(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2024년08월29일
(11) 등록번호 10-2700111
(24) 등록일자 2024년08월23일

(51) 국제특허분류(Int. Cl.)
G06F 13/42 (2006.01)
(52) CPC특허분류
G06F 13/4282 (2013.01)
G06F 2213/0016 (2013.01)
(21) 출원번호 10-2023-0178965
(22) 출원일자 2023년12월11일
심사청구일자 2023년12월11일
(30) 우선권주장
1020230050172 2023년04월17일 대한민국(KR)
(56) 선행기술조사문헌
JP2016134047 A
(뒷면에 계속)
전체 청구항 수 : 총 10 항

(73) 특허권자
국방과학연구소
대전광역시 유성구 북유성대로488번길 160 (수남동)
(72) 발명자
류성재
경기도 성남시 수정구 창업로 54, LH기업성장센터 나동 232호(시흥동)
하재현
경기도 성남시 수정구 창업로 54, LH기업성장센터 나동 232호(시흥동)
(74) 대리인
특허법인 광장리앤고

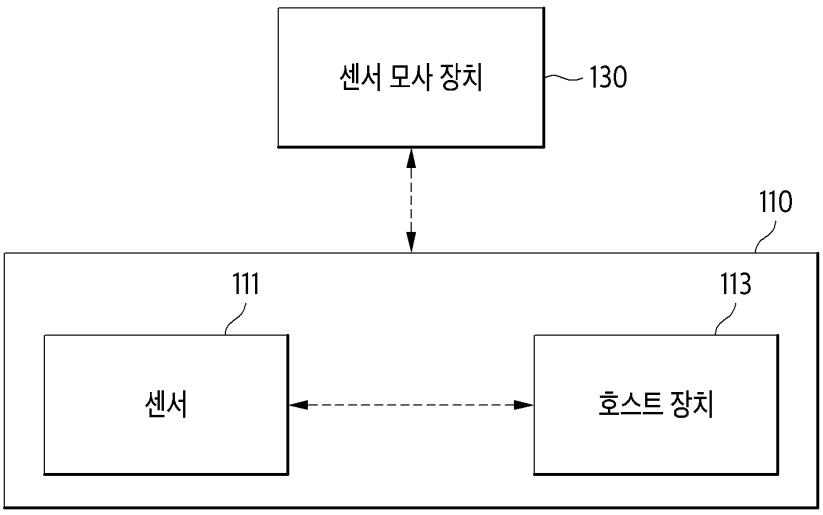
심사관 : 이진

(54) 발명의 명칭 **센서 모사 방법 및 이를 수행하는 장치**

(57) 요 약

센서 모사 장치가 시스템의 센서를 모의하여 호스트 장치에 비인가접근을 할 경우 시스템이 이러한 비인가 접근을 인지하지 못하는지 시스템의 방어 성능을 평가할 수 있는 센서 모사 방법이 개시된다. 상기 방법은, 안티 탬퍼링(Anti-Tampering) 대상이 되는 센서의 핀맵 정보를 탐지하는 단계, 상기 센서의 상기 핀맵 정보에 기반하여 복수의 핀 중에서 기 설정된 제1 핀과 제2 핀에 대응하는 신호를 획득하는 단계, 상기 제1 핀과 상기 제2 핀에 대응하는 상기 신호와 동기화된 신호를 생성하는 단계, 상기 센서에 대응하는 호스트(Host) 장치로 상기 동기화된 신호를 전송하는 단계를 포함할 수 있다.

대 표 도 - 도1



(56) 선행기술조사문헌
US20210051055 A1
KR1020180074684 A
WO2022148360 A1
KR1020210133832 A

명 세 서

청구범위

청구항 1

센서 모사 장치에 의해 수행되는 센서 모사 방법에 있어서,

무기 체계에 적용되는 시스템에 포함되는 복수의 센서와 상기 복수의 센서 별로 각각 대응하는 호스트 장치 중에서, 안티 탬퍼링(Anti-Tampering) 대상이 되는 상기 복수의 센서 중에서 전압 센서의 핀맵 정보를 탐지하는 단계;

상기 전압 센서의 상기 핀맵 정보에 기반하여 복수의 핀 중에서 기 설정된 제1 핀과 제2 핀에 대응하는 신호를 획득하는 단계;

상기 제1 핀과 상기 제2 핀에 대응하는 상기 신호와 동기화된 신호를 생성하는 단계;

상기 전압 센서에 대응하는 호스트(Host) 장치로 상기 동기화된 신호를 전송하는 단계; 및

상기 호스트 장치가 상기 동기화된 신호에 기반하여 비인가 접근 상태인지 여부를 검출하는지 여부에 기초하여 상기 무기 체계에 포함된 상기 복수의 센서 중에서 상기 전압 센서와 관련하여 설정된 상기 무기 체계에 적용되는 상기 시스템의 방어 성능을 평가하는 단계를 포함하는,

센서 모사 방법.

청구항 2

제1항에 있어서,

상기 전압 센서의 상기 핀맵 정보에 기반하여 복수의 핀 중에서 기 설정된 제1 핀과 제2 핀에 대응하는 신호를 획득하는 단계는,

상기 전압 센서와 상기 호스트 장치 간의 연결이 온(on) 상태인 동안 상기 전압 센서의 상기 제1 핀과 상기 제2 핀에서 상기 호스트 장치로 전송되는 신호를 획득하는 단계를 포함하는,

센서 모사 방법.

청구항 3

제2항에 있어서,

상기 전압 센서와 연결된 호스트(Host) 장치로 상기 동기화된 신호를 전송하는 단계는,

상기 전압 센서와 상기 호스트 장치 간의 연결을 오프(off) 상태로 처리하는 단계; 및

상기 오프 상태인 상기 전압 센서를 대신하여 상기 센서 모사 장치에서 상기 호스트 장치로 상기 동기화된 신호를 전송하는 단계를 포함하는,

센서 모사 방법.

청구항 4

제3항에 있어서,

상기 전압 센서와 상기 호스트 장치는, 기 설정된 I2C(Inter-Integrated Circuit) 통신 방식에 의해 연결되고,

상기 호스트 장치가 상기 동기화된 신호에 기반하여 비인가 접근 상태인지 여부를 검출하는지 여부에 기초하여 상기 무기 체계에 포함된 상기 복수의 센서 중에서 상기 전압 센서와 관련하여 설정된 방어 성능을 평가하는 단계는,

상기 호스트 장치가 상기 센서 모사 장치에서 전송된 상기 동기화된 신호에 기반하여 비인가 접근 상태를 검출하지 못할 경우, 상기 무기 체계에 포함된 상기 복수의 센서 중에서 상기 전압 센서와 관련하여 설정된 상기 시

스템의 방어를 회피하였다고 평가하는 단계를 포함하는,

센서 모사 방법.

