. Engineering Applications of Artificial Intelligence, 95:103904,2020.)와 같이 자력계에 악성 자기 신호를 주입하는 공격을 다룬 바 있다.

[0006] IMU 센서는 다양한 장치에 내장되어 다양한 서비스를 제공하기 때문에 신호 주입 공격이 발생할 경우 정상적인 서비스 제공이 불가능하고 재산 또는 인명 피해가 발생할 수 있다. 따라서 IMU 센서를 타겟으로 하는 신호 주입 공격에 대응할 수 있는 기술이 무엇보다 중요하다.

[0007] 기존에 제안된 대응책은 하드웨어 기반과 소프트웨어 기반으로 나눌 수 있다. 하드웨어 기반 방법은 차폐를 기반으로 하거나 공격 감지를 위한 추가 센서가 필요하기 때문에 이미 배포되어 활용중인 장치에 적용하기 어렵다. 또한, 대표적인 소프트웨어 기반 방식으로는 센서 융합 방식이 있지만 최근에는 신호 주입 공격이 침투할 수 있다는 것이 입증되었다. 또한 모든 대응책은 공격 탐지에만 집중하며 신호 주입 공격에 대한 복원력은 고려하지 않는다. 실제로, 하드웨어 기반 방법과 소프트웨어 기반 방법 모두 복원력을 제공할 수 없기 때문에 복원력과 관련이 없다. 즉, 하드웨어 기반 방법은 차폐를 통해 악성 신호가 주입되는 것을 막거나 마이크와 같은 추가 센서를 통해 악성 신호를 감지하기 때문에 복원력을 제공할 수 없고, 소프트웨어 기반 방식인 센서 융합 방식 역시 미래의 센서 데이터를 예측하기 보다는 현 상황에서 센서 데이터를 비교 분석하기 때문에 복원력을 제공하지 못한다.

[0008] 신호 주입 공격에 대한 대응 없이 탐지 동작만을 수행하는 경우, 공격을 받은 장치가 정상적으로 작동할 수 없게 되어 충돌이나 추락을 초래할 가능성이 높다. 따라서, 신호 주입 공격을 탐지하고 대응할 수 있는 방법, 즉 복원력을 제공하는 방법이 필요하다. 이러한 복원력에 대한 요구가 최근 증가함에 따라 신호 주입 공격을 감지하고 센서 시스템을 모델링하여 복원력을 제공할 수 있는 방법을 개발하려는 노력이 있었다. 그러나, 이로 인해 도출된 방법은 정확한 센서 시스템 모델이 필요하고 10초 동안만의 탄력성 지속 시간을 제공할 수 있다는 한계가 있다. 최근 신호 주입 공격은 최대 1분 동안 지속될 수 있기 때문에, 보다 충분히 긴 시간 동안 복원력을 제공하는 기법이 필요하다.

선행기술문헌

특허문헌

[0009] (특허문헌 0001) 대한민국 공개특허 제2022-0069775호 (2022.05.27. 공개)

(특허문헌 0002) 대한민국 등록특허 제2194127호 (2020.12.22. 공고)

(특허문헌 0003) 대한민국 등록특허 제1770913호 (2017.08.24. 공고)

(특허문헌 0004) 대한민국 등록특허 제1008360호 (2011.01.14. 공고)

발명의 내용

해결하려는 과제

[0010] 본 발명이 이루고자 하는 기술적인 과제는 센서를 대상으로 하는 신호 주입 공격을 효율적으로 탐지하고, 신호 주입 공격이 발생한 경우 복원력을 제공할 수 있는 장치 및 방법을 제공하는 것이다.

과제의 해결 수단

[0011] 본 발명의 일 실시예에 따른 신호 주입 공격 탐지 장치는 제1 센서와 제2 센서를 포함하는 센서부, 상기 제1 센서와 상기 제2 센서 중 어느 하나 센서에 의해 측정된 데이터로부터 상기 제1 센서와 상기 제2 센서 중 다른 하나의 센서의 출력을 추정하는 추정부, 및 상기 측정된 데이터와 추정된 데이터를 비교하여 신호 주입 공격(signal injection attack)을 탐지하는 공격 탐지부를 포함한다.

[0012] 또한, 본 발명의 다른 실시예에 따른 신호 주입 공격 탐지 장치는 자이로스코프와 자력계를 포함하고 측정된 자이로스코프 데이터와 측정된 자력계 데이터를 출력하는 센서부, 상기 측정된 자이로스코프 데이터로부터 추정된 자력계 데이터를 생성하고, 상기 자력계 데이터로부터 추정된 자이로스코프 데이터를 생성하는 추정부, 및 상기 측정된 자이로스코프 데이터와 상기 추정된 자이로스코프 데이터를 비교하여 상기 자이로스코프를 타겟으로 하는 신호 주입 공격을 탐지하고, 상기 측정된 자력계 데이터와 상기 추정된 자력계 데이터를 비교하여 상기 자력계를 타겟으로 하는 신호 주입 공격을 탐지하는 공격 탐지부를 포함한다.

[0013] 본 발명의 일 실시예에 따른 신호 주입 공격 탐지 방법은 신호 주입 공격 탐지 장치에 의해 수행되고, 자이로스코프에 의해 측정된 자이로스코프 데이터와 자력계에 의해 측정된 자력계 데이터를 획득하는 단계, 상기 측정된 자이로스코프 데이터로부터 추정된 자력계 데이터를 생성하고, 상기 측정된 자력계 데이터로부터 추정된 자이로스코프 데이터를 생성하는 단계, 상기 측정된 자이로스코프 데이터와 상기 추정된 자이로스코프 데이터를 비교하고, 상기 측정된 자력계 데이터와 상기 추정된 자력계 데이터를 비교하는 단계, 및 비교 결과에 기초하여, 상기 자이로스코프 또는 상기 자력계를 타겟으로 하는 신호 주입 공격을 탐지하는 단계를 포함한다.

발명의 효과

[0014] 본 발명의 실시예들에 의할 경우, 자이로스코프에 대한 음향 신호 주입 공격과 자력계에 대한 자기 신호 주입 공격 등의 신호 주입 공격을 탐지하고 장기적인 복원력을 제공할 수 있는 효과가 있다.

[0015] 또한, 본 발명은 자이로스코프와 자력계 간의 관계를 기반으로 하기 때문에 이미 활용중인 장치에 용이하게 적용할 수 있다. 특히, 센서 등과 같은 추가적인 하드웨어가 필요하지 않으며 자이로스코프 및 자력계 데이터를 추정하는 데 합리적인 계산 비용만 필요하다.

도면의 간단한 설명

[0016] 본 발명의 상세한 설명에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 상세한 설명이 제공된다.

도 1은 고정 좌표계의 3가지 회전을 도시한다.

도 2는 고정 좌표계와 관련하여 자력계 데이터에 의해 형성되는 각을 도시한다.

도 3은 고정 좌표계와 관련하여 x-축, y-축, 및 z-축으로 iPhone 13 Pro Max가 회전할 때 측정된 자이로스코프 데이터와 추정된 자이로스코프 데이터를 도시한다.

