



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2021-0052161
(43) 공개일자 2021년05월10일

(51) 국제특허분류(Int. Cl.)
B60R 25/24 (2013.01) B60R 25/10 (2006.01)
B60R 25/34 (2013.01)
(52) CPC특허분류
B60R 25/245 (2013.01)
B60R 25/10 (2013.01)
(21) 출원번호 10-2020-0052702
(22) 출원일자 2020년04월29일
심사청구일자 2020년04월29일
(30) 우선권주장
1020190135525 2019년10월29일 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 망우로 18가길 61-10, 4층 (뚝섬에 계속)
(74) 대리인
김홍석

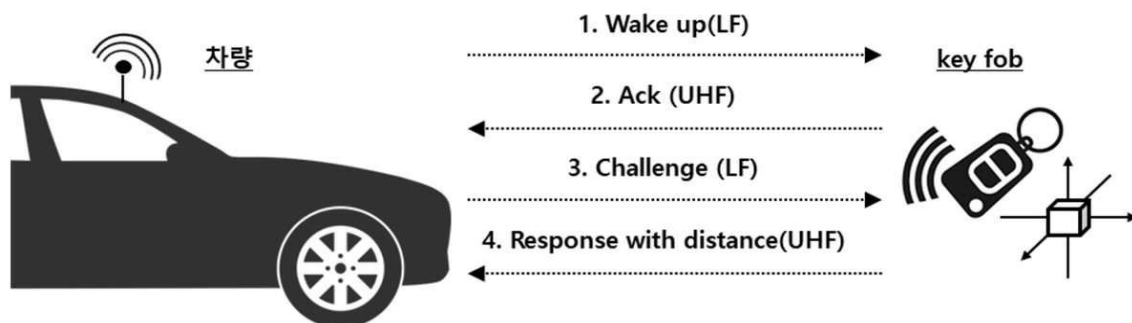
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 키 팍의 이동 거리 산출을 통한 릴레이 공격 방지 방법

(57) 요약

스마트 키의 이동 거리 산출을 통한 릴레이 공격(relay attack) 탐지 방법이 개시된다. 상기 릴레이 공격 탐지 방법은 차량이 제1 메시지를 스마트 키로 송신하는 단계, 상기 제1 메시지에 응답하여, 상기 스마트 키가 제1 응답 메시지를 상기 차량으로 송신하는 단계, 상기 차량이 상기 제1 응답 메시지에 기초하여 상기 차량과 상기 스 (뒷면에 계속)

대표도 - 도1



마트 키 사이의 제1 거리를 산출하는 단계, 상기 차량이 질의값을 포함하는 제2 메시지를 상기 스마트 키로 송신하는 단계, 상기 제2 메시지에 응답하여, 상기 스마트 키가 상기 스마트 키의 이동 거리 또는 상기 이동 거리를 산출하기 위한 정보와 상기 질의값에 대응하는 응답값을 포함하는 제2 응답 메시지를 상기 차량으로 송신하는 단계, 상기 응답값에 기초하여, 상기 차량이 상기 스마트 키가 정당한 키인지 여부를 결정하는 단계, 상기 스마트 키가 정당한 키로 결정되는 경우, 상기 차량이 상기 제2 응답 메시지에 기초하여 상기 차량과 상기 스마트 키 사이의 제2 거리를 산출하는 단계, 및 상기 이동 거리를 산출하기 위한 정보를 이용하여 산출된 이동 거리 또는 제2 응답 메시지에 포함된 상기 이동 거리 및 상기 제1 거리와 상기 제2 거리의 차이를 이용하여 산출된 이동 거리를 비교하여 릴레이 공격 여부를 결정하는 단계를 포함한다.

(52) CPC특허분류

B60R 25/34 (2013.01)

(72) 발명자

최원석

서울특별시 강북구 삼양로 256, 105동 501호

주경호

서울특별시 성북구 지봉로 24길 52-8

명세서

청구범위

청구항 1

차량이 제1 메시지를 스마트 키로 송신하는 단계;

상기 제1 메시지에 응답하여, 상기 스마트 키가 제1 응답 메시지를 상기 차량으로 송신하는 단계;

상기 차량이 상기 제1 응답 메시지에 기초하여 상기 차량과 상기 스마트 키 사이의 제1 거리를 산출하는 단계;

상기 차량이 질의값을 포함하는 제2 메시지를 상기 스마트 키로 송신하는 단계;

상기 제2 메시지에 응답하여, 상기 스마트 키가 상기 스마트 키의 이동 거리 또는 상기 이동 거리를 산출하기 위한 정보와 상기 질의값에 대응하는 응답값을 포함하는 제2 응답 메시지를 상기 차량으로 송신하는 단계;

상기 응답값에 기초하여, 상기 차량이 상기 스마트 키가 정당한 키인지 여부를 결정하는 단계;

상기 스마트 키가 정당한 키로 결정되는 경우, 상기 차량이 상기 제2 응답 메시지에 기초하여 상기 차량과 상기 스마트 키 사이의 제2 거리를 산출하는 단계; 및

상기 이동 거리를 산출하기 위한 정보를 이용하여 산출된 이동 거리 또는 제2 응답 메시지에 포함된 상기 이동 거리 및 상기 제1 거리와 상기 제2 거리의 차이를 이용하여 산출된 이동 거리를 비교하여 릴레이 공격 여부를 결정하는 단계를 포함하는 릴레이 공격 탐지 방법.

