(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2024-0158023
(43) 공개일자 2024년11월04일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *B60R 25/01* (2013.01)
B60R 25/24 (2013.01)
(52) CPC특허분류
H04L 9/3297 (2013.01)
B60R 25/01 (2013.01)
(21) 출원번호 10-2023-0054858
(22) 출원일자 2023년04월26일
심사청구일자 없음

(71) 출원인
현대자동차주식회사
서울특별시 서초구 헌릉로 12 (양재동)
기아 주식회사
서울특별시 서초구 헌릉로 12 (양재동)
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
조아람
서울특별시 중구 만리재로33길 21, LIG 서울역 리가 104-1304
최원석
서울특별시 강북구 삼양로 256, 래미안미아1차아파트 105-501
(뒷면에 계속)
(74) 대리인
특허법인태평양

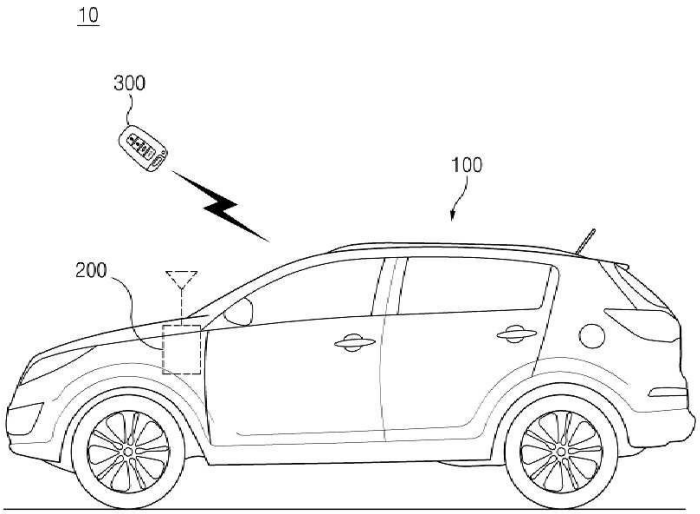
전체 청구항 수 : 총 20 항

(54) 발명의 명칭 **차량을 위한 개선된 보안 기능 제공 방법과, 이를 지원하는 컴퓨팅 시스템 및 차량**

(57) 요 약

본 발명은 차량, 이를 위한 컴퓨팅 시스템 및 그 방법에 관한 것으로, 차량의 안테나부를 통해 차량 제어 신호를 수신하는 동작, 상기 차량 제어 신호 중 STS 필드(Scrambled Timestamp Sequence field)를 추출하는 동작, 상기 추출된 STS 필드를 사전 정의된 일정 길이의 서브 필드들로 분할하는 동작, 상기 분할된 서브 필드들과 상기 저장부에 사전 저장된 서브 템플릿들 각각을 상호 상관 연산하는 동작, 상기 상호 상관 연산 결과들로부터 상기 차량 제어 신호의 수신 시점들을 추출하는 동작, 상기 상호 상관 연산 결과들 내에서 상기 수신 시점들의 분포 위치들의 일관성이 사전 정의된 기준 값 이상인 경우 상기 차량 제어 신호를 정상 신호로 판단하고, 상기 일관성이 사전 정의된 기준 값 미만 경우 상기 차량 제어 신호를 비정상 신호로 판단하는 동작을 수행하는 컴퓨팅 시스템, 이를 포함하는 차량, 이의 수행 방법을 개시할 수 있다.

대 표 도 - 도1



(52) CPC특허분류
B60R 25/246 (2013.01)
H04L 2209/84 (2013.01)
(72) 발명자
이세영
서울특별시 동대문구 망우로18가길 61-10, 4층
이동훈
서울특별시 종로구 사직로8길 34, 1404호
주경호
서울특별시 성북구 지봉로24길 52-8
정연선
강원도 춘천시 안마산로 133, e편한세상 춘천 한숲시티
윤경은
경기도 고양시 덕양구 세솔로 105, 삼송마을동원로얄듀크 1710-1902

명 세 서

청구범위

청구항 1

차량 안테나부;

상기 차량 안테나부를 통해 수신된 신호의 처리를 수행하는 프로세서; 및

상기 프로세서 운용을 위한 적어도 하나의 명령어를 저장하는 저장부;를 포함하고,

상기 프로세서는,

상기 차량 안테나부를 통해 차량 제어 신호를 수신하고,

상기 차량 제어 신호 중 STS 필드(Scrambled Timestamp Sequence field)를 추출하고,

추출된 STS 필드를 사전 정의된 일정 길이의 서브 필드들로 분할하고,

상기 분할된 서브 필드들과 상기 저장부에 사전 저장된 서브 템플릿들 각각을 상호 상관 연산하고,

상기 상호 상관 연산 결과들로부터 상기 차량 제어 신호의 수신 시점들을 추출하고,

상기 수신 시점들을 기반으로 상기 수신된 차량 제어 신호의 정상 여부를 판단하도록 설정된 것을 특징으로 하는 개선된 보안 기능을 제공하는 차량.

청구항 2

제1항에 있어서,

상기 프로세서는,

상기 상호 상관 연산 결과들 내에서 상기 수신 시점들의 분포 위치에 대한 일관성을 기반으로 상기 차량 제어 신호의 정상 여부를 판단하도록 설정된 것을 특징으로 하는 개선된 보안 기능을 제공하는 차량.

청구항 3

제1항에 있어서,

상기 프로세서는

상기 저장부에 사전 저장된 로컬 템플릿을 상기 분할된 서브 필드의 길이에 대응하여 복수개의 서브 템플릿들로 분할하도록 설정된 것을 특징으로 하는 개선된 보안 기능을 제공하는 차량.

청구항 4

제1항에 있어서,

상기 프로세서는

상기 수신 시점들의 추출과 관련하여 상기 상호 상관 연산 결과에 해당하는 주파수 그래프에서, 최대 피크를 결정하고, 상기 최대 피크로부터 일정 길이 이내에 위치한 피크 후보들을 산출하고, 산출된 피크 후보들 중 상기 최대 피크로부터 가장 멀리 떨어진 피크를 상기 수신 시점으로 산출하도록 설정된 것을 특징으로 하는 개선된 보안 기능을 제공하는 차량.

청구항 5

제1항에 있어서,

상기 프로세서는

상기 수신 시점들의 분포 위치 차이에 대한 누적 오프셋 값을 산출하고, 상기 누적 오프셋 값이 사전 정의된 파

라미터 값을 초과하는 경우 상기 차량 제어 신호를 비정상 신호에 해당하는 공격 신호로 판단하도록 설정된 것을 특징으로 하는 개선된 보안 기능을 제공하는 차량.

청구항 6

제5항에 있어서,

상기 프로세서는

상기 차량 제어 신호가 비정상 신호인 경우 상기 수신된 차량 제어 신호를 무효화 처리하도록 설정된 것을 특징으로 하는 개선된 보안 기능을 제공하는 차량.

청구항 7

제5항에 있어서,

상기 프로세서는

상기 차량 제어 신호가 비정상 신호인 경우 상기 차량 제어 신호의 수신 시각, 수신 횟수, 수신 위치 중 적어도 하나를 사전 정의된 장치에 전송하도록 설정된 것을 특징으로 하는 개선된 보안 기능을 제공하는 차량.

청구항 8

제1항에 있어서,

상기 프로세서는

상기 수신 시점들의 분포 위치 차이에 대한 누적 오프셋 값을 산출하고, 상기 누적 오프셋 값이 사전 정의된 파라미터 값 이하인 경우 상기 차량 제어 신호를 정상 신호로 판단하도록 설정된 것을 특징으로 하는 개선된 보안 기능을 제공하는 차량.

청구항 9

제8항에 있어서,

상기 프로세서는

상기 차량 제어 신호가 정상 신호인 경우, 수신된 차량 제어 신호에 대응하여 상기 차량의 도어락을 해제하거나, 상기 차량의 시동을 턴-온하거나, 상기 차량의 공기 순환 장치를 턴-온하도록 설정된 것을 특징으로 하는 개선된 보안 기능을 제공하는 차량.

청구항 10

차량의 프로세서가, 상기 차량의 안테나부를 통해 차량 제어 신호를 수신하는 단계;

상기 차량 제어 신호 중 STS 필드(Scrambled Timestamp Sequence field)를 추출하는 단계;

상기 추출된 STS 필드를 사전 정의된 일정 길이의 서브 필드들로 분할하는 단계;

상기 분할된 서브 필드들과 상기 저장부에 사전 저장된 서브 템플릿들 각각을 상호 상관 연산하는 단계;

상기 상호 상관 연산 결과들로부터 상기 차량 제어 신호의 수신 시점들을 추출하는 단계;

상기 수신 시점들을 기반으로 상기 수신된 차량 제어 신호의 정상 여부를 판단하는 단계;를 포함하는 것을 특징으로 하는 차량의 개선된 보안 기능 제공 방법.

청구항 11

제10항에 있어서,

상기 판단하는 단계는,

상기 상호 상관 연산 결과들 내에서 상기 수신 시점들의 분포 위치에 대한 일관성을 기반으로 상기 차량 제어 신호의 정상 여부를 판단하는 단계;를 포함하는 것을 특징으로 하는 차량의 개선된 보안 기능 제공 방법.

청구항 12

제10항에 있어서,

상기 저장부에 사전 저장된 로컬 템플릿을 상기 분할된 서브 필드의 길이에 대응하여 복수개의 서브 템플릿들로 분할하는 단계;를 더 포함하는 것을 특징으로 하는 차량의 개선된 보안 기능 제공 방법.

청구항 13

제10항에 있어서,

상기 수신 시점들을 추출하는 단계는,

상기 상호 상관 연산 결과에 해당하는 주파수 그래프에서, 최대 피크를 결정하는 단계;

상기 최대 피크로부터 일정 길이 이내에 위치한 피크 후보들을 산출하는 단계;

상기 산출된 피크 후보들 중 상기 최대 피크로부터 가장 멀리 떨어진 피크를 상기 수신 시점으로 산출하는 단계;를 포함하는 것을 특징으로 하는 차량의 개선된 보안 기능 제공 방법.

청구항 14

제10항에 있어서,

상기 판단하는 단계는,

상기 수신 시점들의 분포 위치 차이에 대한 누적 오프셋 값을 산출하는 단계;

상기 누적 오프셋 값이 사전 정의된 파라미터 값을 초과하는 경우 상기 차량 제어 신호를 비정상 신호에 해당하는 공격 신호로 판단하는 단계;를 포함하는 것을 특징으로 하는 차량의 개선된 보안 기능 제공 방법.

청구항 15

제14항에 있어서,

상기 차량 제어 신호가 비정상 신호인 경우 상기 수신된 차량 제어 신호를 무효화 처리하는 단계;를 더 포함하는 것을 특징으로 하는 차량의 개선된 보안 기능 제공 방법.

청구항 16

제14항에 있어서,

상기 차량 제어 신호가 비정상 신호인 경우 상기 차량 제어 신호의 수신 시각, 수신 횟수, 수신 위치 중 적어도 하나를 사전 정의된 장치에 전송하는 단계;를 더 포함하는 것을 특징으로 하는 차량의 개선된 보안 기능 제공 방법.