도 4는 고정 좌표계와 관련하여 x-축, y-축, 및 z-축으로 iPhone 13 Pro Max가 회전할 때 측정된 자력계 데이터와 추정된 자력계 데이터를 도시한다.

도 5는 제안하는 기법의 전체적인 프로세스를 도시한다.

도 6은 스푸핑된 자이로스코프 데이터에 대한 시뮬레이션과 측정된 데이터로부터 추적된 경로, 공격이 수행된 데이터로부터 추적된 경로, 및 추정된 데이터로부터 추적된 경로를 도시한다.

도 7은 본 발명의 일 실시예에 따른 장치를 도시한다.

도 8은 도 7에 도시된 장치에 의해 수행되는 방법을 설명하기 위한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0017] 본 명세서에 개시되어 있는 본 발명의 개념에 따른 실시예들에 대해서 특정한 구조적 또는 기능적 설명들은 단지 본 발명의 개념에 따른 실시예들을 설명하기 위한 목적으로 예시된 것으로서, 본 발명의 개념에 따른 실시예들은 다양한 형태들로 실시될 수 있으며 본 명세서에 설명된 실시예들에 한정되지 않는다.

[0018] 본 발명의 개념에 따른 실시예들은 다양한 변경들을 가할 수 있고 여러 가지 형태들을 가질 수 있으므로 실시예

들을 도면에 예시하고 본 명세서에서 상세하게 설명하고자 한다. 그러나, 이는 본 발명의 개념에 따른 실시예들을 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 실시예를 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 실시예들을 상세히 설명한다. 그러나, 특허출원의 범위가 이러한 실시예들에 의해 제한되거나 한정되는 것은 아니다. 각 도면에 제시된 동일한 참조 부호는 동일한 부재를 나타낸다.

[0024] **좌표계(Coordinate System)**

[0025] 센서는 물리량(physical quantity)을 측정하고 이를 장치 등이 읽을 수 있는 신호로 변환할 수 있다. 일반적으로, 측정된 물리량을 분석하는 좌표 프레임들(coordinate frames)로써, 고정 좌표계(body frame, 동체 좌표)와 관성 좌표계(inertial frame)가 있다.

[0026] **고정 좌표계(Body frame).** 물체 좌표계, 동체 좌표계, 또는 물체 고정 좌표계(Body-fixed frame)로도 명명되는 고정 좌표계는 센서가 내장된 물체의 좌표계(즉, 측정 센서의 축과 일치하는 좌표계)로 정의된다. 예컨대, 스마트폰이 평평한 테이블 위에 놓여 있을 때, x-축은 오른쪽을, z-축은 윗쪽을, y-축은 앞쪽을 가리킨다. 여기서, IMU 센서는 IMU 센서의 고정 좌표계와 관련된 물리량을 측정한다.

[0027] **관성 좌표계(Inertial frame).** 관성 좌표계는 지구 고정 좌표계(Earth-fixed coordinate system)이다. 좌표는 방위(cardinal directions) 또는 임의의 방향에 기초할 수 있다.

[0028] 물체의 이동을 분석하기 위하여, 고정 좌표계로 측정된 데이터 b를 관성 좌표계로 측정된 데이터 n으로 변환하는 것이 편리하다. 관성 좌표계와 고정 좌표계에 대응하는 단위 벡터(unit vector)를 각각 $[X,Y,Z]^n$와 $[x,y,z]^b$로 나타낸다. 하나의 벡터를 다른 벡터로 변환하는 유용한 방법은 행렬 곱(matrix multiplication)을 이용하는 것이다. 변환을 위한 행렬은 DCM(direction cosine matrix) 또는 회전 행렬(rotation matrix)로 불리며 R로 나타낸다. 여기서, 전치 행렬(transpose matrix) R^T은 역행렬 R^{-1}과 같다(즉, $R^T = R^{-1}$)는 성질을 주목할 필요가 있다. 이 행렬은 직교하는 단위 벡터들(orthogonal unit vectors)로 구성되어 있기 때문이다. 도 1은 고정 좌표계와 관련하여 x, y, 및 z(즉, ψ, θ, 및 ϕ) 순으로의 순차적인 3개의 회전을 도시한다. 도 1에

도시된 바와 같이, z^b, y^b, 및 x^b(즉, Body 3-2-1) 순으로의 순차 변환(sequential transformation)을 수행하기 위해 일반적인 표준 기법이 이용될 수 있다. 다시 말하면, $[X,Y,Z]^n$ 벡터가 우선 ψ 회전에 의해 곱해지고, 다음으로 θ 회전, 마지막으로 결과는 ϕ 회전 행렬에 의해 곱해진다. ϕ, θ, 및 ψ의 회전들 각각은 고정 좌표계의 x-축, y-축, 및 z-축 회전을 나타낸다. 결과적으로, 회전 행렬 R은 수학식 1과 같이 표현된다.

[0029] [수학식 1]

[0030]
$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & cos(\phi) & sin(\phi) \\ 0 & -sin(\phi) & cos(\phi) \end{bmatrix} \begin{bmatrix} cos(\theta) & 0 & -sin(\theta) \\ 0 & 1 & 0 \\ sin(\theta) & 0 & cos(\theta) \end{bmatrix} \begin{bmatrix} cos(\psi) & sin(\psi) & 0 \\ -sin(\psi) & cos(\psi) & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

[0031] 수학식 1의 3개의 회전 행렬들은 관성 좌표계 n을 직각 좌표계 b로 변환하는 하나의 행렬로 간략화될 수 있다. 간략화된 행렬 R은 다음과 같다.

[0032]
$$\begin{bmatrix} cos(\theta)cos(\psi) & cos(\theta)sin(\psi) & -sin(\theta) \\ -cos(\phi)sin(\psi)+sin(\phi)sin(\theta)cos(\psi) & cos(\phi)cos(\psi)+sin(\phi)sin(\theta)sin(\psi) & sin(\phi)cos(\theta) \\ sin(\phi)sin(\psi)+cos(\phi)sin(\theta)cos(\psi) & -sin(\phi)cos(\psi)+cos(\phi)sin(\theta)sin(\psi) & cos(\phi)cos(\theta) \end{bmatrix}$$

[0033] 결과적으로, 고정 좌표계 b로부터 관성 좌표계 n으로의 역방향 회전을 수행한 이후의 식은 수학식 2와 같다.

[0034] [수학식 2]

[0035]
$$\begin{bmatrix} X \\ Y \\ Z \end{bmatrix}^n = R^{-1} \begin{bmatrix} x \\ y \\ z \end{bmatrix}^b = R^T \begin{bmatrix} x \\ y \\ z \end{bmatrix}^b$$

[0036] **IMU 센서 타입(IMU sensor Types)**

[0037] **자이로스코프(Gyroscope).** 자이로스코프는 코리올리 효과(Coriolis effect)를 통해 고정 좌표계 b에 관한 3축의 각 속도(angular velocity) $[\omega_x, \omega_y, \omega_z]^b$를 측정할 수 있다. 코리올리 힘(Coriolis force)은 관성 좌표계와 관련하여 회전하는 고정 좌표계 내에서 움직이는 물체에 작용하는 관성력(inertial force)이다. 예를 들어, 시계방향으로 회전하는 고정 좌표계에 있어서, 힘은 물체의 움직임의 왼쪽으로 작용한다. 반시계방향으로 회전하는 고정 좌표계에 있어서, 힘은 오른쪽으로 작용한다. 여기서, 코리올리 힘에 의한 물체의 편향(deflection)을 코리올리 효과라 부른다. 일반적으로, 자이로스코프는 두 개의 질량체(masses)가 스프링에 의해 연결된 튜닝 포크 구성(tuning fork configuration)을 이용한다. 각 속도가 가해질 때, 각 질량체에 대한 코리올리 힘은 반대 방향으로 작용하고, 결과적으로 유도되는 캐패시턴스의 변화는 각 속도에 비례하게 된다. 반대로, 선 가속도(linear acceleration)가 가해질 때, 두 질량체는 동일한 방향으로 움직이고, 이는 캐패시턴스의 변화를 유도하지 않는다. 결국, 측정된 각 속도는 0이다.