청구항 2

제1항에 있어서,

상기 제1 메시지와 상기 제2 메시지는 제1 주파수 대역을 이용하여 송신되고,

상기 제1 응답 메시지와 상기 제2 응답 메시지는 제2 주파수 대역을 이용하여 송신되고,

상기 제1 주파수 대역과 상기 제2 주파수 대역은 서로 상이한,

릴레이 공격 탐지 방법.

청구항 3

제1항에 있어서,

상기 제1 거리는 상기 제1 응답 메시지의 RSSI(Received Signal Strength Indication, 수신 신호 강도)를 이용하여 산출되고,

상기 제2 거리는 상기 제2 응답 메시지의 RSSI를 이용하여 산출되는,

릴레이 공격 탐지 방법.

청구항 4

제1항에 있어서,

상기 제2 응답 메시지에 포함된 상기 이동 거리 또는 상기 이동 거리를 산출하기 위한 정보는 상기 차량과 상기 스마트 키 사이에 미리 공유된 대칭키를 이용하여 암호화된,

릴레이 공격 탐지 방법.

청구항 5

제1항에 있어서,

상기 정한한 키인지 여부를 결정하는 단계에서 상기 스마트 키가 정한한 키가 아닌 것으로 결정되는 경우, 상기 차량은 프로토콜의 진행을 중단하는,

릴레이 공격 탐지 방법.

청구항 6

제1항에 있어서,

상기 릴레이 공격 여부를 결정하는 단계는, 상기 제1 거리와 상기 제2 거리의 차이로부터 산출된 상기 이동 거리와 상기 제2 응답 메시지에 포함된 상기 이동 거리의 차이가 미리 정해진 임계값을 초과하는 경우, 상기 릴레이 공격이 발생한 것으로 결정하는,

릴레이 공격 탐지 방법.

청구항 7

제1항에 있어서,

상기 스마트 키는 적어도 제1 시점에서의 가속도와 제2 시점의 가속도를 이용하여 상기 스마트 키의 상기 이동 거리를 산출하는,

릴레이 공격 탐지 방법.

청구항 8

제7항에 있어서,

상기 제1 시점은 제1 메시지를 수신한 시점을 의미하고,

상기 제2 시점은 제2 메시지를 수신한 시점을 의미하는,

릴레이 공격 탐지 방법.

청구항 9

차량이 웨이크업(wake up) 메시지를 LF(Low frequency) 대역을 이용하여 스마트 키로 송신하는 단계;

상기 웨이크업 메시지에 응답하여, 상기 스마트 키가 존재 확인 메시지를 UHF(Ultra High Frequency) 대역을 이용하여 상기 차량으로 송신하는 단계;

상기 차량이 상기 존재 확인 메시지의 RSSI를 이용하여 상기 차량과 상기 스마트 키 사이의 제1 거리를 산출하는 단계;

상기 차량이 질의 메시지(challenge message)를 상기 LF 대역을 이용하여 상기 스마트 키로 송신하는 단계;

상기 질의 메시지에 응답하여, 상기 스마트 키가 상기 스마트 키의 이동 거리를 포함하는 응답 메시지(response message)를 상기 UHF 대역을 이용하여 상기 차량으로 송신하는 단계;

상기 차량이 상기 응답 메시지의 RSSI를 이용하여 상기 차량과 상기 스마트 키 사이의 제2 거리를 산출하는 단

계; 및

상기 차량이 상기 제1 거리와 상기 제2 거리의 차이를 이용하여 산출된 이동 거리와 상기 응답 메시지에 포함된 상기 이동 거리를 비교하여 릴레이 공격 여부를 결정하는 단계를 포함하는 릴레이 공격 탐지 방법.

청구항 10

제9항에 있어서,

상기 스마트 키는 상기 웨이크업 메시지를 수신한 시점에서의 상기 스마트 키의 가속도와 상기 질의 메시지를 수신한 시점에서의 상기 스마트 키의 가속도를 이용하여 상기 스마트 키의 상기 이동 거리를 산출하는,

릴레이 공격 탐지 방법.

발명의 설명

기술 분야

[0001] 본 발명은 PKES(Passive Keyless Entry and Start) 시스템에서의 릴레이 공격(relay attack)을 방지하기 위한 방법에 관한 것으로, 특히 키 팍(key fob) 내의 MEMS(Micro-Electro Mechanical System) 센서를 이용하여 계산한 이동 거리와 차량에서 수신한 신호의 RSSI(Received Signal Strength Indication)를 바탕으로 계산된 이동 거리를 비교함으로써 릴레이 공격 여부를 탐지하는 방법에 관한 것이다.

배경 기술

[0002] PKES(Passive Keyless Entry and Start) 시스템은 운전자의 편의 증대를 위해 운전자의 키 팍(key fob)과 차량이 통신함으로써 운전자가 키 팍을 직접 동작하지 않고 차량에서 키 팍의 근접성을 확인하여 차량 문(door)의 개폐 및/또는 시동을 켤 수 있도록 하는 시스템이다. PKES 시스템에서 차량과 스마트 키(smart key)는 서로 통신하기 위해 두 가지 주파수 채널 신호를 사용한다. 차량은 도달 거리가 2 내지 3 미터로 짧은 LF(Low Frequency) 신호를 사용하며 키 팍은 먼 거리에서 차량을 제어하기 위해 도달 거리가 20 내지 50 미터인 UHF(Ultra High Frequency) 신호를 사용한다.