청구항 17

제10항에 있어서,

상기 판단하는 단계는,

상기 수신 시점들의 분포 위치 차이에 대한 누적 오프셋 값을 산출하는 단계;

상기 누적 오프셋 값이 사전 정의된 파라미터 값 이하인 경우 상기 차량 제어 신호를 정상 신호로 판단하는 단계;를 포함하는 것을 특징으로 하는 차량의 개선된 보안 기능 제공 방법.

청구항 18

제17항에 있어서,

상기 차량 제어 신호가 정상 신호인 경우, 수신된 차량 제어 신호에 대응하여 상기 차량의 도어락을 해제하거나, 상기 차량의 시동을 턴-온하거나, 상기 차량의 공기 순환 장치를 턴-온하도록 제어하는 단계;를 더 포함하는 것을 특징으로 하는 차량의 개선된 보안 기능 제공 방법.

청구항 19

차량 운행을 지원하는 프로세서; 및

상기 프로세서 운용을 위한 적어도 하나의 명령어를 저장하는 저장부;를 포함하고, 상기 저장부에 저장된 적어도 하나의 명령어는, 상기 프로세서가,

상기 차량의 안테나부를 통해 차량 제어 신호를 수신하는 동작;

상기 차량 제어 신호 중 STS 필드(Scrambled Timestamp Sequence field)를 추출하는 동작;

상기 추출된 STS 필드를 사전 정의된 일정 길이의 서브 필드들로 분할하는 동작;

상기 분할된 서브 필드들과 상기 저장부에 사전 저장된 서브 템플릿들 각각을 상호 상관 연산하는 동작;

상기 상호 상관 연산 결과들로부터 상기 차량 제어 신호의 수신 시점들을 추출하는 동작;

상기 상호 상관 연산 결과들 내에서 상기 수신 시점들의 분포 위치들의 일관성이 사전 정의된 기준 값 이상인 경우 상기 차량 제어 신호를 정상 신호로 판단하고, 상기 일관성이 사전 정의된 기준 값 미만 경우 상기 차량 제어 신호를 비정상 신호로 판단하는 동작;을 수행하도록 설정된 것을 특징으로 하는 개선된 보안 기능을 제공하는 차량의 컴퓨팅 시스템.

청구항 20

청구항 19에 있어서,

상기 적어도 하나의 명령어는, 상기 프로세서가,

상기 차량 제어 신호가 비정상 신호인 경우 상기 수신된 차량 제어 신호를 무효화 처리하는 동작;

상기 차량 제어 신호가 정상 신호인 경우, 수신된 차량 제어 신호에 대응하여 상기 차량의 도어락을 해제하거나, 상기 차량의 시동을 턴-온하거나, 상기 차량의 공기 순환 장치를 턴-온하도록 제어하는 동작;을 수행하도록 설정된 것을 특징으로 하는 개선된 보안 기능을 제공하는 차량의 컴퓨팅 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명은 차량의 보안 기능 개선 지원에 관한 것으로, 보다 상세하게는 전자키를 이용한 차량 제어 과정에서 보안 성능을 개선할 수 있는 기술에 관한 것이다.

배 경 기 술

[0002] 일반적으로 무선통신 시스템에서 수신부는 사전에 알려진 신호 템플릿과 수신 신호 간의 cross correlation 연산을 통해 신호의 수신 여부를 판단한다. 특히, 시간동기화에 필수적인 Preamble 영역은 표준에 정의된 코드를 이용하여 고정 값으로 구성되기 때문에, 수신부는 Preamble 영역을 통해 신호의 수신여부 및 시간동기화를 수행할 수 있다. 일 예로, IEEE 802.15.4z 표준은 HRP UWB(high rate pulse repetition ultra-wide band) 기기가 cross correlation을 통해 수신된 STS(Scrambled Timestamp Sequence)를 검증하도록 명시하고 있다.

[0003] 한편, Non Line-of-Sight (NLoS) 채널 환경에서 패킷의 정확한 수신 시점을 측정하기 위해서는 송신부와 수신부의 직선거리에 해당하는 direct path를 식별 하는 것이 중요다. 이를 위해 UWB 수신부는 Back-search 알고리즘을 사용하여 reflected path와 direct path를 구분한다. back-search 알고리즘이 필요한 다중 경로(multi-path) 채널 환경에서는 reflected path를 통해 수신된 신호의 세기가 direct path를 통해 수신된 신호보다 강하다. 만약 수신부가 maximum peak (reflected path)를 기준으로 수신 시점을 측정한다면 두 path간의 거리차이만큼 오차가 발생할 수 있다. 따라서 수신부는 maximum peak로부터 일정 범위내의 peak들을 분석하여 direct path에 해당하는 leading edge를 식별 해야 한다. 하지만, back-search 알고리즘은 상호상관(cross correlation) 출력의 무결성을 검증할 수 없는 구조를 가진다. 즉, 수신부는 상호 상관 출력을 항상 신뢰하기 때문에 공격자는 사전에 공유된 비밀키를 모르더라도 STS 필드에 강한 신호를 주입하여 CIR(Channel Impulse Response) 출력을 오염시킬 수 있으며, 이를 통해 fake leading edge를 생성할 수 있다. 결과적으로 수신부는 정상 시점보다

빠른 시점을 기준으로 수신 시점을 측정하기 때문에 단축된 거리 값이 산출되는 오류를 범할 수 있다.

[0004] 일 예로, 공격자가 STS 필드에 대해 약한 세기로 preamble 및 SFD 필드(Start of Frame Delimiter)를 전송하며, STS 필드는 강한 세기로 신호를 주입하여, 실제 상용 제품에 대한 단축 공격을 시도할 수 있다. 즉, 상술한 필드 별 세기 조절을 통해, 공격자는 10m 거리에 위치한 기기간의 거리를 2m로 위조할 수 있다. 상술한 바와 같이, 상호상관 기반의 STS 검증은 기존의 메시지 인증 코드 (message authentication code, MAC)에서 수행하는 비트 단위의 무결성 검증 방식과 달리, 수신된 STS 필드 (4,096비트)와 로컬 템플릿 (4,096비트)간의 상호 상관 연산을 통해 검증이 이루어진다. 이러한 환경은 공격자로 하여금 4,096비트에 대한 정확한 정보를 모르더라도 일정수준 이상의 상호 상관 출력을 달성할 경우, 성공적으로 fake leading edge를 생성할 수 있게 만드는 security hole을 발생시킨다. 이는 HRP UWB 통신을 사용하는 디지털키 기반의 스마트키 시스템에서 자동차가 원거리에 있는 스마트 키를 근처에 있다고 인식하도록 속여 차량을 절도할 수 있는 기회를 제공할 수 있음을 의미한다.

발명의 내용

해결하려는 과제

[0005] 상술한 일련의 기술 환경 예시와 관련하여, 본 발명은, 기존 취약한 STS 검증 방식을 강화하여 세밀한 STS 검증과 거리 측정 기능을 동시에 제공할 수 있는, 차량을 위한 개선된 보안 기능 제공 방법과, 이를 지원하는 컴퓨팅 시스템 및 차량을 제공함에 있다.

[0006] 또한, 본 발명은 세밀한 STS 검증으로 인한 거리측정 성능의 저하를 최소화 시키는 동시에 기존보다 향상된 보안성을 제공할 수 있는, 차량을 위한 개선된 보안 기능 제공 방법과, 이를 지원하는 컴퓨팅 시스템 및 차량을 제공함에 있다.

[0007] 또한, 본 발명은 현재 시장에서 유통되는 UWB 칩 내부의 digital signal processor (DSP) 내에서 간단한 소프트웨어 변형만을 통해 용이한 기술 구현을 제공할 수 있는 차량을 위한 개선된 보안 기능 제공 방법과, 이를 지원하는 컴퓨팅 시스템 및 차량을 제공함에 있다.

[0008] 본 발명의 기술적 과제들은 이상에서 언급한 기술적 과제들로 제한되지 않으며, 언급되지 않은 또 다른 기술적 과제들은 아래의 기재들로부터 당업자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0009] 본 발명의 실시예에 따른 개선된 보안 기능을 제공하는 차량은, 차량 안테나부, 상기 차량 안테나부를 통해 수신된 신호의 처리를 수행하는 프로세서 및 상기 프로세서 운용을 위한 적어도 하나의 명령어를 저장하는 저장부를 포함하고, 상기 프로세서는, 상기 차량 안테나부를 통해 차량 제어 신호를 수신하고, 상기 차량 제어 신호 중 STS 필드(Scrambled Timestamp Sequence field)를 추출하고, 추출된 STS 필드를 사전 정의된 일정 길이의 서브 필드들로 분할하고, 상기 분할된 서브 필드들과 상기 저장부에 사전 저장된 서브 템플릿들 각각을 상호 상관 연산하고, 상기 상호 상관 연산 결과들로부터 상기 차량 제어 신호의 수신 시점들을 추출하고, 상기 수신 시점들을 기반으로 상기 수신된 차량 제어 신호의 정상 여부를 판단하도록 설정될 수 있다.

[0010] 일 실시 예에 따른, 상기 프로세서는 상기 상호 상관 연산 결과들 내에서 상기 수신 시점들의 분포 위치에 대한 일관성을 기반으로 상기 차량 제어 신호의 정상 여부를 판단하도록 설정될 수 있다.

[0011] 일 실시 예에 따른, 상기 프로세서는 상기 저장부에 사전 저장된 로컬 템플릿을 상기 분할된 서브 필드의 길이에 대응하여 복수개의 서브 템플릿들로 분할하도록 설정될 수 있다.

[0012] 일 실시 예에 따른, 상기 프로세서는 상기 수신 시점들의 추출과 관련하여 상기 상호 상관 연산 결과에 해당하는 주파수 그래프에서, 최대 피크를 결정하고, 상기 최대 피크로부터 일정 길이 이내에 위치한 피크 후보들을 산출하고, 산출된 피크 후보들 중 상기 최대 피크로부터 가장 멀리 떨어진 피크를 상기 수신 시점으로 산출하도록 설정될 수 있다.

[0013] 일 실시 예에 따른, 상기 프로세서는 상기 수신 시점들의 분포 위치 차이에 대한 누적 오프셋 값을 산출하고, 상기 누적 오프셋 값이 사전 정의된 파라미터 값을 초과하는 경우 상기 차량 제어 신호를 비정상 신호에 해당하는 공격 신호로 판단하도록 설정될 수 있다.

[0014] 일 실시 예에 따른, 상기 프로세서는 상기 차량 제어 신호가 비정상 신호인 경우 상기 수신된 차량 제어 신호를

무효화 처리하도록 설정될 수 있다.

[0015] 일 실시 예에 따른, 상기 프로세서는 상기 차량 제어 신호가 비정상 신호인 경우 상기 차량 제어 신호의 수신 시각, 수신 횟수, 수신 위치 중 적어도 하나를 사전 정의된 장치에 전송하도록 설정될 수 있다.

[0016] 일 실시 예에 따른, 상기 프로세서는 상기 수신 시점들의 분포 위치 차이에 대한 누적 오프셋 값을 산출하고, 상기 누적 오프셋 값이 사전 정의된 파라미터 값 이하인 경우 상기 차량 제어 신호를 정상 신호로 판단하도록 설정될 수 있다.