청구항 5

제4항에 있어서,

상기 센서 모사 장치와 상기 호스트 장치는, 상기 기 설정된 I2C(Inter-Integrated Circuit) 통신 방식에 의해 연결되고,

상기 호스트 장치가 상기 동기화된 신호에 기반하여 비인가 접근 상태인지 여부를 검출하는지 여부에 기초하여 상기 무기 체계에 포함된 상기 복수의 센서 중에서 상기 전압 센서와 관련하여 설정된 방어 성능을 평가하는 단계는,

상기 호스트 장치가 상기 센서 모사 장치에서 전송된 상기 동기화된 신호에 기반하여 비인가 접근 상태를 검출할 경우, 상기 무기 체계에 포함된 상기 복수의 센서 중에서 상기 전압 센서와 관련하여 설정된 상기 시스템의 방어가 성공하였다고 평가하는 단계를 포함하는,

센서 모사 방법.

청구항 6

제1항에 있어서,

상기 전압 센서의 핀맵 정보를 탐지하는 단계는,

상기 전압 센서의 핀맵 정보와 함께 상기 호스트 장치의 핀맵 정보를 탐지하는 단계를 포함하는,

센서 모사 방법.

청구항 7

제6항에 있어서,

상기 호스트 장치의 상기 핀맵 정보를 탐지하는 단계는,

상기 호스트 장치의 모든 핀에 상기 센서 모사 장치를 연결하여 상기 전압 센서의 상기 제1 핀 및 상기 제2 핀에 대응하는 상기 신호와 동일한 신호가 획득되는 핀 정보를 탐지하는 단계를 포함하는,

센서 모사 방법.

청구항 8

제3항에 있어서,

상기 제1 핀은, 상기 전압 센서에서 상기 호스트 장치로 기준 클럭 신호를 전송하는 핀에 대응하고,

상기 제2 핀은, 상기 전압 센서에서 상기 호스트 장치로 상기 기준 클럭 신호에 따라 데이터 신호를 전송하는 핀에 대응하는 것을 특징으로 하는,

센서 모사 방법.

청구항 9

비일시적 컴퓨터 판독 가능 저장 매체로서,

컴퓨터 판독 가능 명령어들을 저장하도록 구성되는 매체를 포함하고,

상기 컴퓨터 판독 가능 명령어들은 프로세서에 의해 실행되는 경우 상기 프로세서가:

무기 체계에 적용되는 시스템에 포함되는 복수의 센서와 상기 복수의 센서 별로 각각 대응하는 호스트 장치 중에서, 안티 탬퍼링(Anti-Tampering) 대상이 되는 상기 복수의 센서 중에서 전압 센서의 핀맵 정보를 탐지하는 단계;

상기 전압 센서의 상기 핀맵 정보에 기반하여 복수의 핀 중에서 기 설정된 제1 핀과 제2 핀에 대응하는 신호를

획득하는 단계;

상기 제1 핀과 상기 제2 핀에 대응하는 상기 신호와 동기화된 신호를 생성하는 단계;

상기 전압 센서에 대응하는 호스트(Host) 장치로 상기 동기화된 신호를 전송하는 단계; 및

상기 호스트 장치가 상기 동기화된 신호에 기반하여 비인가 접근 상태인지 여부를 검출하는지 여부에 기초하여 상기 무기 체계에 포함된 상기 복수의 센서 중에서 상기 전압 센서와 관련하여 설정된 상기 무기 체계에 적용되는 상기 시스템의 방어 성능을 평가하는 단계를 수행하도록 하는, 비일시적 컴퓨터 판독 가능 저장 매체.

청구항 10

적어도 하나의 명령어(instruction)를 저장하는 메모리; 및

무기 체계에 적용되는 시스템에 포함되는 복수의 센서와 상기 복수의 센서 별로 각각 대응하는 호스트 장치 중에서, 안티 탬퍼링(Anti-Tampering) 대상이 되는 상기 복수의 센서 중에서 전압 센서의 핀맵 정보를 탐지하고, 상기 전압 센서의 상기 핀맵 정보에 기반하여 복수의 핀 중에서 기 설정된 제1 핀과 제2 핀에 대응하는 신호를 획득하고, 상기 제1 핀과 상기 제2 핀에 대응하는 상기 신호와 동기화된 신호를 생성하고, 상기 전압 센서와 연결된 호스트(Host) 장치로 상기 동기화된 신호를 전송하고, 상기 호스트 장치가 상기 동기화된 신호에 기반하여 비인가 접근 상태인지 여부를 검출하는지 여부에 기초하여 상기 무기 체계에 포함된 상기 복수의 센서 중에서 상기 전압 센서와 관련하여 설정된 상기 무기 체계에 적용되는 상기 시스템의 방어 성능을 평가하도록 지시하는, 제어부(controller)를 포함하는,

센서 모사 장치.

발명의 설명

기 술 분 야

[0001] 본 명세서의 실시 예는 안티 탬퍼링(Anti-Tampering)이 적용된 시스템의 방어 성능을 평가하기 위하여 시스템에 내장된 센서를 모사하는 방법 및 장치에 관한 것이다.

배 경 기 술

[0002] 안티 탬퍼링은 시스템의 정보 보안을 위해 사용되는 방식으로서, 시스템이 탬퍼를 검출한 경우 시스템은 보안이 필요한 데이터를 소거하여 데이터의 보안을 유지하는 기술이다. 무기체계와 같은 정보 보안이 중요한 기술 분야의 경우 안티 탬퍼링이 적용된 시스템의 방어 성능의 검증이 중요하다. 탬퍼에 의한 시스템에 대한 비인가접근이 성공할 경우 시스템의 방어를 회피하였다고 볼 수 있고, 탬퍼에 의한 시스템에 대한 비인가접근이 실패할 경우 시스템의 방어가 성공하였다고 볼 수 있어 이러한 안티 탬퍼링에 의한 방어 성능을 검증할 수 있는 기술이 필요하다.

발명의 내용

해결하려는 과제

[0003] 본 명세서의 실시 예는 상술한 문제점을 해결하기 위하여 제안된 것으로 안티 탬퍼링(Anti-Tampering)이 적용된 시스템의 방어 성능을 평가하기 위하여 시스템에 내장된 센서를 모사하는 방법 및 장치에 관한 것이다. 본 실시 예가 이루고자 하는 기술적 과제는 상기된 바와 같은 기술적 과제들로 한정되지 않으며, 이하의 실시 예 들로부터 또 다른 기술적 과제들이 유추될 수 있다.