[0003] 우선, 차량은 주기적으로 LF 신호(키 팍의 존재 확인 및/또는 웨이크업(wake up) 신호)를 차량 주위로 송신하며, 이를 수신한 키 팍은 웨이크업되면서 수신된 LF 신호에 대한 응답 신호로 UHF 신호(존재 확인 신호)를 차량으로 송신한다. 키 팍의 존재가 확인된 경우, 차량은 질의(Challenge) 정보가 포함된 LF 신호를 다시 키 팍에게 전송하고, 키 팍은 질의에 대응하는 응답(Response) 정보가 포함된 UHF 신호를 차량으로 송신한다. 수신한 응답 정보가 정상적으로 확인된 경우, 차량은 차량 제어(문의 개폐, 시동 등)를 수행한다.

[0004] 이러한 PKES 시스템에서 공격자는 릴레이 공격을 수행할 수 있다. 릴레이 공격은 차량과 운전자의 키 팍 사이에서 두 개의 신호 중계기를 이용하여 차량과 키 팍에서 송신되는 신호를 각각 증폭하여 정상 거리 보다 먼 거리에 있는 차량과 키 팍이 서로 근접되어 있다고 판단하게 하여 정상 과정과 동일하게 차량 제어(문의 개폐, 시동 등)를 수행하는 공격을 의미한다. 차량은 키 팍에서 송신한 질의에 대응하는 응답 신호가 실제 정당한 키 팍이 전송한 신호인지 파악할 수 없기 때문에 이러한 공격이 가능하다.

선행기술문헌

특허문헌

[0005] (특허문헌 0001) 대한민국 공개특허 제10-2016-0149500호

(특허문헌 0002) 대한민국 등록특허 제10-1562124호

발명의 내용

해결하려는 과제

[0006] 본 발명이 이루고자 하는 기술적인 과제는 키 팝의 이동 거리 정보와 차량에서 수신한 신호를 바탕으로 측정된 이동 거리 정보를 비교함으로써 릴레이 공격을 방지하는 방법 및 시스템을 제공하는 것이다.

과제의 해결 수단

[0007] 본 발명의 실시예에 따른 릴레이 공격 탐지 방법은 차량이 제1 메시지를 스마트 키로 송신하는 단계, 상기 제1 메시지에 응답하여, 상기 스마트 키가 제1 응답 메시지를 상기 차량으로 송신하는 단계, 상기 차량이 상기 제1 응답 메시지에 기초하여 상기 차량과 상기 스마트 키 사이의 제1 거리를 산출하는 단계, 상기 차량이 질의값을 포함하는 제2 메시지를 상기 스마트 키로 송신하는 단계, 상기 제2 메시지에 응답하여, 상기 스마트 키가 상기 스마트 키의 이동 거리 또는 상기 이동 거리를 산출하기 위한 정보와 상기 질의값에 대응하는 응답값을 포함하는 제2 응답 메시지를 상기 차량으로 송신하는 단계, 상기 응답값에 기초하여, 상기 차량이 상기 스마트 키가 정당한 키인지 여부를 결정하는 단계, 상기 스마트 키가 정당한 키로 결정되는 경우, 상기 차량이 상기 제2 응답 메시지에 기초하여 상기 차량과 상기 스마트 키 사이의 제2 거리를 산출하는 단계, 및 상기 이동 거리를 산출하기 위한 정보를 이용하여 산출된 이동 거리 또는 제2 응답 메시지에 포함된 상기 이동 거리 및 상기 제1 거리와 상기 제2 거리의 차이를 이용하여 산출된 이동 거리를 비교하여 릴레이 공격 여부를 결정하는 단계를 포함한다.

[0008] 본 발명의 다른 실시예에 따른 릴레이 공격 탐지 방법은 차량이 웨이크업(wake up) 메시지를 LF(Low frequency) 대역을 이용하여 스마트 키로 송신하는 단계, 상기 웨이크업 메시지에 응답하여, 상기 스마트 키가 존재 확인 메시지를 UHF(Ultra High Frequency) 대역을 이용하여 상기 차량으로 송신하는 단계, 상기 차량이 상기 존재 확인 메시지의 RSSI를 이용하여 상기 차량과 상기 스마트 키 사이의 제1 거리를 산출하는 단계, 상기 차량이 질의 메시지(challenge message)를 상기 LF 대역을 이용하여 상기 스마트 키로 송신하는 단계, 상기 질의 메시지에 응답하여, 상기 스마트 키가 상기 스마트 키의 이동 거리를 포함하는 응답 메시지(response message)를 상기 UHF 대역을 이용하여 상기 차량으로 송신하는 단계, 상기 차량이 상기 응답 메시지의 RSSI를 이용하여 상기 차량과 상기 스마트 키 사이의 제2 거리를 산출하는 단계, 및 상기 차량이 상기 제1 거리와 상기 제2 거리의 차이를 이용하여 산출된 이동 거리와 상기 응답 메시지에 포함된 상기 이동 거리를 비교하여 릴레이 공격 여부를 결정하는 단계를 포함한다.

발명의 효과

[0009] 본 발명의 실시 예에 따른 키 팝의 이동 거리 산출은 통한 릴레이 공격 방지 방법에 의할 경우, 악의적인 사용자에게 의한 릴레이 공격을 방지할 수 있다.

[0010] 또한, 이를 통해 운전자의 차량 도난 사고 및 차량 내부의 물품 도난을 예방하고 운전자에게 편의를 제공하는 안전한 PKES 시스템을 구축할 수 있다.

도면의 간단한 설명

[0011] 본 발명의 상세한 설명에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 상세한 설명이 제공된다.

도 1은 본 발명의 일 실시예에 따른 PKES 시스템을 도시한다.

도 2는 도 1에 도시된 차량에서 수행되는 릴레이 공격 탐지 방법을 설명하기 위한 흐름도이다.