[0017] 일 실시 예에 따른, 상기 프로세서는 상기 차량 제어 신호가 정상 신호인 경우, 수신된 차량 제어 신호에 대응하여 상기 차량의 도어락(door-lock)을 해제하거나, 상기 차량의 시동을 턴-온하거나, 상기 차량의 공기 순환 장치를 턴-온하도록 설정될 수 있다.

[0018] 본 발명의 실시 예에 따른 개선된 보안 기능을 제공하는 차량의 운용 방법은, 차량의 프로세서가, 상기 차량의 안테나부를 통해 차량 제어 신호를 수신하는 단계, 상기 차량 제어 신호 중 STS 필드(Scrambled Timestamp Sequence field)를 추출하는 단계, 상기 추출된 STS 필드를 사전 정의된 일정 길이의 서브 필드들로 분할하는 단계, 상기 분할된 서브 필드들과 상기 저장부에 사전 저장된 서브 템플릿들 각각을 상호 상관 연산하는 단계, 상기 상호 상관 연산 결과들로부터 상기 차량 제어 신호의 수신 시점들을 추출하는 단계, 상기 수신 시점들을 기반으로 상기 수신된 차량 제어 신호의 정상 여부를 판단하는 단계를 포함할 수 있다.

[0019] 일 실시 예에 따른, 상기 판단하는 단계는, 상기 상호 상관 연산 결과들 내에서 상기 수신 시점들의 분포 위치에 대한 일관성을 기반으로 상기 차량 제어 신호의 정상 여부를 판단하는 단계를 포함할 수 있다.

[0020] 일 실시 예에 따른, 상기 방법은, 상기 저장부에 사전 저장된 로컬 템플릿을 상기 분할된 서브 필드의 길이에 대응하여 복수개의 서브 템플릿들로 분할하는 단계를 더 포함할 수 있다.

[0021] 일 실시 예에 따른, 상기 수신 시점들을 추출하는 단계는, 상기 상호 상관 연산 결과에 해당하는 주파수 그래프에서, 최대 피크를 결정하는 단계, 상기 최대 피크로부터 일정 길이 이내에 위치한 피크 후보들을 산출하는 단계, 상기 산출된 피크 후보들 중 상기 최대 피크로부터 가장 멀리 떨어진 피크를 상기 수신 시점으로 산출하는 단계를 포함할 수 있다.

[0022] 일 실시 예에 따른, 상기 판단하는 단계는, 상기 수신 시점들의 분포 위치 차이에 대한 누적 오프셋 값을 산출하는 단계, 상기 누적 오프셋 값이 사전 정의된 파라미터 값을 초과하는 경우 상기 차량 제어 신호를 비정상 신호에 해당하는 공격 신호로 판단하는 단계를 포함할 수 있다.

[0023] 일 실시 예에 따른, 상기 방법은, 상기 차량 제어 신호가 비정상 신호인 경우 상기 수신된 차량 제어 신호를 무효화 처리하는 단계를 더 포함할 수 있다.

[0024] 일 실시 예에 따른, 상기 방법은, 상기 차량 제어 신호가 비정상 신호인 경우 상기 차량 제어 신호의 수신 시각, 수신 횟수, 수신 위치 중 적어도 하나를 사전 정의된 장치에 전송하는 단계를 더 포함할 수 있다.

[0025] 일 실시 예에 따른, 상기 판단하는 단계는, 상기 수신 시점들의 분포 위치 차이에 대한 누적 오프셋 값을 산출하는 단계, 상기 누적 오프셋 값이 사전 정의된 파라미터 값 이하인 경우 상기 차량 제어 신호를 정상 신호로 판단하는 단계를 포함할 수 있다.

[0026] 일 실시 예에 따른, 상기 방법은, 상기 차량 제어 신호가 정상 신호인 경우, 수신된 차량 제어 신호에 대응하여 상기 차량의 도어락을 해제하거나, 상기 차량의 시동을 턴-온하거나, 상기 차량의 공기 순환 장치를 턴-온하도록 제어하는 단계를 더 포함할 수 있다.

[0027] 본 발명의 실시 예에 따른 개선된 보안 기능을 제공하는 차량에 적용되는 컴퓨팅 시스템은, 차량 운행을 지원하는 프로세서 및 상기 프로세서 운용을 위한 적어도 하나의 명령어를 저장하는 저장부를 포함하고, 상기 저장부에 저장된 적어도 하나의 명령어는, 상기 프로세서가, 상기 차량의 안테나부를 통해 차량 제어 신호를 수신하는 동작, 상기 차량 제어 신호 중 STS 필드(Scrambled Timestamp Sequence field)를 추출하는 동작, 상기 추출된 STS 필드를 사전 정의된 일정 길이의 서브 필드들로 분할하는 동작, 상기 분할된 서브 필드들과 상기 저장부에 사전 저장된 서브 템플릿들 각각을 상호 상관 연산하는 동작, 상기 상호 상관 연산 결과들로부터 상기 차량 제어 신호의 수신 시점들을 추출하는 동작, 상기 상호 상관 연산 결과들 내에서 상기 수신 시점들의 분포 위치들의 일관성이 사전 정의된 기준 값 이상인 경우 상기 차량 제어 신호를 정상 신호로 판단하고, 상기 일관성이 사전 정의된 기준 값 미만 경우 상기 차량 제어 신호를 비정상 신호로 판단하는 동작을 수행하도록 설정될 수 있

다.

[0028] 일 실시 예에 따르면, 상기 적어도 하나의 명령어는, 상기 프로세서가, 상기 차량 제어 신호가 비정상 신호인 경우 상기 수신된 차량 제어 신호를 무효화 처리하는 동작, 상기 차량 제어 신호가 정상 신호인 경우, 수신된 차량 제어 신호에 대응하여 상기 차량의 도어락을 해제하거나, 상기 차량의 시동을 턴-온하거나, 상기 차량의 공기 순환 장치를 턴-온하도록 제어하는 동작을 수행하도록 설정될 수 있다.

발명의 효과

[0029] 본 발명은 차세대 스마트키 시스템의 보안성 강화를 제공할 수 있다.

[0030] 또한, 본 발명은 차세대 스마트키 시스템 (디지털키 표준)에 탑재되고 있는 HRP UWB에 대한 거리 단축(위조) 공격을 방지할 수 있다.

[0031] 또한, 본 발명을 통해 차세대 스마트키 시스템에 대한 공격 가능성을 원천적으로 차단할 수 있을 뿐만 아니라, HRP UWB가 사용되는 (측위 정보가 사용되는) 다양한 어플리케이션 (실내 로봇, 무인 이동체 등)에 활용 가능성을 제공할 수 있다.

[0032] 이 외에, 본 문서를 통해 직접적 또는 간접적으로 파악되는 다양한 효과들이 제공될 수 있다.

도면의 간단한 설명

[0033] 도 1은 본 발명의 일 실시 예에 따른 보안 기능 개선을 지원하는 차량 운용 환경의 한 예를 나타낸 도면이다.

도 2는 본 발명의 실시 예에 따른 차량 및 디지털 키 장치의 각 구성들의 한 예를 나타낸 도면이다.

도 3은 본 발명의 실시 예에 따른 차량 제어 장치 구성 중 일부 구성의 세부 구조의 한 예를 나타낸 도면이다.

도 4는 본 발명의 실시 예에 따른 STS 신호 처리에서의 측정부 운용과 관련한 설명을 위한 도면이다.

도 5는 본 발명의 실시 예에 따른 차량 제어 장치의 신호 처리와 관련한 신호들의 한 예를 나타낸 도면이다.

도 6은 본 발명의 실시 예에 따른 정상 상태에서의 리딩 에지를 나타낸 도면이다.

도 7은 본 발명의 실시 예에 따른 비정상 상태에서 리딩 에지를 나타낸 도면이다.

도 8은 본 발명의 실시 예에 따른 차량을 위한 개선된 보안 기능 제공 방법의 한 예를 나타낸 도면이다.

도 9는 본 발명의 일 실시 예에 따른 컴퓨팅 시스템을 도시한다.

발명을 실시하기 위한 구체적인 내용

[0034] 이하, 본 발명의 일부 실시예들을 예시적인 도면을 통해 상세하게 설명한다. 각 도면의 구성요소들에 참조부호를 부가함에 있어서, 동일한 구성요소들에 대해서는 비록 다른 도면상에 표시되더라도 가능한 한 동일한 부호를 가지도록 하고 있음에 유의해야 한다. 또한, 본 발명의 실시예를 설명함에 있어, 관련된 공지 구성 또는 기능에 대한 구체적인 설명이 본 발명의 실시예에 대한 이해를 방해한다고 판단되는 경우에는 그 상세한 설명은 생략한다.

[0035] 본 발명의 실시예의 구성 요소를 설명하는 데 있어서, 제 1, 제 2, A, B, (a), (b) 등의 용어를 사용할 수 있다. 이러한 용어는 그 구성 요소를 다른 구성 요소와 구별하기 위한 것일 뿐, 그 용어에 의해 해당 구성 요소의 본질이나 차례 또는 순서 등이 한정되지 않는다. 또한, 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 가진 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0036] 이하, 도 1 내지 도 9를 참조하여, 본 발명의 실시예들을 구체적으로 설명하기로 한다.

[0037] 도 1은 본 발명의 일 실시 예에 따른 보안 기능 개선을 지원하는 차량 운용 환경의 한 예를 나타낸 도면이며, 도 2는 본 발명의 실시 예에 따른 차량 및 디지털 키 장치의 각 구성들의 한 예를 나타낸 도면이다.

[0038] 도 1 및 도 2를 참조하면, 본 발명의 실시 예에 따른 차량 운용 환경(10)은 차량(100) 및 디지털 키 장치(300)

를 포함할 수 있다.

[0039] 상기 디지털 키 장치(300)는 차량 제어와 관련하여 사전 정의된 디지털 키 신호를 포함하는 차량 제어 신호를 사용자 입력에 따라 생성하고, 생성된 차량 제어 신호를 무선 방식으로 상기 차량 제어 장치(200)에 전송할 수 있다. 이와 관련하여, 상기 디지털 키 장치(300)는 디지털 키 안테나부(310) 및 디지털 키 몸체부(320)를 포함할 수 있다. 상기 디지털 키 몸체부(320)는 차량 제어 신호를 생성할 수 있는 회로, 회로에 전력을 공급할 수 있는 배터리, 상기 회로 및 배터리를 감싸는 케이스를 포함할 수 있다. 추가로, 디지털 키 몸체부(320)는 사용자 입력을 발생시키기 위한 적어도 하나의 물리 키 버튼 또는 터치 키를 가지는 입력부를 포함할 수 있다. 상기 디지털 키 몸체부(320)에 마련된 입력부 조작에 따라 차량 제어 신호가 생성되면, 사전 정의된 무선 통신 방식(예: UWB 방식)을 기반으로 차량 제어 신호를 디지털 키 안테나부(310)를 통해 송출할 수 있다.

