(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2019-0009868
(43) 공개일자 2019년01월30일

(51) 국제특허분류(Int. Cl.)
G01S 7/537 (2006.01)
(52) CPC특허분류
G01S 7/537 (2013.01)
(21) 출원번호 10-2017-0091454
(22) 출원일자 2017년07월19일
심사청구일자 2017년07월19일

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
이선우
서울특별시 서초구 남부순환로309길 38, 5동 522호 (방배동, 서초중앙하이츠빌라)
이동훈
서울특별시 종로구 사직로8길 34, 1404호(내수동, 경희궁의아침3단지아파트)
최원석
서울특별시 강북구 삼양로 256 105동 501호 (미아동,삼성래미안미아1차아파트)
(74) 대리인
김등용, 김홍석

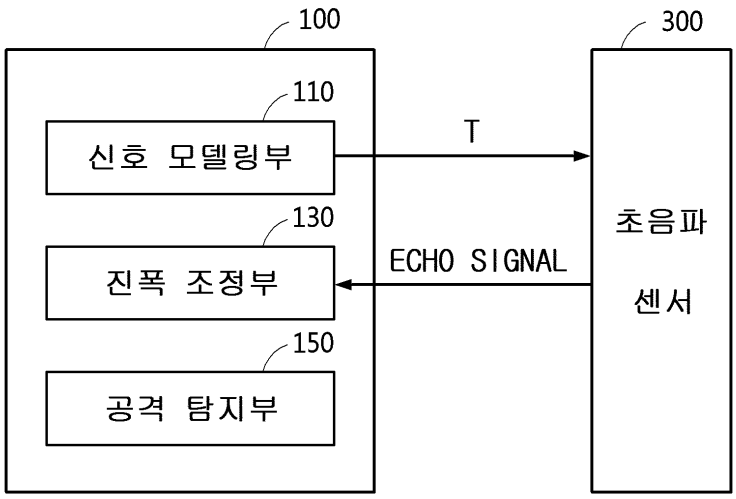
전체 청구항 수 : 총 12 항

(54) 발명의 명칭 **초음파 센서에 대한 신호 삽입 공격 탐지 장치 및 방법**

(57) 요 약

초음파 센서의 신호 삽입 공격 탐지 장치가 개시된다. 상기 신호 삽입 공격 탐지 장치는 임의의 트리거링 시간을 갖는 트리거 신호에 대응하는 에코 포락선 신호를 모델링하여 제1 에코 포락선 신호를 생성하고, 상기 임의의 트리거링 시간에 대한 정보 또는 상기 트리거 신호를 초음파 센서로 송신하는 신호 모델링부, 상기 트리거 신호에 대응하는 초음파 신호에 대응하는 에코 신호를 상기 초음파 센서로부터 수신하고, 상기 에코 신호의 포락선 신호인 제2 에코 포락선 신호를 생성하고, 상기 제1 에코 포락선 신호의 진폭을 조정하여 제3 에코 포락선 신호를 생성하는 진폭 조정부, 및 상기 제2 에코 포락선 신호와 상기 제3 에코 포락선 신호를 비교하여 신호 삽입 공격의 유무를 결정하는 공격 탐지부를 포함한다.

대 표 도 - 도1



이 발명을 지원한 국가연구개발사업
과제고유번호 20160001390021001
부처명 미래창조과학부
연구관리전문기관 정보통신기술진흥센터
연구사업명 정보통신방송연구개발사업
연구과제명 자율주행 스마트자동차용 이상징후 탐지 핵심기술개발
기 여 율 1/1
주관기관 고려대학교 산학협력단
연구기간 2017.01.01 ~ 2017.12.31

명 세 서

청구범위

청구항 1

임의의 트리거링 시간을 갖는 트리거 신호에 대응하는 에코 포락선 신호를 모델링하여 제1 에코 포락선 신호를 생성하고, 상기 임의의 트리거링 시간에 대한 정보 또는 상기 트리거 신호를 초음파 센서로 송신하는 신호 모델링부;

상기 트리거 신호에 대응하는 초음파 신호에 대응하는 에코 신호를 상기 초음파 센서로부터 수신하고, 상기 에코 신호의 포락선 신호인 제2 에코 포락선 신호를 생성하고, 상기 제1 에코 포락선 신호의 진폭을 조정하여 제3 에코 포락선 신호를 생성하는 진폭 조정부; 및

상기 제2 에코 포락선 신호와 상기 제3 에코 포락선 신호를 비교하여 신호 삽입 공격의 유무를 결정하는 공격 탐지부를 포함하는,

초음파 센서의 신호 삽입 공격 탐지 장치.

청구항 2

제1항에 있어서,

상기 진폭 조정부는 상기 제1 에코 포락선 신호의 최대 진폭의 크기와 상기 제2 에코 포락선 신호의 최대 진폭의 크기가 같도록 상기 제1 에코 포락선 신호의 진폭을 조정하는,

초음파 센서의 신호 삽입 공격 탐지 장치.

청구항 3

제1항에 있어서,

상기 신호 모델링부는 복수의 트리거링 신호 중 어느 하나를 선택하여 상기 임의의 트리거링 시간을 결정하는,

초음파 센서의 신호 삽입 공격 탐지 장치.

청구항 4

제1항에 있어서,

상기 공격 탐지부는 상기 제2 에코 포락선 신호와 상기 제3 에코 포락선 신호의 오차가 미리 정해진 임계값을 초과하는 경우를 신호 삽입 공격으로 결정하는,

초음파 센서의 신호 삽입 공격 탐지 장치.

청구항 5

제4항에 있어서,

상기 오차(error)는 수학식을 이용하여 계산되고,

상기 수학식은 $$error = \sum_{i} |envelope(t_i) - model(t_i)$$ 이고,

상기 $envelope(t_i)$ 는 t_i 시점에서 상기 제2 에코 포락선 신호의 값이고,

상기 $model(t_i)$ 는 t_i 시점에서 상기 제3 에코 포락선 신호의 값인,

초음파 센서의 신호 삽입 공격 탐지 장치.

청구항 6

복수의 트리거링 시간 중 어느 하나를 선택하여 선택된 트리거링 시간에 대한 정보 또는 상기 선택된 트리거링 시간에 대응하는 트리거 신호를 초음파 센서로 송신하고, 복수의 모델링된 에코 포락선 신호 중 상기 선택된 트리거링 시간에 대응하는 포락선 신호인 제1 에코 포락선 신호를 선택하는 신호 모델링부;

상기 트리거 신호에 대응하는 초음파 신호에 대응하는 에코 신호를 상기 초음파 센서로부터 수신하여 제2 에코 포락선 신호를 생성하거나 상기 초음파 센서로부터 상기 제2 에코 포락선 신호를 수신하고, 동일한 최대 진폭을 갖도록 상기 제1 에코 포락선 신호와 상기 제2 에코 포락선 신호 중 적어도 하나의 신호의 진폭을 조정하는 진폭 조정부; 및

상기 진폭 조정부의 진폭 조정 동작으로 생성된 최대 진폭이 동일한 두 개의 에코 포락선 신호를 이용하여 신호 삽입 공격 유무를 결정하는 공격 탐지부를 포함하는,

초음파 센서의 신호 삽입 공격 탐지 장치.