과제의 해결 수단

[0004] 상술한 과제를 달성하기 위하여, 본 명세서의 일 실시 예에 따르는 센서 모사 방법은, 안티 탬퍼링(Anti-Tampering) 대상이 되는 센서의 핀맵 정보를 탐지하는 단계; 상기 센서의 상기 핀맵 정보에 기반하여 복수의 핀 중에서 기 설정된 제1 핀과 제2 핀에 대응하는 신호를 획득하는 단계; 상기 제1 핀과 상기 제2 핀에 대응하는 상기 신호와 동기화된 신호를 생성하는 단계; 및 상기 센서에 대응하는 호스트(Host) 장치로 상기 동기화된 신호를 전송하는 단계를 포함할 수 있다.

[0005] 실시 예에 따르면, 상기 센서의 상기 핀맵 정보에 기반하여 복수의 핀 중에서 기 설정된 제1 핀과 제2 핀에 대

응하는 신호를 획득하는 단계는, 상기 센서와 상기 호스트 장치 간의 연결이 온(on) 상태인 동안 상기 센서의 상기 제1 핀과 상기 제2 핀에서 상기 호스트 장치로 전송되는 신호를 획득하는 단계를 포함할 수 있다.

[0006] 실시 예에 따르면, 상기 센서와 연결된 호스트(Host) 장치로 상기 동기화된 신호를 전송하는 단계는, 상기 센서와 상기 호스트 장치 간의 연결을 오프(off) 상태로 처리하는 단계; 및 상기 오프 상태인 상기 센서를 대신하여 상기 센서 모사 장치에서 상기 호스트 장치로 상기 동기화된 신호를 전송하는 단계를 포함할 수 있다.

[0007] 실시 예에 따르면, 상기 센서와 상기 호스트 장치는, 기 설정된 I2C(Inter-Integrated Circuit) 통신 방식에 의해 연결되는 것을 특징으로 할 수 있다.

[0008] 실시 예에 따르면, 상기 센서 모사 장치와 상기 호스트 장치는, 상기 기 설정된 I2C(Inter-Integrated Circuit) 통신 방식에 의해 연결되는 것을 특징으로 할 수 있다.

[0009] 실시 예에 따르면, 상기 센서의 핀맵 정보를 탐지하는 단계는, 상기 센서의 핀맵 정보와 함께 상기 호스트 장치의 핀맵 정보를 탐지하는 단계를 포함할 수 있다.

[0010] 실시 예에 따르면, 상기 호스트 장치의 상기 핀맵 정보를 탐지하는 단계는, 상기 호스트 장치의 모든 핀에 상기 센서 모사 장치를 연결하여 상기 센서의 상기 제1 핀 및 상기 제2 핀에 대응하는 상기 신호와 동일한 신호가 획득되는 핀 정보를 탐지하는 단계를 포함할 수 있다.

[0011] 실시 예에 따르면, 상기 제1 핀은, 상기 센서에서 상기 호스트 장치로 기준 클럭 신호를 전송하는 핀에 대응하고, 상기 제2 핀은, 상기 센서에서 상기 호스트 장치로 상기 기준 클럭 신호에 따라 데이터 신호를 전송하는 핀에 대응하는 것을 특징으로 할 수 있다.

[0012] 상술한 과제를 달성하기 위하여, 본 명세서의 일 실시 예에 따르는 비일시적 컴퓨터 판독 가능 저장 매체는, 컴퓨터 판독 가능 명령어들을 저장하도록 구성되는 매체를 포함하고, 상기 컴퓨터 판독 가능 명령어들은 프로세서에 의해 실행되는 경우 상기 프로세서가: 안티 탬퍼링(Anti-Tampering) 대상이 되는 센서의 핀맵 정보를 탐지하는 단계; 상기 센서의 상기 핀맵 정보에 기반하여 복수의 핀 중에서 기 설정된 제1 핀과 제2 핀에 대응하는 신호를 획득하는 단계; 상기 제1 핀과 상기 제2 핀에 대응하는 상기 신호와 동기화된 신호를 생성하는 단계; 및 상기 센서와 연결된 호스트(Host) 장치로 상기 동기화된 신호를 전송하는 단계를 수행하도록 할 수 있다.

[0013] 상술한 과제를 달성하기 위하여, 본 명세서의 일 실시 예에 따르는 센서 모사 장치는, 적어도 하나의 명령어(instruction)를 저장하는 메모리; 및 안티 탬퍼링(Anti-Tampering) 대상이 되는 센서의 핀맵 정보를 탐지하고, 상기 센서의 상기 핀맵 정보에 기반하여 복수의 핀 중에서 기 설정된 제1 핀과 제2 핀에 대응하는 신호를 획득하고, 상기 제1 핀과 상기 제2 핀에 대응하는 상기 신호와 동기화된 신호를 생성하고, 상기 센서와 연결된 호스트(Host) 장치로 상기 동기화된 신호를 전송하도록 지시하는 제어부(controller)를 포함할 수 있다.

[0014] 기타 실시 예들의 구체적인 사항들은 상세한 설명 및 도면들에 포함되어 있다.

발명의 효과

[0015] 본 명세서의 실시 예에 따르면 아래와 같은 효과가 하나 혹은 그 이상 있다.

[0016] 첫째, 센서 모사 장치가 시스템의 센서를 모의하여 시스템이 비인가접근 상태임을 인지하지 못할 경우 시스템의 방어를 회피하였다고 평가될 수 있고, 센서 모사 장치가 시스템 내부의 특정한 하나의 센서를 모의하였으나 시스템이 비인가접근 상태임을 인지할 경우 시스템의 방어를 회피하지 못하였다고 평가될 수 있다.

[0017] 둘째, 시스템의 센서 및 호스트 장치에 대한 데이터 쉬트(data sheet)가 없더라도 센서 및 호스트 장치의 핀맵 정보를 자동으로 탐지할 수 있다.

[0018] 셋째, 호스트 장치와 센서 간의 오프 상태로 처리될 경우 호스트 장치는 주기적인 신호를 수신하지 못하더라도, 센서 모사 장치에 의해 센서와 동기화된 신호를 전송하여 시스템의 방어가 회피될 수 있다.