[0040] 상기 차량(100)은 운전자 및 동승자 중 적어도 한명이 탑승할 수 있는 차체, 차체의 이동을 위한 복수개의 바퀴들, 상기 복수의 바퀴들의 구동을 위한 동력을 생성할 수 있는 구동 장치, 상기 구동 장치가 생성한 동력을 상기 복수의 바퀴들에 전달하는 적어도 하나의 샤프트와 기어들, 상기 차량(100)의 조향을 위한 조향 장치, 상기 차량(100)의 속도 조절을 위한 브레이크 시스템을 포함할 수 있다. 특히, 상기 차량(100)의 운행을 지원하면서 본 발명의 개선된 보안 기능 지원을 위한 차량 제어 장치(200)(또는 차량용 컴퓨팅 장치, 컴퓨팅 시스템, 제어 장치, 모터 제어 유닛, 차량 제어 장치)를 포함할 수 있다. 상기 차량 제어 장치(200)는 상기 차량(100)의 일측에 내장된 형태로 배치될 수 있다. 상기 차량 제어 장치(200)는 차량(100)의 운행 지원과 관련하여 적어도 하나의 센서를 포함하고, 차량(100)의 주행에 따른 센싱 정보를 수집하여 차량(100) 주행에 필요한 제어를 수행할 수 있다. 일 예로, 상기 차량 제어 장치(200)는 차량(100)이 정지된 이후 시동이 턴-오프될 경우, 상기 디지털 키 장치(300)와의 통신을 위하여 통신 회로를 대기 상태로 유지할 수 있다. 상기 차량 제어 장치(200)는 상기 디지털 키 장치(300)로부터 전송된 차량 제어 신호를 수신하면, 수신된 차량 제어 신호가 사전 정의된 규칙에 맞는지 확인하고, 사전 정의된 규칙에 맞는 경우, 차량(100)의 램프 또는 경적 장치, 차량(100)의 사이드 미러 배치 상태 제어, 차량(100)의 도어락 해제 및 시동 턴-온, 차량(100) 내 내기 순환, 차량(100) 내 온도 조절 중 적어도 하나를 자동으로 제어할 수 있다. 상기 차량 제어 장치(200)는 디지털 키 장치(300)로부터 수신된 차량 제어 신호가 사전 정의된 규칙에 맞지 않는 경우, 별도의 추가적인 동작을 수행하지 않고 현재 상태(예: 시동 턴-오프 상태)를 유지할 수 있다. 추가적으로 상기 차량 제어 장치(200)는 차량 제어 신호를 수신한 시각 및 수신 횟수, 수신 위치 등에 대한 정보를 수집하고, 수집된 정보를 저장부에 저장하거나, 디스플레이에 출력하거나 또는 사전 지정된 사용자 단말에 전송하도록 제어할 수 있다.

[0041] 상술한 동작 지원을 위하여 상기 차량 제어 장치(200)는 차량 안테나부(210), 전단부(211), ADC(212)(analog to digital converter), DSP(220)(digital signal processor), MCU(240)(motor control unit), 저장부(230)를 포함할 수 있다. 상기 차량 제어 장치(200)의 구성 중 상기 차량 안테나부(210)와 상기 DSP(220)(또는 프로세서), 저장부(230)를 제외하고 나머지 구성은 생략되거나 또는 차량(100)의 다른 장치에 배치될 수도 있다.

[0042] 상기 차량 안테나부(210)는 상기 디지털 키 장치(300)로부터 송출된 차량 제어 신호를 수신할 수 있도록 마련된 제1 안테나부를 포함할 수 있다. 또한, 상기 차량 안테나부(210)는 사전 정의된 메시지에 대응하는 무선 신호를 사용자 단말에 전송할 수 있도록 마련된 제2 안테나부를 더 포함할 수 있다. 상기 제2 안테나부는 사용자 단말에 메시지 송신 기능이 제거된 경우, 제외될 수 있다.

[0043] 상기 전단부(211)는 상기 차량 안테나부(210)와 상기 ADC(212) 사이에 배치되는 다양한 통신 회로 소자를 포함할 수 있다. 일 예로 상기 전단부(211)는 수신된 신호의 노이즈를 필터링하는 필터, 필터링된 신호를 증폭하는 증폭기, 신호를 믹싱하는 믹서 등을 포함할 수 있다. 또한, 상기 전단부(211)는 상기 차량 안테나부(210)의 임피던스 매칭을 위한 매칭 소자를 포함할 수 있다. 이러한 전단부(211)는 상기 차량 안테나부(210)가 수신한 아날로그 형태의 차량 제어 신호를 ADC(212)에 전달할 수 있다.

[0044] 상기 ADC(212)는 상기 전단부(211) 및 DSP(220) 사이에 배치되어 전단부(211)가 전달한 아날로그 신호를 디지털 신호로 변환한 후 DSP(220)에 전달할 수 있다. 예컨대, 상기 ADC(212)는 아날로그 형태의 차량 제어 신호를 디지털 형태의 차량 제어 신호로 변환할 수 있다. 추가로, 상기 ADC(212)는 DSP(220) 요청에 대응하여 디지털 신호를 아날로그 신호로 변환하는 구성(예: digital to analog converter, DAC)를 더 포함할 수도 있다.

[0045] 상기 DSP(220)는 상기 ADC(212)와 MCU(240)와 신호를 교환할 수 있도록 배치되고, 본 발명의 실시 예에 따른 차량 제어 신호에 대한 처리를 수행할 수 있다. 이와 관련하여 상기 DSP(220)는 ADC(212)로부터 디지털 형태의 차량 제어 신호를 수신하면, 수신된 신호에 대한 필터링을 디지털 필터(222)를 이용하여 처리할 수 있다. 이 과정

에서, 왜곡이나 감쇄된 신호가 있는 신호 복구부(223)를 이용하여 신호 복구를 수행할 수 있다. 복구된 차량 제어 신호에 대하여 상기 DSP(220)는 신호 처리부(221)를 이용하여 해당 차량 제어 신호가 정상 신호인지 또는 비정상 신호인지 판단할 수 있다. 신호 처리부(221)는 정상 신호로 판단되면, 차량 제어 신호를 MCU(240)에 전달할 수 있다. 상기 신호 처리부(221)는 비정상 신호로 판단되면, 차량 제어 신호를 폐기할 수 있다. 추가로 상기 신호 처리부(221)는 비정상 신호 수신 상황에 대한 리포트를 MCU(240)에 전달할 수 있다. 한편, 상술한 설명에서는 신호 처리부(221)가 DSP(220)의 세부 구성으로 설명하였으나, 별도의 신호 처리부(221)를 대체하여 DSP(220)가 신호 처리부의 역할을 수행할 수도 있다. 상기 DSP(220) 및 신호 처리부(221)는 적어도 하나의 프로세서로 구성될 수 있으며, 이에 따라, 프로세서로 명명될 수도 있다.

[0046] 상기 MCU(240)는 상기 DSP(220)로부터 전달된 차량 제어 신호에 대응하여 차량(100) 제어를 수행할 수 있다. 예컨대, 상기 MCU(240)는 전달된 차량 제어 신호가 도어 오픈인 경우, 차량(100)을 제어하여 차량(100)의 도어락을 해제할 수 있다. 또한, 상기 MCU(240)는 차량 제어 신호가 차량(100)의 백도어를 해제한 후, 백도어 개방을 요청하는 신호인 경우, 차량 제어 신호에 따라 백도어 해제 및 개방을 제어할 수 있다. 또는, 상기 MCU(240)는 차량 제어 신호가 위치 알림을 요청하는 신호인 경우, 차량 제어 신호에 대응하여 차량(100)의 램프 점멸 또는 지정된 경적을 출력하도록 제어할 수 있다. 추가로, 상기 MCU(240)는 전달된 차량 제어 신호의 종류에 따라 사전 정의된 차량(100) 제어 기능을 수행하도록 제어할 수 있다.

[0047] 상기 저장부(230)는 상기 DSP(220) 운용에 필요한 다양한 데이터, 알고리즘 또는 프로그램을 저장할 수 있다. 일 예로서, 상기 저장부(230)는 상기 차량 제어 신호가 정상인지 또는 비정상인지를 확인하기 위한 기준 신호(또는 참조 신호)를 저장하고, DSP(220) 요청에 대응하여 DSP(220)에 전달할 수 있다. 일 예로서, 상기 저장부(230)는 기준 신호로서 로컬 템플릿을 저장할 수 있다. 또한, 상기 저장부(230)는 차량 안테나부(210)를 통해 수신된 차량 제어 신호의 적어도 일부를 포함하는 신호 샘플을 임시 또는 반영구적으로 저장할 수 있다.

[0048] 도 3은 본 발명의 실시 예에 따른 차량 제어 장치 구성 중 일부 구성의 세부 구조의 한 예를 나타낸 도면이며, 도 4는 본 발명의 실시 예에 따른 STS 신호 처리에서의 측정부 운용과 관련한 설명을 위한 도면이다.

[0049] 도 3을 참조하면, 상기 차량 제어 장치(200)의 적어도 일부 구성을 나타낸 것이다. 예컨대, 차량 제어 장치(200)는 적어도 신호 처리부(221)(또는 적어도 하나의 프로세서) 및 저장부(230)를 포함할 수 있다. 상기 저장부(230)는 신호 샘플(232)을 저장할 수 있다. 상술한 차량 제어 장치(200)의 적어도 일부는 UWB 기기로 구현될 수 있다. 여기서, 신호 처리부(221)가 수신하는 UWB 신호의 패킷 구조는 프리앰블, SFD(Start of Frame Delimiter), physical layer header (PHR), 페이로드(payload) 영역을 포함할 수 있다. 상기 UWB 기기는 DSP(220)를 포함하고, 상기 DSP(220)는 수신된 STS (Received STS field) 에 대한 검증 및 수신 시점 (time-of-arrival, ToA 또는 toa) 측정하고, 유효성을 검증할 수 있는 신호 처리부(221)를 포함할 수 있다. 상기 신호 처리부(221)는 수신된 STS (Received STS field)와 로컬 템플릿 (Local template)을 여러 개의 서브 필드(sub-field) 및 서브 템플릿 (sub-template)으로 분할하여, 개별 상호 상관 연산 및 back-search 를 통해 신호의 수신 시점 (time-of-arrival, ToA)를 측정하고, 여러 개의 ToA 측정값의 일관성 검증 (consistency verification)을 수행하여 수신된 STS의 유효성을 검증할 수 있다. 이를 위하여, 상기 신호 처리부(221)는 예컨대, 수신 제어부(221a) , 생성부(221b), 연산부(221c), 측정부(221d) 및 검증부(221e)를 포함할 수 있다.

[0050] 상기 수신 제어부(221a)는 상기 차량 안테나부(210)를 통해 차량 제어 신호를 수신할 수 있는 상태를 제어할 수 있다. 예컨대, 상기 수신 제어부(221a)는 차량(100)의 시동이 턴-온 상태일 때는 차량 제어 신호 수신과 관련한 장치 또는 회로들의 전원을 턴-오프하도록 제어하고, 차량(100)의 시동이 턴-오프된 상태일 때 차량 안테나부(210)를 통해 차량 제어 신호를 수신할 수 있도록 전원 공급 상태를 제어할 수 있다. 상기 수신 제어부(221a)는 상기 차량 안테나부(210)를 통해 차량 제어 신호가 수신되면, 수신된 차량 제어 신호를 신호 샘플(232)로서 저장부(230)에 저장하도록 제어할 수 있다.