[0038] **자력계(Magnetometer).** 자력계는 고정 좌표계 b에 관하여 자기장(magnetic field)의 강도(strength)와 방향(direction)을 측정한다. 자력계에 의해 출력된 3축의 요소들(components) $[M_x, M_y, M_z]^b$은 센서의 현재 위치에서의 자기력선(magnetic field line)에 접하는 벡터를 나타낸다. 지구의 자극들(Earth's magnetic poles)에서 자기력선과 지구의 수평면(Earth's horizontal planes)은 직교한다(즉, 경사 각도(angle of inclination)는 90도임). 반면에, 적도(equator)에서 자기력선은 수평면과 평행하기 때문에 경사 각도는 0도이다. 일반적으로, 자력계는 주변 자기장을 측정하기 위하여 자기장 내에서의 이동에 따라 변화하는 퍼멀로이(permalloy)의 자기 저항(magneto-resistance)에 의존한다.

[0039] 자력계는 일반적으로 3차원 회전의 전 대역(full range)에 걸쳐 회전하기 때문에, 이상적인 자기 데이터(magnetic data)는 완전 구체(perfect sphere)를 형성하여야 한다. 그러나, 대부분의 응용에서, 자력계 데이터는 센서 회로 보드(sensor circuti board)나 주변 환경에 의해 생성되는 자기장에 의해 왜곡된다. 일반적으로, 왜곡은 강철(hard iron)과 연철(soft iron)의 두 가지 카테고리 중 하나이다. 강철 왜곡(hard iron

distortion)은 자기장을 생성하는 물체에 의해 발생한다. 예컨대, 자성체(magnetic material)가 물리적으로 센서에 부착된 경우, 강철 왜곡이 발생하고 센서 출력 내에 영구적인 바이어스(permanent bias)가 생성된다. 이러한 왜곡은 구의 중심(center of the sphere)이 원점(origin)으로부터 멀어지게 한다. 반면에, 연철 왜곡(soft iron distortion)은 기존의 자기장을 늘어지게 하거나(streches) 왜곡시키는데, 이는 일반적으로 니켈(niclel)이나 철(iron)과 같은 금속에 의해 야기된다. 이러한 왜곡은 구(sphere)를 타원체(ellipsoid)로 변화하게 만든다. 캘리브레이션(calibration)은 자력계 데이터에 대한 강철 왜곡과 연철 왜곡에 의한 효과를 제거할 수 있다. 즉, 바이어스되고 왜곡된 타원체를 원점에 중심을 둔 구로 재배치할 수 있다.

[0040] **신호 주입 공격(Signal Injection Attacks)**

[0041] 자이로스코프가 센서의 공진 주파수(resonant frequency)를 갖는 음향 신호(acoustic signals)에 민감하다는 것은 널리 알려진 바 있다. 최근, Khazaaleh et al.은 자이로스코프의 감지 축(sensing axis)과 구동 축(drive axis)의 정렬 불량(misalignment)이 음향에 취약한 주요 원인임을 보였다((Shadi Khazaaleh, Georgios Korres, Mohammed Eid, Mahmoud Rasras, and Mohammed F Daqaq. Vulnerability of mems gyroscopes to targeted acoustic attacks. IEEE Access, 7:89534-89543, 2019.).

[0042] 자력계를 타겟으로 하는 공격 방법에 대한 연구들이 존재한다. 첫번째 공격 방법으로써, 자기-기반 휠 속도 센서(magnetic-based wheel speed sensors)에 기반하는 ABS 시스템을 타겟으로하는 공격 방법이 Shoukry et al.에 의해 증명되었다. 자기 센서 근처에 얇은 전자기 액츄에이터를 위치시킴으로써, 공격자는 휠 스피드를 스푸핑(spoof)하기 위한 의도적인 자기장(즉, 악의적인 신호(malicious signals))을 주입하였다(Yasser Shoukry, Paul Martin, Paulo Tabuada, and Mani Srivastava. Non-invasive spoofing attacks for anti-lock braking systems. In International Conference on Cryptographic Hardware and Embedded Systems, pages 55-72. Springer, 2013.)

[0043] **공격 모델(ATTACK MODEL)**

[0044] 공격자는 장치의 정상적인 동작에 간섭을 유발하거나 악의적인 신호를 IMU 센서에 주입함으로써 장치가 다르게 동작하도록 할 수 있다. 본 발명에서는 IMU 센서로의 신호 주입 공격에 대한 복원력을 갖는 시스템을 제안한다. 예컨대, IMU 센서가 구비된 장치가 드론(drone)이나 SBV(self-balancing vehicle)일 때, 본 발명의 목적은 악의적인 신호가 주입된 경우라도 장치가 최초의 의도나 기능과 유사한 패턴을 따르도록 하는 것이다.

[0045] 자이로스코프에 대한 음향 신호 주입 공격(acoustic signal injection attacks)과는 다르게, 자력계에 대한 자기 신호 주입 공격(magnetic signal injection attacks)은 타겟이 되는 자력계와 매우 근접한 거리에서 수행된다. 예컨대, 자이로스코프에 대한 음향 신호 주입 공격은 7.8m에서 가능하다. 그러나, 자력계에 대한 신호 주입 공격을 위해서, 악의적인 자기 신호는 타겟 센서나 타겟 센서와 매우 근접한 범위에 공격자의 센서를 물리적으로 부착함으로써 주입된다. 따라서, 공격의 실현 가능성을 고려할 때, 공격자는 자이로스코프와 자력계 중 어느 하나에 대한 신호 주입 공격만을 수행할 수 있다고 가정할 수 있다. 추가적으로, 공격자는 타겟 장치에 물리적인 손상을 가하거나 소프트웨어를 수정하거나 조작할 수 없다고 가정한다. 여기서, 본 명세서 상에서 장치(device)라 함은 IMU 센서(예컨대, 자이로스코프와 자력계)가 구비된 장치를 의미할 수 있다.

[0046] 아하에서는, 센서(예컨대, IMU 센서로써 자이로스코프 및/또는 자력계를 의미할 수 있음)를 대상으로 하는 신호 주입 공격의 탐지 및/또는 복원력 제공 방법과 장치에 관해 상세히 설명한다.