[0019] 실시 예의 효과들은 이상에서 언급한 효과들로 제한되지 않으며, 언급되지 않은 또 다른 효과들은 청구범위의 기재로부터 당해 기술 분야의 통상의 기술자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

[0020] 도 1은 일 실시예에 따른 센서 모사 장치를 이용하여 시스템에 대한 안티 탬퍼링 성능을 검증하는 것을 설명하기 위한 도면이다.

도 2는 일 실시예에 따른 센서 모사 장치가 센서의 핀맵 정보와 호스트 장치의 핀맵 정보를 탐지하는 것을 설명하기 위한 도면이다.

도 3은 일 실시예에 따른 센서 모사 장치가 센서의 제1 핀과 제2 핀에서 발생하는 신호를 획득하는 것을 설명하기 위한 도면이고, 도 4는 일 실시예에 따른 센서 모사 장치가 센서와 동기화된 신호를 생성하는 것을 설명하기 위한 도면이고, 도 5는 일 실시예에 따른 센서와 호스트 장치 간의 연결이 오프 상태인 동안 센서 모사 장치가 센서와 동일한 신호를 호스트 장치로 전송하는 것을 설명하기 위한 도면이다.

도 6은 일 실시예에 따른 센서 모사 방법의 흐름도를 나타낸다.

도 7은 일 실시예에 따른 센서 모사 장치의 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0021] 실시 예들에서 사용되는 용어는 본 개시에서의 기능을 고려하면서 가능한 현재 널리 사용되는 일반적인 용어들을 선택하였으나, 이는 당 분야에 종사하는 기술자의 의도 또는 판례, 새로운 기술의 출현 등에 따라 달라질 수 있다. 또한, 특정한 경우는 출원인이 임의로 선정한 용어도 있으며, 이 경우 해당되는 설명 부분에서 상세히 그 의미를 기재할 것이다. 따라서 본 개시에서 사용되는 용어는 단순한 용어의 명칭이 아닌, 그 용어가 가지는 의미와 본 개시의 전반에 걸친 내용을 토대로 정의되어야 한다.

[0022] 명세서 전체에서 어떤 부분이 어떤 구성요소를 “포함”한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있음을 의미한다. 또한, 명세서에 기재된 “~부”, “~모듈” 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어 또는 소프트웨어로 구현되거나 하드웨어와 소프트웨어의 결합으로 구현될 수 있다.

[0023] 명세서 전체에서 기재된 “a, b, 및 c 중 적어도 하나”의 표현은, ‘a 단독’, ‘b 단독’, ‘c 단독’, ‘a 및 b’, ‘a 및 c’, ‘b 및 c’, 또는 ‘a,b,c 모두’를 포괄할 수 있다.

[0024] 이하에서 언급되는 "단말"은 네트워크를 통해 전자 장치나 타 단말에 접속할 수 있는 컴퓨터나 휴대용 단말로 구현될 수 있다. 여기서, 컴퓨터는 예를 들어, 웹 브라우저(WEB Browser)가 탑재된 노트북, 데스크톱(desktop), 랩톱(laptop) 등을 포함하고, 휴대용 단말은 예를 들어, 휴대성과 이동성이 보장되는 무선 통신 장치로서, IMT(International Mobile Telecommunication), CDMA(Code Division Multiple Access), W-CDMA(W-Code Division Multiple Access), LTE(Long Term Evolution) 등의 통신 기반 단말, 스마트폰, 태블릿 PC 등과 같은 모든 종류의 핸드헬드(Handheld) 기반의 무선 통신 장치를 포함할 수 있다.

[0025] 아래에서는 첨부한 도면을 참고하여 본 개시의 실시 예에 대하여 본 개시가 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 개시는 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시 예에 한정되지 않는다.

[0026] 이하에서는 도면을 참조하여 본 개시의 실시 예들을 상세히 설명한다.

[0027] 도 1은 일 실시예에 따른 센서 모사 장치를 이용하여 시스템에 대한 안티 탬퍼링 성능을 검증하는 것을 설명하기 위한 도면이다.

[0028] 도 1을 참조하면, 시스템(110)은 적어도 하나의 센서(111)와 적어도 하나의 호스트 장치(113)를 포함할 수 있다. 시스템(110)은 도 1에 도시된 센서(111) 및 호스트 장치(113) 외에도 복수의 센서 및 호스트 장치를 더 포함할 수 있으며, 본 명세서의 권리범위가 도 1로 제한되는 것은 아니다.

[0029] 센서(111)는 호스트 장치(113)와 기 설정된 I2C(Inter-Integrated Circuit) 통신 방식에 의해 관련 정보를 송수신할 수 있다. 센서(111)와 호스트 장치(113) 간을 연결하는 복수의 통신 방식이 있을 수 있으나, 본 명세서에 기재된 내용은 I2C 통신 방식의 특징을 이용하므로 I2C 통신 방식에만 제한적으로 적용될 수 있다.

[0030] 센서(111)는 시스템(110)에 내장되어 호스트 장치(113)와 I2C 통신 방식에 의해 관련 정보를 송수신하는 복수의 센서 중 하나로서, 예컨대, 조도감지 센서, 스위치 센서, 전압 센서 등 다양한 종류의 센서에 대응할 수 있다.

[0031] 시스템(110)은 무기 체계에 적용될 수 있으며, 이 경우 시스템(110)에 대한 비인가 접근을 방지할 필요가 있다. 예를 들면, 센서(111)가 조도감지 센서일 경우, 시스템(110)을 개봉하여 시스템(110) 내부로 빛이 들어갈 경우 조도감지 센서가 이를 감지할 수 있고 비인가 접근을 방지하기 위하여 메모리에 저장된 데이터는 삭제될 수 있다. 또는, 센서(111)가 스위치 센서일 경우, 시스템(110) 내부의 물리적인 연결의 차단 여부를 스위치 센서가

감지할 수 있고 비인가 접근을 방지하기 위하여 메모리에 저장된 데이터가 삭제될 수 있다.