[0051] 상기 생성부(221b)는 저장부(230)에 있는 신호 샘플(232) 및 사전 저장된 로컬 템플릿(231)을 획득하고, 획득된 신호 샘플(232) 및 로컬 템플릿(231)을 사전 정의된 길이로 분할하여 복수의 서브 필드(sub-field), 복수의 서브 템플릿 (sub-template)을 생성할 수 있다. 상기 생성부(221b)는 생성된 복수의 서브 필드 및 복수의 서브 템플릿을 연산부(221c)에 전달할 수 있다.

[0052] 상기 연산부(221c)는 상기 복수의 서브 필드들 및 복수의 서브 템플릿들 각각에 대하여 개별 서브 필드($s_i[\tau]$)와 서브 템플릿(g_{ioc}^{i})을 입력으로 받을 수 있다. 상기 연산부(221c)는 입력받은 개별 서브 필드와 서브 템플릿에 대

하여 다음 수학식 1에서 정의한 상호 상관 연산을 수행하여 $\mathrm{CIR}_i[\tau]$를 산출할 수 있다.

수학식 1

[0053] $$\mathrm{CIR}_i[\tau] = s_i[c_correlation]g^i_{\mathrm{loc}}[\tau] = \sum_{n=0}^{|g^i_{\mathrm{loc}}|} \overline{g^i_{\mathrm{loc}}[n]} \cdot s[n+\tau]$$

[0054] 상기 CIR을 산출하는 수식에서, $[c_correlation]$는 상호 상관(cross correlation) 연산을 의미하며, $[\tau]$는 시간을 의미할 수 있으며, n은 0을 포함하는 자연수일 수 있다.

[0055] 상기 측정부(221d)는 연산부(221c)에서 산출된 개별 $\mathrm{CIR}_i[\tau]$를 이용하여 신호의 수신 시점 (toa_i)을 산출할 수 있다. 신호 수신 시점 (toa_i)의 측정은 기존의 역탐색(back-search) 알고리즘을 활용하여 수행할 수 있다. 구체적으로, 도 4에서, leading edge는 maximum peak로부터 W 길이만큼의 윈도우 내에 있는 Peak candidate을 산출하고, 산출된 Peak candidates 중 가장 작은 index를 가지는 (즉, maximum peak로부터 가장 멀리 떨어진) peak의 위치를 toa_i로 산출할 수 있다. P_{rms}는 피크 값들의 평균 전력(root-mean-square) 값일 수 있다.

[0056] 역탐색 알고리즘에 사용되는 파라미터는 일반적으로 역탐색 윈도우 W, maximum peak to earlier peak ratio (MPEP)와 peak to average power ratio (PAPR)이 있다. Maximum peak로부터 W 범위 내에 있는 peak들의 집합 P는 아래 수학식 2와 같이 나타낼 수 있다.

수학식 2

[0057] $$P = \{(\tau_0, p_0), (\tau_1, p_1), \ldots, (\tau_j, p_j), \ldots, (\tau_N, p_N)\}$$

[0058] τ_i는 i번째 peak의 index를 의미하며, p_i는 peak의 전력(power)을 나타낼 수 있다. 역탐색 알고리즘은 Peak들의 집합 중 maximum peak와의 전력차가 MPEP보다 작으면서, CIR_i의 평균 전력인 P_{rms}보다 PAPR만큼 큰 peak를 찾는다. 이를 수식으로 나타내면 아래 수학식 3과 같으며, 해당 peak의 index인 τ_i를 기준으로 toa_i를 측정할 수 있다.

수학식 3

[0059] $$toa_i = \tau_{le} = \min_{\tau_j}\left(\frac{P_{max}}{p_j} < \mathrm{MPEP} \bigwedge \frac{p_j}{P_{rms}} > PAPR\right)$$

[0060] 차량 제어 신호가 정상인 상황에서는 서브 필드(sub-field)와 서브 템플릿(sub-template)간의 cross-correlation 일정 위치에 maximum peak들이 존재할 수 있다. 비정상상황에서는 서브 필드와 서브 템플릿 간의 cross-correlation에서 개별 leading edge가 불규칙하게 존재하거나 또는, 정상범위에서 벗어나 불규칙한 위치에 존재할 수 있다.

[0061] 상기 검증부(221e)는 측정부(221d)에서 산출한 toa 정보들(신호 수신 시점들)을 분석하여 수신한 STS가 적법한 장치에서 전송되었는지 여부 (즉, 무결성)를 검증할 수 있다. 해당 검증은 일관성(consistency) 검증을 통해 수행 가능하며, 대표적으로는 누적 오프셋(offset accumulation)을 통해 일관성을 검증할 수 있다. 검증부(221e)가 수행하는 검증은 개별 toa와 사전에 정의된 탐지 파라미터인 μ, Γ^{acc} 등을 활용할 수 있으며, 누적 오프셋

값이 사전 정의된 탐지 파라미터 Γ^{acc}를 초과할 경우 이를 공격으로 탐지할 수 있다. 누적 오프셋 값이 사전 정의된 탐지 파라미터를 넘지 않는 경우, 검증부(221e)는 수신된 차량 제어 신호를 적법한 STS로 판단할 수 있다. 누적 오프셋은 아래 수학식 4를 통해 산출될 수 있다.

수학식 4

[0062] $$O_{acc} = \sum_{i=0}^{N_t} \tau_i - \mu$$

[0063] 위 수학식 3에서, O_{acc}는 누적 오프셋이며, N_t는 서브 템플릿(서브 필드)의 개수를 나타낼 수 있다. 공격으로 탐지된 경우, 수신된 STS 및 해당 프레임은 무효화 처리될 수 있다. 검증을 통과할 경우, 수신 제어부(221a)는 τ_i의 평균값(μ_τ)을 프레임의 수신시점으로 산출하여 거리 측정에 활용할 수 있다.

[0064] 상기 검증부(221e)는 앞서 설명한 바와 같이 개별 toa의 측정값들의 일관성을 검증하는 부분이며, 일관성 검증은 다양한 통계적 지표 혹은 기계학습 (machine learning) 기법을 이용하여 일관성을 수치화 할 수 있다. 일 예로서, 상기 검증부(221e)는 측정값들의 분산 (Variance)을 측정할 수 있으며, 따라서 검증부(221e)는 다양한 형태로 구현 가능하므로, 함수 $f(\cdot)$의 형태로 표현 가능하다.

[0065] 상술한 바와 같이, 본 발명의 실시 예에 따른 신호 처리부(221)는 차세대 스마트키 시스템 (디지털키 표준)에 탑재되고 있는 HRP UWB에 대한 거리 단축(위조) 공격을 방지할 수 있을 뿐만 아니라, HRP UWB가 사용되는 (측위 정보가 사용되는) 다양한 어플리케이션 (실내 로봇, 무인 이동체 등)에 활용할 수 있다.

[0066] 도 5는 본 발명의 실시 예에 따른 차량 제어 장치의 신호 처리와 관련한 신호들의 한 예를 나타낸 도면이며, 도 6은 본 발명의 실시 예에 따른 정상 상태에서의 리딩 에지를 나타낸 도면이고, 도 7은 본 발명의 실시 예에 따른 비정상 상태에서 리딩 에지를 나타낸 도면이다.

[0067] 먼저, 도 5를 참조하면, 차량 제어 장치(200)가 차량 안테나부(210)를 통해 차량 제어 신호를 수신하면, 신호 처리부(221)는 수신된 차량 제어 신호(또는 수신된 STS 신호(Received STS field))를 신호 샘플(232)로서 저장부(230)에 저장할 수 있다. 수신된 STS 신호(Received STS field)는 일 예로서, 도 5의 501 상태에서와 같은 형태가 될 수 있다. 한편, 상기 수신된 STS 신호(Received STS field)와 비교하기 위하여 저장부(230)에 저장된 로컬 템플릿(Local Template)은 501 상태에서와 같은 형태가 될 수 있다.

[0068] 상기 신호 처리부(221)의 생성부(221b)는 상술한 수신된 STS 신호(Received STS field)를 사전 정의된 일정 길이(예: 수신된 STS 신호를 복수개의 서브 필드로 나눌 수 있는 길이로서, 적어도 하나 이상의 리딩 에지를 포함하는 길이)로 분할하여 503 상태에서와 같이, 복수개의 서브 필드들(Received sub-fields) (Received sub-fields, STS`$_0$[t], STS`$_1$[t], ... STS`$_{N1-1}$[t])로 분할할 수 있다. 또한, 상기 생성부(221b)는 상술한 로컬 템플릿(Local Template)들을 사전 정의된 일정 길이로 분할하여 503 상태에서와 같이, 복수개의 서브 템플릿들(Local sub-templates) (Local sub-templates들, LT_0[t], LT_1[t], ... LT_{N1-1}[t])로 분할할 수 있다. 일 예로, 상기 각 서브 템플릿들의 길이와 상기 각 서브 필드들의 길이는 동일할 수 있다. 다른 예로서, 상기 생성부(221b)는 수신된 STS 신호의 길이에 따라 분할하는 서브 필드의 길이를 다르게 할 수 있다. 예컨대, 상기 수신된 STS 신호의 길이가 사전 정의된 기준 길이보다 긴 경우, 상기 생성부(221b)는 분할하는 서브 필드의 길이를 기준 보다 길게 하고, 수신된 STS 신호의 길이가 사전 정의된 기준 길이보다 짧은 경우 상기 생성부(221b)는 분할하는 서브 필들의 길이를 기준 보다 짧게 할 수 있다. 이에 대응하여, 상기 생성부(221b)는 수신된 STS 신호의 길이에 대응하여 로컬 템플릿을 분할하는 길이를 다르게 할 수 있다. 예컨대, 생성부(221b)는 상기 수신된 STS 신호의 길이가 사전 정의된 기준 길이보다 긴 경우, 분할하는 서브 템플릿의 길이를 기준 보다 길게 하고, 수신된 STS 신호의 길이가 사전 정의된 기준 길이보다 짧은 경우 상기 생성부(221b)는 분할하는 서브 템플릿의 길이를 기준 보다 짧게 할 수 있다. 또 다른 예로서, 상기 로컬 템플릿을 서브 템플릿들로 분할하는 과정에서, 서브 템플릿들의 길이는 고정될 수 있다. 이 경우 생성부(221b)는 서브 템플릿들의 개수에 맞추어, 상기 수신된 STS 신호의 분할 개수를 일치시킬 수 있다. 이에 따라, 수신된 STS 신호의 길이가 다른 경우, 생성부(221b)가

분할하는 서브 템플릿들의 개수는 동일하고 길이가 달라질 수 있다.

[0069] 상기 연산부(221c)는 CIR 값들을 산출할 수 있다. 예컨대, 상기 연산부(221c)는 신호 샘플(232)에 해당하는 수신된 STS 신호를 사전 정의된 일정 길이로 분할한 서브 필드들 각각과, 저장부(230)에 사전 저장된 로컬 템플릿을 사전 정의된 일정 길이로 분할한 서브 템플릿들 각각을 상호 상관 연산할 수 있다.

[0070] 상기 측정부(221d)는 상기 연산부(221c)가 상호 상관 연산한 값들에 대하여 toa 값들을 산출할 수 있다. 측정부(221d)는 역탐색 알고리즘을 적용하여, Peak들의 집합 중 maximum peak와의 전력차가 MPEP보다 작으면서, CIR_i의 평균 전력인 P_{rms} 보다 PAPR만큼 큰 peak를 찾는다(i는 0 ~ N_1-1).