[0047] 본 발명에서는 두 개의 수학적 모델을 제안한다. 하나는 자력계 데이터로부터 자이로스코프 데이터(즉, 각속도)를 추정하는 것이고, 다른 하나는 자이로스코프 데이터로부터 자력계 데이터를 추정하는 것이다. 이 두 개의 수학적 모델에 기초하여, 본 발명은 신호 주입 공격을 탐지하고, 및/또는 복원력을 제공할 수 있다.

[0048] **자이로스코프 데이터의 추정(Gyroscope Estimation)**

[0049] 자력계는 시간 t에서 자기력선(magnetic field line)에 접하는 자기장 벡터 $M^b(t) = [M_x(t), M_y(t), M_z(t)]^b$를 출력한다. 다시 말하면, 자력계가 회전하는 경우라도, 자력계는 항상 센서의 현재 위치에서 자기력선에 접하는 자기장 벡터를 출력한다. 따라서, 자이로스코프 데이터는 고정 좌표계 b의 각 축과 관련하여 자기장 벡터의 각의 변화율(change rate)이 된다. 도 2에 도시된 바와 같이, 각들 $\theta^b(t) = [\theta_x(t), \theta_y(t), \theta_z(t)]^b$은 시간 t에서 고정 좌표계 b의 각 축과 관련된 자기장 벡터 $M^b(t)$에 의해

형성된다. 이는 수학식 3 내지 수학식 5와 같다.

[0050] [수학식 3]

[0051] $$\theta_x^b(t) = \arctan \frac{M_y^b(t)}{M_z^b(t)}$$

[0052] [수학식 4]

[0053] $$\theta_y^b(t) = \arctan \frac{M_z^b(t)}{M_x^b(t)}$$

[0054] [수학식 5]

[0055] $$\theta_z^b(t) = \arctan \frac{M_x^b(t)}{M_y^b(t)}$$

[0056] 결과적으로, 자이로스코프 데이터는 시간 t에 대하여 각 $\theta^b(t)$의 일계 도함수(first derivative)로써 추정될 수 있다. 추정된 자이로스코프 데이터 $\widehat{\omega}^b(t)$는 수학식 6 내지 수학식 8과 같이 계산된다.

[0057] [수학식 6]

[0058] $$\widehat{\omega}_x^b(t) = \frac{\frac{d}{dt}M_y^b(t) \cdot M_z^b(t) - M_y^b(t) \cdot \frac{d}{dt}M_z^b(t)}{(M_y^b(t))^2 + (M_z^b(t))^2}$$

[0059] [수학식 7]

[0060] $$\widehat{\omega}_y^b(t) = \frac{M_x^b(t) \cdot \frac{d}{dt}M_z^b(t) - \frac{d}{dt}M_x^b(t) \cdot M_z^b(t)}{(M_x^b(t))^2 + (M_z^b(t))^2}$$

[0061] [수학식8]

[0062] $$\widehat{\omega}_z^b(t) = \frac{\frac{d}{dt}M_x^b(t) \cdot M_y^b(t) - M_x^b(t) \cdot \frac{d}{dt}M_y^b(t)}{(M_x^b(t))^2 + (M_y^b(t))^2}$$

[0063] 이산적인 센서 측정(discrete sensor measurements)으로 인하여, 연속적인 도함수(continuous derivative)가 이용될 수 없고, 따라서 시간 t에서의 도함수 값(derivative value)은 미분 계수(differential quotient, 또는 차분 계수)에 의해 근사될 수 있다. 미분 계수는 구간(interval)에 대하여 함수의 평균 변화율(aeveage rate of change)을 의미한다. 도함수를 근사화하는 방법으로, 전향 차분(forward difference), 후방 차분(backward difference), 및 중심 차분(central difference)의 3가지 방법이 있다. 이 중 가장 근접한 근사 결과를 제공하는 중심 차분이 이용될 수 있다. 그러나, 본 발명이 이에 제한되는 것은 아니며, 실시예에 따라 전향 차분이나 후방 차분이 이용될 수도 있다. 시간 t에서의 이산 도함수는 시간 t-1과 시간 t+1에서의 측정값 사이의 차이를 평균한 후 측정들 사이의 실제 경과 시간(actual elapsed time)으로 나누어 줌으로써 계산될 수 있다. 따라서, 샘플링 레이트(sampling rate) f에 대하여, 시간 t에서 $M^b(t)$의 일계 이산 도함수는 수학식 9와 같이 표현될 수 있다.

[0064] [수학식 9]

[0065] $$\frac{d}{dt}M^b(t) = \frac{f}{2} \cdot (M^b(t+1) - M^b(t-1))$$

[0066] 도 3은 iPhone 13 Pro Max가 각 축을 기준으로 회전할 때, 고정 좌표계와 관련하여 측정된 자이로스코프 데이터와 추정된 자이로스코프 데이터를 보여준다. 각 회전에 대하여 3-축의 자이로스코프 데이터의 측정치와 추정치

사이의 차이의 평균 에러(average error)는 각각 0.0565 (rad/s), 0.0788 (rad/s), 및 0.1003 (rad/s)이다.

[0067] **자력계 추정(Magnetometer Estimation)**

[0068] QSF(quasi-static magnetic field)에 따라, 자이로스코프 데이터 $\omega^b(t)$와 자력계 데이터 $M^b(t)$ 사이의 관계는 $\frac{d}{dt}M^b(t) = -\omega^b(t) \wedge M^b(t)$로 표현된다. 여기서, ^는 벡터의 외적(cross product)을 나타낸다. 이러한 관계는 감지된 자기장이 지구 자기장과 상이한 경우에도 유효하다. 따라서, 자력계 데이터의 시간 t에 관한 일계 도함수 $\frac{d}{dt}M^b(t)$는 수학식 10 내지 수학식 12와 같이 계산될 수 있다.

[0069] [수학식 10]

[0070] $$\frac{d}{dt}M_x^b(t) = -\omega_y^b(t)M_z^b(t) + \omega_z^b(t)M_y^b(t)$$

[0071] [수학식 11]

[0072] $$\frac{d}{dt}M_y^b(t) = \omega_x^b(t)M_z^b(t) - \omega_z^b(t)M_x^b(t)$$

[0073] [수학식 12]

[0074] $$\frac{d}{dt}M_z^b(t) = -\omega_x^b(t)M_y^b(t) + \omega_y^b(t)M_x^b(t)$$

[0075] 일반적으로, 현재 시간 t에서의 자력계 데이터 $M^b(t)$는 $M^b(t) = M^b(t-1) + \frac{d}{dt}M^b(t) \cdot \Delta t$로 표현될 수 있다. 여기서, Δt는 센서의 샘플링 주기(sampling period)이다(즉, $\Delta t = \frac{1}{f}$). 이러한 표현은 자력계 데이터의 일계 도함수 $\frac{d}{dt}M^b(t)$의 적분(integral)을 수학적으로 계산하는 것과 동일하다. 여기서, 일계 도함수 값은 짧은 시간 구간(즉, 샘플링 주기)에 걸쳐 의미있게(significantly) 변화할 수 없음을 가정한다. 따라서, 시간 t에서 자력계 데이터의 일계 도함수 $\frac{d}{dt}M^b(t)$는 스몰 α에 대하여 $\frac{d}{dt}M^b(t-1)+\alpha$로 표현될 수 있고, 따라서 현재 시간 t에서 자력계 데이터 $M^b(t)$는 $M^b(t) = M^b(t-1) + \frac{d}{dt}M^b(t-1) \cdot \Delta t + \alpha \cdot \Delta t$이 된다. 여기서 $\|\alpha \cdot \Delta t\| < \epsilon$이다. 결과적으로, 추정된 자력계 데이터 $\widehat{M}^b(t)$는 수학식 13 내지 수학식 15와 같이 근사될 수 있다.