[0032] 이러한 시스템(110)에 대한 비인가 접근을 방지하기 위하여 시스템(110)에 대한 안티 탬퍼링 성능이 검증될 필요가 있다. 센서 모사 장치(130)는 공격자 입장에서 비인가 접근을 위하여 시스템(110)에 내장된 센서(111)를 모사하여 센서(111)와 동일한 신호를 호스트 장치(113)로 전송하여 시스템(110)이 비인가 접근 상태임을 인지하지 못하게 하는 장치이다. 만약, 센서 모사 장치(130)에 의해 시스템(110)이 비인가 접근 상태임을 인지하지 못할 경우 무기 체계에 설정된 방어를 회피하였다고 판단될 수 있으며, 센서 모사 장치(130)에 의해 시스템(110)이 비인가 접근 상태임을 인지할 경우 무기 체계에 설정된 방어를 회피하지 못하였다고 판단될 수 있다. 따라서, 센서 모사 장치(130)에 의해 무기체계의 안티 탬퍼링에 의한 방어 성능이 평가될 수 있다. 센서 모사 장치는 시스템에 내장된 복수의 센서들 중에서 일부 센서의 신호를 모사할 수 있다. 예컨대, 센서 모사 장치는 조도감지 센서를 모사할 수 없지만, 센서 모사 장치는 전압 센서를 모사하여 전압 센서와 동기화된 신호를 전송할 수 있어 시스템의 방어를 회피할 수 있다. 따라서, 센서 모사 장치(130)에 의해 시스템 내부의 복수의 센서 중에서 특정 센서의 모사 여부에 기초하여 특정 센서에 대한 안티 탬퍼링에 의한 성능이 평가될 수 있다.

[0033] 도 2는 일 실시예에 따른 센서 모사 장치가 센서의 핀맵 정보와 호스트 장치의 핀맵 정보를 탐지하는 것을 설명하기 위한 도면이다.

[0034] 도 2를 참조하면, 시스템에 내장된 센서(210)과 호스트 장치(250)의 핀맵 정보는 안티 탬퍼링에 의해 보호되어 외부에서는 알 수 없는 정보이다. 센서 모사 장치(230)가 센서(210)를 모사하여 호스트 장치(250)로 센서(210)와 동기화된 신호를 전송하기 위해서는 센서(210)와 호스트 장치(250)의 핀맵 정보를 먼저 확인할 필요가 있다. 안티 탬퍼링에 의해 보호되어 데이터 쉬트(data sheet)가 없음에도 불구하고 센서(210)와 호스트 장치(250)의 핀맵 정보를 센서 모사 장치(230)가 확인할 수 있다.

[0035] 센서 모사 장치(230)는 센서(210)의 모든 핀과 연결하여 센서(210)의 핀맵 정보를 확인할 수 있다. 이때, 센서(210)는 호스트 장치(250)와 I2C 통신 방식에 의한 통신을 수행하는 핀을 포함하고 있어, I2C 통신 방식에서 요구되는 신호는 각 핀을 통해 센서(210)에서 호스트 장치(250)로 전송되고 있으므로 센서 모사 장치(230)는 각 핀에서 검출된 신호를 확인하여 핀맵 정보를 탐지할 수 있다. 예를 들면, 제1 핀은 센서에서 호스트 장치로 기준 클럭 신호(주기적인 신호)를 전송하는 핀에 대응하고, 제2 핀은 센서에서 호스트 장치로 기준 클럭 신호에 따라 데이터 신호를 전송하는 핀에 대응할 수 있다. 이외에도, 전원이 들어오는 핀과 GND에 대응하는 핀 등 다양한 핀이 센서에 위치할 수 있다. 본 명세서에서 기준 클럭 신호를 전송하는 제1 핀과 데이터 신호를 전송하는 제2 핀뿐만 아니라, 데이터 신호를 전송하는 제1 핀과 기준 클럭 신호를 전송하는 제2 핀으로 변경하여 사용될 수 있다. 따라서, 센서 모사 장치(230)는 센서(210)의 핀맵 정보에 기반하여 복수의 핀 중에서 기 설정된 제1 핀과 제2 핀을 탐지할 수 있다.

[0036] 또한, 센서 모사 장치(230)는 호스트 장치(250)의 모든 핀과 연결하여 호스트 장치(250)의 핀맵 정보를 확인할 수 있다. 이때, 호스트 장치(250)는 센서(210)와 I2C 통신 방식에 의한 통신을 수행하는 핀을 포함하고 있어, I2C 통신 방식에서 요구되는 신호는 각 핀을 통해 센서(210)에서 호스트 장치(250)로 전송되고 있으므로 센서 모사 장치(230)는 호스트 장치(250)의 각 핀에서 검출된 신호를 확인하여 핀맵 정보를 탐지할 수 있다. 예를 들면, 센서(210)의 제1 핀과 호스트 장치(250)의 제1 핀이 연결되므로, 호스트 장치(250)의 미지의 핀 중에서 센서(210)의 제1 핀과 동일한 신호가 검출된 경우, 센서 모사 장치(230)는 해당 핀을 제1 핀으로 탐지할 수 있다. 또는, 센서(210)의 제2 핀과 호스트 장치(250)의 제2 핀이 연결되므로, 호스트 장치(250)의 미지의 핀 중에서 센서(210)의 제2 핀과 동일한 신호가 검출된 경우, 센서 모사 장치(230)는 해당 핀을 제2 핀으로 탐지할 수 있다. 따라서, 센서 모사 장치(230)는 호스트 장치(250)의 핀맵 정보에 기반하여 복수의 핀 중에서 기 설정된 제1 핀과 제2 핀을 탐지할 수 있다.

[0037] 도 3은 일 실시예에 따른 센서 모사 장치가 센서의 제1 핀과 제2 핀에서 발생하는 신호를 획득하는 것을 설명하기 위한 도면이고, 도 4는 일 실시예에 따른 센서 모사 장치가 센서와 동기화된 신호를 생성하는 것을 설명하기 위한 도면이고, 도 5는 일 실시예에 따른 센서와 호스트 장치 간의 연결이 오프 상태인 동안 센서 모사 장치가 센서와 동일한 신호를 호스트 장치로 전송하는 것을 설명하기 위한 도면이다.

[0038] 전술한 기재에 따라 센서 모사 장치(330)는 센서(310)와 호스트 장치(350)에 대한 핀맵 정보를 탐지할 수 있으며, 센서 모사 장치(330)는 센서(310)와 호스트 장치(350)에 각각 대응하는 제1 핀과 제2 핀에 연결될 수 있다.

