



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2019-0090446
(43) 공개일자 2019년08월02일

(51) 국제특허분류(Int. Cl.)
B60R 25/24 (2013.01) B60R 25/10 (2006.01)
(52) CPC특허분류
B60R 25/246 (2013.01)
B60R 25/10 (2013.01)
(21) 출원번호 10-2018-0009106
(22) 출원일자 2018년01월25일
심사청구일자 2018년01월25일

(71) 출원인
서강대학교산학협력단
서울특별시 마포구 백범로 35 (신수동, 서강대학교)
(72) 발명자
소재우
서울특별시 마포구 백범로 35, R관 709호
정혜라
서울특별시 마포구 백범로 35, R관 709호
(74) 대리인
특허법인충현

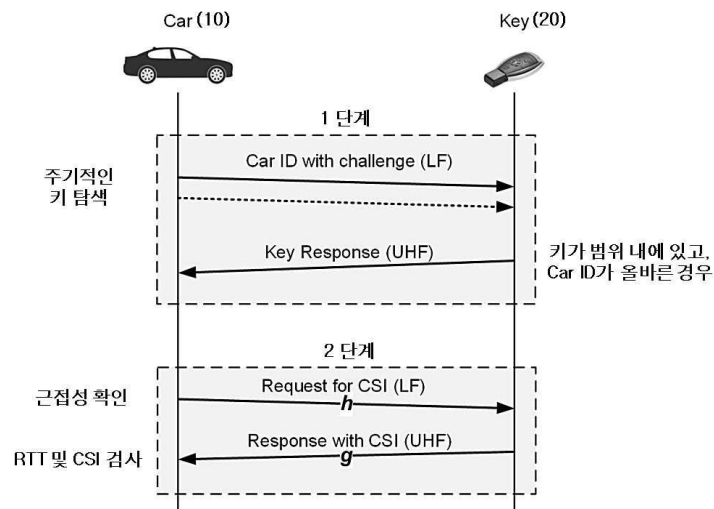
전체 청구항 수 : 총 20 항

(54) 발명의 명칭 스마트 키 시스템에서 채널 상태 정보에 기반하여 자동차와 키의 근접성을 인증하는 방법

(57) 요약

본 발명은 스마트 키 시스템에서 자동차와 키의 근접성을 인증하는 기술에 관한 것으로, 자동차가 키와 챌린지-응답(Challenge-Response) 과정을 통해 키를 확인하고, 자동차와 키 사이에 형성된 양방향 채널로부터 송신단과 수신단 사이의 채널 특징을 나타내는 복수 개의 채널 상태 정보를 획득하고, 양방향 채널 상태 정보의 상관관계 값을 산출하며, 산출된 상관관계 값이 임계치보다 큰 경우 자동차와 키가 유효 범위 내에 근접하였다고 판단한다.

대표도 - 도4



(52) CPC특허분류
B60R 25/241 (2013.01)

명세서

청구범위

청구항 1

자동차 스마트 키 시스템에서 자동차와 키의 근접성을 인증하는 방법에 있어서,

- (a) 자동차가 키와 챌린지-응답(Challenge-Response) 과정을 통해 상기 키를 확인하는 단계;
- (b) 상기 자동차가 상기 자동차와 상기 키 사이에 형성된 양방향 채널로부터 송신단과 수신단 사이의 채널 특징을 나타내는 복수 개의 채널 상태 정보를 획득하는 단계;
- (c) 상기 자동차가 연속하여 획득한 제 1 양방향 채널 상태 정보와 제 2 양방향 채널 상태 정보 사이의 상관관계 값을 산출하는 단계; 및
- (d) 산출된 상기 상관관계 값이 임계치보다 큰 경우, 상기 자동차는 상기 자동차와 상기 키가 유효 범위 내에 근접하였다고 판단하는 단계를 포함하는 자동차 스마트 키 시스템의 근접성 인증 방법.

청구항 2

제 1 항에 있어서,

상기 (b) 단계는,

- (b1) 상기 자동차가 채널 상태 정보 요청 메시지를 전송하는 단계; 및
- (b2) 상기 자동차가 상기 채널 상태 정보 요청 메시지에 대응하는 채널 상태 정보 응답 메시지를 수신하는 단계를 포함하는 자동차 스마트 키 시스템의 근접성 인증 방법.

청구항 3

제 2 항에 있어서,

상기 (b2) 단계에서,

상기 채널 상태 정보 응답 메시지는 수신 채널의 채널 상태 정보를 포함하는 것을 특징으로 하는 자동차 스마트 키 시스템의 근접성 인증 방법.

청구항 4

제 2 항에 있어서,

상기 (b) 단계는,

- (b3) 상기 자동차가 상기 채널 상태 정보 응답 메시지의 프리앰블(preamble) 정보를 사용하여 수신 채널의 채널 상태 정보를 산출하는 단계를 더 포함하는 자동차 스마트 키 시스템의 근접성 인증 방법.

청구항 5

제 1 항에 있어서,

상기 (c) 단계는,

상기 자동차가 연속하여 획득한 양방향 채널 정보로부터 채널별로 각각 공분산을 이용하여 상관관계 값을 산출하는 것을 특징으로 하는 자동차 스마트 키 시스템의 근접성 인증 방법.

청구항 6

제 1 항에 있어서,

상기 채널 상태 정보는,

스캐터링(scattering), 페이딩(fading), 신호 지연, 신호 위상 및 신호 세기 감쇄 중 적어도 하나를 포함하는 것을 특징으로 하는 자동차 스마트 키 시스템의 근접성 인증 방법.

청구항 7

자동차 스마트 키 시스템에서 자동차와 키의 근접성을 인증하는 방법에 있어서,

- (a) 키가 자동차와 키 간의 챌린지-응답(Challenge-Response) 과정을 통해 상기 자동차로 하여금 상기 키를 확인시키는 단계;
- (b) 상기 키가 상기 자동차와 상기 키 사이에 형성된 양방향 채널을 통해 채널 상태 정보 요청 메시지를 수신하는 단계; 및
- (c) 상기 키가 채널 상태 정보 요청에 대응하여 수신 채널의 채널 상태 정보를 포함하는 응답 메시지를 전송하는 단계를 포함하되,

상기 키는, 상기 자동차로 하여금 연속하여 획득한 제 1 양방향 채널 상태 정보와 제 2 양방향 채널 상태 정보 사이의 상관관계 값을 산출하되, 산출된 상기 상관관계 값이 임계치보다 큰 경우 상기 자동차와 상기 키가 유효 범위 내에 근접하였다고 판단하도록 유도하는 것을 특징으로 하는 자동차 스마트 키 시스템의 근접성 인증 방법.

청구항 8

제 7 항에 있어서,

상기 (c) 단계는,

- (c1) 상기 키가 상기 채널 상태 정보 요청 메시지의 프리앰블(preamble) 정보를 사용하여 수신 채널의 채널 상태 정보를 산출하는 단계; 및
- (c2) 상기 키가 산출된 상기 수신 채널의 채널 상태 정보를 포함하는 채널 상태 정보 응답 메시지를 상기 자동차에 전송하는 단계를 포함하는 자동차 스마트 키 시스템의 근접성 인증 방법.

청구항 9

제 7 항에 있어서,

상기 키가,

상기 (a) 단계의 챌린지-응답 과정에서 키 응답 메시지를 전송한 후, 상기 (b) 단계의 채널 상태 정보 요청 메시지를 상기 자동차로부터 수신하기 위해 연속적으로 대기함으로써, 상기 (c) 단계에서 고정된 처리 시간에 따라 상기 수신 채널의 채널 상태 정보를 포함하는 응답 메시지를 전송하는 것을 특징으로 하는 것을 특징으로 하는 자동차 스마트 키 시스템의 근접성 인증 방법.

청구항 10

자동차 스마트 키 시스템에서 자동차와 키의 근접성을 인증하는 방법에 있어서,

- (a) 자동차가 키와 챌린지-응답(Challenge-Response) 과정을 통해 상기 키를 확인하는 단계;
- (b) 상기 자동차가 상기 자동차와 상기 키 사이에 형성된 양방향 채널로부터 송신단과 수신단 사이의 채널 특성을 나타내는 채널 상태 정보를 획득하는 단계;
- (c) 상기 자동차가 획득한 채널 상태 정보로부터 메시지의 왕복 시간을 산출하는 단계; 및
- (d) 산출된 상기 왕복 시간의 차이가 임계치보다 작은 경우, 상기 자동차는 상기 자동차와 상기 키가 유효 범위 내에 근접하였다고 판단하는 단계를 포함하는 자동차 스마트 키 시스템의 근접성 인증 방법.