도 3은 도 1에 도시된 스마트 키에서 수행되는 릴레이 공격 탐지 방법을 설명하기 위한 흐름도이다.

도 4는 도 1에 도시된 차량의 기능 블록도이다.

도 5는 도 1에 도시된 스마트 키의 기능 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0012] 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.

[0013] 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.

- [0014] 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.
- [0015] 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.
- [0016] 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.
- [0017] 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.
- [0018] 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.
- [0020] 도 1은 본 발명의 일 실시예에 따른 PKES 시스템을 도시하고, 도 2는 도 1에 도시된 차량에서 수행되는 릴레이 공격 탐지 방법을 설명하기 위한 흐름도이고, 도 3은 도 1에 도시된 스마트 키에서 수행되는 릴레이 공격 탐지 방법을 설명하기 위한 흐름도이다.
- [0021] 도 1 내지 도 3을 참조하면, PKES 시스템은 차량과 스마트 키(smart key, 키 팍(key fob)이라 명명될 수도 있음)를 포함한다. 차량과 스마트 키는 미리 정해진 주파수 대역을 이용하여 서로 통신할 수 있다. 즉, 차량은 제1 주파수 대역의 신호를 스마트 키로 송신하고, 스마트 키는 제2 주파수 대역의 신호를 차량으로 송신할 수 있다. 제1 주파수 대역과 제2 주파수 대역은 서로 상이하거나, 동일하거나, 또는 일부 대역이 서로 중첩될 수도 있다. 예컨대, 차량은 도달 거리가 2 내지 3 미터로 짧은 LF(Low Frequency) 신호를 통해 소정의 정보를 스마트 키로 송신하고, 스마트 키는 도달 거리가 20 내지 50 미터인 UHF(Ultra High Frequency) 신호를 통해 소정의 정보를 차량으로 송신할 수 있다.
- [0022] PKES 시스템 상에서의 차량과 스마트 키는 다음과 같은 동작을 통해 정당한 스마트 키(또는 정당한 운전자)를 인증하고 차량 및/또는 스마트 키를 대상으로 하는 릴레이 공격을 탐지할 수 있다.
- [0023] 우선, 차량은 제1 신호(제1 메시지, 웨이크업 신호, 또는 웨이크업 메시지 등으로 명명될 수도 있음)를 스마트 키로 송신한다. 제1 신호는 제1 주파수 대역의 신호일 수 있으며, 스마트 키의 존재 확인 및/또는 웨이크업 신호를 의미할 수 있다. 또한, 제1 신호는 주기적으로 또는 비주기적으로 송신될 수 있다.
- [0024] 제1 신호의 도달 거리 내에 스마트 키가 존재하는 경우, 스마트 키는 제1 신호를 수신하고 제1 신호에 대응하는 제1 응답 신호(제1 응답 메시지, ACK 신호, ACK 메시지, 존재 확인 신호, 또는 존재 확인 메시지 등으로 명명될 수도 있음)를 차량으로 송신한다. 제1 응답 신호는 제2 주파수 대역의 신호일 수 있으며, 제1 신호의 도달 거리 내에 스마트 키가 존재함을 알리는 존재 확인 신호를 의미할 수 있다. 또한, 스마트 키는 제1 신호를 수신한 시

점 또는 제1 응답 신호를 송신한 시점(t_1)에서 스마트 키의 위치 정보(예컨대, 스마트 키의 좌표) 및/또는 가속도 정보(예컨대, 스마트 키의 가속도)를 스마트 키 내에 저장할 수 있다. 이를 위해, 스마트 키는 위치 정보 산출을 위한 GPS 수신기 및/또는 가속도 정보 산출을 위한 가속도 센서를 포함할 수 있다. 실시예에 따라, t_1 은 제1 신호가 수신된 시점을 의미하거나 제1 신호가 수신된 시점과 제1 응답 신호가 송신된 시점 사이의 임의의 시점을 의미할 수도 있다. 일 예로, t_1 시점은 제1 신호의 수신 시점으로부터 미리 정해진 시간이 경과한 시점을 의미하거나 제1 응답 신호가 송신되는 시점으로부터 미리 정해진 시간이 앞선 시점을 의미할 수 있다.

[0025] 스마트 키로부터 제1 응답 신호를 수신한 차량은 제1 응답 신호의 RSSI(Received Signal Strength Indication, 수신 신호 강도)를 이용하여 t_1 시점(예컨대, 스마트 키가 제1 신호를 송신한 시점)에서 차량과 스마트 키의 거리(d_1)를 계산할 수 있다. RSSI로부터 거리를 계산하는 방법은 널리 알려져 있으므로 이에 관한 구체적인 설명은 생략하기로 한다.

[0026] 또한, 차량은 제2 신호(제2 메시지, 질의 신호, 또는 질의 메시지 등으로 명명될 수도 있음)를 스마트 키로 송신한다. 제2 신호는 제1 주파수 대역의 신호일 수 있으며, 정당한 스마트 키인지 여부를 확인하기 위한 질의값 및/또는 차량의 식별 정보(예컨대, 차량의 ID)를 포함할 수도 있다.

[0027] 제2 신호를 수신한 스마트 키는 제2 응답 신호(제2 응답 메시지 등으로 명명될 수도 있음)를 차량으로 송신할 수 있다. 제2 신호는 제2 주파수 대역의 신호일 수 있다. 제2 신호에는 차량으로부터 수신된 질의값에 대한 응답값 및/또는 스마트 키의 이동 거리에 관한 정보 또는 이동 거리를 산출할 수 있는 정보를 포함할 수 있다.