[0039] 도 3을 참조하면, 센서(310)의 제1 핀 및 제2 핀에서 호스트 장치(350)의 제1 핀 및 제2 핀으로 신호를 전송하는 동안, 센서 모사 장치(330)는 센서(310)의 제1 핀 및 제2 핀에 연결될 수 있으며, 센서(310)의 제1 핀과 제2

핀에서 호스트 장치(350)로 전송되는 신호를 획득할 수 있다. 구체적으로, 센서 모사 장치(330)는 동기화를 위하여 센서(310)의 제1 핀에서 호스트 장치(350)로 전송되는 신호와 관련된 모든 정보를 획득할 수 있다. 예를 들면, 센서(310)의 제1 핀에서 호스트 장치(350)로 전송되는 신호의 형식, 신호의 세기, 시간 정보 등 신호와 관련된 모든 정보를 획득할 수 있다. 또한, 센서 모사 장치(330)는 동기화를 위하여 센서(310)의 제2 핀에서 호스트 장치(350)로 전송되는 신호와 관련된 모든 정보를 획득할 수 있다. 예를 들면, 센서(310)의 제2 핀에서 호스트 장치(350)로 전송되는 신호는 주기적인 신호로서, 센서(310)와 호스트 장치(350) 간의 연결이 오프 상태로 처리될 경우 호스트 장치(350)에서 이상 상태를 인지할 수 있도록 하는 신호로서, 센서 모사 장치(330)는 센서(310)의 제2 핀에서 호스트 장치(350)로 전송되는 신호의 주기, 신호의 세기 등 모든 정보를 획득할 수 있다.

[0040] 도 4를 참조하면, 센서 모사 장치(330)는 센서(310)의 제1 핀과 제2 핀으로부터 획득한 신호와 동기화된 신호를 생성할 수 있다. 이때, 센서 모사 장치가(330)가 생성한 동기화된 신호는 센서(310)의 제1 핀과 제2 핀에서 호스트 장치(350)로 전송되는 신호와 동일한 신호일 수 있다.

[0041] 도 5를 참조하면, 센서 모사 장치(330)는 호스트 장치(350)의 제1 핀 및 제2 핀에 연결될 수 있으며, 동기화된 신호를 호스트 장치(350)의 제1 핀 및 제2 핀으로 전송할 수 있다. 이때, 센서(310)와 호스트 장치(350) 간의 연결은 오프 상태로 처리될 수 있다. 즉, 센서 모사 장치(330)가 센서(310)를 모사하여 호스트 장치(350)로 동기화된 신호를 전송하고, 호스트 장치(350)에서 센서 모사 장치(330)에 의한 비인가 접근을 인지하지 못할 경우 센서 모사 장치(330)는 시스템의 센서(310)를 모의하여 시스템의 방어를 회피하였다고 평가될 수 있다.

[0042] 도 6은 일 실시예에 따른 센서 모사 방법의 흐름도를 나타낸다.

[0043] 도 6을 참조하면, S610에서 센서 모사 장치는 안티 탬퍼링(Anti-Tampering) 대상이 되는 센서의 핀맵 정보를 탐지할 수 있다. 센서와 호스트 장치는 여러 통신 방식 중에서 I2C(Inter-Integrated Circuit) 통신 방식을 이용하여 통신 할 경우에, 본 명세서에 기재된 내용이 적용될 수 있다. 센서와 호스트 장치, 센서와 센서 모사 장치, 센서 모사 장치와 호스트 장치 간의 통신 방식은 모두 I2C 통신 방식이 적용될 수 있다. 센서의 모든 핀에 센서 모사 장치가 연결될 수 있고, 센서의 모든 핀에서 방출되는 신호 중에서 기 설정된 제1 핀과 제2 핀으로부터 방출되는 신호와 대응하는 특징이 있는 신호를 방출하는 핀 정보에 기반하여 제1 핀과 제2 핀이 확인될 수 있다. 이때, 제1 핀과 제2 핀에서 방출되는 신호의 특징은 다른 핀과 구분되는 특징을 가질 수 있다.

[0044] 센서 모사 장치는 센서뿐만 아니라 호스트 장치의 핀맵 정보도 탐지할 수 있다. 호스트 장치의 모든 핀에 센서 모사 장치가 연결될 수 있고, 호스트 장치의 모든 핀 중에서 센서의 제1 핀에서 감지된 신호와 동일한 신호가 감지되는 핀을 호스트 장치의 제1 핀으로 결정하고, 센서의 제2 핀에서 감지된 신호와 동일한 신호가 감지되는 핀을 호스트 장치의 제2 핀으로 결정할 수 있다.

[0045] S620에서 센서 모사 장치는 센서의 핀맵 정보에 기반하여 복수의 핀 중에서 기 설정된 제1 핀과 제2 핀에 대응하는 신호를 획득할 수 있다. 센서와 호스트 장치 간의 연결이 온(on) 상태인 동안 센서의 제1 핀과 제2 핀에서 호스트 장치로 전송되는 신호를 획득할 수 있다.

[0046] S630에서 센서 모사 장치는 제1 핀과 제2 핀에 대응하는 신호와 동기화된 신호를 생성할 수 있다. 이때, 제1 핀과 제2 핀에서 각각 전송되는 신호의 특징을 모사하여 동기화된 신호가 생성될 수 있다.

[0047] S640에서 센서 모사 장치는 센서에 대응하는 호스트 장치로 동기화된 신호를 전송할 수 있다. 이때, 센서와 호스트 장치 간의 연결은 오프(off) 상태로 처리될 수 있으며, 오프 상태인 센서를 대신하여 센서 모사 장치에서 호스트 장치로 동기화된 신호를 전송할 수 있다. 만약, 호스트 장치가 센서가 아닌 센서 모사 장치에 의한 비인가 접근을 인지하지 못할 경우 센서 모사 장치는 시스템의 센서를 모의하여 시스템의 방어를 회피하였다고 평가될 수 있다.

[0048] 도 7은 일 실시예에 따른 센서 모사 장치의 블록도이다. 도 7은 본 실시 예와 관련된 구성요소들이 도시되어 있으나 이에 제한되는 것은 아니며 도 7에 도시된 구성요소들 외에 다른 범용적인 구성요소들이 더 포함될 수 있다. 전술한 기재와 중복되는 내용이 생략될 수 있다.

[0049] 도 7의 센서 모사 장치(700)는 전술한 센서 모사 방법을 수행할 수 있다. 도 7을 참조하면, 센서 모사 장치(700)는 메모리(710), 제어부(720) 및 버스(730)를 포함할 수 있다. 메모리(710) 및 제어부(720)는 버스(bus)(730)를 통하여 서로 통신할 수 있다. 메모리(710) 및 제어부(720) 각각은 적어도 하나의 기능이나 동작을 처리하는 단위를 의미할 수 있으며, 하드웨어나 소프트웨어, 또는, 하드웨어 및 소프트웨어의 결합으로 구현될 수 있다.