청구항 11

제 10 항에 있어서,

상기 (b) 단계는,

- (b1) 상기 자동차가 채널 상태 정보 요청 메시지를 전송하는 단계; 및
- (b2) 상기 자동차가 상기 채널 상태 정보 요청 메시지에 대응하는 채널 상태 정보 응답 메시지를 수신하는 단계를 포함하는 자동차 스마트 키 시스템의 근접성 인증 방법.

청구항 12

제 11 항에 있어서,

상기 (b2) 단계에서,

상기 채널 상태 정보 응답 메시지는 수신 채널의 채널 상태 정보를 포함하는 것을 특징으로 하는 자동차 스마트 키 시스템의 근접성 인증 방법.

청구항 13

제 11 항에 있어서,

상기 (b) 단계는,

(b3) 상기 자동차가 상기 채널 상태 정보 응답 메시지의 프리앰블(preamble) 정보를 사용하여 수신 채널의 채널 상태 정보를 산출하는 단계를 더 포함하는 자동차 스마트 키 시스템의 근접성 인증 방법.

청구항 14

제 10 항에 있어서,

상기 (c) 단계는,

상기 자동차가 전송한 채널 상태 정보 요청 메시지와 상기 자동차가 수신한 채널 상태 정보 응답 메시지의 시간 차이로부터 상기 메시지의 왕복 시간을 산출하는 것을 특징으로 하는 자동차 스마트 키 시스템의 근접성 인증 방법.

청구항 15

제 10 항에 있어서,

상기 채널 상태 정보는,

스캐터링(scattering), 페이딩(fading), 신호 지연, 신호 위상 및 신호 세기 감쇄 중 적어도 하나를 포함하는 것을 특징으로 하는 자동차 스마트 키 시스템의 근접성 인증 방법.

청구항 16

자동차 스마트 키 시스템에서 자동차와 키의 근접성을 인증하는 방법에 있어서,

(a) 키가 자동차와 키 간의 챌린지-응답(Challenge-Response) 과정을 통해 상기 자동차로 하여금 상기 키를 확인시키는 단계;

(b) 상기 키가 상기 자동차와 상기 키 사이에 형성된 양방향 채널을 통해 채널 상태 정보 요청 메시지를 수신하는 단계; 및

(c) 상기 키가 채널 상태 정보 요청에 대응하여 수신 채널의 채널 상태 정보를 포함하는 응답 메시지를 전송하는 단계를 포함하되,

상기 키는, 상기 자동차로 하여금 채널 상태 정보로부터 메시지의 왕복 시간을 산출하되, 산출된 상기 왕복 시간의 차이가 임계치보다 작은 경우 상기 자동차와 상기 키가 유효 범위 내에 근접하였다고 판단하도록 유도하는 것을 특징으로 하는 자동차 스마트 키 시스템의 근접성 인증 방법.

청구항 17

제 16 항에 있어서,

상기 (c) 단계는,

(c1) 상기 키가 상기 채널 상태 정보 요청 메시지의 프리앰블(preamble) 정보를 사용하여 수신 채널의 채널 상태 정보를 산출하는 단계; 및

(c2) 상기 키가 산출된 상기 수신 채널의 채널 상태 정보를 포함하는 채널 상태 정보 응답 메시지를 상기 자동차에 전송하는 단계를 포함하는 자동차 스마트 키 시스템의 근접성 인증 방법.

청구항 18

제 16 항에 있어서,

상기 키가,

상기 (a) 단계의 챌린지-응답 과정에서 키 응답 메시지를 전송한 후, 상기 (b) 단계의 채널 상태 정보 요청 메시지를 상기 자동차로부터 수신하기 위해 연속적으로 대기함으로써, 상기 (c) 단계에서 고정된 처리 시간에 따라 상기 수신 채널의 채널 상태 정보를 포함하는 응답 메시지를 전송하는 것을 특징으로 하는 것을 특징으로 하는 자동차 스마트 키 시스템의 근접성 인증 방법.

청구항 19

자동차 스마트 키 시스템에서 자동차와 키의 근접성을 인증하는 방법에 있어서,

(a) 자동차가 키와 챌린지-응답(Challenge-Response) 과정을 통해 상기 키를 확인하는 단계;

(b) 상기 자동차가 상기 자동차와 상기 키 사이에 형성된 양방향 채널로부터 송신단과 수신단 사이의 채널 특징을 나타내는 복수 개의 채널 상태 정보를 획득하는 단계;

(c) 상기 자동차가 연속하여 획득한 제 1 양방향 채널 상태 정보와 제 2 양방향 채널 상태 정보 사이의 상관관계 값 및 메시지의 왕복 시간을 산출하는 단계; 및

(d) 산출된 상기 상관관계 값이 임계치보다 크고, 산출된 상기 왕복 시간의 차이가 임계치보다 작은 경우, 상기 자동차는 상기 자동차와 상기 키가 유효 범위 내에 근접하였다고 판단하는 단계를 포함하는 자동차 스마트 키 시스템의 근접성 인증 방법.

청구항 20

자동차 스마트 키 시스템에서 자동차와 키의 근접성을 인증하는 방법에 있어서,

(a) 키가 자동차와 키 간의 챌린지-응답(Challenge-Response) 과정을 통해 상기 자동차로 하여금 상기 키를 확인시키는 단계;

(b) 상기 키가 상기 자동차와 상기 키 사이에 형성된 양방향 채널을 통해 채널 상태 정보 요청 메시지를 수신하는 단계; 및

(c) 상기 키가 채널 상태 정보 요청에 대응하여 수신 채널의 채널 상태 정보를 포함하는 응답 메시지를 전송하는 단계를 포함하되,

상기 키는, 상기 자동차로 하여금 연속하여 획득한 제 1 양방향 채널 상태 정보와 제 2 양방향 채널 상태 정보 사이의 상관관계 값 및 메시지의 왕복 시간을 산출하되, 산출된 상기 상관관계 값이 임계치보다 크고, 산출된 상기 왕복 시간의 차이가 임계치보다 작은 경우, 상기 자동차와 상기 키가 유효 범위 내에 근접하였다고 판단하도록 유도하는 것을 특징으로 하는 자동차 스마트 키 시스템의 근접성 인증 방법.

발명의 설명

기술 분야

[0001] 본 발명은 스마트 키를 소지한 사용자가 자동차에 접근하여 차량의 문 잠금을 해제하거나 시동을 켤 수 있는 스마트 키 시스템에 관한 것으로, 특히 이러한 스마트 키 시스템에서 자동차와 키의 근접성을 인증함에 있어서 릴레이 공격을 방어할 수 있도록 보안이 강화된 근접성 인증 방법에 관한 것이다.

배경 기술

[0002] 최근 출시되는 차량들은 키의 근접성을 검사하여 자동으로 문을 열고 닫으며, 엔진의 시동을 켤 수 있는 PKES(Passive Keyless Entry and Start) 시스템을 채택하고 있다. 그러나 PKES 시스템은 이하에서 제시되는 선행기술문헌에서 지적인 바와 같이 릴레이 공격에 취약하다고 알려져 있다.

[0003] PKES 시스템에서 릴레이 공격에 대응하기 위한 많은 연구가 진행되었다. 대표적인 릴레이 공격 대응 방식은 RSS(Received Signal Strength) 기반 거리 추정 방식, 위상(Phase) 기반 거리 추정 방식, TOA(Time of Arrival) 또는 TOF(Time of Flight) 기반 거리 추정 방식 등이 있다. 그러나 이들 대응 방식을 고려하더라도 릴레이 공격자가 신호를 증폭하거나 아날로그 릴레이를 사용하는 경우 릴레이 공격을 대응하기 어렵다는 점이 약점으로 지적되었다.

선행기술문헌

비특허문헌

[0004] (비특허문헌 0001) A. I. Alrabady and S. M. Mahmud, "Analysis of attacks against the security of keyless-entry systems for vehicles and suggestions for improved designs," IEEE Trans. Veh. Tech., vol. 54, no. 1, pp. 41-50, 2005.

발명의 내용

해결하려는 과제

[0005] 본 발명이 해결하고자 하는 기술적 과제는, 종래의 PKES 시스템과 같은 자동차 스마트 키 시스템이 릴레이 공격에 취약하다는 약점을 극복하고, 공격자가 신호를 증폭하거나 아날로그 릴레이를 사용하는 경우에 쉽게 보안이 해제되는 문제를 해소하고자 한다.