[0076] [수학식 13]

[0077] $$\widehat{M}_x^b(t) = M_x^b(t-1) + \frac{1}{f} \cdot (-\omega_y^b(t-1)M_z^b(t-1) + \omega_z^b(t-1)M_y^b(t-1))$$

[0078] [수학식 14]

[0079] $$\widehat{M}_y^b(t) = M_y^b(t-1) + \frac{1}{f} \cdot (\omega_x^b(t-1)M_z^b(t-1) - \omega_z^b(t-1)M_x^b(t-1))$$

[0080] [수학식 15]

[0081] $$\widehat{M}_z^b(t) = M_z^b(t-1) + \frac{1}{f} \cdot (-\omega_x^b(t-1)M_y^b(t-1) + \omega_y^b(t-1)M_x^b(t-1))$$

[0082] 도 4는 iPhone 13 Pro Max가 각 축으로 회전할 때 고정 좌표계와 관련하여 측정된 자력계 데이터와 추정된 자력계 데이터를 도시한다. 각 회전에 대하여 측정된 3-축 자력계 데이터와 추정된 3-축 자력계 데이터 사이의 차이의 평균 에러는 0.0801 (μT), 0.2656 (μT), 및 0.1909 (μT)이다.

[0083] **공격 복원력(Attack Resilience)**

[0084] 제안하는 기법의 전체적인 프로세스는 도 5에 도시되어 있다. 자이로스코프 데이터의 추정을 위해서, 수집된 자력계 데이터는 노이즈를 제거하기 위하여 캘리브레이션 및/또는 필터링될 수 있다. 그런 다음, 자이로스코프 데이터는 수학식 6 내지 수학식 9를 이용하여 (필터링된) 자력계 데이터로부터 추정될 수 있다. 추정된 자이로스코프 데이터는 윈도우(window) N(N은 임의의 실수) 내에서 MAE(mean absolute error)에 기초하여 실제 자이로스코프 데이터와 비교될 수 있다. 실시예에 따라, MAE가 아닌 다른 오차 측정 방식이 이용될 수도 있다. 추정된 자이로스코프 데이터 $\widehat{\omega}^b$와 측정된 자이로스코프 데이터 ω^b와 관련하여, 자이로스코프 추정 에러(gyroscope estimation error, GEE)는 수학식 16과 같이 계산될 수 있다.

[0085] [수학식 16]

[0086] $$GEE = \frac{1}{N}\sum_{k=1}^{N}\|\widehat{\omega}_k^b - \omega_k^b\|$$

[0087] GEE가 특정 임계값보다 크다면, 자이로스코프에 대한 음향 신호 주입 공격이 발생한 것으로 판단될 수 있고, 정상 기능과 유사한 패턴으로 행동하기 위하여 추정된 자이로스코프 데이터가 실제 측정된 자이로스코프 데이터 대신 사용될 수 있다. 후에, GEE가 임계값보다 작아지면, 공격이 중단된 것으로 판단될 수 있고, 실제 측정된 자이로스코프 데이터가 다시 이용될 수 있다. 임계값은 사용자나 관리자에 의하여 미리 정해질 수 있는 값으로, 실험 결과를 통해 도출될 수 있다.

[0088] 자력계 데이터의 추정을 위해서, 측정된 자이로스코프 데이터는 노이즈를 제거하기 위하여 필터링될 수 있고, 자력계 데이터는 수학식 13 내지 수학식 15를 이용하여 필터링된 자이로스코프 데이터로부터 추정될 수 있다. 그런 다음, 추정된 자력계 데이터는 윈도우 N 내에서 MAE에 기초하여 실제 자력계 데이터와 비교될 수 있다. 유사하게, 추정된 자력계 데이터 $\widehat{M}^b$과 측정된 자력계 데이터 M^b와 관련하여, 자력계 추정 에러(magnetometer estimation error, MEE)는 수학식 17과 같이 계산될 수 있다. 또한, 마찬가지로, MEE는 미리 정해진 임계치와 비교됨으로써, 공격 여부가 탐지되고, 탐지 결과에 따라 복원력이 제공될 수 있다. 실시예에 따라, MAE가 아닌 다른 오차 측정 방식이 이용될 수도 있다.

[0089] [수학식 17]

[0090] $$MEE = \frac{1}{N}\sum_{k=1}^{N}\|\widehat{M}_k^b - M_k^b\|$$

[0091] 예를 들어, 0.1m의 둘레(circumference)를 갖는 사각 형상(square shape) 내에서 움직인 후 아래로 0.1m 다시 위로 0.1m를 움직이는 iPhone 13 Pro Max의 가속도계 데이터, 자이로스코프 데이터, 및 자력계 데이터를 측정하였다. iPhone 13 Pro Max의 움직임은 도 6의 (b)와 (c)의 검정색 선(black solid lines)으로 나타난다. 도 6의 (a)에 도시된 바와 같이, 스푸핑된(spoofed) 자이로스코프 데이터를 시뮬레이션하였다. 여기서, 측정된 자이로스코프 데이터와 스프핑된 자이로스코프 데이터의 평균 에러는 8.1407 (rad/s)이다. 스푸핑된 자이로스코프 데이터로부터 추적된 경로는 도 6의 (b)에서 파란색의 점선(blue dotted lines)으로 나타났다. 결과적으로, 실제 측정된 데이터와 공격된 데이터로부터 추적된 경로들의 좌표 사이의 코릴레이션은, 도 6의 (b)에 도시된 바와 같이, (0.8767, -0.2566, 0.8263)이고, 3개의 코릴레이션 값의 평균은 0.4821이다. 다시 말하면, 자이로스코프가 스푸핑된 후의 경로는 실제 경로와 낮은 유사도를 보인다. 반면에, 도 6의 (c)에서 파란색의 점선은 제안 기법에 의해 추정된 데이터로부터 추적된 경로를 도시한다. 도 6의 (c)에 도시된 바와 같이, 실제 데이터로부터 추적된 경로와 추정된 데이터로부터 추적된 경로 사이의 코릴레이션은 (0.9999, 0.9999, 0.9995)로 매우 높은 값을 보였다. 따라서, 제안 기법은, 심지어 신호 주입 공격이 발생한 경우라도, 장치가 정상적인 상황과 유사하게 행동하도록 할 수 있다.

[0092] 도 7은 본 발명의 일 실시예에 따른 장치를 도시하고, 도 8은 도 7에 도시된 장치에 의해 수행되는 방법을 설명하기 위한 흐름도이다. 도 7의 장치와 도 8의 방법을 설명함에 있어, 앞선 기재와 중복되는 내용에 관하여는 그 상세한 설명을 생략하기로 한다.