[0028] 구체적으로, 스마트 키는 제2 신호를 수신한 시점, 제2 응답 신호를 송신한 시점, 또는 제2 신호를 수신한 시점과 제2 응답 신호를 송신한 시점 사이의 임의의 시점인 t_2 에서의 위치 정보 및/또는 가속도 정보를 측정 및/또는 저장할 수 있다. 일 예로, t_2 시점은 제2 신호를 수신한 시점으로부터 미리 정해진 시간이 경과한 시점을 의미하거나 제2 응답 신호를 송신한 시점으로부터 미리 정해진 시간이 앞선 시점을 의미할 수도 있다.

[0029] 또한, 스마트 키는 t_1 시점의 가속도와 t_2 시점의 가속도를 이용하여 스마트 키(또는 스마트 키를 소지하고 있는 운전자)의 이동 거리를 산출할 수 있다. 이를 위해 스마트 키는 가속도 정보를 두 번 적분하여 스마트 키의 이동 거리(dk)를 산출할 수 있다. 예컨대, 스마트 키는 t_1 시점의 가속도와 t_2 시점의 가속도를 이용하여 스마트 키의 가속도에 관한 1차 함수를 생성한 후, t_1 시점과 t_2 시점에서 두 번의 적분을 통해 스마트 키의 이동 거리를 산출할 수 있다. 실시예에 따라, 스마트 키는 t_1 시점과 t_2 시점 사이의 적어도 하나의 시점 t_3 에서의 가속도를 측정하고 스마트 키의 가속도에 관한 n (n 은 자연수)차 함수를 생성한 후, t_1 시점과 t_2 시점에서 두 번의 적분을 통해 스마트 키의 이동 거리를 산출할 수도 있다. 일 예로, 생성되는 함수의 차수 n 은 시점 t_3 의 개수에 '1'을 더한 값을 가질 수 있다.

[0030] 스마트 키에 GPS 수신기가 구비된 경우, 스마트 키는 t_1 시점에서의 위치와 t_2 시점에서의 위치에 기초하여 스마트 키의 이동 거리를 산출할 수도 있다.

[0031] 또한, 스마트 키의 이동 거리는 차량과 스마트 키 간에 미리 공유된 대칭키를 이용하여 암호화된 후에 제2 응답 신호에 포함되어 전송될 수도 있다.

[0032] 또 다른 실시예에 따르면, 스마트 키는 이동 거리를 산출할 수 있는 정보를 제2 응답 신호에 포함시켜 전송할 수도 있다. 이동 거리를 산출할 수 있는 정보는 t_1 시점과 t_2 시점에서의 가속도 정보를 포함하며, t_1 시점과 t_2 시점 사이의 적어도 하나의 t_3 시점에서의 가속도 정보를 포함할 수도 있다. 이 경우, 차량은 스마트 키가 이동 거리를 산출한 과정과 동일한 과정을 거쳐 스마트 키의 이동 거리를 산출할 수 있다. 또한, 스마트 키에 GPS 수신기가 구비된 경우, 스마트 키는 t_1 시점과 t_2 시점에서의 위치 정보를 제2 응답 신호에 포함시켜 전송할 수도 있다. 또한, 이동 거리를 산출할 수 있는 정보는 마찬가지로 대칭키를 이용하여 암호화된 후 제2 응답 신호에 포함될 수도 있다.

[0033] 스마트 키로부터 수신된 제2 응답 신호에 포함된 응답값이 질의값에 대응되는 값인 경우, 차량은 제2 응답 신호 및/또는 제1 응답 신호를 송신한 스마트 키가 정당한 키로 결정하고 릴레이 공격 여부를 판단한다. 응답값이 질의값에 대응되지 않는 경우, 차량은 프로토콜의 진행을 중단할 수 있다.

[0034] 정당한 스마트 키로 판단된 후 릴레이 공격을 탐지하기 위해, 차량은 제2 응답 신호에 포함된 이동 거리(dk)를 복호화한다. 물론, 이동 거리(dk)가 암호화되어 있지 않은 경우, 이 동작은 생략될 수 있다.

[0035] 또한, 차량은 제1 응답 신호의 RSSI로부터 t_1 시점의 스마트 키와의 거리(d_1)를 산출하고 제2 응답 신호의 RSSI로부터 t_2 시점의 스마트 키와의 거리(d_2)를 산출한다. 이후, d_1 과 d_2 의 차이를 이용하여 t_1 시점과 t_2 시점 동

안에 스마트 키가 이동한 거리(dv)를 산출한다.