과제의 해결 수단

[0006] 상기 기술적 과제를 해결하기 위하여, 본 발명의 일 실시예에 따른 자동차 스마트 키 시스템에서 자동차와 키의 근접성을 인증하는 방법은, 자동차가 키와 챌린지-응답(Challenge-Response) 과정을 통해 상기 키를 확인하는 단계; 상기 자동차가 상기 자동차와 상기 키 사이에 형성된 양방향 채널로부터 송신단과 수신단 사이의 채널 특성을 나타내는 복수 개의 채널 상태 정보를 획득하는 단계; 상기 자동차가 연속하여 획득한 제 1 양방향 채널 상태 정보와 제 2 양방향 채널 상태 정보 사이의 상관관계 값을 산출하는 단계; 및 산출된 상기 상관관계 값이 임계치보다 큰 경우, 상기 자동차는 상기 자동차와 상기 키가 유효 범위 내에 근접하였다고 판단하는 단계를 포함한다.

[0007] 일 실시예에 따른 자동차 스마트 키 시스템의 근접성 인증 방법에서, 상기 복수 개의 채널 상태 정보를 획득하는 단계는, 상기 자동차가 채널 상태 정보 요청 메시지를 전송하는 단계; 및 상기 자동차가 상기 채널 상태 정보 요청 메시지에 대응하는 채널 상태 정보 응답 메시지를 수신하는 단계를 포함한다. 또한, 상기 채널 상태 정보 응답 메시지를 수신하는 단계에서, 상기 채널 상태 정보 응답 메시지는 수신 채널의 채널 상태 정보를 포함할 수 있다. 나아가, 상기 복수 개의 채널 상태 정보를 획득하는 단계는, 상기 자동차가 상기 채널 상태 정보 응답 메시지의 프리앰블(preamble) 정보를 사용하여 수신 채널의 채널 상태 정보를 산출하는 단계를 더 포함할 수 있다.

[0008] 일 실시예에 따른 자동차 스마트 키 시스템의 근접성 인증 방법에서, 상기 상관관계 값을 산출하는 단계는, 상기 자동차가 연속하여 획득한 양방향 채널 정보로부터 채널별로 각각 공분산을 이용하여 상관관계 값을 산출할 수 있다.

[0009] 일 실시예에 따른 자동차 스마트 키 시스템의 근접성 인증 방법에서, 상기 채널 상태 정보는, 스퀈터링(scattering), 페이딩(fading), 신호 지연, 신호 위상 및 신호 세기 감쇄 중 적어도 하나를 포함할 수 있다.

[0010] 상기 기술적 과제를 해결하기 위하여, 본 발명의 일 실시예에 따른 자동차 스마트 키 시스템에서 자동차와 키의 근접성을 인증하는 방법은, 키가 자동차와 키 간의 챌린지-응답(Challenge-Response) 과정을 통해 상기 자동차로 하여금 상기 키를 확인시키는 단계; 상기 키가 상기 자동차와 상기 키 사이에 형성된 양방향 채널을 통해 채널 상태 정보 요청 메시지를 수신하는 단계; 및 상기 키가 채널 상태 정보 요청에 대응하여 수신 채널의 채널

상태 정보를 포함하는 응답 메시지를 전송하는 단계를 포함하되, 상기 키는, 상기 자동차로 하여금 연속하여 획득한 제 1 양방향 채널 상태 정보와 제 2 양방향 채널 상태 정보 사이의 상관관계 값을 산출하되, 산출된 상기 상관관계 값이 임계치보다 큰 경우 상기 자동차와 상기 키가 유효 범위 내에 근접하였다고 판단하도록 유도한다.

- [0011] 일 실시예에 따른 자동차 스마트 키 시스템의 근접성 인증 방법에서, 상기 응답 메시지를 전송하는 단계는, 상기 키가 상기 채널 상태 정보 요청 메시지의 프리앰블(preamble) 정보를 사용하여 수신 채널의 채널 상태를 산출하는 단계; 및 상기 키가 산출된 상기 수신 채널의 채널 상태 정보를 포함하는 채널 상태 정보 응답 메시지를 상기 자동차에 전송하는 단계를 포함할 수 있다.
- [0012] 일 실시예에 따른 자동차 스마트 키 시스템의 근접성 인증 방법에서, 상기 키가, 챌린지-응답 과정에서 키 응답 메시지를 전송한 후, 채널 상태 정보 요청 메시지를 상기 자동차로부터 수신하기 위해 연속적으로 대기함으로써, 고정된 처리 시간에 따라 상기 수신 채널의 채널 상태 정보를 포함하는 응답 메시지를 전송할 수 있다.
- [0013] 상기 기술적 과제를 해결하기 위하여, 본 발명의 다른 실시예에 따른 자동차 스마트 키 시스템에서 자동차와 키의 근접성을 인증하는 방법은, 자동차가 키와 챌린지-응답(Challenge-Response) 과정을 통해 상기 키를 확인하는 단계; 상기 자동차가 상기 자동차와 상기 키 사이에 형성된 양방향 채널로부터 송신단과 수신단 사이의 채널 특징을 나타내는 채널 상태 정보를 획득하는 단계; 상기 자동차가 획득한 채널 상태 정보로부터 메시지의 왕복 시간을 산출하는 단계; 및 산출된 상기 왕복 시간의 차이가 임계치보다 작은 경우, 상기 자동차는 상기 자동차와 상기 키가 유효 범위 내에 근접하였다고 판단하는 단계를 포함한다.
- [0014] 다른 실시예에 따른 자동차 스마트 키 시스템의 근접성 인증 방법에서, 상기 채널 상태 정보를 획득하는 단계는, 상기 자동차가 채널 상태 정보 요청 메시지를 전송하는 단계; 및 상기 자동차가 상기 채널 상태 정보 요청 메시지에 대응하는 채널 상태 정보 응답 메시지를 수신하는 단계를 포함한다. 또한, 상기 채널 상태 정보 응답 메시지를 수신하는 단계에서, 상기 채널 상태 정보 응답 메시지는 수신 채널의 채널 상태 정보를 포함한다. 나아가, 상기 채널 상태 정보를 획득하는 단계는, 상기 자동차가 상기 채널 상태 정보 응답 메시지의 프리앰블(preamble) 정보를 사용하여 수신 채널의 채널 상태 정보를 산출하는 단계를 더 포함할 수 있다.
- [0015] 다른 실시예에 따른 자동차 스마트 키 시스템의 근접성 인증 방법에서, 상기 메시지의 왕복 시간을 산출하는 단계는, 상기 자동차가 전송한 채널 상태 정보 요청 메시지와 상기 자동차가 수신한 채널 상태 정보 응답 메시지의 시간 차이로부터 상기 메시지의 왕복 시간을 산출할 수 있다.
- [0016] 다른 실시예에 따른 자동차 스마트 키 시스템의 근접성 인증 방법에서, 상기 채널 상태 정보는, 스퀈터링(scattering), 페이딩(fading), 신호 지연, 신호 위상 및 신호 세기 감쇄 중 적어도 하나를 포함할 수 있다.
- [0017] 상기 기술적 과제를 해결하기 위하여, 본 발명의 다른 실시예에 따른 자동차 스마트 키 시스템에서 자동차와 키의 근접성을 인증하는 방법은, 키가 자동차와 키 간의 챌린지-응답(Challenge-Response) 과정을 통해 상기 자동차로 하여금 상기 키를 확인시키는 단계; 상기 키가 상기 자동차와 상기 키 사이에 형성된 양방향 채널을 통해 채널 상태 정보 요청 메시지를 수신하는 단계; 및 상기 키가 채널 상태 정보 요청에 대응하여 수신 채널의 채널 상태 정보를 포함하는 응답 메시지를 전송하는 단계를 포함하되, 상기 키는, 상기 자동차로 하여금 채널 상태 정보로부터 메시지의 왕복 시간을 산출하되, 산출된 상기 왕복 시간의 차이가 임계치보다 작은 경우 상기 자동차와 상기 키가 유효 범위 내에 근접하였다고 판단하도록 유도한다.
- [0018] 다른 실시예에 따른 자동차 스마트 키 시스템의 근접성 인증 방법에서, 상기 응답 메시지를 전송하는 단계는, 상기 키가 상기 채널 상태 정보 요청 메시지의 프리앰블(preamble) 정보를 사용하여 수신 채널의 채널 상태를 산출하는 단계; 및 상기 키가 산출된 상기 수신 채널의 채널 상태 정보를 포함하는 채널 상태 정보 응답 메시지를 상기 자동차에 전송하는 단계를 포함할 수 있다.
- [0019] 다른 실시예에 따른 자동차 스마트 키 시스템의 근접성 인증 방법에서, 상기 키가, 챌린지-응답 과정에서 키 응답 메시지를 전송한 후, 채널 상태 정보 요청 메시지를 상기 자동차로부터 수신하기 위해 연속적으로 대기함으로써, 고정된 처리 시간에 따라 상기 수신 채널의 채널 상태 정보를 포함하는 응답 메시지를 전송할 수 있다.
- [0020] 상기 기술적 과제를 해결하기 위하여, 본 발명의 또 다른 실시예에 따른 자동차 스마트 키 시스템에서 자동차와 키의 근접성을 인증하는 방법은, 자동차가 키와 챌린지-응답(Challenge-Response) 과정을 통해 상기 키를 확인하는 단계; 상기 자동차가 상기 자동차와 상기 키 사이에 형성된 양방향 채널로부터 송신단과 수신단 사이의 채널 특징을 나타내는 복수 개의 채널 상태 정보를 획득하는 단계; 상기 자동차가 연속하여 획득한 제 1 양방향