[0093] 도 7의 장치(100)는 소정의 센서를 대상으로 하는 신호 주입 공격을 탐지하거나, 및/또는 복원력을 제공하는 장치로써, 공격 탐지 장치, 공격 탐지 및 복원력 제공 장치, 신호 주입 공격 탐지 장치, 또는 신호 주입 공격 탐

지 및 복원력 제공 장치 등으로 명명될 수 있다. 또한, 장치(100)는 복수의 센서들이 탑재된 장치로써, 스마트폰, PC(Personal Computer), 태블릿 PC, 노트 PC, 드론, 비행체, 무인 비행체, 스마트 안경, 스마트 와치, HMD(Head Mounted Device), SBV(Self-Balancing Vehicle), 차량, 커넥티드카(connected car), 자율주행차, 스쿠터(scooter), 스태빌라이저(stabilizer), 스크루드라이버(screwdreiver), VR 헤드셋(VR headset) 등으로 구현될 수 있다.

[0094] 또한, 도 8에 도시된 방법은 도 7에 도시된 장치에 의해 수행되는 방법으로써, 공격 탐지 방법, 공격 탐지 및 복원력 제공 방법, 신호 주입 공격 탐지 방법, 또는 신호 주입 공격 탐지 및 복원력 제공 방법 등으로 명명될 수도 있다.

[0095] 장치(100)는 센서부(110), 추정부(120), 및 공격 탐지부(130)를 포함한다. 실시예에 따라, 장치(100)는 저장부(140)를 더 포함할 수도 있다.

[0096] 센서부(110)는 복수의 센서들을 포함한다. 센서부(110)는 센싱 동작을 수행하고, 이에 따라 센서값들을 획득할 수 있다(S110). 복수의 센서들은 적어도 자이로스코프와 자력계를 포함한다. 따라서, 센서부(110)는 적어도 자이로스코프 데이터(자이로스코프에 의한 감지 결과)와 자력계 데이터(자력계에 의한 감지 결과)를 획득할 수 있다.

[0097] 추정부(120)는 획득된 또는 측정된 센서값들(자이로스코프 데이터, 자력계 데이터) 중 어느 하나로부터 다른 하나의 센서값을 추정할 수 있다(S120). 예컨대, 추정부(120)는 측정된 자이로스코프 데이터로부터 자력계 데이터를 추정하거나, 측정된 자력계 데이터로부터 자이로스코프 데이터를 추정할 수 있다. 실시예에 따라, 추정부(120)는 측정된 자이로스코프 데이터로부터 자력계 데이터를 추정하고 측정된 자력계 데이터로부터 자이로스코프 데이터를 추정할 수도 있다. 이때, 추정부(120)는 수학식 6 내지 수학식 9를 이용하여 자력계 데이터로부터 자이로스코프 데이터를 추정하고, 수학식 13 내지 수학식 15를 이용하여 자이로스코프 데이터로부터 자력계 데이터를 추정할 수 있다.

[0098] 실시예에 따라, 추정부(120)는 측정된 데이터에 대한 전처리 동작(예컨대, 좌표 변환 동작), 캘리브레이션 동작 및/또는 필터링 동작을 수행하고, 전처리 동작, 캘리브레이션 동작 및/또는 필터링 동작이 수행된 신호를 이용하여 추정 동작을 수행할 수도 있다.

[0099] 공격 탐지부(130)는 센서부(110)를 대상으로 하는 공격을 탐지할 수 있다(S130). 공격은 신호 주입 공격으로써, 자이로스코프를 타겟으로 하는 음향 신호 주입 공격 및/또는 자력계를 타겟으로 하는 자기 신호 주입 공격을 의미할 수 있다. 구체적으로, 공격 탐지부(130)는 추정된 자이로스코프 데이터와 측정된 자이로스코프 데이터를 비교함으로써 자이로스코프를 대상으로 하는 신호 주입 공격을 탐지하거, 및/또는 추정된 자력계 데이터와 측정된 자력계 데이터를 비교함으로써 자력계를 대상으로 하는 신호 주입 공격을 탐지할 수 있다. 탐지 동작을 위해서는 비교 결과(차이로써, 자이로스코프 추정 에러 및/또는 자력계 추정 에러를 의미할 수 있음)를 임계치와 비교하고, 산출된 에러가 임계치를 초과하는 경우를 공격이 발생한 것으로 판단할 수 있다.

[0100] 공격 탐지부(130)가 신호 주입 공격을 탐지한 경우, 공격 탐지부(130)는 공격 대상 센서(자이로스코프 또는 자력계)에 의해 측정된 데이터가 아닌 추정된 데이터를 이용하여 장치(100)의 위치나 자세를 제어하거나, 및/또는 위치나 자세를 추정할 수 있다(S140). 즉, 추정된 데이터를 이용하여 장치(100)의 자세나 위치를 추정(제어)함으로써 복원력을 제공할 수 있다.

[0101] 또한, 공격 탐지부(130)는 산출된 에러가 임계치 미만인 경우, 신호 주입 공격이 중단된 것으로 판단하고, 추정된 데이터가 아닌 측정된 데이터를 이용하여 장치(100)의 위치나 자세를 제어하거나, 및/또는 위치나 자세를 추정할 수 있다.

[0102] 이와는 달리, 장치(100)는 자세 제어부(미도시) 및/또는 위치 추정부(미도시)를 더 포함할 수 있다. 신호 주입 공격이 발생한 경우, 공격 탐지부(130)는 자세 제어부 및/또는 위치 추정부로 공격 발생을 알리는 알림 신호를 전송할 수 있다. 이 경우, 자세 제어부는 측정된 데이터가 아닌 추정된 데이터를 이용하여 자세를 제어하거나, 및/또는 자세를 추정할 수 있다. 위치 추정부는 측정된 데이터가 아닌 추정된 데이터를 이용하여 위치를 제어하거나, 및/또는 위치를 추정할 수 있다. 여기서, 추정된 데이터는 추정부(120)로부터 수신되거나, 저장부(140)에 저장되어 있을 수 있다.

[0103] 또한, 신호 주입 공격이 중단된 경우, 공격 탐지부(130)는 자세 제어부 및/또는 위치 추정부로 공격 발생이 중단되었음을 알리는 알림 신호를 전송할 수 있다. 이 경우, 자세 제어부는 추정된 데이터가 아닌 측정된 데이터를 이용하여 자세를 제어하거나, 및/또는 자세를 추정할 수 있다. 위치 추정부는 추정된 데이터가 아닌 측정된

데이터를 이용하여 위치를 제어하거나, 및/또는 위치를 추정할 수 있다. 여기서, 측정된 데이터는 센서부(110)로부터 수신되거나, 저장부(140)에 저장되어 있을 수 있다.

[0104] 저장부(140)에는 장치(100)의 동작에 필요한 OS(Operating System), 프로그램 등이 저장되어 있을 수 있다. 또한, 저장부(140)에는 센서부(110)에 의한 감지인 자이로스코프 데이터, 자력계 데이터, 추정부(120)에 의한 추정의 결과, 공격 탐지부(130)에 의한 탐지 결과 등이 저장될 수 있다.