[0071] 상기 검증부(221e)는 일관성 검증(Consistency Verification)을 수행하여, 현재 수신된 STS 신호가 정상 상태 신호(Valid ToA)인지 또는 비정상 상태 신호(Attack)인지 확인할 수 있다. 예컨대, 검증부(221e)는 505 상태에서 검출된 toa 값들의 분포 위치가 사전 정의된 일정 비율 이상으로 일관성을 나타내는 경우, 정상 상태 신호로 판단하고, 사전 정의된 일정 비율 미만의 일관성(또는 전체 toa 값들 중 일정 비율 이상이 서로 다른 분포 위치를 가지는 불규칙성)을 나타내는 경우 비정상 상태 신호로 판단할 수 있다.

[0072] 도 6을 참조하면, 정상 상태 신호는 서브 필드들과 서브 템플릿들의 상호 상관 관계에 해당하는 주파수 그래프 600a 내지 600c에 나타낸 바와 같이, 최대 피크들(maximum peak)에 해당하는 리딩 에지들(611, 613, 615)이 지정된 정상 범위들(601, 603, 605) 내에 위치함을 알 수 있다. 예컨대, 리딩 에지들(611, 613, 615)은 상호 상관 관계를 나타내는 주파수 그래프들의 후반부 영역에서 일관되게 검출된다. 한편, 상기 주파수 그래프 600a 내지 600c는 앞서 도 5에서 예시적으로 설명한 신호 샘플(232)(또는 수신된 STS 필드)을 복수개로 나눈 서브 필드들 각각과 저장부(230)에 사전 저장한 로컬 템플릿(231)을 복수개로 나눈 서브 템플릿들 각각을 상호 상관 연산을 수행한 값들에 해당할 수 있다. 특히, 도 6에서는 차량(100)에 사전 등록된 정상 사용자의 디지털 키 장치(300)로부터 송출된 차량 제어 신호에서 추출된 STS 필드를 사전 정의된 일정 길이의 서브 필드들로 구분한 것에 해당할 수 있다.

[0073] 도 7을 참조하면, 비정상 상태 신호는, 서브 필드들과 서브 템플릿들의 상호 상관 관계에 해당하는 주파수 그래프 700a 내지 700c에 나타낸 바와 같이, 최대 피크들(maximum peak)에 해당하는 리딩 에지들(711, 713, 715)이 지정된 정삼 범위들(701, 703, 705)을 벗어난 지점들에 위치함을 알 수 있다. 예컨대, 리딩 에지들(711, 713, 715)은 상호 상관 관계를 나타내는 주파수 그래프들의 초반 또는 중반부 영역에서 불규칙하게 검출된다. 상술한 바와 같이, 비정상 상태 신호는 리딩 에지들(711, 713, 715)이 정삼 범위들(701, 703, 705) 내에서 검출되지 않고 다른 부분들에서 불규칙하게 검출되는 것을 확인할 수 있다. 일 예로, 상기 주파수 그래프 700a 내지 700c는, 차량(100)에 사전 등록되지 않은 비정상 사용자의 디지털 키 장치로부터 송출된 차량 제어 신호를 차량(100)이 수신한 후, 수신된 차량 제어 신호에서 추출된 STS 필드를 사전 정의된 일정 길이의 서브 필드들로 구분한 것에 해당할 수 있다.

[0074] 도 8은 본 발명의 실시 예에 따른 차량을 위한 개선된 보안 기능 제공 방법의 한 예를 나타낸 도면이다.

[0075] 도 8을 참조하면, 본 발명의 개선된 보안 기능 제공 방법과 관련하여, 차량(100)의 프로세서(또는 신호 처리부(221))는 801 단계에서 신호 샘플을 수집할 수 있다. 이와 관련하여, 차량(100)의 프로세서는 디지털 키 장치(300)로부터 신호를 수신할 수 있는 신호 수신 대기 상태를 가질 수 있다. 상기 차량(100)의 프로세서는 디지털 키 장치(300)가 송출한 차량 제어 신호를 수신하면, 수신된 차량 제어 신호 중 STS field를 신호 샘플로 추출하여 저장부(230)에 임시 저장할 수 있다.

[0076] 803 단계에서, 차량(100)의 프로세서는 서브 필드들과 서브 템플릿들을 생성할 수 있다. 예컨대, 차량(100)의 프로세서는 저장부(230)에 저장된 STS field를 사전 정의된 일정 길이(STS field 길이보다는 짧은 길이)로 분할하여 복수개의 서브 필드들을 생성할 수 있다. 또한, 차량(100)의 프로세서는 저장부(230)에 미리 저장된 로컬 템플릿을 상기 분할된 복수개의 서브 필드들의 개수 또는 길이 중 적어도 하나에 따라 분할하여, 복수개의 서브 템플릿들을 생성할 수 있다.

[0077] 805 단계에서, 차량(100)의 프로세서는 CIR 값들을 산출할 수 있다. 예컨대, 차량(100)의 프로세서는 상기 각각의 서브 필드들과 각각의 서브 템플릿들에 대한 상호 상관 연산을 수행하여, 각각의 CIR 값들을 산출할 수 있다.

[0078] 807 단계에서, 차량(100)의 프로세서는 ToA 값들을 측정할 수 있다. 구체적으로, 차량(100)의 프로세서는 산출

된 CIR 값들 중 가장 높은 전력 값을 나타내는 최대 피크 지점(maximum peak)을 기준으로 평균 전력 값 이상이면서, 상기 최대 피크 지점으로부터 가장 먼 거리의 지점을 각각의 서브 필드들에 대한 ToA 값으로 측정할 수 있다.

[0079] 809 단계에서, 차량(100)의 프로세서는 각각의 서브 필드들의 ToA 값들의 일관성과 관련한 누적 오프셋 값(O_{acc})(또는 누적 ToA의 일관성 값)이 사전 정의된 기준 값(Γ^{acc})(또는 탐지 파리미터 값) 이상인지 확인할 수 있다. 누적 오프셋 값(O_{acc})이 사전 정의된 탐지 파라미터 Γ^{acc}를 초과하지 않을 경우(또는 탐지 파라미터 값 이하인 경우, 또는 ToA 값들의 분포의 일관성이 사전 정의된 기준 값 이상으로 일관성을 가지는 경우) 정상 상태 신호 수신으로 판단할 수 있다. 일 예로, 상기 차량(100)의 프로세서는 100개의 ToA 값들 중 9개의 ToA 값들이 제1 위치에 있고, 나머지 1개의 ToA 값들이 상기 제1 위치와 다른 위치에 있는 경우 정상 신호로 판단할 수 있다. 상기 정상 신호 판단 기준의 비율(예: 10%)은 수정될 수 있다. 정상 상태 신호로 판단된 경우, 상기 차량(100)의 프로세서는 811 단계에서 검증 패스로 처리한 후, 검증 패스에 따른 후처리를 수행할 수 있다. 예컨대, 상기 차량(100)의 프로세서는 상기 차량 제어 신호가 정상 신호인 경우, 수신된 차량 제어 신호에 대응하여 상기 차량의 도어락을 해제하거나, 차량(100)의 백도어를 개방하거나, 상기 차량(100)의 시동을 턴-온하거나, 상기 차량(100)의 공기 순환 장치를 턴-온하도록 설정될 수 있다. 또는, 상기 차량(100)의 프로세서는 사전 정의된 차량 관련 기능을 활성화하도록 설정될 수 있다. 추가로, 상기 차량(100)의 프로세서는 상기 수신 시점들을 기반으로 상기 차량 제어 신호를 송출한 디지털 키 장치(300)와의 거리를 판단하도록 설정될 수 있다. 또한, 상기 차량(100)의 프로세서는 산출된 거리 값을 지정된 장치(예: 사용자 단말)에 전송할 수 있다. 여기서, 상기 거리 판단 동작은 상기 차량 제어 신호가 정상 신호로 판단되는 경우 수행될 수도 있다.

[0080] 누적 오프셋 값(O_{acc})이 사전 정의된 탐지 파라미터 Γ^{acc}를 초과할 경우(또는, ToA 값들의 분포의 일관성이 사전 정의된 기준 값 미만인 경우, 또는 서브 필드들 전체 ToA 값들 중 지정 비율 이상의 ToA 값들의 제1 위치와 다른 위치에 분포한 ToA 값들이 기준치 이상인 경우) 이를 공격으로 판단할 수 있다. 일 예로, 상기 차량(100)의 프로세서는 100개의 ToA 값들 중 7개의 ToA 값들이 제1 위치에 있고, 나머지 3개의 ToA 값들이 상기 제1 위치와 다른 위치에 있는 경우 공격으로 판단할 수 있다. 상기 공격 신호 판단 기준(또는 비정상 신호 판단 기준)의 비율(예: 30%)은 수정될 수 있다. 상기 비정상 신호 수신 또는 공격 신호 수신으로 판단되면, 상기 차량(100)의 프로세서는 813 단계에서 수신 패킷 무효화 처리를 수행할 수 있다. 추가로, 상기 차량(100)의 프로세서는 상기 차량 제어 신호가 비정상 신호인 경우 상기 차량 제어 신호의 수신 시각, 수신 횟수, 수신 위치 중 적어도 하나를 사전 정의된 장치(예: 차량(100)에 배치된 디스플레이 장치, 또는 차량(100)의 통신 회로를 통해 연결될 수 있는 사용자 단말)에 전송할 수 있다.

[0081] 다음으로, 815 단계에서, 상기 차량(100)의 프로세서는 검증 종료와 관련한 이벤트 수신이 있는지 확인할 수 있다. 예컨대, 상기 차량(100)의 프로세서는 사전 정의된 일정 시간 동안 차량 제어 신호 수신이 없는 경우, 대기 상태로 전환하고, 차량 제어 신호를 수신할 수 있는 전력만을 유지하고, 슬립 상태로 천이할 수 있다. 차량 제어 신호가 지정된 시간 이내에 다시 수신되는 경우, 801 단계 이전으로 분기하여 이하 동작을 재수행할 수 있다.

[0082] 이상에서 설명한 바와 같이, 본 발명의 실시 예에 따른 차량의 개선된 보안 기능을 제공하는 방법은, 서브 템플릿들 및 서브 필드들을 생성함으로써, 전체 STS 필드에 대한 단일 검증이 아닌, 짧은 길이로 분할된 여러 개의 서브 필드들 및 서브 템플릿들 간의 상호상관 연산 결과를 기반으로 STS 필드를 검증하는 특징과, 검증 과정에서 서브 필드들 및 서브 템플릿들 간의 상호상관 결과로부터 측정된 toa값들의 일관성을 검증함과 동시에 거리 측정을 동시에 수행할 수 있도록 지원한다. 즉, 본 발명의 일 특징으로서, 프레임의 수신시점인 toa를 측정하는 시점에, 동시적으로 STS 필드의 무결성을 검증할 수 있도록 지원한다.

[0083] 도 9는 본 발명의 일 실시 예에 따른 컴퓨팅 시스템을 도시한다.