채널 상태 정보와 제 2 양방향 채널 상태 정보 사이의 상관관계 값 및 메시지의 왕복 시간을 산출하는 단계; 및 산출된 상기 상관관계 값이 임계치보다 크고, 산출된 상기 왕복 시간의 차이가 임계치보다 작은 경우, 상기 자동차는 상기 자동차와 상기 키가 유효 범위 내에 근접하였다고 판단하는 단계를 포함한다.

[0021] 상기 기술적 과제를 해결하기 위하여, 본 발명의 또 다른 실시예에 따른 자동차 스마트 키 시스템에서 자동차와 키의 근접성을 인증하는 방법은, 키가 자동차와 키 간의 챌린지-응답(Challenge-Response) 과정을 통해 상기 자동차로 하여금 상기 키를 확인시키는 단계; 상기 키가 상기 자동차와 상기 키 사이에 형성된 양방향 채널을 통해 채널 상태 정보 요청 메시지를 수신하는 단계; 및 상기 키가 채널 상태 정보 요청에 대응하여 수신 채널의 채널 상태 정보를 포함하는 응답 메시지를 전송하는 단계를 포함하되, 상기 키는, 상기 자동차로 하여금 연속하여 획득한 제 1 양방향 채널 상태 정보와 제 2 양방향 채널 상태 정보 사이의 상관관계 값 및 메시지의 왕복 시간을 산출하되, 산출된 상기 상관관계 값이 임계치보다 크고, 산출된 상기 왕복 시간의 차이가 임계치보다 작은 경우, 상기 자동차와 상기 키가 유효 범위 내에 근접하였다고 판단하도록 유도한다.

[0022] 한편, 이하에서는 상기 기재된 자동차 스마트 키 시스템의 근접성 인증 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공한다.

발명의 효과

[0023] 본 발명의 실시예들은, 자동차 스마트 키 시스템에서 응답 시간과 함께 자동차와 키 사이에 측정된 마지막 채널 상태 정보와 현재 측정된 채널 상태 정보 간의 변환된 공분산을 사용하여 자동차와 키 사이의 거리를 추정함으로써 아날로그 릴레이 공격뿐만 아니라 디지털 릴레이 공격에도 효율적으로 대응할 수 있다.

도면의 간단한 설명

[0024] 도 1은 PKES(Passive Keyless Entry and Start) 시스템에서 챌린지-응답(Challenge-Response) 프로토콜을 설명하기 위한 도면이다.

도 2는 PKES 시스템에서의 릴레이 공격을 설명하기 위한 도면이다.

도 3은 시간에 따른 신호 세기 변화를 예시한 도면이다.

도 4는 본 발명의 실시예들에 따른 스마트 키 시스템에서 채널 상태 정보에 기반하여 자동차와 키의 근접성을 인증하는 방법을 도시한 도면이다.

도 5는 본 발명의 일 실시예에 따른 스마트 키 시스템에서 채널 상태 정보에 기반한 상관관계 값을 이용하여 자동차와 키의 근접성을 인증하는 방법을 도시한 흐름도이다.

도 6은 키가 자동차와 떨어진 후 다시 가까워지는 경우를 범위와 연관하여 예시한 도면이다.

도 7은 본 발명의 다른 실시예에 따른 스마트 키 시스템에서 채널 상태 정보에 기반한 왕복 시간을 이용하여 자동차와 키의 근접성을 인증하는 방법을 도시한 흐름도이다.

도 8은 본 발명의 실시예들이 채택하고 있는 자동차와 키 사이의 근접성을 판단하는 방법을 도시한 흐름도이다.

도 9는 본 발명의 실시예들에 따른 자동차와 키의 근접성을 인증하는 방법에서 릴레이 공격에 대응하는 과정을 설명하기 위한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0025] 본 발명의 실시예들을 설명하기에 앞서, 본 발명이 속하는 스마트 키 시스템이 적용된 기술 분야에서 차량과 키의 근접성을 인식하여 잠금을 해제하는 방식과 이러한 방식이 릴레이 공격에 노출되는 과정을 살펴본 후, 예상되는 문제점들을 해결하기 위해 본 발명의 실시예들이 채택하고 있는 아이디어와 기술적 수단을 순차적으로 소개하도록 한다.

[0026] 도 1은 PKES(Passive Keyless Entry and Start) 시스템에서 챌린지-응답(Challenge-Response) 프로토콜을 설명하기 위한 도면으로서, 자동차(10)와 키(20) 사이의 근접성을 다음과 같은 일련의 과정에 따라 검사한다.

[0027] PKES 시스템은 자동차(10)와 키(20) 사이의 근접성을 확인하기 위해 2가지 주파수 채널을 사용한다. 자동차(10)는 LF 채널(120~135 kHz)을 통해 "Challenge 메시지"를 주기적으로 방송(broadcast)한다. 키(20)는 주기적으로 LF 주파수 채널을 모니터링 하다가 자동차의 "Challenge 메시지" 신호를 감지하면, UHF 채널(315~433 MHz)을

통해 자동차(10)로 "키 응답 메시지"를 전송한다. 이후, 자동차(10)는 응답 메시지의 키(Key) 정보가 확인되면 잠금을 해제한다.

[0028] 도 2는 PKES 시스템에서의 릴레이 공격을 설명하기 위한 도면으로서, 릴레이 공격은 공격자 1명 또는 공격자 2명이 필요하며, 도 2에서는 공격자가 2명일 때의 릴레이 공격을 예시하였다.

[0029] 일례로 자동차 소유주는 키(20)를 가지고 카페에 있고, 자동차(10)는 주차장에 주차되어 있다고 가정하자. 공격자 1(31)은 자동차(10) 근처에 있으며, 공격자 2(32)는 자동차 소유주 근처에 있다. 공격자 1(31)과 공격자 2(32) 사이는 유선 또는 무선으로 통신한다. 공격자 1(31)은 자동차(10)에서 방송되는 "Challenge 메시지"를 공격자 2(32)에게 릴레이한다. 공격자 2(32)는 "Challenge 메시지" 신호를 증폭하여 자동차 소유주에게 방송한다. 이제, 자동차 소유주의 키(20)는 "Challenge 메시지" 신호를 감지하고 키는 "키 응답 메시지"를 전송한다. 공격자 2(32)는 "키 응답 메시지"를 공격자 1(31)로 릴레이하고, 공격자 1(31)은 "키 응답 메시지" 신호를 증폭하여 자동차(10)로 전송한다. 응답 메시지는 자동차의 암호화 방식과 관계없이 자동차의 키(20)에서 전송되는 데이터와 동일하므로 자동차(10)는 잠금을 해제한다.

[0030] 따라서, 상기된 보안상의 약점을 해결하기 위해서 안출된 본 발명의 실시예들에서는, 자동차와 키는 챌린지-응답(Challenge-Response) 과정 후에 아날로그 릴레이 공격 및 디지털 릴레이 공격 모두에 강한 채널 상태 정보(Channel State Information, CSI)를 교환하여 인증을 수행한다. 이를 위해, 자동차는 키에 수신 채널 상태 정보를 요청하는 메시지를 발송하고, 자동차는 키로부터 채널 상태 정보 응답 메시지를 수신함으로써, 양방향 채널 상태 정보를 획득한다. 자동차는 가장 최근의 양방향 채널 상태 정보와 획득한 양방향 채널 상태 정보의 상관관계를 조사하여 근접성을 판단함으로써 릴레이 공격을 방어하게 된다.