청구항 7

초음파 센서의 신호 삽입 공격 탐지 장치에 의해 수행되는 신호 삽입 공격 탐지 방법에 있어서,

상기 신호 삽입 공격 탐지 장치에 포함되는 신호 모델링부가 임의의 트리거링 시간을 갖는 트리거 신호에 대응하는 에코 포락선 신호를 모델링하여 제1 에코 포락선 신호를 생성하는 단계;

상기 신호 모델링부가 상기 임의의 트리거링 시간에 대한 정보 또는 상기 트리거 신호를 상기 초음파 센서로 송신하는 단계;

상기 신호 삽입 공격 탐지 장치에 포함되는 진폭 조정부가 상기 트리거 신호에 대응하는 초음파 신호에 대응하는 에코 신호를 상기 초음파 센서로부터 수신하는 단계;

상기 진폭 조정부가 상기 에코 신호의 포락선 신호인 제2 에코 포락선 신호를 생성하는 단계;

상기 진폭 조정부가 상기 제1 에코 포락선 신호의 진폭을 조정하여 제3 에코 포락선 신호를 생성하는 단계; 및

상기 신호 삽입 공격 탐지 장치에 포함되는 공격 탐지부가 상기 제2 에코 포락선 신호와 상기 제3 에코 포락선 신호를 비교하여 신호 삽입 공격의 유무를 결정하는 단계를 포함하는,

초음파 센서의 신호 삽입 공격 탐지 방법.

청구항 8

제7항에 있어서,

상기 제3 에코 포락선 신호를 생성하는 단계는, 상기 제1 에코 포락선 신호의 최대 진폭의 크기와 상기 제2 에코 포락선 신호의 최대 진폭의 크기가 같도록 상기 제1 에코 포락선 신호의 진폭을 조정하는,

초음파 센서의 신호 삽입 공격 탐지 방법.

청구항 9

제8항에 있어서,

상기 제1 에코 포락선 신호를 생성하는 단계는 트리거링 신호 중 어느 하나를 선택하여 상기 임의의 트리거링 시간을 결정하는,

초음파 센서의 신호 삽입 공격 탐지 방법.

청구항 10

제9항에 있어서,

상기 신호 삽입 공격의 유무를 결정하는 단계는 상기 제2 에코 포락선 신호와 상기 제3 에코 포락선 신호의 오차가 미리 정해진 임계값을 초과하는 경우를 신호 삽입 공격으로 결정하는,

초음파 센서의 신호 삽입 공격 탐지 방법.

청구항 11

초음파 센서의 신호 삽입 공격 탐지 장치에 의해 수행되는 신호 삽입 공격 탐지 방법에 있어서,

상기 신호 삽입 공격 탐지 장치에 포함되는 신호 모델링부가 복수의 트리거링 시간 중 어느 하나를 선택하여 선택된 트리거링 시간에 대한 정보 또는 상기 선택된 트리거링 시간에 대응하는 트리거 신호를 초음파 센서로 송신하는 단계;

상기 신호 모델링부가 복수의 모델링된 에코 포락선 신호 중 상기 선택된 트리거링 시간에 대응하는 포락선 신호인 제1 에코 포락선 신호를 선택하는 단계;

상기 신호 삽입 공격 탐지 장치에 포함되는 진폭 조정부가 상기 트리거 신호에 대응하는 초음파 신호에 대응하는 에코 신호를 상기 초음파 센서로부터 수신하여 제2 에코 포락선 신호를 생성하는 단계;

상기 진폭 조정부가, 동일한 최대 진폭을 갖도록 상기 제1 에코 포락선 신호와 상기 제2 에코 포락선 신호 중 적어도 하나의 신호의 진폭을 조정하는 단계; 및

상기 신호 삽입 공격 탐지 장치에 포함되는 공격 탐지부가, 상기 진폭을 조정하는 단계의 수행 결과로 생성된 최대 진폭이 동일한 두 개의 에코 포락선 신호를 이용하여 신호 삽입 공격 유무를 결정하는 단계를 포함하는,

초음파 센서의 신호 삽입 공격 탐지 방법.

청구항 12

초음파 센서의 신호 삽입 공격 탐지 장치에 의해 수행되는 신호 삽입 공격 탐지 방법에 있어서,

상기 신호 삽입 공격 탐지 장치에 포함되는 신호 모델링부가 복수의 트리거링 시간 중 어느 하나를 선택하여 선택된 트리거링 시간에 대한 정보 또는 상기 선택된 트리거링 시간에 대응하는 트리거 신호를 초음파 센서로 송신하는 단계;

상기 신호 모델링부가 복수의 모델링된 에코 포락선 신호 중 상기 선택된 트리거링 시간에 대응하는 포락선 신호인 제1 에코 포락선 신호를 선택하는 단계;

상기 신호 삽입 공격 탐지 장치에 포함되는 진폭 조정부가 상기 초음파 센서로부터 상기 제2 에코 포락선 신호를 수신하는 단계;

상기 진폭 조정부가, 동일한 최대 진폭을 갖도록 상기 제1 에코 포락선 신호와 상기 제2 에코 포락선 신호 중 적어도 하나의 신호의 진폭을 조정하는 단계; 및

상기 신호 삽입 공격 탐지 장치에 포함되는 공격 탐지부가, 상기 진폭을 조정하는 단계의 수행 결과로 생성된 최대 진폭이 동일한 두 개의 에코 포락선 신호를 이용하여 신호 삽입 공격 유무를 결정하는 단계를 포함하는,

초음파 센서의 신호 삽입 공격 탐지 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 초음파 센서에 대한 신호 삽입 공격 탐지 장치에 관한 것으로, 특히 모델링된 에코 포락선 신호와 수신된 에코 포락선 신호를 비교하여 신호 삽입 공격을 탐지할 수 있는 장치 및 방법에 관한 것이다.