[0050] 실시 예에서, 센서 모사 장치(700)는 장치(700)와 관련된 다양한 데이터를 저장하는 메모리(710)를 포함할 수 있다. 예를 들어 메모리(710)에는 장치(700)의 동작을 위한 적어도 하나의 명령어(instruction)가 저장될 수 있다. 이러한 경우 메모리(710) 및 제어부(720)는 이러한 명령어를 기반으로 다양한 동작을 수행할 수 있다. 제어부(720)는 메모리(710)에 저장된 명령어가 제어부(720)에서 실행됨에 따라 앞서 언급된 동작들을 수행할 수 있다. 메모리(710)는 휘발성 메모리 또는 비휘발성 메모리일 수 있다. 예를 들어, 메모리(710)는 제어부(720)에서 처리된 데이터들 및 처리될 데이터들을 저장할 수 있다. 메모리(710)는 DRAM(Dynamic Random Access Memory), SRAM(Static Random Access Memory)등과 같은 RAM(Random Access Memory), ROM(Read-Only Memory), EEPROM(Electrically Erasable Programmable Read-Only Memory), CD-ROM, 블루레이 또는 다른 광학 디스크 스토리지, HDD(Hard Disk Drive), SSD(Solid State Drive) 또는 플래시 메모리를 포함할 수 있다.

[0051] 실시 예에서, 명령어가 제어부(720)에서 실행되며, 제어부(720)는 안티 탬퍼링(Anti-Tampering) 대상이 되는 센서의 핀맵 정보를 탐지하고, 상기 센서의 상기 핀맵 정보에 기반하여 복수의 핀 중에서 기 설정된 제1 핀과 제2 핀에 대응하는 신호를 획득하고, 상기 제1 핀과 상기 제2 핀에 대응하는 상기 신호와 동기화된 신호를 생성하고, 상기 센서와 연결된 호스트(Host) 장치로 상기 동기화된 신호를 전송하도록 지시할 수 있다.

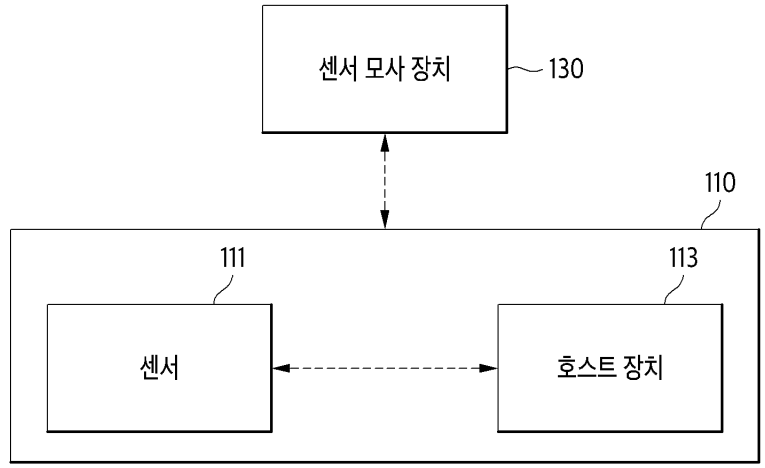
[0052] 전술한 실시 예들에 따른 장치 또는 단말은, 제어부, 프로그램 데이터를 저장하고 실행하는 메모리, 디스크 드라이브와 같은 영구 저장부(permanent storage), 외부 장치와 통신하는 통신 포트, 터치 패널, 키(key), 버튼 등과 같은 사용자 인터페이스 장치 등을 포함할 수 있다. 소프트웨어 모듈 또는 알고리즘으로 구현되는 방법들은 상기 제어부상에서 실행 가능한 컴퓨터가 읽을 수 있는 코드들 또는 프로그램 명령들로서 컴퓨터가 읽을 수 있는 기록 매체 상에 저장될 수 있다. 여기서 컴퓨터가 읽을 수 있는 기록 매체로 마그네틱 저장 매체(예컨대, ROM(read-only memory), RAM(random-Access memory), 플로피 디스크, 하드 디스크 등) 및 광학적 판독 매체(예컨대, 시디롬(CD-ROM), 디브이디(DVD: Digital Versatile Disc)) 등이 있다. 컴퓨터가 읽을 수 있는 기록 매체는 네트워크로 연결된 컴퓨터 시스템들에 분산되어, 분산 방식으로 컴퓨터가 판독 가능한 코드가 저장되고 실행될 수 있다. 매체는 컴퓨터에 의해 판독가능하며, 메모리에 저장되고, 제어부에서 실행될 수 있다.

[0053] 본 실시 예는 기능적인 블록 구성들 및 다양한 처리 단계들로 나타내어질 수 있다. 이러한 기능 블록들은 특정 기능들을 실행하는 다양한 개수의 하드웨어 또는/및 소프트웨어 구성들로 구현될 수 있다. 예를 들어, 실시 예는 하나 이상의 마이크로제어부들의 제어 또는 다른 제어 장치들에 의해서 다양한 기능들을 실행할 수 있는, 메모리, 프로세싱, 로직(logic), 룩 업 테이블(look-up table) 등과 같은 집적 회로 구성들을 채용할 수 있다. 구성 요소들이 소프트웨어 프로그래밍 또는 소프트웨어 요소들로 실행될 수 있는 것과 유사하게, 본 실시 예는 데이터 구조, 프로세스들, 루틴들 또는 다른 프로그래밍 구성들의 조합으로 구현되는 다양한 알고리즘을 포함하여, C, C++, C#, 파이썬(python), 자바(Java), 어셈블러(assembler) 등과 같은 프로그래밍 또는 스크립팅 언어로 구현될 수 있다. 기능적인 측면들은 하나 이상의 제어부들에서 실행되는 알고리즘으로 구현될 수 있다. 또한, 본 실시 예는 전자적인 환경 설정, 신호 처리, 및/또는 데이터 처리 등을 위하여 종래 기술을 채용할 수 있다. “매커니즘”, “요소”, “수단”, “구성”과 같은 용어는 넓게 사용될 수 있으며, 기계적이고 물리적인 구성들로서 한정되는 것은 아니다. 상기 용어는 제어부 등과 연계하여 소프트웨어의 일련의 처리들(routines)의 의미를 포함할 수 있다.