[0031] 본 발명의 실시예들이 제안하는 인증 방식은 자동차와 키 사이의 근접성을 자동차와 키 사이의 채널 상태 정보에 기반하여 판단한다. 채널 상태 정보는 송신단과 수신단 사이의 채널 특징을 나타내는 것으로, 스퀈터링(scattering), 페이딩(fading), 신호 지연, 신호 위상 또는 신호 세기 감쇄 중 적어도 하나를 포함하는 정보이다. 도 3은 LOS(Line-of-Sight)와 NLOS(Non LOS) 채널에서 시간에 따른 신호 세기 변화를 보여 준다.

[0032] LF 채널에서 자동차가 송신하는 신호를 x 로 표현할 때, 키가 수신하는 신호 y 는 " $y = hx + w$ "와 같이 표현할 수 있다. 여기서 h 는 자동차와 키 사이의 채널을 나타내며, w 는 평균이 0이고 분산이 0인 가우시안 잡음을 나타낸다.

[0033] 이하에서는 도면을 참조하여 본 발명의 실시예들을 구체적으로 설명하도록 한다. 다만, 하기의 설명 및 첨부된 도면에서 본 발명의 요지를 흐릴 수 있는 공지 기능 또는 구성에 대한 상세한 설명은 생략한다. 덧붙여, 명세서 전체에서, 어떤 구성 요소를 '포함'한다는 것은, 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라, 다른 구성요소를 더 포함할 수 있는 것을 의미한다.

[0034] 또한, 제 1, 제 2 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성 요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성 요소를 다른 구성 요소로부터 구별하는 목적으로 사용될 수 있다. 예를 들어, 본 발명의 권리 범위로부터 이탈되지 않은 채 제 1 구성 요소는 제 2 구성 요소로 명명될 수 있고, 유사하게 제 2 구성 요소도 제 1 구성 요소로 명명될 수 있다.

[0035] 본 발명에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, "포함하다" 또는 "구비하다" 등의 용어는 실시된 특징, 숫자, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0036] 특별히 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미이다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미인 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0037] 도 4는 본 발명의 실시예들에 따른 스마트 키 시스템에서 채널 상태 정보에 기반하여 자동차와 키의 근접성을 인증하는 방법을 도시한 도면으로서, 제안하는 인증 방식은 크게 2 단계로 구성된다. 1 단계는 종래의 챌린지-응답(Challenge-Response) 프로토콜과 동일 내지 유사하다. 2 단계는 자동차(10)가 자동차(10)와 키(20) 사이의

채널 상태 정보(CSI)를 수집하고 왕복시간(Round Trip Time, RTT)을 측정하는 과정이다.

- [0038] 키(20)의 동작 과정은 다음과 같다. 키는 1 단계에서 "키 응답 메시지"를 전송한 후에 자동차로부터 "CSI 요청 메시지"를 수신하기 위해 연속적으로 대기한다. 그리고 2 단계에서 자동차(10)로부터 "CSI 요청 메시지"를 수신하면, "CSI 요청 메시지"의 프리앰블(preamble) 정보를 사용하여 수신 채널의 CSI(채널 벡터 h)를 계산한다. 그리고 수신 채널의 CSI를 포함한 "CSI 응답 메시지"를 전송한다.
- [0039] 이에 대응하는 자동차(10)의 동작 과정은 다음과 같다. 자동차(10)는 1 단계에서 "키 응답 메시지"를 수신한 후에 2 단계에서 "CSI 요청 메시지"를 방송하고 "CSI 응답 메시지"를 수신하기 위해 대기한다. "CSI 응답 메시지"를 수신하면 자동차(10)는 자동차(10)와 키(20) 사이의 RTT를 정확히 계산할 수 있다. 왜냐하면 키(20)는 1 단계에서 "키 응답 메시지"를 전송한 후에 연속적으로 대기하므로 "CSI 응답 메시지"를 전송할 때, 처리 시간이 짧으며 고정값이다. 참고로 종래의 챌린지-응답(Challenge-Response) 프로토콜에서 키(20)는 주기적으로 자동차(10)의 챌린지(Challenge) 메시지 신호를 감지하여야 하므로 "키 응답 메시지"를 전송할 때, 처리 시간이 4~196 ms로 가변적이다.
- [0040] 도 4에서 기술한 바와 같이, 본 발명의 실시예들이 구현하고자 하는 스마트 키 시스템에서 자동차(10)와 키(20)는 챌린지-응답 과정 및 채널 상태 정보의 교환 과정을 수행하기 위해 각각 통신 수단을 구비하며, 전달된 정보를 처리하여 근접성 인증을 처리하기 위한 일련의 명령어를 포함하는 알고리즘을 저장하는 저장 수단과 이러한 알고리즘을 수행하는 처리 수단을 구비할 수 있다. 물리적인 하드웨어 구성에 대한 자세한 설명은 본 발명의 본질을 흐릴 우려가 있으므로 여기서는 일련의 처리 과정과 데이터의 흐름을 중심으로 수행 주체만을 개괄적으로 소개하도록 한다.
- [0041] 도 5는 본 발명의 일 실시예에 따른 스마트 키 시스템에서 채널 상태 정보에 기반한 상관관계 값을 이용하여 자동차와 키의 근접성을 인증하는 방법을 도시한 흐름도이다.
- [0042] S510 단계에서, 자동차는 키와 챌린지-응답(Challenge-Response) 과정을 통해 상기 키를 확인한다.
- [0043] S520 단계에서, 상기 자동차는 상기 자동차와 상기 키 사이에 형성된 양방향 채널로부터 송신단과 수신단 사이의 채널 특징을 나타내는 복수 개의 채널 상태 정보를 획득한다. 이 과정에서는, 상기 자동차가 채널 상태 정보 요청 메시지를 전송하고, 상기 채널 상태 정보 요청 메시지에 대응하는 채널 상태 정보 응답 메시지를 키로부터 수신하게 된다. 특히, 상기 채널 상태 정보 응답 메시지는 수신 채널의 채널 상태 정보를 포함한다. 즉, 상기 키가 상기 채널 상태 정보 요청 메시지의 프리앰블(preamble) 정보를 사용하여 수신 채널의 채널 상태 정보를 산출하고, 산출된 상기 수신 채널의 채널 상태 정보를 포함하는 채널 상태 정보 응답 메시지를 상기 키가 상기 자동차에 전송하게 된다. 이후 상기 자동차는 상기 채널 상태 정보 응답 메시지의 프리앰블(preamble) 정보를 사용하여 수신 채널의 채널 상태 정보를 산출할 수 있다.
- [0044] S530 단계에서, 상기 자동차는 연속하여 획득한 제 1 양방향 채널 상태 정보와 제 2 양방향 채널 상태 정보 사이의 상관관계 값을 산출한다. 이 과정에서, 상기 자동차는 연속하여 획득한 양방향 채널 정보로부터 채널별로 각각 공분산을 이용하여 상관관계 값을 산출하게 된다. 보다 구체적인 상관관계 값의 연산 과정은 이후 수학적 식 1, 2를 통해 자세히 설명하도록 한다.
- [0045] S540 단계의 검사 과정을 통해 앞서 산출된 상기 상관관계 값이 임계치보다 큰 경우, S550 단계로 진행하여 상기 자동차는 상기 자동차와 상기 키가 유효 범위 내에 근접하였다고 판단하고, 그 외의 경우에는 S560 단계를 통해 근접성 인증 실패 처리한다.
- [0046] 한편, 상기 키는, 상기 S510 단계의 챌린지-응답 과정에서 키 응답 메시지를 전송한 후, 상기 S520 단계 단계의 채널 상태 정보 요청 메시지를 상기 자동차로부터 수신하기 위해 연속적으로 대기함으로써, 고정된 처리 시간에 따라 상기 수신 채널의 채널 상태 정보를 포함하는 응답 메시지를 상기 자동차에 전송할 수 있게 된다.
- [0047] 이하에서는, 양방향 채널 상태 정보로부터 상관관계 값과 응답 시간을 도출하는 원리와 그 과정을 구체적으로 설명한다.
- [0048] 앞서 설명하였던 도 4를 재차 참조하면, 자동차(10)는 "CSI 응답 메시지"의 프리앰블 정보를 사용하여 수신 채널의 CSI(채널 벡터 g)를 계산한다. 따라서 자동차(10)는 "CSI 응답 메시지"에 포함된 자동차(10)와 키(20) 사이의 채널 정보 h 를 포함하여, 양방향 채널 정보 (h , g) 정보를 모두 획득한다. 자동차(10)는 획득한 양방향 채널 정보 (h , g)와 가장 최근의 양방향 채널 정보 (h' , g') 사이의 변환된 공분산 ρ_1 , ρ_2 를 다음의 수학적 식 1, 2와 같이 각각 계산한다.