배 경 기 술

[0003] 초음파 센서(ultrasonic sensor)는 거리 측정이나 장애물 탐지가 필요한 산업 분야에서 널리 사용되고 있다. 또한, 초음파 센서는 저렴한 비용과 낮은 구동 전력 등의 장점으로 인해 그 수요가 점차 증가하는 추세이다. 최근, 초음파 센서는 차량의 운전자 보조 시스템을 위해 이용된다. 예를 들어, 운전자가 차선을 변경하거나 주차할 때 초음파 센서를 통해 사각 지대의 물체를 감지할 수 있다.

[0004] 초음파 센서는 수신기(receiver)와 송신기(transmitter)로 구성되며, 트리거(trigger)라고 하는 입력 신호가 송신기에 주어지면 송신기는 트리거 신호에 대응하는 초음파 신호를 송신한다. 송신된 초음파 신호의 형태는 송신기가 트리거되는 시간, 즉 트리거링 시간(triggering time)에 의존한다. 초음파 신호가 물체에 도달하면 수신기로 다시 반사되며, 이 반사된 신호를 에코(echo) 또는 에코 신호라 한다. 초음파 센서와 물체 사이의 거리는 초음파 신호의 전송과 에코 신호의 도달 사이의 시간 차이를 이용하여 추정될 수 있다.

[0005] 그러나, 최근 공격자가 초음파 센서에 악의적인 신호를 주입함으로써 의도적으로 시스템의 오작동을 일으킬 수 있음이 알려졌다. Yan 등은 차량용 초음파 센서가 재밍(jamming)되거나 스푸핑(spoofing)될 수 있음을 보여주었다(Yan, Chen, X. Wenyuan, and Jianhao Liu. "Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle." DEFCON (2016).). 이와 같이 초음파 센서를 대상으로 하는 공격으로 인하여 장애물이 실제로 차량 전방에 존재하지만 장애물 감지 시스템이 제대로 작동하지 않는 경우가 발생할 수 있다. 이는 초음파 센서를 사용하는 대부분의 시스템이 악의적인 신호를 삽입하는 공격에 취약함을 의미한다. 따라서, 초음파 센서를 사용하는 시스템의 원활한 기능을 위하여 초음파 센서에 대한 신호 삽입 공격을 탐지하기 위한 안전한 기법이 구축되어야 한다.

[0006] 이와 같은 상황에서, 악의적인 신호 주입으로부터 센서를 보호하기 위해 센서가 수신하는 신호의 무결성을 검증하는 방법이 소개되어 왔다. 그러나 현재까지 알려진 방법들은 초음파 센서가 아닌 일반적인 센서를 중심으로 설계되어 초음파 센서에 직접적으로 적용하기 어렵다.

[0007] Ivanov 등은 센서 융합 알고리즘을 기반으로 악의적인 신호를 검출할 수 있는 방법을 제안하였다(Ivanov, Radosslav, Miroslav Pajic, and Insup Lee. "Attack-resilient sensor fusion for safty-critical cyber-physical systems." ACM Transactions on Embedded Computing Systems (TECS) (2016)). 센서 융합 알고리즘은 같은 데이터를 측정하는 여러 센서들(이종의 센서들)이 필요하다. 그러나, 차량을 포함한 일반적인 시스템은 초음파 센서 하나만을 사용하는 경우가 많고, 이러한 경우에 Ivanov 등이 제안한 방법을 적용하는 것은 불가능하다

[0008] Shoukry 등은 센서에 들어오는 신호의 무결성을 검증하기 위해 도전-응답(challenge-response) 구조를 갖는 "PyCRA" 기법을 제안하였다(Shoukry, Yasser, et al. "PyCRA: Physical challenge-response authentication for active sensors under spoofing attacks." Proceeding of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM, 2015.). Shoukry 등이 제안한 기법에서 센서의 송신기는 임의의 구간 동안 "0"으로 구동되고(즉, 임의의 구간 동안 신호 송출을 멈추는 것을 의미하며, 챌린지라고 부름), PyCRA는 수신되는 신호(즉, 응답)를 검증한다. 즉, 응답 신호에서 "0"으로 구동되는 부분(즉, 챌린지)이 "0"이 아니면 악의적인 신호를 주입하려는 시도로 간주된다. 센서 융합 기법과 달리 PyCRA는 단일 센서에서도 사용할 수 있지만, 모든 종류의 단일 센서, 특히 초음파 센서에는 적용이 불가능하다. 초음파 센서의 경우, 송신기가 정해진 구동 구간 내에서 챌린지가 이루어져도, 송신되는 신호의 챌린지 부분은 "0"이 아닌, 진폭만 약간 감소하는 형태를 띈다. 이후 챌린지를 포함한 초음파 신호가 물체에 반사되고 돌아오는 과정에서, 응답 신호의 챌린지 부분이 처음 송신했을 때의 모양과 달라진다. 따라서, PyCRA에 의할 경우 응답 신호의 챌린지 부분을 정확하게 검증하지 못하게 된다.

[0009] 이에 본 발명은 단일 초음파 센서에도 적용 가능한 신호 삽입 공격을 탐지하는 방법을 제안하고자 한다. 본 발명은 초음파 센서의 신호 입출력 관계에 대한 수학적 모델을 기반으로 하였으며, 이에 대한 상세한 설명은 후술하기로 한다.

선행기술문헌

비특허문헌

[0011] (비특허문헌 0001) Yan, Chen, X. Wenyuan, and Jianhao Liu. "Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle." DEFCON (2016).

(비특허문헌 0002) Ivanov, Radosslav, Miroslav Pajic, and Insup Lee. "Attack-resilient sensor fusion for safty-critical cyber-physical systems." ACM Transactions on Embedded Computing Systems (TECS) (2016)

(비특허문헌 0003) Shoukry, Yasser, et al. "PyCRA: Physical challenge-response authentication for active sensors under spoofing attacks." Proceeding 냴 the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM, 2015.

발명의 내용

해결하려는 과제

[0012] 본 발명이 이루고자 하는 기술적인 과제는 단일의 초음파 센서에도 적용이 가능한 신호 삽입 공격 탐지 장치 및 방법을 제공하는 것이다.

과제의 해결 수단

[0014] 본 발명의 일 실시 예에 따른 초음파 센서의 신호 삽입 공격 탐지 장치는 임의의 트리거링 시간을 갖는 트리거 신호에 대응하는 에코 포락선 신호를 모델링하여 제1 에코 포락선 신호를 생성하고, 상기 임의의 트리거링 시간에 대한 정보 또는 상기 트리거 신호를 초음파 센서로 송신하는 신호 모델링부, 상기 트리거 신호에 대응하는 초음파 신호에 대응하는 에코 신호를 상기 초음파 센서로부터 수신하고, 상기 에코 신호의 포락선 신호인 제2 에코 포락선 신호를 생성하고, 상기 제1 에코 포락선 신호의 진폭을 조정하여 제3 에코 포락선 신호를 생성하는 진폭 조정부, 및 상기 제2 에코 포락선 신호와 상기 제3 에코 포락선 신호를 비교하여 신호 삽입 공격의 유무를 결정하는 공격 탐지부를 포함한다.