[0105] 이상에서 설명된 장치는 하드웨어 구성 요소, 소프트웨어 구성 요소, 및/또는 하드웨어 구성 요소 및 소프트웨어 구성 요소의 집합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성 요소는, 예를 들어, 프로세서, 콘트롤러, 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 콘트롤러를 포함할 수 있다. 또한, 병렬 프로세서(Parallel Processor)와 같은, 다른 처리 구성(Processing Configuration)도 가능하다.

[0106] 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.

[0107] 실시예에 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 실시예를 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 실시예의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0108] 본 발명은 도면에 도시된 실시예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 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

[0109] 100 : 장치

110 : 센서부

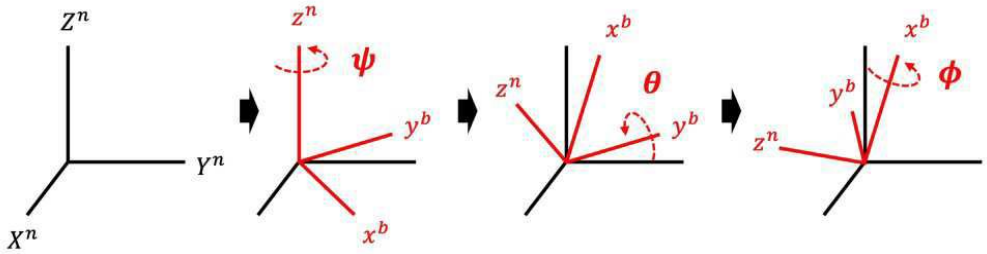
120 : 추정부

130 : 공격 탐지부

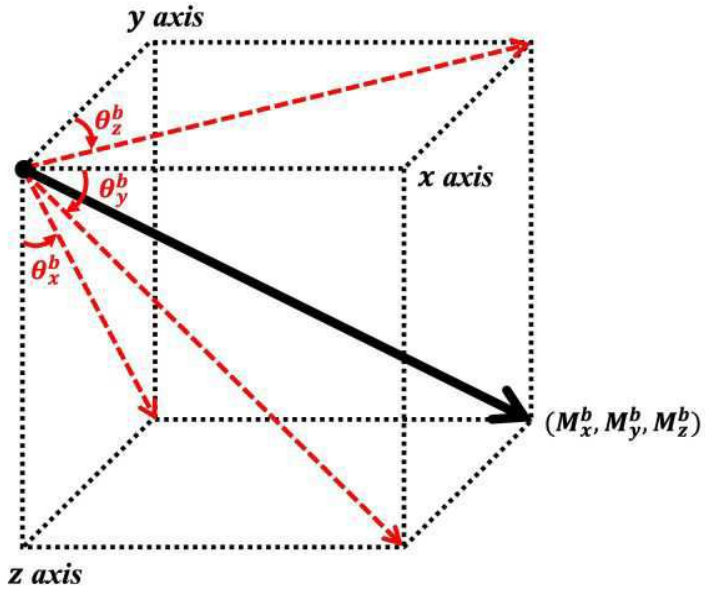
140 : 저장부

도면

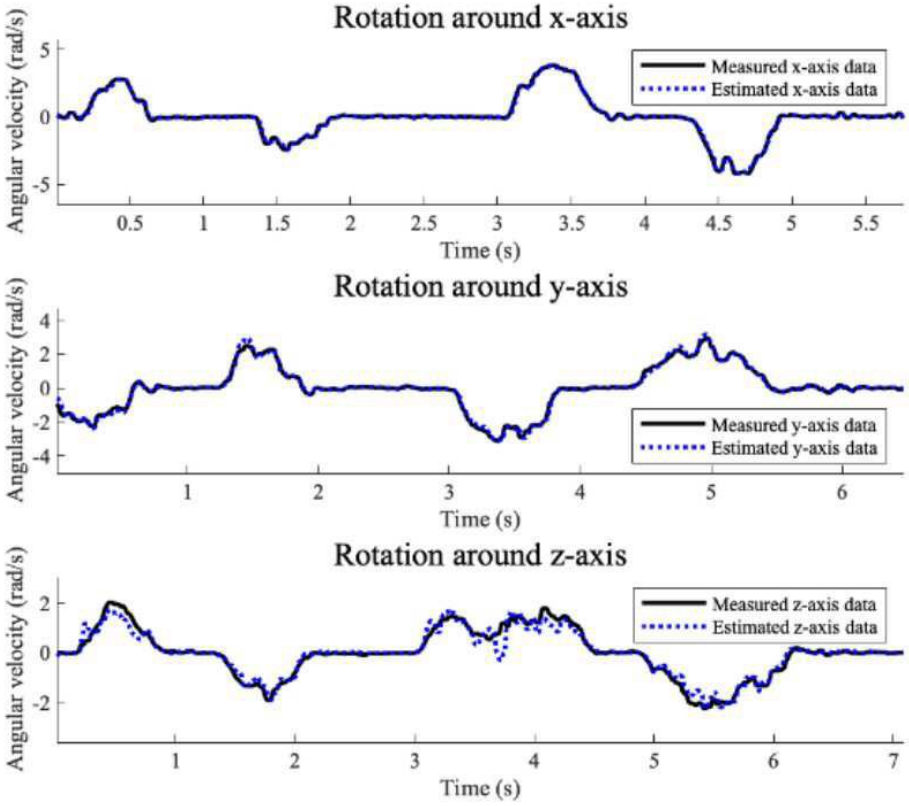
도면1



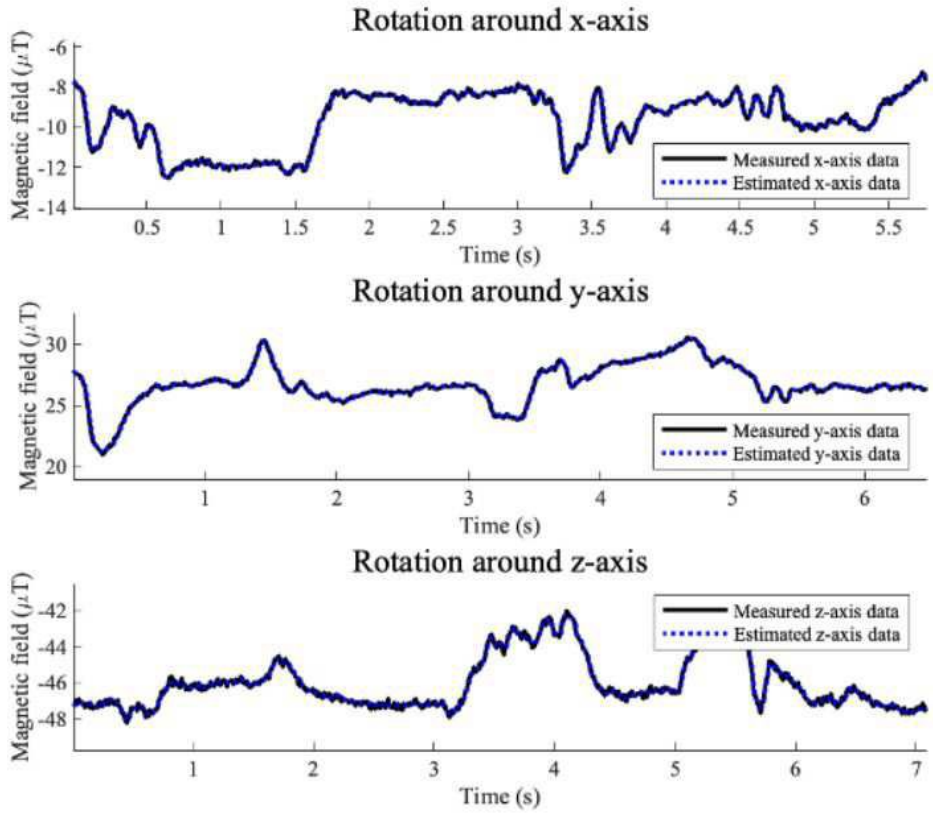
도면2



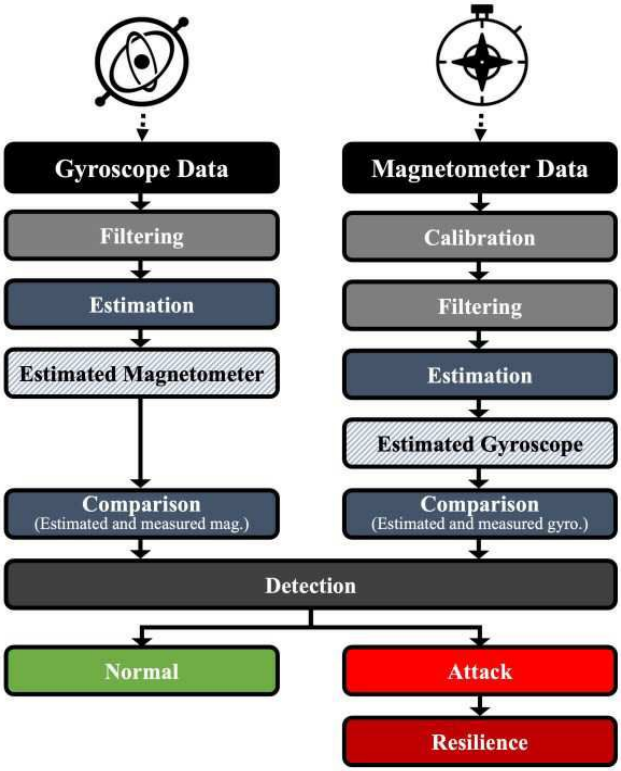
도면3