수학식 1

$$\rho_1 = E\left(\left(\frac{h}{10\sigma_h} - \frac{\mu_h}{\sigma_h}\right) \cdot \left(\frac{h'}{10\sigma_{h'}} - \frac{\mu_{h'}}{\sigma_{h'}}\right)\right)$$

수학식 2

$$\rho_2 = E\left(\left(\frac{g}{10\sigma_g} - \frac{\mu_g}{\sigma_g}\right) \cdot \left(\frac{g'}{10\sigma_{g'}} - \frac{\mu_{g'}}{\sigma_{g'}}\right)\right)$$

여기서 μ_h 와 σ_h 는 각각 채널 벡터 h 의 평균과 분산이고, μ_g 와 σ_g 는 각각 채널 벡터 g 의 평균과 분산이다.

도 6은 키가 자동차와 떨어진 후 다시 가까워지는 경우를 유효 범위와 연관하여 예시한 도면으로서, 키(20)를 가진 자동차 소유주가 ①→②→③→④의 순서로 이동할 때, 현재 i 지점에서 획득한 양방향 채널 정보를 (h , g)라고 하면 가장 최근의 양방향 채널 정보 (h' , g')는 시점 $i-1$ 지점에서 획득한 정보이다.

이제 자동차는, 응답 시간(RTT)이 미리 설정된 임계치 δ_{RTT} 보다 작고, 변환된 공분산 ρ_1 이 미리 설정된 임계치 δ_1 보다 크고, ρ_2 가 미리 설정된 임계치 δ_2 보다 클 때에만 잠금을 해제한다.

도 7은 본 발명의 다른 실시예에 따른 스마트 키 시스템에서 채널 상태 정보에 기반한 왕복 시간을 이용하여 자동차와 키의 근접성을 인증하는 방법을 도시한 흐름도이다.

S710 단계에서, 자동차는 키와 챌린지-응답(Challenge-Response) 과정을 통해 상기 키를 확인한다.

S720 단계에서, 상기 자동차는 상기 자동차와 상기 키 사이에 형성된 양방향 채널로부터 송신단과 수신단 사이의 채널 특징을 나타내는 채널 상태 정보를 획득한다. 이 과정에서는, 상기 자동차가 채널 상태 정보 요청 메시지를 전송하고, 상기 채널 상태 정보 요청 메시지에 대응하는 채널 상태 정보 응답 메시지를 키로부터 수신한다. 특히, 상기 채널 상태 정보 응답 메시지는 수신 채널의 채널 상태 정보를 포함한다. 즉, 상기 키가 상기 채널 상태 정보 요청 메시지의 프리앰블(preamble) 정보를 사용하여 수신 채널의 채널 상태 정보를 산출하고, 산출된 상기 수신 채널의 채널 상태 정보를 포함하는 채널 상태 정보 응답 메시지를 상기 키가 상기 자동차에 전송하게 된다. 이후 상기 자동차는 상기 채널 상태 정보 응답 메시지의 프리앰블(preamble) 정보를 사용하여 수신 채널의 채널 상태 정보를 산출할 수 있다.

S730 단계에서, 상기 자동차는 획득한 채널 상태 정보로부터 메시지의 왕복 시간을 산출한다. 이 과정에서, 상기 자동차가 전송한 채널 상태 정보 요청 메시지와 상기 자동차가 수신한 채널 상태 정보 응답 메시지의 시간 차이로부터 상기 메시지의 왕복 시간을 산출하게 된다.

S740 단계의 검사 과정을 통해 앞서 산출된 상기 왕복 시간의 차이가 임계치보다 작은 경우, S750 단계로 진행하여 상기 자동차는 상기 자동차와 상기 키가 유효 범위 내에 근접하였다고 판단하고, 그 외의 경우에는 S760 단계를 통해 근접성 인증 실패 처리한다.

한편, 상기 키는, 상기 S710 단계의 챌린지-응답 과정에서 키 응답 메시지를 전송한 후, 상기 S720 단계의 채널 상태 정보 요청 메시지를 상기 자동차로부터 수신하기 위해 연속적으로 대기함으로써, 고정된 처리 시간에 따라 상기 수신 채널의 채널 상태 정보를 포함하는 응답 메시지를 전송하게 된다.

도 8은 본 발명의 실시예들이 채택하고 있는 자동차와 키 사이의 근접성을 판단하는 방법을 도시한 흐름도로서, 앞서 도 5 및 도 7에서 근접성 인증의 판단 근거로서 활용되었던 상관관계 값과 메시지 응답 시간을 종합적으로 활용하여 릴레이 공격에 강인한 인증을 수행하는 과정을 제시하였다.

우선, S810 단계를 통해 수학식 1, 2에서 제시한 변환된 상관관계 값 ρ_1 , ρ_2 와 응답 시간 RTT를 산출한다.

그런 다음, S820 단계 내지 S840 단계를 통해 각각 해당 값들을 미리 설정된 임계치 δ_{RTT} , δ_1 , δ_2 와 비교하여

이들 조건을 모두 만족하는 경우에만 S850 단계를 통해 근접성 인증에 성공하고, 그 외의 경우에는 모두 S860 단계를 통해 근접성 인증 실패 처리한다.

[0063] 요약하건대, 자동차 스마트 키 시스템에서 자동차와 키의 근접성을 인증하는 방법은, 자동차가 키와 챌린지-응답(Challenge-Response) 과정을 통해 상기 키를 확인하고, 상기 자동차가 상기 자동차와 상기 키 사이에 형성된 양방향 채널로부터 송신단과 수신단 사이의 채널 특징을 나타내는 복수 개의 채널 상태 정보를 획득하고, 상기 자동차가 연속하여 획득한 제 1 양방향 채널 상태 정보와 제 2 양방향 채널 상태 정보 사이의 상관관계 값 및 메시지의 왕복 시간을 산출하며, 산출된 상기 상관관계 값이 임계치보다 크고, 산출된 상기 왕복 시간의 차이가 임계치보다 작은 경우, 상기 자동차는 상기 자동차와 상기 키가 유효 범위 내에 근접하였다고 판단한다.

[0064] 이하에서는, 본 발명의 실시예들이 제안하는 스마트 키 시스템 인증 방식에서 릴레이 공격에 대응하는 과정을 소개하도록 한다.

[0065] 도 9는 본 발명의 실시예들에 따른 자동차(10)와 키(20)의 근접성을 인증하는 방법에서 릴레이 공격에 대응하는 과정을 설명하기 위한 도면으로서, 공격자 1(31)과 공격자 2(32)에서의 처리 시간을 각각 t_1 , t_2 라고 하고, LF 채널과 UHF 채널에서 릴레이 공격으로 추가되는 전파 전달 시간을 각각 τ_1 , τ_2 라 하자. 그러면 릴레이 공격에서의 응답 시간 RTT_R 은 다음의 수학식 3과 같다.

수학식 3

[0066]
$$RTT_R = RTT_{\max} + t_1 + t_2 + \tau_1 + \tau_2$$

[0067] 여기서 $RTT_{\max}$ 는 릴레이 공격이 없을 때의 최대 RTT 이다. 즉, 릴레이 공격으로 인해 RTT 값은 $\Delta_R = t_1 + t_2 + \tau_1 + \tau_2$ 만큼 증가한다.

[0068] 도 9에서 노드 i에서 노드 j로의 채널을 $h_{i,j}$ 또는 $g_{i,j}$ 라고 하고, 노드 i에서 노드 j로의 잡음을 $w_{i,j}$ 라고 하자. 그리고 자동차(10)에서 키(20)로의 방향에 공격자 1(31)이 수신하는 신호를 y_1 이라 하고 공격자 2(32)가 수신하는 신호를 y_2 라 하자. LF 채널에서 자동차(10)가 송신하는 신호를 x 로 표현할 때, 키(20)가 수신하는 신호 y 는 다음과 같다.