[0015] 본 발명의 다른 실시 예에 따른 초음파 센서의 신호 삽입 공격 탐지 장치는 복수의 트리거링 시간 중 어느 하나를 선택하여 선택된 트리거링 시간에 대한 정보 또는 상기 선택된 트리거링 시간에 대응하는 트리거 신호를 초음파 센서로 송신하고, 복수의 모델링된 에코 포락선 신호 중 상기 선택된 트리거링 시간에 대응하는 포락선 신호인 제1 에코 포락선 신호를 선택하는 신호 모델링부, 상기 트리거 신호에 대응하는 초음파 신호에 대응하는 에코 신호를 상기 초음파 센서로부터 수신하여 제2 에코 포락선 신호를 생성하거나 상기 초음파 센서로부터 상기 제2 에코 포락선 신호를 수신하고, 동일한 최대 진폭을 갖도록 상기 제1 에코 포락선 신호와 상기 제2 에코 포락선 신호 중 적어도 하나의 신호의 진폭을 조정하는 진폭 조정부, 및 상기 진폭 조정부의 진폭 조정 동작으로 생성된 최대 진폭이 동일한 두 개의 에코 포락선 신호를 이용하여 신호 삽입 공격 유무를 결정하는 공격 탐지부를 포함한다.

[0016] 본 발명의 일 실시 예에 따른 초음파 센서의 신호 삽입 공격 탐지 방법은 초음파 센서의 신호 삽입 공격 탐지 장치에 의해 수행되고, 상기 신호 삽입 공격 탐지 장치에 포함되는 신호 모델링부가 임의의 트리거링 시간을 갖는 트리거 신호에 대응하는 에코 포락선 신호를 모델링하여 제1 에코 포락선 신호를 생성하는 단계, 상기 신호 모델링부가 상기 임의의 트리거링 시간에 대한 정보 또는 상기 트리거 신호를 상기 초음파 센서로 송신하는 단계, 상기 신호 삽입 공격 탐지 장치에 포함되는 진폭 조정부가 상기 트리거 신호에 대응하는 초음파 신호에 대응하는 에코 신호를 상기 초음파 센서로부터 수신하는 단계, 상기 진폭 조정부가 상기 에코 신호의 포락선 신호

인 제2 에코 포락선 신호를 생성하는 단계, 상기 진폭 조정부가 상기 제1 에코 포락선 신호의 진폭을 조정하여 제3 에코 포락선 신호를 생성하는 단계, 및 상기 신호 삽입 공격 탐지 장치에 포함되는 공격 탐지부가 상기 제2 에코 포락선 신호와 상기 제3 에코 포락선 신호를 비교하여 신호 삽입 공격의 유무를 결정하는 단계를 포함한다.

[0017] 본 발명의 다른 실시 예에 따른 초음파 센서의 신호 삽입 공격 탐지 방법은 초음파 센서의 신호 삽입 공격 탐지 장치에 의해 수행되고, 상기 신호 삽입 공격 탐지 장치에 포함되는 신호 모델링부가 복수의 트리거링 시간 중 어느 하나를 선택하여 선택된 트리거링 시간에 대한 정보 또는 상기 선택된 트리거링 시간에 대응하는 트리거 신호를 초음파 센서로 송신하는 단계, 상기 신호 모델링부가 복수의 모델링된 에코 포락선 신호 중 상기 선택된 트리거링 시간에 대응하는 포락선 신호인 제1 에코 포락선 신호를 선택하는 단계, 상기 신호 삽입 공격 탐지 장치에 포함되는 진폭 조정부가 상기 트리거 신호에 대응하는 초음파 신호에 대응하는 에코 신호를 상기 초음파 센서로부터 수신하여 제2 에코 포락선 신호를 생성하는 단계, 상기 진폭 조정부가, 동일한 최대 진폭을 갖도록 상기 제1 에코 포락선 신호와 상기 제2 에코 포락선 신호 중 적어도 하나의 신호의 진폭을 조정하는 단계, 및 상기 신호 삽입 공격 탐지 장치에 포함되는 공격 탐지부가, 상기 진폭을 조정하는 단계의 수행 결과로 생성된 최대 진폭이 동일한 두 개의 에코 포락선 신호를 이용하여 신호 삽입 공격 유무를 결정하는 단계를 포함한다.

[0018] 본 발명의 또 다른 실시 예에 따른 초음파 센서의 신호 삽입 공격 탐지 방법은 초음파 센서의 신호 삽입 공격 탐지 장치에 의해 수행되고, 상기 신호 삽입 공격 탐지 장치에 포함되는 신호 모델링부가 복수의 트리거링 시간 중 어느 하나를 선택하여 선택된 트리거링 시간에 대한 정보 또는 상기 선택된 트리거링 시간에 대응하는 트리거 신호를 초음파 센서로 송신하는 단계, 상기 신호 모델링부가 복수의 모델링된 에코 포락선 신호 중 상기 선택된 트리거링 시간에 대응하는 포락선 신호인 제1 에코 포락선 신호를 선택하는 단계, 상기 신호 삽입 공격 탐지 장치에 포함되는 진폭 조정부가 상기 초음파 센서로부터 상기 제2 에코 포락선 신호를 수신하는 단계, 상기 진폭 조정부가, 동일한 최대 진폭을 갖도록 상기 제1 에코 포락선 신호와 상기 제2 에코 포락선 신호 중 적어도 하나의 신호의 진폭을 조정하는 단계, 및 상기 신호 삽입 공격 탐지 장치에 포함되는 공격 탐지부가, 상기 진폭을 조정하는 단계의 수행 결과로 생성된 최대 진폭이 동일한 두 개의 에코 포락선 신호를 이용하여 신호 삽입 공격 유무를 결정하는 단계를 포함한다.

발명의 효과

[0020] 본 발명의 실시 예에 따른 신호 삽입 공격 탐지 장치 및 방법에 의할 경우, 단일의 초음파 센서를 대상으로 하는 신호 삽입 공격을 탐지할 수 있는 효과가 있다.

[0021] 또한, 트리거 신호의 트리거링 시간을 랜덤하게 결정하거나, 초음파 신호의 송신과 에코 신호의 수신 동작을 반복적으로 수행함으로써 본 발명의 안전성을 향상시킬 수 있다.

도면의 간단한 설명

[0023] 본 발명의 상세한 설명에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 상세한 설명이 제공된다.