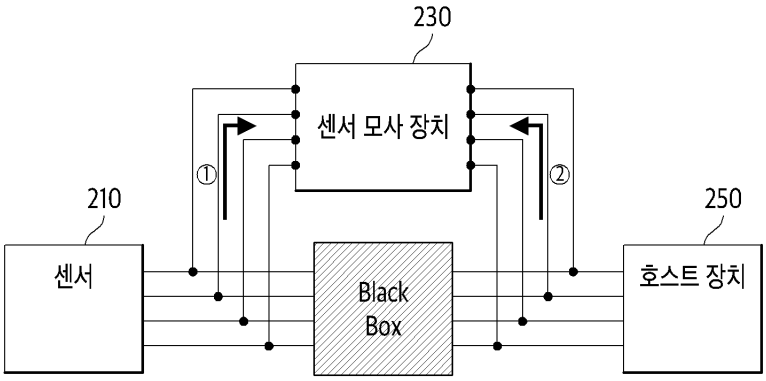
[0054] 전술한 실시예들은 일 예시일 뿐 후술하는 청구항들의 범위 내에서 다른 실시예들이 구현될 수 있다.

도면

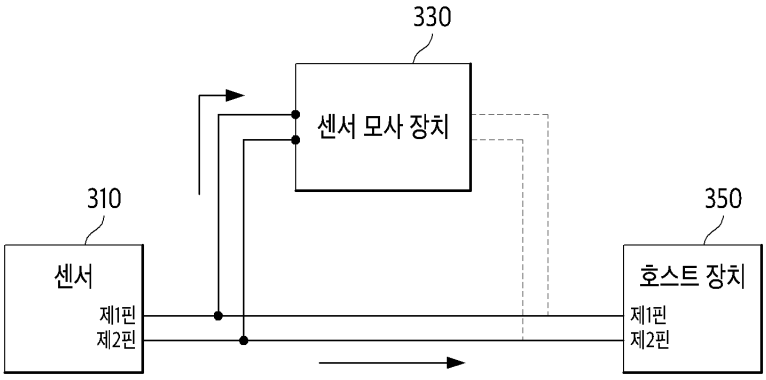
도면1



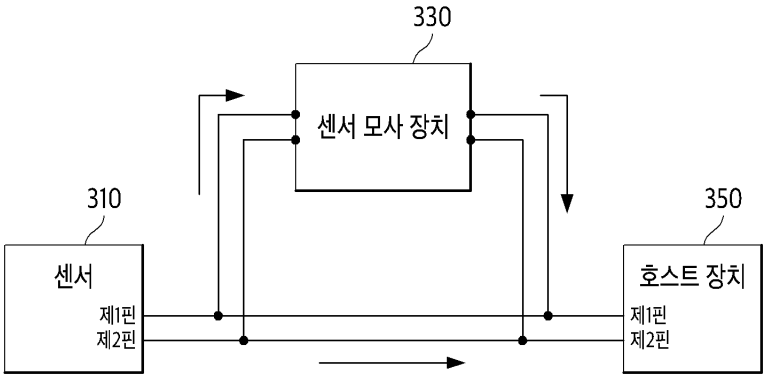
도면2



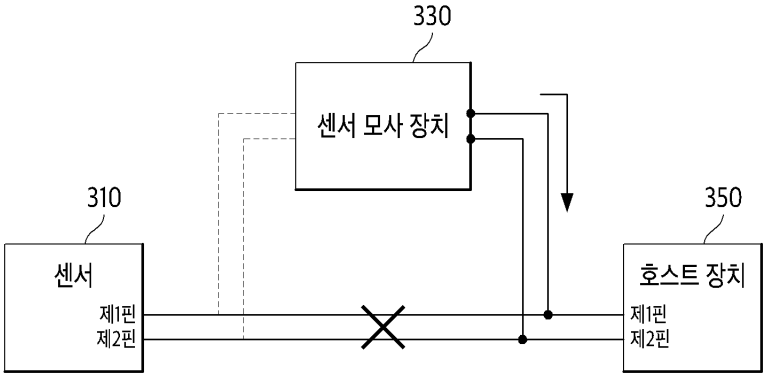
도면3



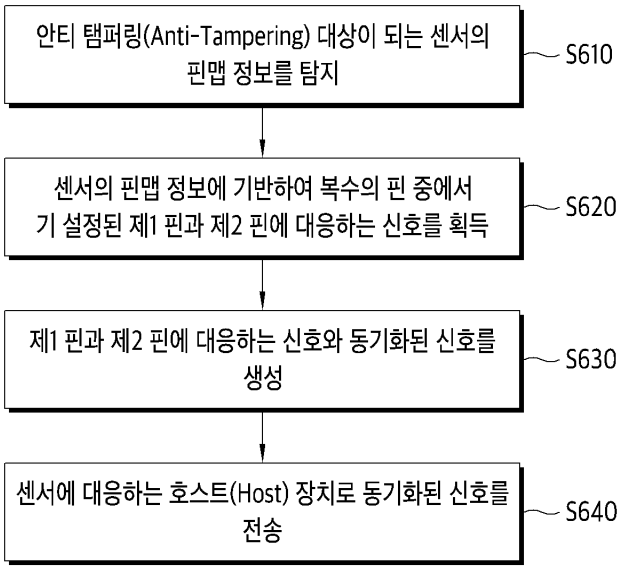
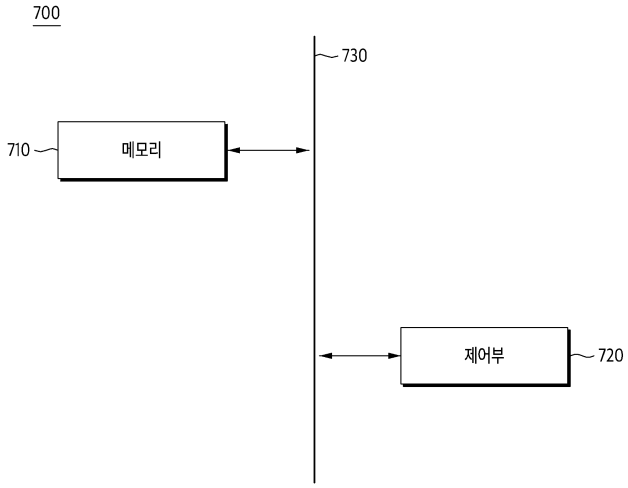
도면4


330
센서 모사 장치
310
센서
제1핀
제2핀
350
호스트 장치
제1핀
제2핀

도면5


330
센서 모사 장치
310
센서
제1핀
제2핀
350
호스트 장치
제1핀
제2핀

도면6


안티 탬퍼링(Anti-Tampering) 대상이 되는 센서의 핀맵 정보를 탐지
S610
센서의 핀맵 정보에 기반하여 복수의 핀 중에서 기 설정된 제1 핀과 제2 핀에 대응하는 신호를 획득
S620
제1 핀과 제2 핀에 대응하는 신호와 동기화된 신호를 생성
S630
센서에 대응하는 호스트(Host) 장치로 동기화된 신호를 전송
S640

도면7