[0084] 도 9를 참조하면, 컴퓨팅 시스템(1000)은 버스(1200)를 통해 연결되는 적어도 하나의 프로세서(1100), 메모리(1300), 사용자 인터페이스 입력 장치(1400), 사용자 인터페이스 출력 장치(1500), 스토리지(1600), 및 네트워크 인터페이스(1700)를 포함할 수 있다. 도 9에서 설명하는 컴퓨팅 시스템(1000)은 앞서 도 1 내지 도 3에서 설명한 차량(100)에 적어도 일부가 적용될 수 있는 시스템이 될 수 있으며, 도 8에서 설명한 차량의 개선된 보안 기능 제공 방법을 수행할 수 있는 컴퓨팅 시스템이 될 수 있다.

[0085] 프로세서(1100)는 중앙 처리 장치(CPU) 또는 메모리(1300) 및/또는 스토리지(1600)에 저장된 명령어들에 대한 처리를 실행하는 반도체 장치일 수 있다. 메모리(1300) 및 스토리지(1600)는 다양한 종류의 휘발성 또는 불휘발성 저장 매체를 포함할 수 있다. 예를 들어, 메모리(1300)는 ROM(Read Only Memory) 및 RAM(Random Access Memory)을 포함할 수 있다.

[0086] 따라서, 본 명세서에 개시된 실시예들과 관련하여 설명된 방법 또는 알고리즘의 단계는 프로세서(1100)에 의해 실행되는 하드웨어, 소프트웨어 모듈, 또는 그 2 개의 결합으로 직접 구현될 수 있다. 소프트웨어 모듈은 RAM 메모리, 플래시 메모리, ROM 메모리, EPROM 메모리, EEPROM 메모리, 레지스터, 하드 디스크, 착탈형 디스크, CD-ROM과 같은 저장 매체(즉, 메모리(1300) 및/또는 스토리지(1600))에 상주할 수도 있다.

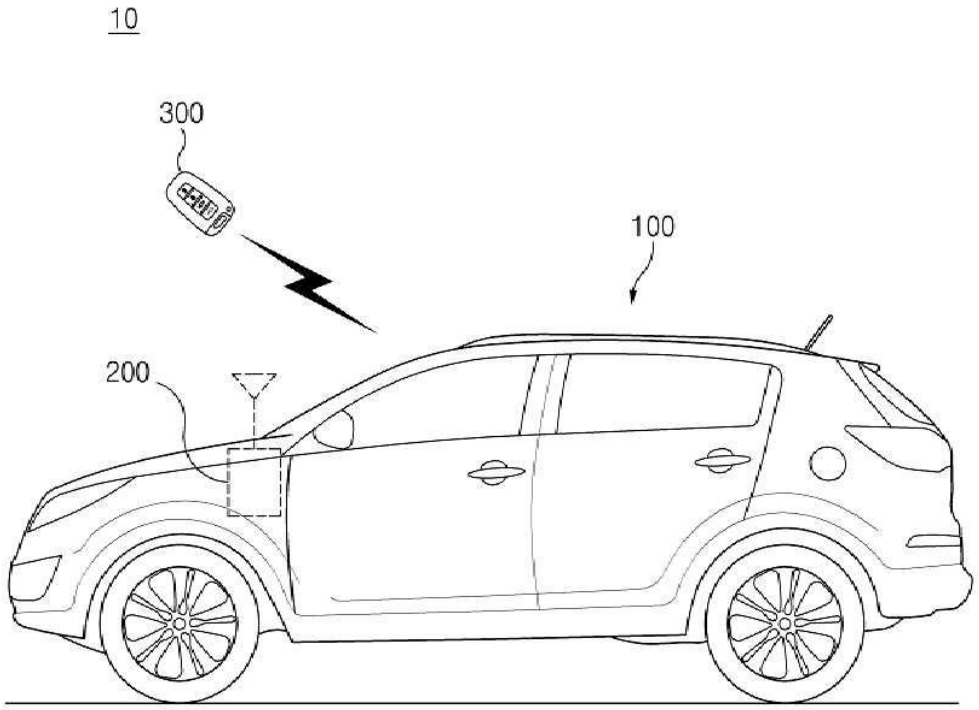
[0087] 예시적인 저장 매체는 프로세서(1100)에 커플링되며, 그 프로세서(1100)는 저장 매체로부터 정보를 판독할 수 있고 저장 매체에 정보를 기입할 수 있다. 다른 방법으로, 저장 매체는 프로세서(1100)와 일체형일 수도 있다. 프로세서 및 저장 매체는 주문형 집적회로(ASIC) 내에 상주할 수도 있다. ASIC는 사용자 단말기 내에 상주할 수도 있다. 다른 방법으로, 프로세서 및 저장 매체는 사용자 단말기 내에 개별 컴포넌트로서 상주할 수도 있다.

[0088] 이상의 설명은 본 발명의 기술 사상을 예시적으로 설명한 것에 불과한 것으로서, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자라면 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 다양한 수정 및 변형이 가능할 것이다.

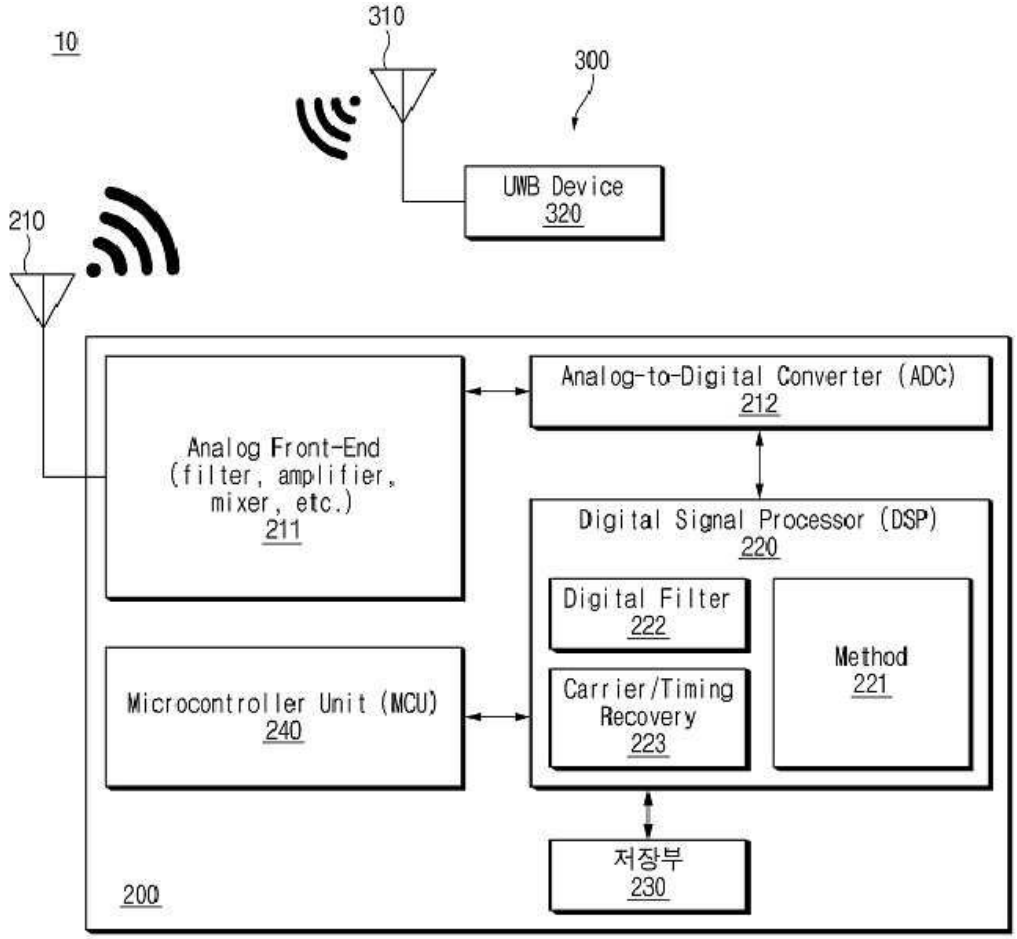
[0089] 따라서, 본 발명에 개시된 실시예들은 본 발명의 기술 사상을 한정하기 위한 것이 아니라 설명하기 위한 것이고, 이러한 실시예에 의하여 본 발명의 기술 사상의 범위가 한정되는 것은 아니다. 본 발명의 보호 범위는 아래의 청구범위에 의하여 해석되어야 하며, 그와 동등한 범위 내에 있는 모든 기술 사상은 본 발명의 권리범위에 포함되는 것으로 해석되어야 할 것이다.

도면

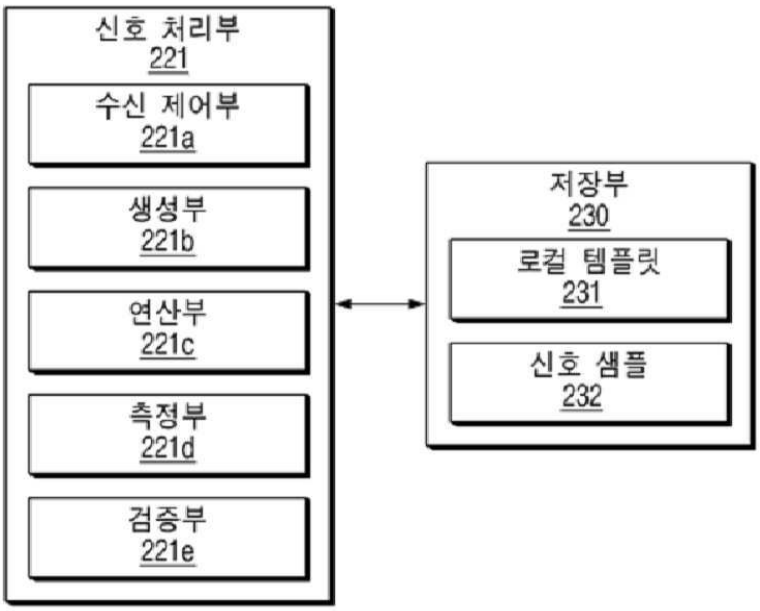
도면1



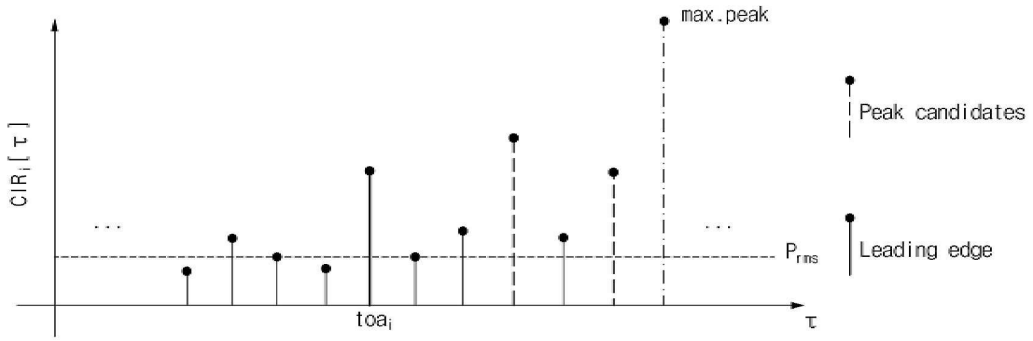
도면2


10
310
300
UWB Device
320
210
Analog Front-End
(filter, amplifier,
mixer, etc.)
211
Analog-to-Digital Converter (ADC)
212
Digital Signal Processor (DSP)
220
Digital Filter
222
Method
221
Carrier/Timing
Recovery
223
Microcontroller Unit (MCU)
240
저장부
230
200