도 1은 본 발명의 일 실시 예에 따른 탐지 장치와 초음파 센서의 기능 블럭도이다.

도 2는 도 1에 도시된 초음파 센서에 의해 수신된 에코 신호와 신호 모델링부에 의해 모델링된 에코 포락선 신호의 파형을 도시하는 그래프이다.

도 3은 수신된 에코 포락선 신호와 모델링된 에코 포락선 신호 사이의 에러를 도시하는 그래프이다.

도 4는 도 1에 도시된 탐지 장치에 의해 수행되는 탐지 방법을 설명하기 위한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0024] 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 형태들로 실시될 수 있으며 본 명세서에 설명된 실시 예들에 한정되지 않는다.

[0025] 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.

[0026] 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.

[0027] 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.

[0028] 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.

[0029] 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.

[0030] 이하, 본 명세서에 첨부된 도면들을 참조하여 본 발명의 실시 예들을 상세히 설명한다.

[0032] 도 1은 본 발명의 일 실시 예에 따른 탐지 장치와 초음파 센서의 기능 블럭도이다. 도 1에서 탐지 장치(100)와 초음파 센서(300)는 별개의 구성으로 구분되어 도시되어 있으나, 실시 예에 따라 탐지 장치(100)는 초음파 센서(300)를 포함하는 개념으로 이해될 수도 있다.

[0033] 도 1을 참조하면, 공격 탐지 장치, 신호 삽입(또는 주입) 공격 탐지 장치, 초음파 센서(또는 초음파 신호)에 대한 신호 삽입 공격 탐지 장치 등으로 명명될 수 있는 탐지 장치(100)는 초음파 센서(300)의 송신기가 트리거되는 시간, 즉 트리거링 시간(triggering time, 트리거 신호의 듀레이션(duration) 또는 트리거 신호의 활성 구간의 길이)에 기초하여 에코 신호의 포락선 신호인 에코 포락선 신호(echo envelope signal)를 모델링하고, 모델링된 에코 포락선 신호와 수신된 에코 신호의 포락선 신호를 비교하여 에코 신호에 신호 삽입 여부를 결정함으로써 초음파 센서(300)에 대한 신호 삽입 공격(또는 신호 주입 공격)을 탐지할 수 있다. 탐지 장치(100)는 신호 모델링부(110), 진폭 조정부(130) 및 공격 탐지부(150) 중 적어도 하나를 포함할 수 있다.

[0035] 신호 모델링부(110)는 트리거링 시간에 기초하여 에코 포락선 신호를 모델링할 수 있다. 트리거링 시간과 에코 포락선 신호 사이의 관계는 2차 선형 시간 불변 시스템(second-order linear time-invariant(LTI) system)으로 모델링될 수 있다. 구체적으로, 에코 포락선 신호의 모델은 1) 트리거 신호가 존재할 때와 2) 트리거 신호가 존재하지 않을 때의 두 가지 구간으로 나뉠 수 있다. 첫 번째의 경우, 트리거 신호가 t_0에서 시작하여 t_1에서 끝나면(즉, 트리거 신호가 t_0에서부터 t_1까지 지속), 에코 포락선 신호의 첫 번째 부분은 수학식 1과 같이 모델링될 수 있다.

수학식 1

[0036] $$x_1(t) = KA_1 - KA_1(1 + w_n t)e^{-w_n t}$$

[0037] 수학식 1에서, K는 임의의 상수(constant)이고, A_1는 트리거 신호의 크기(amplitude)이고, w_n은 초음파 센서(300)의 고유 진동수(natural frequency)를 의미할 수 있다.

[0038] 트리거 신호가 존재하지 않는 두 번째의 경우, 즉 t_1 이후의 구간 동안 에코 포락선 신호의 두 번째 부분은 수학식 2와 같이 모델링될 수 있다.

수학식 2

[0039] $$x_2(t) = [x(t_1) + \dot{x}(t_1) + w_n x(t_1)te^{-w_n t}$$

[0040] 결국, 트리거 신호에 대응되는 에코 포락선 신호(이하, 제1 에코 포락선 신호라 함)는 수학식 3과 같이 모델링될 수 있다.

수학식 3

[0041] $$x(t) = \begin{cases} x_1(t), t_0 \le t \le t_1 \ (the\ first\ part\ of\ the\ model) \\ x_2(t), t_1 < t \qquad (the\ second\ part\ of\ the\ model) \end{cases}$$

[0042] 또한, 신호 모델링부(110)는 트리거링 시간에 대한 정보 또는 트리거링 시간을 갖는 트리거 신호를 초음파 센서(300)로 송신할 수 있다. 초음파 센서(300)는 신호 모델링부(110)로부터 수신된 트리거링 시간 또는 트리거 신호에 대응하는 초음파 신호를 송신할 수 있다.

[0043] 실시 예에 따라, 신호 모델링부(110)는 미리 정해진 복수의 트리거링 시간 중 어느 하나를 임의로 선택할 수도 있다. 이 경우, 선택된 트리거링 시간을 갖는 트리거 신호에 대응하는 에코 포락선 신호 역시 미리 모델링된 후 소정의 저장부에 저장되어 있을 수 있으므로, 별도의 모델링 동작은 생략될 수 있다. 즉, 신호 모델링부(110)는 미리 저장된 복수의 모델링된 에코 포락선 신호 중 선택된 트리거링 시간에 대응하는 에코 포락선 신호를 선택할 수 있다.

[0045] 진폭 조정부(130)는 초음파 센서(300)로부터 에코 신호를 수신하고, 수신된 에코 신호로부터 에코 포락선 신호(이하, 제2 에코 포락선 신호라 함)를 생성할 수 있다. 실시 예에 따라, 진폭 조정부(130)는 초음파 센서(300)로부터 상기 제2 에코 포락선 신호 자체를 수신할 수도 있다. 즉, 초음파 센서(300)는 상기 트리거링 신호에 대응하는 초음파 신호를 송신하고, 상기 초음파 신호가 소정의 물체에 의해 반산된 에코 신호를 수신하고, 수신된 에코 신호로부터 제2 에코 포락선 신호를 생성한 후 상기 제2 에코 포락선 신호를 탐지 장치(100)로 송신할 수도 있다.

[0046] 또한, 진폭 조정부(130)는 제1 에코 포락선 신호의 크기(또는 진폭)를 조정하여 제3 에코 포락선 신호를 생성할 수 있다. 초음파 센서(300)와 물체 사이의 거리가 멀수록 초음파 센서(300)가 수신하는 에코 신호의 진폭은 작아지는 경향을 갖는다. 하지만, 에코 포락선 신호의 모델, 즉 제1 에코 포락선 신호는 상수 계수로만 이루어졌으므로, 트리거링 시간이 정해진 후의 모델은 항상 동일하다. 따라서, 에코 신호의 진폭에 따라 모델의 진폭 크기를 조정해주어야 한다. 제1 에코 포락선 신호의 크기를 조정하기 위한 파라미터(이하, 조정 파라미터라 함) K'는 수학식 4와 같다.