- [0036] 차량은 스마트 키로부터 수신된 이동 거리(dk)와 산출된 이동 거리(dv)의 차이가 미리 정해진 임계값(δ) 이하 인지 여부에 따라 릴레이 공격의 유무를 결정한다. 즉, 이동 거리의 차이가 임계값 이하인 경우, 릴레이 공격이 가해지지 않은 것으로 판단할 수 있고, 이 경우 지속적인 차량의 제어(문의 개폐, 시동 등)가 가능하다. 이동 거리의 차이가 임계값을 초과하는 경우, 릴레이 공격이 가해진 것으로 판단할 수 있고, 이 경우 지속적인 차량의 제어를 수행하지 않을 수 있다. 물론, 차량으로부터 이동 거리를 산출할 수 있는 정보를 수신한 경우에는 스마트 키의 동작과 동일한 동작을 거쳐 스마트 키의 이동 거리(dk)를 산출할 수 있다.
- [0037] 도 4는 도 1에 도시된 차량의 기능 블록도이다.
- [0038] 도 4를 참조하면, 차량(100)은 통신부(110), 인증부(120), 공격 탐지부(130), 제어부(140), 저장부(150), 및 차량 제어부(160) 중 적어도 하나 이상을 포함하도록 구현될 수 있다.
- [0039] 통신부(110)는 제어부(140)의 제어 하에, 신호 또는 메시지를 송신하고 이에 대응하는 신호 또는 메시지를 수신할 수 있다. 즉, 통신부(110)는 제1 주파수 대역의 신호를 송신하고 제2 주파수 대역의 신호를 수신할 수 있다. 구체적으로, 통신부(110)는 제1 주파수 대역의 제1 신호를 송신하고, 제1 신호에 대응하는 제2 주파수 대역의 제1 응답 신호를 수신할 수 있다. 또한, 통신부(110)는 제1 주파수 대역의 제2 신호를 송신하고, 제2 신호에 대응하는 제2 주파수 대역의 제2 응답 신호를 수신할 수 있다. 통신부(110)에 의해 송수신 되는 신호 또는 메시지는 저장부(150)에 저장될 수 있다. 실시예에 따라, 통신부(110)는 제1 응답 신호와 제2 응답 신호의 RSSI를 측정하고 측정된 RSSI를 저장부(150)에 저장할 수 있다.
- [0040] 인증부(120)는 제어부(140)의 제어 하에, 통신부(110)에 의해 수신된 제2 응답 신호 또는 저장부(150)에 저장된 제2 응답 신호에 기초하여 스마트 키에 대한 인증 동작을 수행함으로써 정당한 스마트 키 여부를 결정할 수 있다. 구체적으로, 제2 응답 신호에 포함된 응답값이 제2 신호에 포함된 질의값에 대응하는 경우, 인증부(120)는 제1 응답 신호 및/또는 제2 응답 신호를 송신한 스마트 키를 정당한 스마트 키로 판단할 수 있다.
- [0041] 공격 탐지부(130)는 제어부(140)의 제어 하에, 릴레이 공격 여부를 탐지할 수 있다. 즉, 인증부(120)에 의한 인증 동작이 성공적으로 수행된 경우, 제어부는 공격 탐지부(130)로 하여금 릴레이 공격 유무를 탐지하도록 제어할 수 있다. 구체적으로, 공격 탐지부(130)는 제1 응답 메시지의 RSSI로부터 t_1 시점에서 차량과 스마트 키 간의 거리(d_1)를 산출하고, 제2 응답 메시지의 RSSI로부터 t_2 시점에서 차량과 스마트 키 간의 거리(d_2)를 산출할 수 있다. 결국, 공격 탐지부(130)는 t_1 시점에서의 거리(d_1)와 t_2 시점에서의 거리(d_2)의 차이를 이용하여 스마트 키의 이동 거리(dv)를 산출할 수 있다. 또한, 공격 탐지부(130)는 제2 응답 신호에 포함된 이동 거리(dk)와 산출된 이동 거리(dv)의 차이가 임계값 이내에 분포하는 경우 릴레이 공격이 행해지지 않은 것으로 판단하고, 임계값을 초과하는 경우 릴레이 공격이 진행된 것으로 판단할 수 있다. 물론, 이동 거리(dk)가 암호화된 경우, 스마트 키와 미리 공유된 대칭키를 이용하여 복호화한 후 릴레이 공격 유무를 판단할 수 있다.
- [0042] 실시예에 따라, 제2 응답 신호에는 이동 거리를 산출할 수 있는 정보가 포함될 수 있다. 이 경우, 공격 탐지부(130)는 스마트 키의 동작과 동일한 동작을 수행함으로써 스마트 키의 이동 거리(dk)를 산출할 수 있다.
- [0043] 제어부(140)는 차량(100)의 전체적인 동작을 제어할 수 있다. 구체적으로, 제어부(140)는 인증부(120), 공격 탐지부(130), 저장부(150), 및 차량 제어부(160) 중 적어도 하나의 동작을 제어할 수 있다.
- [0044] 저장부(150)에는 통신부(110)에 의해 송수신되는 신호 또는 메시지(즉, 제1 신호, 제1 응답 신호, 제2 신호, 제2 응답 신호), 인증부(120)에 의한 인증 동작의 결과, 공격 탐지부(130)에 의한 공격 탐지 결과, 산출된 거리(d_1 , d_2), 산출된 이동 거리(dk, dv), 대칭키 등이 저장될 수 있다.
- [0045] 차량 제어부(160)는 제어부(140)의 제어 하에, 차량의 제어 동작(문의 개폐, 시동 등)을 위한 제어 신호를 생성하고, 이를 차량의 내부 네트워크를 통해 송신함으로써 이에 따른 차량의 제어 동작이 수행되도록 동작할 수 있다. 이때, 차량 제어부(160)에 의한 제어 신호의 생성은 스마트 키에 대한 인증이 완료되고 릴레이 공격이 수행되지 않았다고 판단되는 경우에 수행될 수 있고, 이러한 차량 제어부(160)의 제어는 제어부(140)에 의해 수행될 수 있다.
- [0046] 도 5는 도 1에 도시된 스마트 키의 기능 블록도이다.
- [0047] 도 5를 참조하면, 스마트 키(300)는 통신부(310), 가속도 센서부(320), 이동 거리 산출부(330), 제어부(340), 및 저장부(350) 중 적어도 하나를 포함하도록 구현될 수 있다.