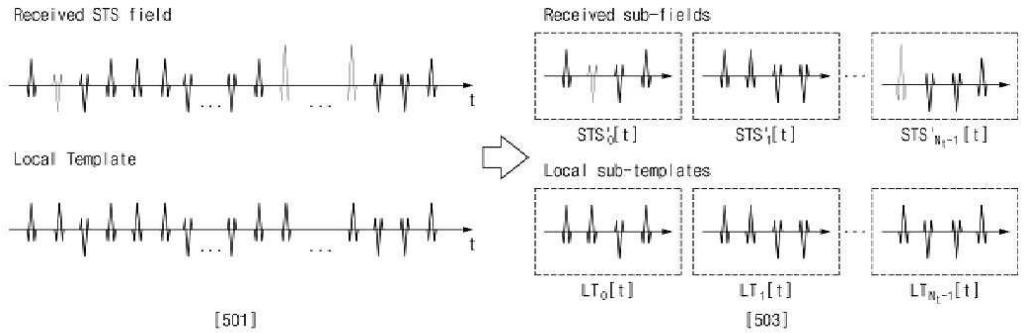
도면3

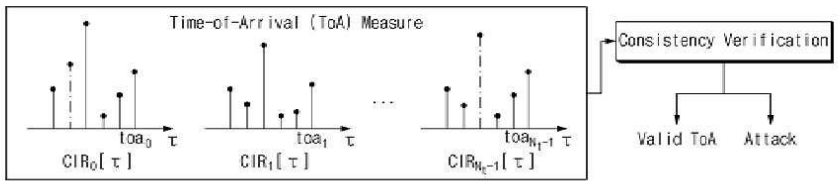

신호 처리부
221
수신 제어부
221a
생성부
221b
연산부
221c
측정부
221d
검증부
221e
저장부
230
로컬 템플릿
231
신호 샘플
232

도면4

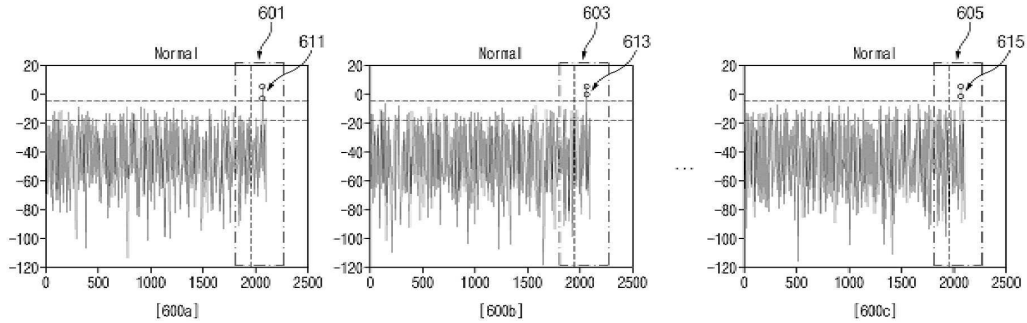

max.peak
Peak candidates
Leading edge
CIR_i[τ]
P_rms
toa_i
τ

도면5

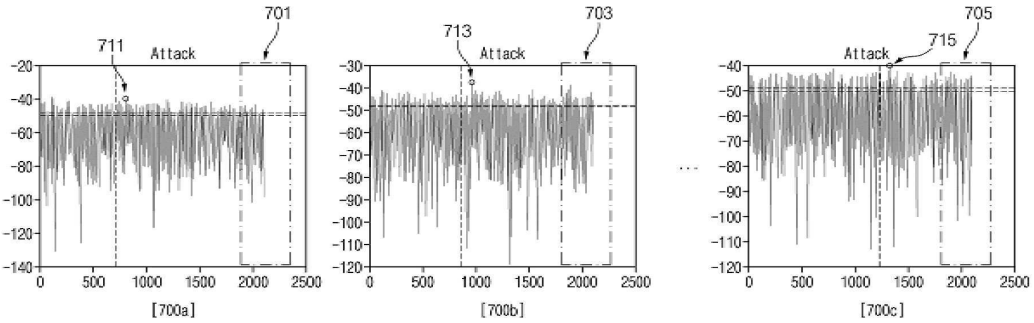

Received STS field
Received sub-fields
Local Template
Local sub-templates
[501]
[503]


Time-of-Arrival (ToA) Measure
Consistency Verification
Valid ToA
Attack
[505]

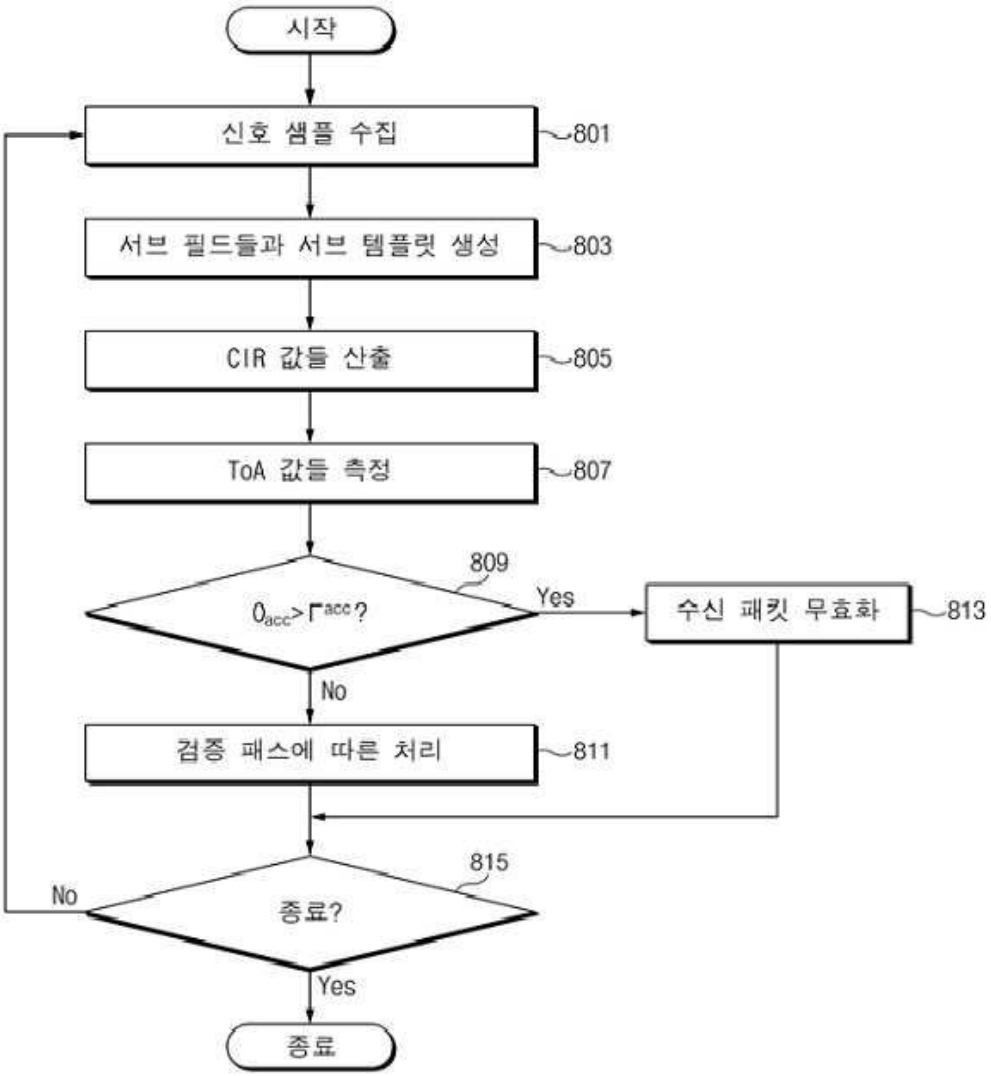
도면6


601
611
603
613
605
615
Normal
[600a]
[600b]
[600c]

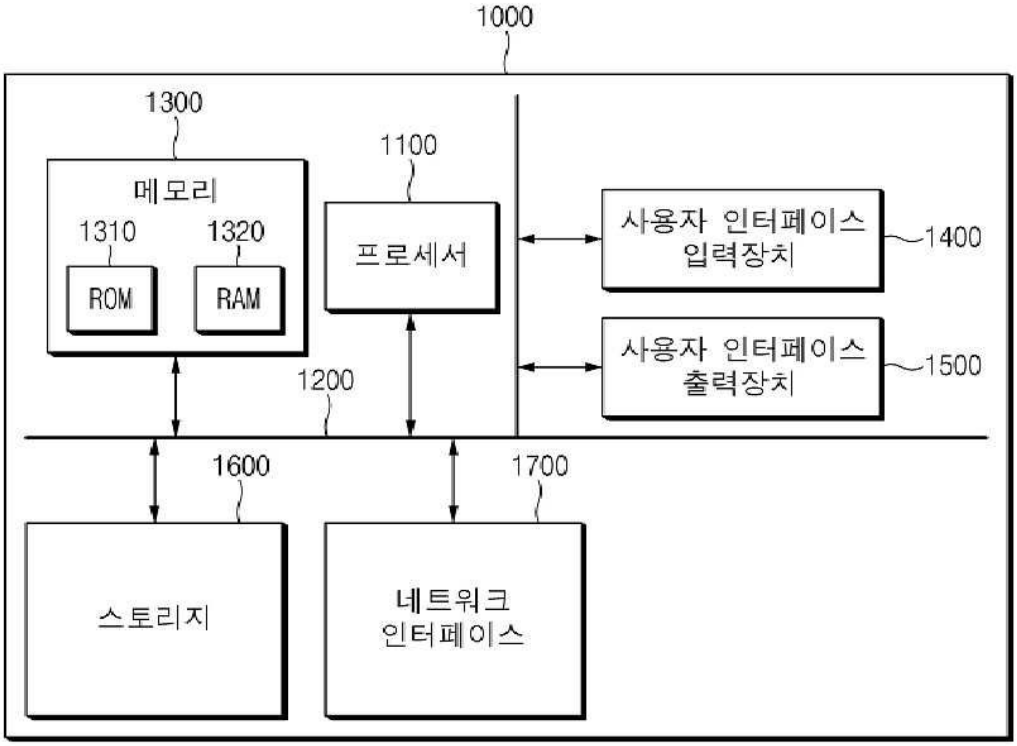
도면7


701
711
Attack
[700a]
703
713
Attack
[700b]
705
715
Attack
[700c]

도면8


시작
신호 샘플 수집
801
서브 필드들과 서브 템플릿 생성
803
CIR 값들 산출
805
ToA 값들 측정
807
809
Yes
수신 패킷 무효화
813
No
검증 패스에 따른 처리
811
815
No
종료?
Yes
종료

도면9


1000
1300
메모리
1310
ROM
1320
RAM
1100
프로세서
사용자 인터페이스
입력장치
1400
사용자 인터페이스
출력장치
1500
1200
1600
스토리지
1700
네트워크
인터페이스