수학식 4

[0047] $$K' = env_max / ref_max$$

[0048] 수학식 4에서, env_max는 제2 에코 포락선 신호의 최대 진폭 값이며, ref_max는 제1 에코 포락선 신호의 최대 진폭 값을 의미할 수 있다. 진폭 조정부(130)는 제1 에코 포락선 신호의 진폭을 조절하기 위하여 파라미터 K'를 제1 에코 포락선 신호에 곱함으로써, 제3 에코 포락선 신호를 생성할 수 있다. 제3 에코 포락선 신호는 수학식 5와 같다.

수학식 5

[0049] $$x'(t) = K' \times x(t)$$

[0050] 상술한 실시 예와는 다르게, 진폭 조정부(130)는 제1 에코 포락선 신호가 아닌 제2 에코 포락선 신호의 크기(또는 진폭)을 조정할 수도 있다. 즉, 진폭 조정부(130)는 제1 에코 포락선 신호와 제2 에코 포락선 신호 중 적어도 하나의 진폭을 조정하여 두 에코 포락선 신호의 최대 진폭이 동일하도록 조정할 수 있다.

[0052] 공격 탐지부(150)는 제2 에코 포락선 신호와 제3 에코 포락선 신호를 이용하여 에코 신호에 대한 신호 삽입 공격의 유무를 결정할 수 있다. 구체적으로, 공격 탐지부(150)는 제2 에코 포락선 신호와 제3 에코 포락선 신호의 오차에 기초하여 신호 삽입 공격의 발생 유무를 판단할 수 있다. 예시적인 오차는 수학식 6을 통해 산출될 수 있다.

수학식 6

[0053] $$error = \sum_i |envelope(t_i) - model(t_i)|$$

[0054] 수학식 6에서, $envelope(t_i)$은 t_i에서의 제2 에코 포락선 신호의 값을 의미하고, $model(t_i)$는 t_i에서의 제3 에코 포락선 신호의 값을 의미할 수 있다. 공격 탐지부(150)는 수학식 6을 이용하여 산출된 오차(error)가 미리 정해진 임계값보다 큰 경우, 신호 삽입 공격이 발생하였다고 판단할 수 있다.

[0055] 진폭 조정부(130)에 의한 진폭 조정은 제1 에코 포락선 신호와 제2 에코 포락선 신호 중 적어도 하나의 신호를 대상으로 수행될 수 있으므로, 공격 탐지부(150)는 진폭 조정의 결과로 생성된 에코 포락선 신호와 진폭 조정이 이루어지지 않은 에코 포락선 신호를 비교하거나, 진폭 조정의 결과로 생성된 두 개의 에코 포락선 신호를 비교함으로써 신호 삽입 공격의 유무를 결정할 수 있다.

[0057] 실시 예에 따라, 탐지 장치(100)는 탐지 동작 중에 수신되거나 생성되는 데이터를 저장하기 위한 저장부(미도시)를 더 포함할 수도 있다. 또한, 탐지 장치(100)는 차량 내에 설치되는 복수의 ECU들(electronic control units) 중 하나로 구현될 수 있다. 이 경우, 탐지 장치(100)는 트리거 신호 또는 트리거링 시간에 대한 정보를 초음파 센서(300)로 송신하고, 초음파 센서는 상기 트리거링 시간 또는 트리거 신호에 대응하는 초음파 신호를 송신할 수 있다. 또한, 초음파 신호가 송신 된 후 물체에 반사되어 초음파 센서(300)로 되돌아 오는 신호, 즉 에코 신호는 다시 초음파 센서(300)에 의해 수신될 수 있다.

[0059] 도 2는 도 1에 도시된 초음파 센서에 의해 수신된 에코 신호와 신호 모델링부에 의해 모델링된 에코 포락선 신

호의 파형을 도시하는 그래프이고, 도 3은 수신된 에코 포락선 신호와 모델링된 에코 포락선 신호 사이의 에러를 도시하는 그래프이다.

[0060] 초음파 센서로 (주)하기소닉 사의 HG-B40C 모델을 사용하였고, 실험을 위해 초음파 센서를 평평한 벽(flat wall)으로부터 2m에 위치하였다. 트리거링 시간은 400㎲와 600㎲를 사용하였으며, 에코 신호는 BitScope Micro 모델을 오실로스코프로 사용하여 66.7㎑로 샘플링하였다.

[0061] 도 2(a)와 도 2(c)는 각각 400㎲와 600㎲의 트리거링 시간을 갖는 트리거 신호에 대응하는 에코 포락선 신호와 모델링된 에코 포락선 신호가 서로 유사함을 보여준다. 반면에, 도 2(b)와 도 2(d)는 일치하지 않는 트리거링 시간에서 에코 포락선 신호와 모델링된 에코 포락선 신호가 서로 상이함을 보여준다.

[0062] 도 3(a)와 도 3(b)는 각각 400㎲와 600㎲의 트리거링 시간에서 에코 포락선 신호와 모델 사이의 오차를 도시하고 있다. 도 3을 참조하면, 올바른 에코 신호와 그렇지 않은 에코 신호는 명확하게 구분되는 에러를 보여주고 있음을 알 수 있다. 공격자에 의해 악의적인 신호가 삽입되었을 경우, 유효한 에코 신호와 비교하면 더욱 큰 에러를 보임을 알 수 있다. 따라서, 트리거링 시간에 대응하는 모델과 에코 포락선 신호의 차이를 비교함으로써, 악의적인 신호의 삽입 여부(또는 신호 삽입 공격의 유무)를 판단할 수 있다.

[0064] 트리거링 시간의 가능한 경우의 수가 많을수록 본 발명의 안전성이 높아질 수 있다. 그러나, 초음파 센서와 초음파의 특성상 많은 트리거링 시간을 랜덤하게 주기는 어려울 수 있다. 예컨대, 트리거링 시간 300㎲와 301㎲ 사이는 거의 차이가 없기 때문이다.