수학식 4

[0069]
$$y_1 = h_{0,1}x + w_{0,1}$$

수학식 5

[0070]
$$y_2 = h_{1,2}y_1 + w_{1,2}$$

수학식 6

[0071]
$$\begin{aligned} y &= h_{2,3}y_2 + w_{2,3} \\ &= \underbrace{h_{2,3}h_{1,2}h_{0,1}}_{h_R}x + \underbrace{h_{2,3}h_{1,2}w_{0,1} + h_{2,3}w_{1,2} + w_{2,3}}_{w_R} \end{aligned}$$

[0072] 여기서 h_R 을 등가 채널, w_R 을 등가 잡음이라고 하자. 그러면 동일한 방식으로 키(20)에서 공격자 방향에 등가 채널과 등가 잡음은 다음과 같다.

수학식 7

$$g_R = g_{1,0}g_{2,1}g_{3,2}$$

수학식 8

$$w_R = g_{1,0}g_{2,1}w_{3,2} + g_{1,0}w_{2,1} + w_{1,0}$$

공격자가 디지털 릴레이를 사용하는 경우 각 구간에서 채널 정보와 잡음을 제거하여 송신 신호를 복구하므로 $h_R \approx h_{2,3}$, $g_R \approx g_{1,0}$, $w_R \approx w$ 이 된다. 그러나 공격자가 아날로그 릴레이를 사용하는 경우 각 구간에서 채널 정보와 잡음이 제거되지 않는다.

자동차(10)는 릴레이 공격이 없을 때의 양방향 채널 정보 (h' , g')와 릴레이 공격일 때의 양방향 채널 정보 (h_R , g_R)를 비교한다.

상기된 본 발명의 실시예들에 따른 스마트 키 시스템에서 채널 상태 정보에 기반하여 자동차와 키의 근접성을 인증하는 방법은, 다음과 같은 관점에서 장점을 갖는다.

● 호환성: 제안하는 인증 방식의 1 단계는 종래의 Challenge-Response 프로토콜과 동일하다. 따라서 제안하는 인증 방식을 탑재한 자동차 또는 키는 종래 방식의 기기와 호환성을 가진다.

● 아날로그 릴레이 공격 대응: 자동차에서 30 m 떨어진 키까지 전파 전달 시간은 약 120 ns이다. 공격자들이 아날로그 릴레이를 사용하는 경우 릴레이에서의 처리 시간은 약 15~20 ns 이다. 따라서 Δ_R 값이 너무 작으므로 종래의 TOA 기반 방식으로는 아날로그 릴레이 공격을 대응할 수 없다. 그러나 제안하는 방식은 CSI의 상관도를 비교하여 대응할 수 있다.

● 디지털 릴레이 공격 대응: 공격자들이 디지털 릴레이를 사용하는 경우 릴레이에서의 처리 시간은 아날로그 릴레이를 사용하는 경우보다 릴레이 1개당 약 15~20 μs 길어진다. 따라서 Δ_R 값이 충분히 크므로 RTT 비교만으로도 충분히 대응할 수 있다.

본 발명의 실시예들에 따르면, PKES 시스템에서 RTT 값과 함께 자동차와 키 사이에 측정된 마지막 채널 상태 정보와 현재 측정된 채널 상태 정보 간의 변환된 공분산을 사용하여 자동차와 키 사이의 거리를 추정함으로써 아날로그 릴레이 공격뿐만 아니라 디지털 릴레이 공격에도 효율적으로 대응할 수 있다.

한편, 본 발명의 실시예들은 컴퓨터로 읽을 수 있는 기록 매체에 컴퓨터가 읽을 수 있는 코드로 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록 매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다.

컴퓨터가 읽을 수 있는 기록 매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광 데이터 저장장치 등을 포함한다. 또한, 컴퓨터가 읽을 수 있는 기록 매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산 방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다. 그리고 본 발명을 구현하기 위한 기능적인 (functional) 프로그램, 코드 및 코드 세그먼트들은 본 발명이 속하는 기술 분야의 프로그래머들에 의하여 용이하게 추론될 수 있다.

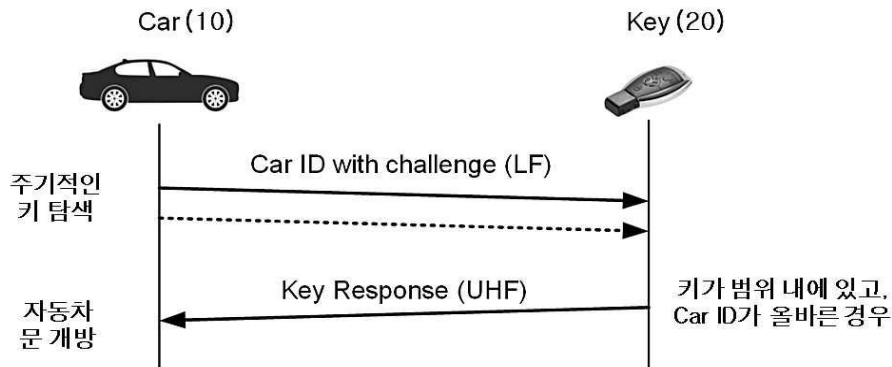
이상에서 본 발명에 대하여 그 다양한 실시예들을 중심으로 살펴보았다. 본 발명에 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