- [0048] 통신부(310) 제어부(340)의 제어 하에, 신호 또는 메시지를 수신하고 이에 대응하는 신호 또는 메시지를 송신할 수 있다. 즉, 통신부(310)는 제1 주파수 대역의 신호를 수신하고 제2 주파수 대역의 신호를 송신할 수 있다. 구체적으로, 통신부(310)는 제1 주파수 대역의 제1 신호를 수신하고, 제1 신호에 대응하는 제2 주파수 대역의 제1 응답 신호를 송신할 수 있다. 또한, 통신부(310)는 제1 주파수 대역의 제2 신호를 수신하고, 제2 신호에 대응하는 제2 주파수 대역의 제2 응답 신호를 송신할 수 있다. 통신부(310)에 의해 송수신 되는 신호 또는 메시지는 저장부(350)에 저장될 수 있다.
- [0049] 가속도 센서부(320)는 제어부(340)의 제어 하에, 각 시점(예컨대, t1 및/또는 t2)에서의 가속도를 측정하고, 측정된 가속도는 저장부(350)에 저장될 수 있다. 실시예에 따라, 가속도 센서부(320)는 t1 시점과 t2 시점 사이의 적어도 하나의 시점(t3)에서의 가속도를 측정하고, 측정된 가속도를 저장부(350)에 저장할 수도 있다. 또한, 스마트 키(300)에는 가속도 센서부(320)과는 무관하게(즉, 가속도 센서부와 GPS 수신부는 적어도 하나만이 구현될 수 있음) GPS 수신부가 구비될 수 있는데, 이 경우 GPS 수신부는 각 시점에서 GPS 신호에 기초하여 각 시점에서의 위치 정보를 산출하고, 산출된 위치 정보를 저장부(350)에 저장할 수 있다.
- [0050] 이동 거리 산출부(330)는 가속도 센서부(320)에 의해 측정된 가속도 정보 및/또는 GPS 수신부에 의해 산출된 위치 정보를 이용하여 t1 시점과 t2 시점 사이에 스마트 키(300)가 이동한 이동 거리를 산출할 수 있다. 이에 대한 동작은 앞선 기재와 중복되므로 생략하기로 한다. 실시예에 따라, 이동 거리는 차량(100)에 의해 산출될 수도 있는 데, 이 경우 이동 거리 산출부(330)는 생략될 수도 있다.
- [0051] 제어부(340)는 스마트 키(300)의 구성, 즉 통신부(310), 가속도 센서부(320), GPS 수신부, 이동 거리 산출부(330), 및 저장부(350) 중 적어도 하나의 동작을 제어할 수 있다.
- [0052] 저장부(350)에는 통신부(310)에 의해 송수신되는 신호 또는 메시지(즉, 제1 신호, 제1 응답 신호, 제2 신호, 제2 응답 신호), 송수신되는 신호 또는 메시지의 송수신 시간, 가속도 센서부(320)에 의해 측정된 각 시점에서의 가속도, GPS 수신부에 의해 수신된 각 시점에서의 위치 정보, 이동 거리 산출부(330)에 의해 산출된 이동 거리(dv), 대칭키 등이 저장될 수 있다.
- [0053] 도 4와 도 5에 도시된 차량(100)과 스마트 키(300)의 구성들 각각은 기능 및 논리적으로 분리될 수 있음으로 나타내는 것이며, 반드시 각각의 구성이 별도의 물리적 장치로 구분되거나 별도의 코드로 작성됨을 의미하는 것이 아님을 본 발명의 기술분야의 평균적 전문가가 용이하게 추론할 수 있을 것이다.
- [0054] 또한, 본 명세서에서 '~부'라 함은, 본 발명의 기술적 사상을 수행하기 위한 하드웨어 및 상기 하드웨어를 구동하기 위한 소프트웨어의 기능적, 구조적 결합을 의미할 수 있다. 예컨대, 상기 모듈은 소정의 코드와 상기 소정의 코드가 수행되기 위한 하드웨어 리소스의 논리적인 단위를 의미할 수 있으며, 반드시 물리적으로 연결된 코드를 의미하거나, 한 종류의 하드웨어를 의미하는 것이 아니다.
- [0055] 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.
- [0056] 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.

[0057] 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.

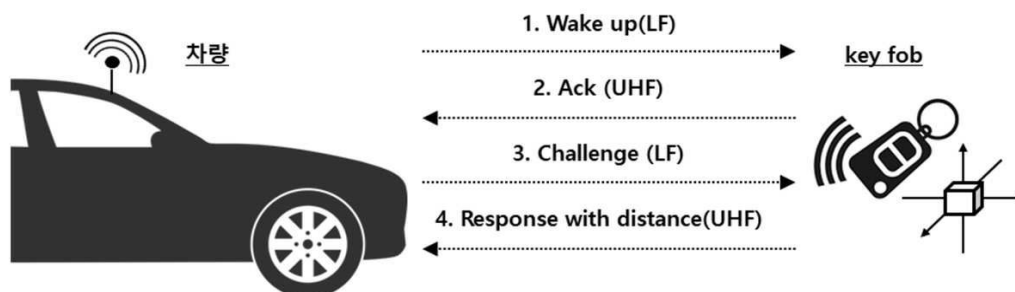
[0058] 본 발명은 도면에 도시된 실시 예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시 예가 가능하다는 점을 이해할 것이다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성 요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성 요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