Rotation around x-axis
Angular velocity (rad/s)
Time (s)
Measured x-axis data
Estimated x-axis data
Rotation around y-axis
Angular velocity (rad/s)
Time (s)
Measured y-axis data
Estimated y-axis data
Rotation around z-axis
Angular velocity (rad/s)
Time (s)
Measured z-axis data
Estimated z-axis data

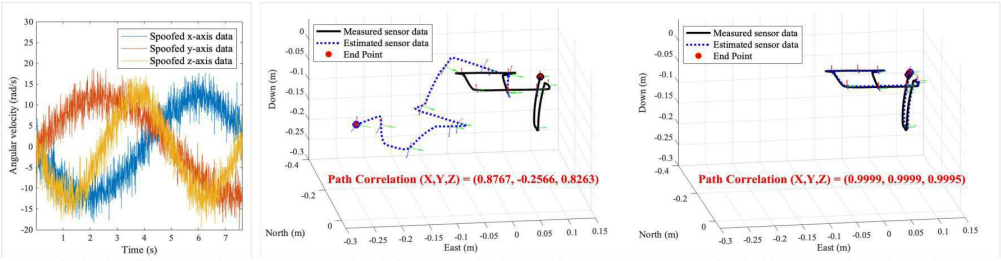
도면4


Rotation around x-axis
Magnetic field (μT)
Time (s)
Measured x-axis data
Estimated x-axis data
Rotation around y-axis
Magnetic field (μT)
Time (s)
Measured y-axis data
Estimated y-axis data
Rotation around z-axis
Magnetic field (μT)
Time (s)
Measured z-axis data
Estimated z-axis data

도면5

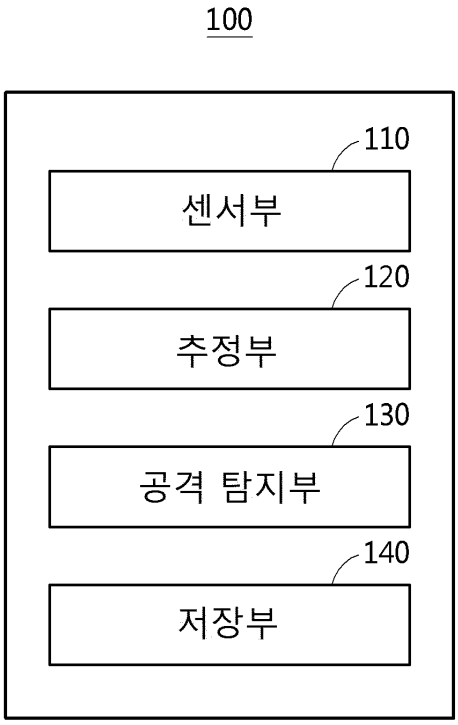


도면6

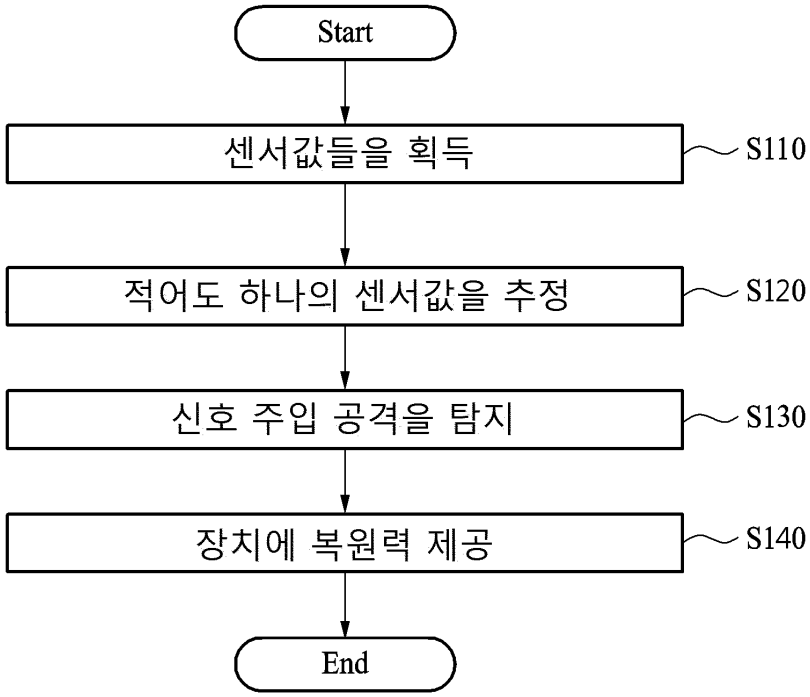


(a) Simulated spoofed gyroscope data (b) Path tracked from measured and spoofed data (c) Path tracked from measured and estimated data

도면7


100
110
센서부
120
추정부
130
공격 탐지부
140
저장부

도면8


Start
센서값들을 획득
S110
적어도 하나의 센서값을 추정
S120
신호 주입 공격을 탐지
S130
장치에 복원력 제공
S140
End