부호의 설명

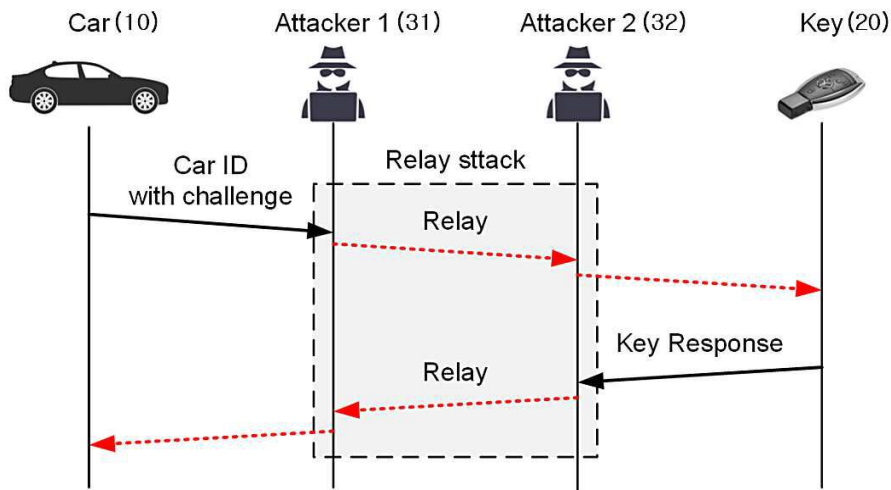
[0085]
 10: 자동차
 20: 키
 31, 32: 공격자

도면

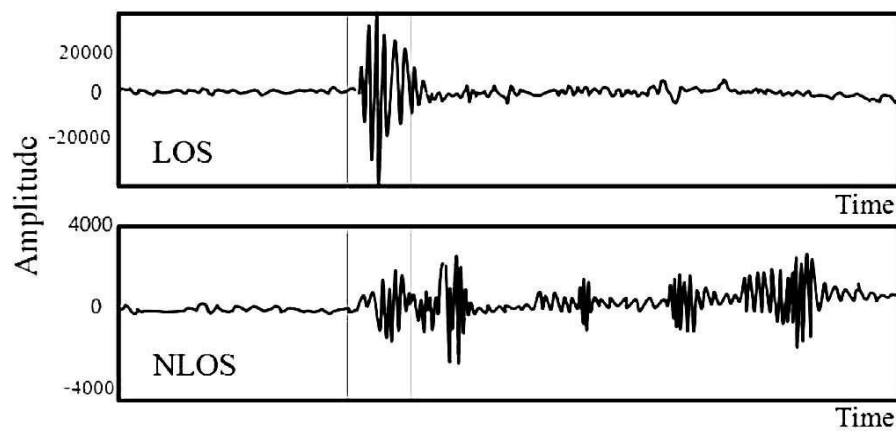
도면1



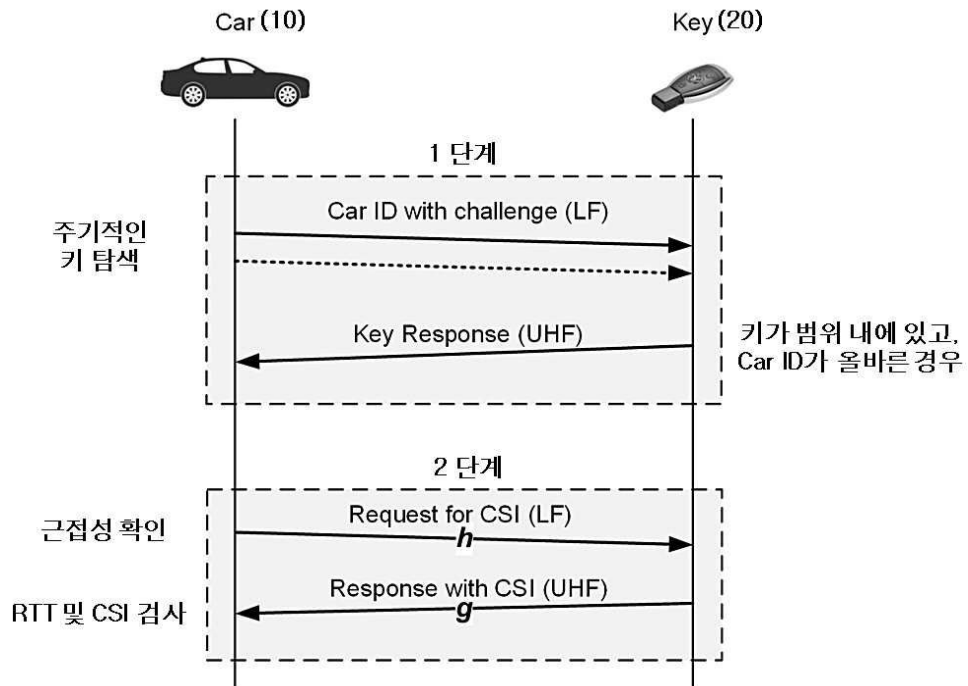
도면2



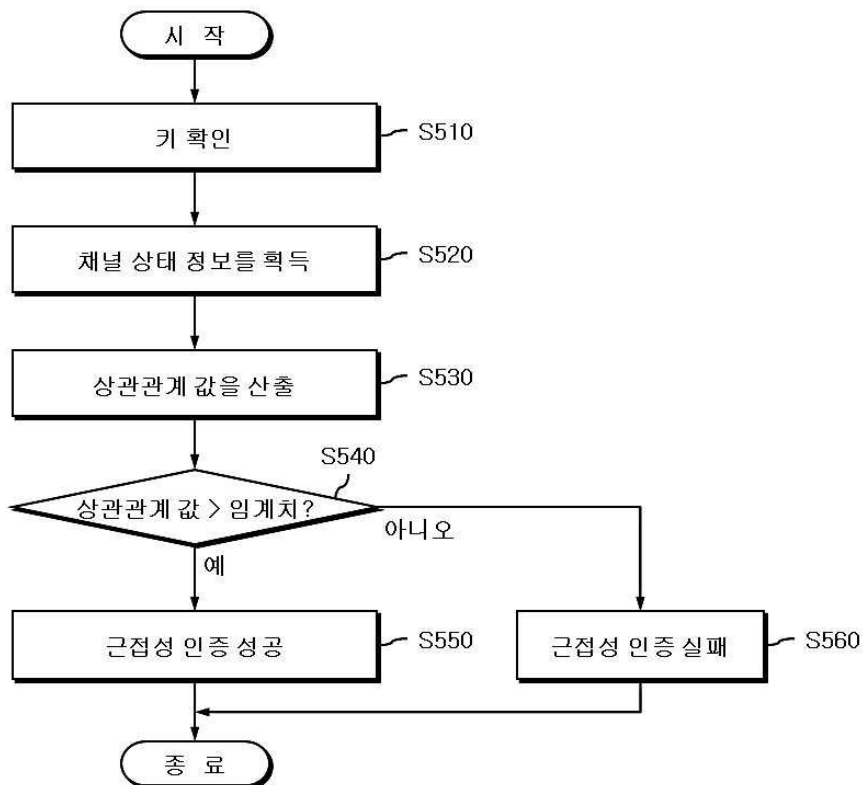
도면3



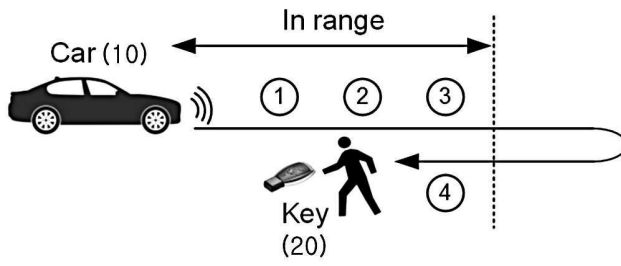
도면4



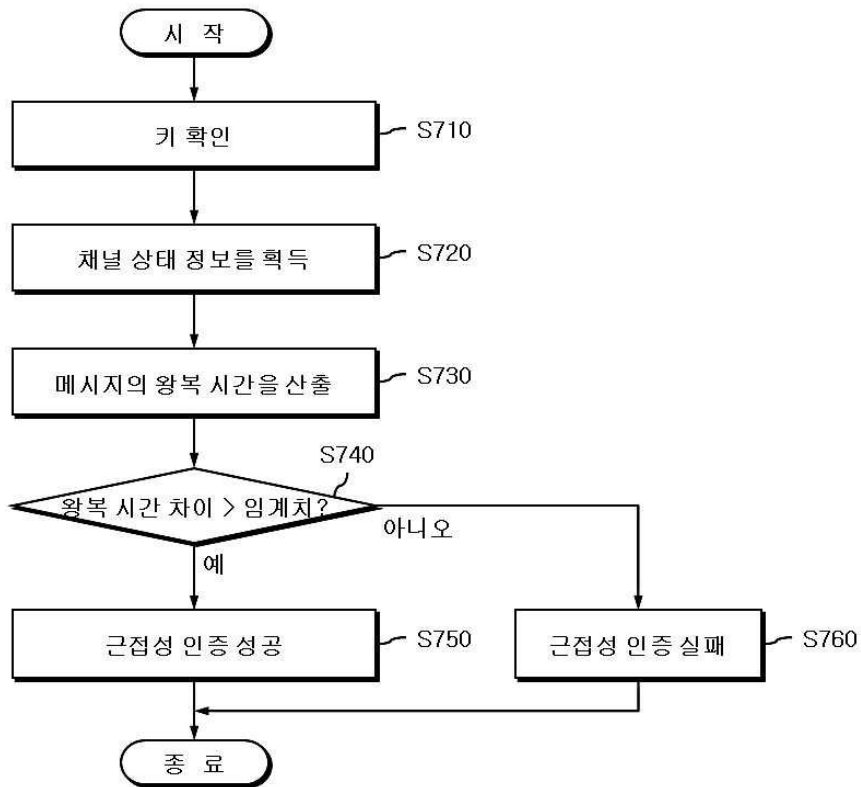
도면5



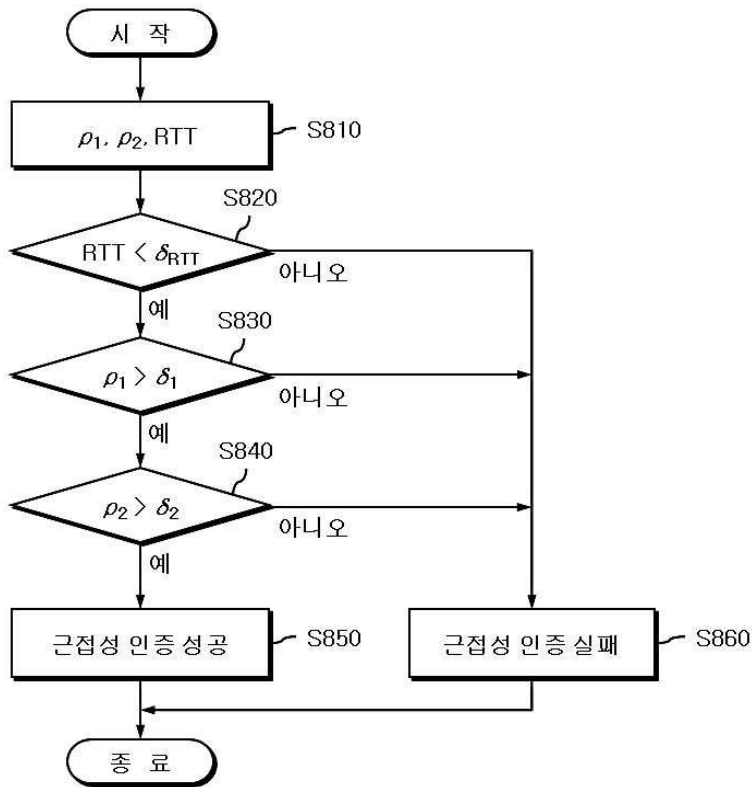
도면6



도면7



도면8



도면9