[0065] 따라서, 본 발명의 안전성은 초음파 센서를 이용한 거리 측정 시에 트리거링 시간이 랜덤으로 정해진 초음파 신호를 여러번 전송함으로써 높일 수 있다. 예컨대, 초음파 센서가 트리거링 시간을 A와 B 중 랜덤하게 선택한 후 10회에 걸쳐 초음파를 송신하는 경우를 생각할 수 있다. 이 경우, 공격자에 의한 신호 삽입 공격이 탐지되지 않기 위해서는 10 개의 초음파 신호에 대한 모든 트리거링 시간을 정확하게 예측하여야 한다. 즉, 공격자에 의한 공격 성공 확률은 (1/2)^10으로 (1/1024)가 된다. 즉, 실제로 공격자가 신호 삽입 공격을 성공할 확률은 거의 없다는 것을 의미하며, 본 발명에 의한 탐지 방법은 신호 삽입 공격으로부터 안전하다고 할 수 있다.

[0067] 도 4는 도 1에 도시된 탐지 장치에 의해 수행되는 탐지 방법을 설명하기 위한 흐름도이다. 탐지 방법을 설명함에 있어, 이미 기술된 내용과 중복되는 내용에 관하여는 그 기재를 생략하기로 한다.

[0068] 도 1 내지 도 4를 참조하면, 탐지 장치(100)의 신호 모델링부(110)는 트리거 신호의 트리거링 시간을 결정한다(S100). 이때, 신호 모델링부(110)는 미리 정해진 복수의 트리거링 시간 중 어느 하나를 선택함으로써 트리거링 신호를 결정할 수 있다.

[0069] 이후, 신호 모델링부(110)는 결정된 트리거링 시간을 갖는 트리거 신호에 대응하는 에코 포락선 신호를 모델링할 수 있다(S200). 이때, 모델링된 에코 포락선 신호를 제1 에코 포락선 신호라 할 수 있다. 실시 예에 따라, 신호 모델링부(110)는 미리 저장된 복수의 모델링된 에코 포락선 신호 중 선택된 트리거링 신호를 갖는 트리거 신호에 대응하는 모델링된 에코 포락선 신호를 선택할 수도 있다.

[0070] 신호 모델링부(110)는 결정된 트리거링 시간에 대한 정보를 초음파 센서(300)로 송신할 수 있다(S300). 실시 예에 따라, 신호 모델링부(110)는 결정된 트리거링 시간을 갖는 트리거 신호 자체를 초음파 센서(300)로 송신할 수도 있다.

[0071] 초음파 센서(300)는 신호 모델링부(110)로부터 수신된 트리거링 시간에 대한 정보 또는 트리거 신호에 대응하는 초음파 신호를 출력하고, 에코 신호를 수신한다(S400).

[0072] 진폭 조정부(130)는 초음파 센서(300)로부터 에코 신호를 수신하고, 수신된 에코 신호로부터 에코 신호 포락선 신호(제2 에코 포락선 신호)를 생성할 수 있다(S500). 실시 예에 따라, 진폭 조정부(130)는 초음파 센서(300)로부터 상기 제2 에코 포락선 신호 자체를 수신할 수도 있다.

[0073] 또한, 진폭 조정부(130)는 제1 에코 포락선 신호의 크기(또는 진폭)를 조정하여 제3 에코 포락선 신호를 생성할 수 있다(S600). 실시 예에 따라, 진폭 조정부(130)가 제1 에코 포락선 신호와 제2 에코 포락선 신호 중 적어도 하나의 진폭을 조정할 수도 있음은 이미 기술된 바와 같다.

[0074] 공격 탐지부(150)는 제2 에코 포락선 신호와 제3 에코 포락선 신호를 비교하여 신호 삽입 공격 유무를 결정할 수 있다(S700). 즉, 공격 탐지부(150)는 비교 대상인 두 개의 신호의 오차가 미리 정해진 임계값보다 큰 경우, 신호 삽입 공격이 발생하였다고 판단할 수 있다.