부호의 설명

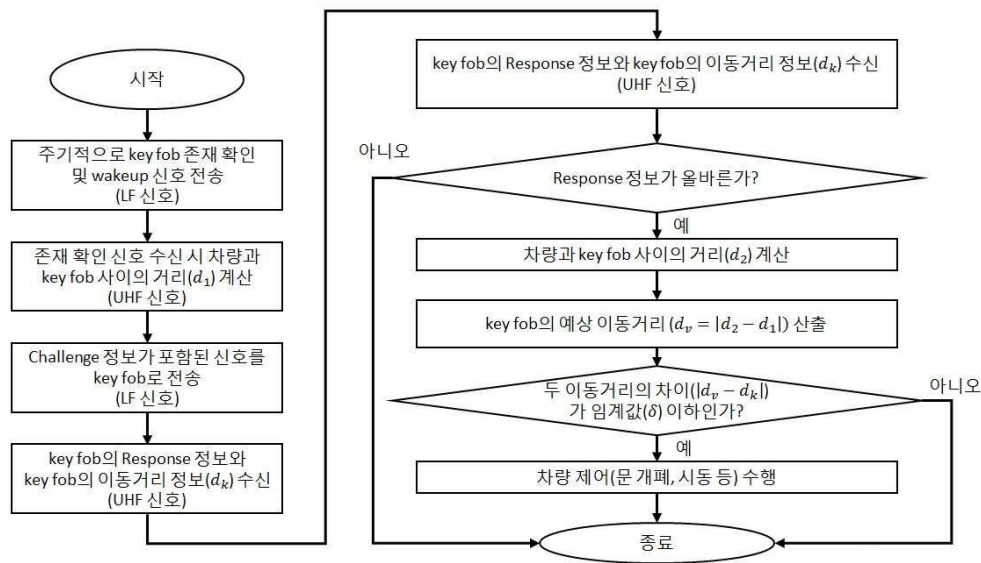
[0059] 100 : 차량 110 : 통신부
120 : 인증부 130 : 공격 탐지부
140 : 제어부 150 : 저장부
160 : 차량 제어부 300 : 스마트 키
310 : 통신부 320 : 가속도 센서부
330 : 이동 거리 산출부 340 : 제어부
350 : 저장부

도면

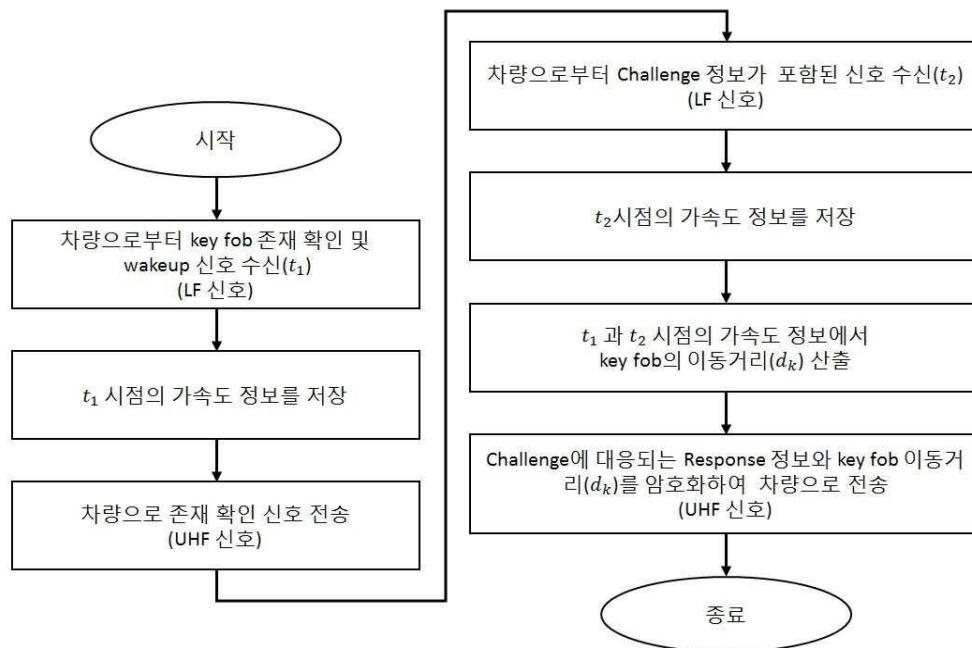
도면1



도면2

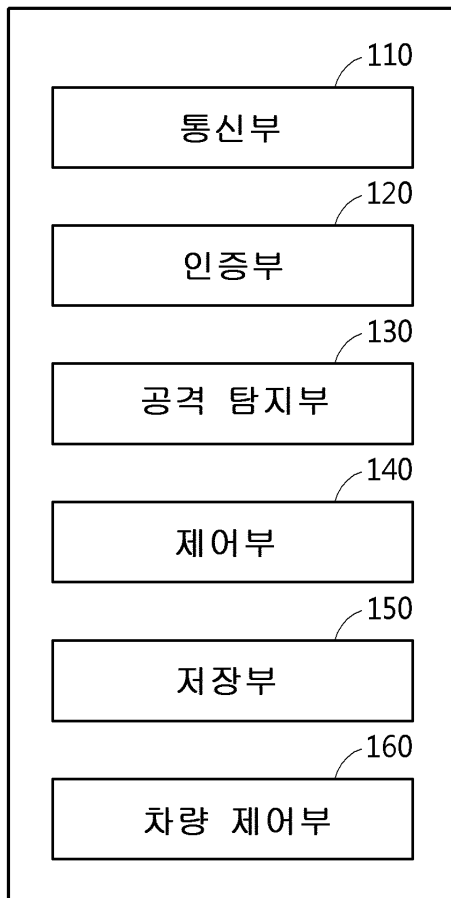


도면3



도면4

100



도면5