[0076] 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

[0078] 100 : 탐지 장치

110 : 신호 모델링부

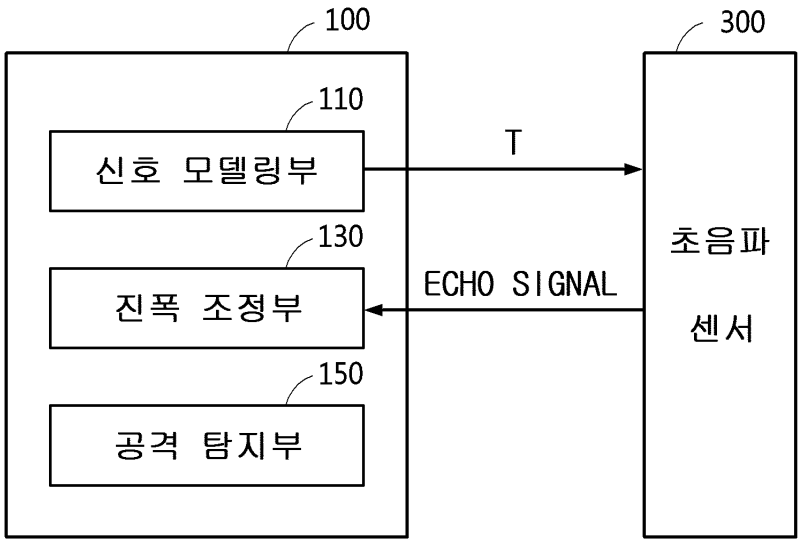
130 : 진폭 조정부

150 : 공격 탐지부

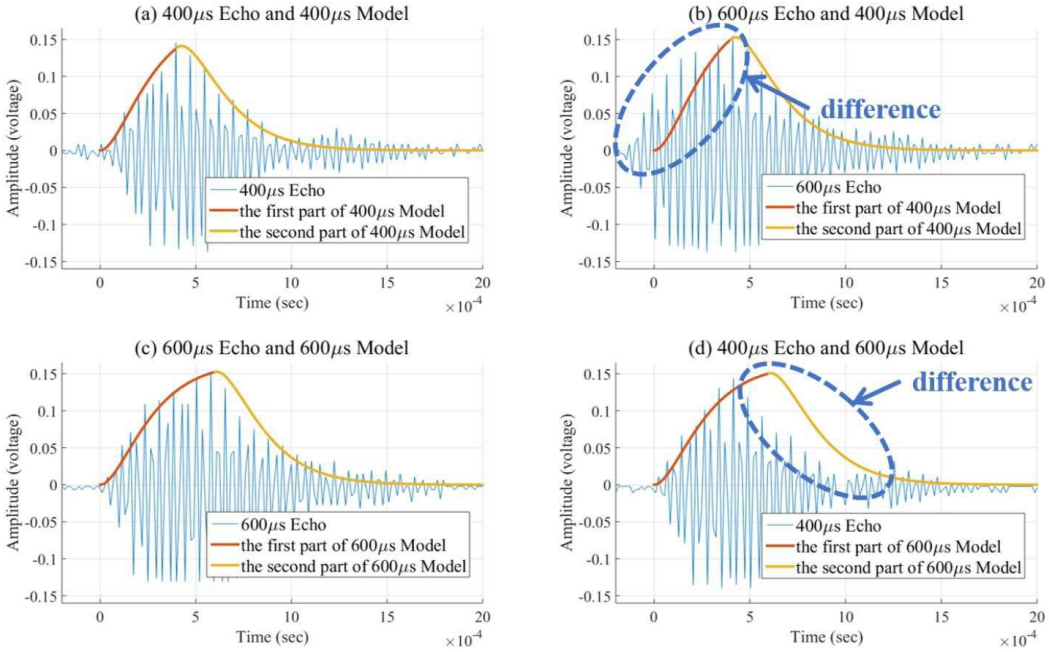
300 : 초음파 센서

도면

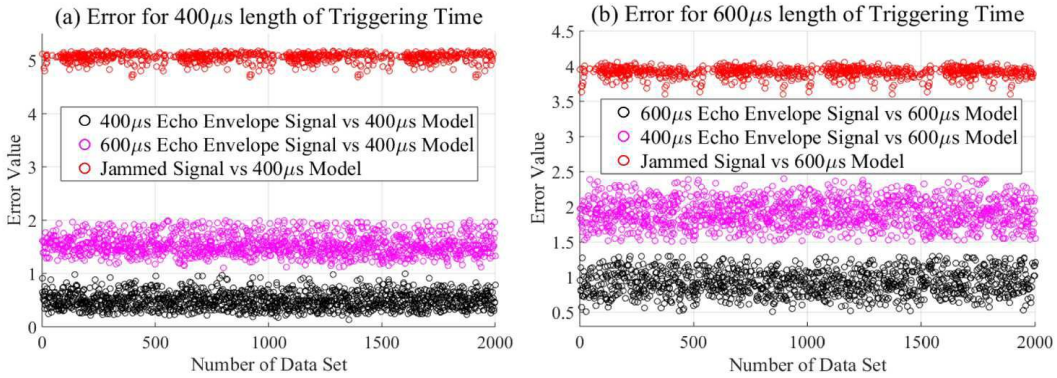
도면1



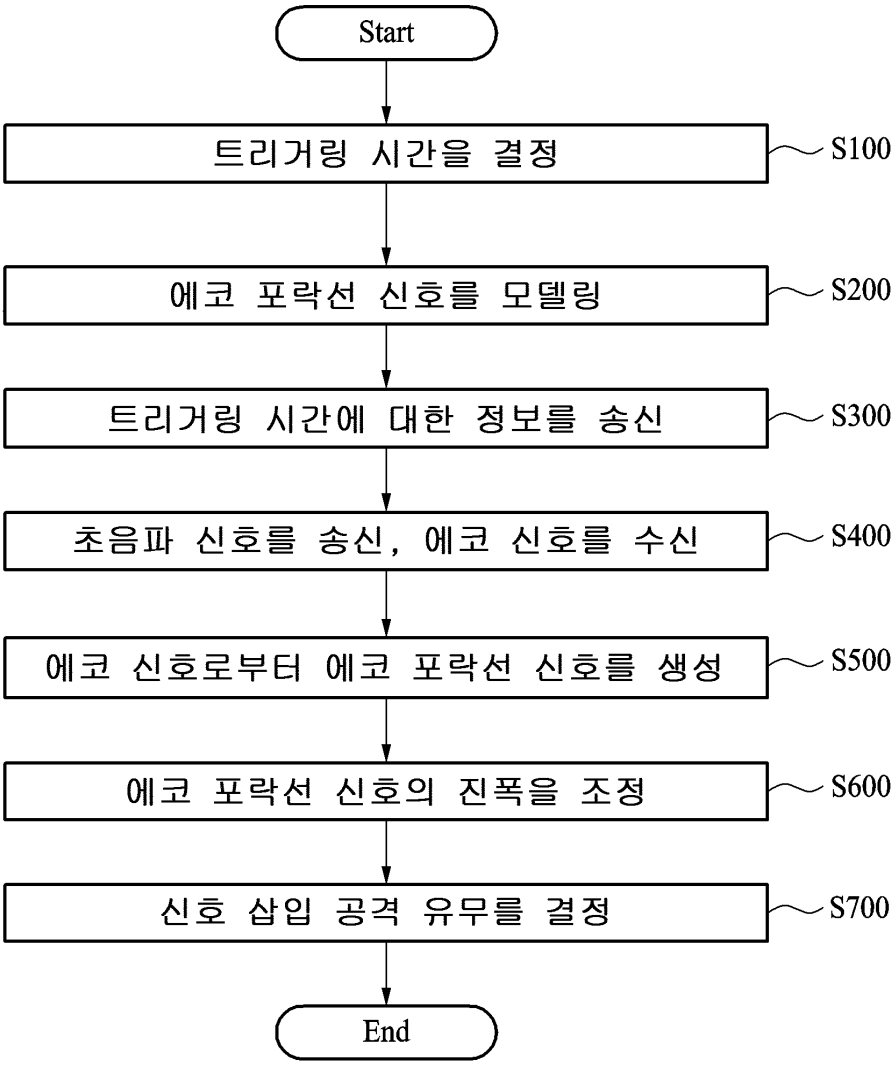
도면2


(a) 400μs Echo and 400μs Model
Amplitude (voltage)
Time (sec)
×10^-4
400μs Echo
the first part of 400μs Model
the second part of 400μs Model
(b) 600μs Echo and 400μs Model
difference
600μs Echo
the first part of 400μs Model
the second part of 400μs Model
(c) 600μs Echo and 600μs Model
600μs Echo
the first part of 600μs Model
the second part of 600μs Model
(d) 400μs Echo and 600μs Model
difference
400μs Echo
the first part of 600μs Model
the second part of 600μs Model

도면3


(a) Error for 400μs length of Triggering Time
400μs Echo Envelope Signal vs 400μs Model
600μs Echo Envelope Signal vs 400μs Model
Jammed Signal vs 400μs Model
Error Value
Number of Data Set
(b) Error for 600μs length of Triggering Time
600μs Echo Envelope Signal vs 600μs Model
400μs Echo Envelope Signal vs 600μs Model
Jammed Signal vs 600μs Model
Error Value
Number of Data Set

도면4


Start
트리거링 시간을 결정
S100
에코 포락선 신호를 모델링
S200
트리거링 시간에 대한 정보를 송신
S300
초음파 신호를 송신, 에코 신호를 수신
S400
에코 신호로부터 에코 포락선 신호를 생성
S500
에코 포락선 신호의 진폭을 조정
S600
신호 삽입 공격 유무를 결정
S700
End