(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2025-0028199
(43) 공개일자 2025년02월28일

(51) 국제특허분류(Int. Cl.)
G01S 11/02 (2010.01) *G06N 20/10* (2019.01)
(52) CPC특허분류
G01S 11/02 (2013.01)
G06N 20/10 (2021.08)
(21) 출원번호 10-2024-0107138
(22) 출원일자 2024년08월09일
심사청구일자 2024년08월09일
(30) 우선권주장
1020230108838 2023년08월21일 대한민국(KR)

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
주경호
서울특별시 성북구 지봉로 24길 52-8
이동훈
서울특별시 종로구 사직로8길 34, 1404호(내수동, 경희궁의아침3단지아파트)
(뒷면에 계속)
(74) 대리인
김등용

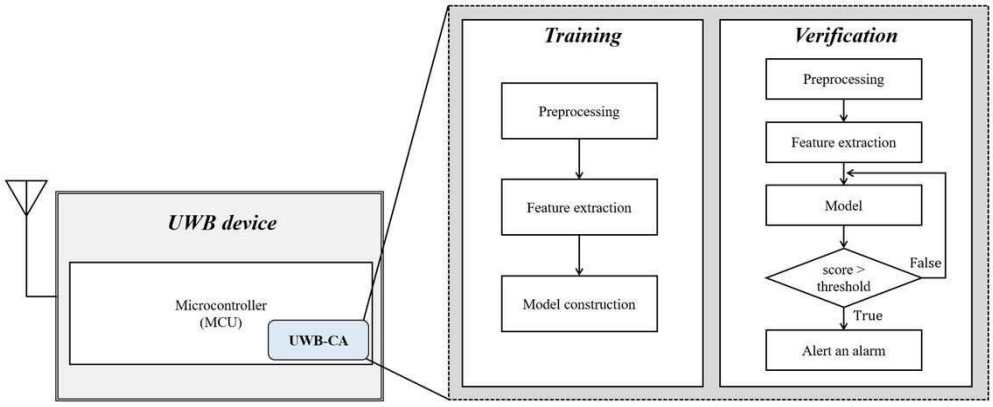
전체 청구항 수 : 총 4 항

(54) 발명의 명칭 **UWB HRP 모드에서의 채널 특성 분석 기반 거리 측정 시스템 및 그 방법**

(57) 요 약

UWB(Ultra-Wide Band)의 HRP(High Rate Pulse) 모드에서 동작하는 수신 장치에 의해 수행되는 거리 위조 공격 탐지 방법이 개시된다. 상기 거리 위조 공격 탐지 방법은 수신되는 RF 신호의 STS(Secure Training Sequence, 보안 훈련 시퀀스) 필드 신호로부터 특징을 추출하는 단계, 및 추출된 특징을 사전학습된 탐지 모델에 입력하여 거리 위조 공격을 탐지하는 단계를 포함하고, 상기 특징을 추출하는 단계는, 리딩 엣지(leading edge)를 탐지하기 위한 임계치, 최대 피크(maximum peak)의 크기와 시간 중 적어도 하나, 및 리딩 엣지의 크기와 시간 중 적어도 하나를 포함한다.

대 표 도 - 도3



(72) 발명자

최원석

서울특별시 강북구 삼양로 256, 105동 501호

이경연

경기도 남양주시 오남읍 진건오남로 735-10, 103동 1603호

이 발명을 지원한 국가연구개발사업

과제고유번호	1711193783
과제번호	2020-0-00374-004
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	정보보호핵심원천기술개발(R&D,정보화)
연구과제명	무인이동체 공통핵심 보안기술 개발 연구
과제수행기관명	고려대학교산학협력단
연구기간	2023.01.01 ~ 2023.12.31

명 세 서

청구범위

청구항 1

UWB(Ultra-Wide Band)의 HRP(High Rate Pulse) 모드에서 동작하는 수신 장치에 의해 수행되는 거리 위조 공격 탐지 방법에 있어서,

수신되는 RF 신호의 STS(Secure Training Sequence, 보안 훈련 시퀀스) 필드 신호로부터 특징을 추출하는 단계; 및

추출된 특징을 사전학습된 탐지 모델에 입력하여 거리 위조 공격을 탐지하는 단계를 포함하고,

상기 특징을 추출하는 단계는, 리딩 엣지(leading edge)를 탐지하기 위한 임계치, 최대 피크(maximum peak)의 크기와 시간 중 적어도 하나, 및 리딩 엣지의 크기와 시간 중 적어도 하나를 포함하는,

거리 위조 공격 탐지 방법.

청구항 2

제1항에 있어서,

상기 탐지 모델은 추출된 특징을 학습 데이터로 활용하여 사전학습된 OC-SVM(One-Class Support Vector Machine) 또는 LOF(Local Outlier Factor)인,

거리 위조 공격 탐지 방법.

청구항 3

제2항에 있어서,

상기 탐지 모델은 정상 신호만을 이용하여 학습된,

거리 위조 공격 탐지 방법.

청구항 4

제3항에 있어서,

상기 특징을 추출하는 단계는,

채널 임펄스 응답(Channel Impulse Response, CIR)을 생성하는 단계;

상기 CIR에 기초하여 최대 피크를 도출하는 단계; 및

백-서치 알고리즘(back-search algorithm)을 이용하여 리딩 엣지를 도출하는 단계를 포함하는,

거리 위조 공격 탐지 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 UWB(Ultra-Wide Band) 기술의 측위 시스템에 대한 채널 특성을 분석하여 보안을 강화하는 기법에 관한 것이다.

배 경 기 술

[0002] UWB(Ultra-Wide Band) 기술은 500MHz의 넓은 대역폭 채널을 사용하여, 1~2 ns의 짧은 펄스 신호로 데이터 통신을 수행하는 무선통신 기술로써 cm의 범위로 기기 간의 거리 측정 기능을 제공한다. UWB 기술은 펄스의 주기와 세기에 따라 LRP(Low Rate Pulse) 모드와 HRP(High Rate Pulse) 모드 중 하나를 사용한다. LRP는 높은 세기와

작은 개수의 펄스를 사용하는 반면, HRP는 작은 세기로 다수의 펄스를 사용한다. UWB 기술은 IEEE 표준으로 채택되어 왔으며, 최근 정확성과 보안이 향상된 802.15.4z 표준으로 정의되었다.

[0003] UWB 기술은 송·수신 단말 사이의 신호 도달 시간 차이(ToA; Time of Arrival)를 측정하는 방식으로 측위 기능을 제공함으로써 차량의 스마트키, 출입 태그와 같은 서비스를 제공한다. 하지만, 최근 UWB 신호의 물리 레벨 구조가 결정적(deterministic)이라는 특성을 악용하여 측위 시스템에 대한 거리 감소 공격이 가능함이 밝혀진 바 있다. 강한 세기의 펄스를 이용하기 때문에 단일 펄스가 쉽게 식별되는 LRP 모드에 대한 거리 위조 공격 방어 기법은 기존에 제안되었지만, HRP 모드에는 해당 보안 기법을 적용할 수 없다.

[0004] 따라서, 본 발명에서는 HRP 모드에서 적용할 수 있는, 거리 위조 공격에 대한 보안 기법을 제안하고자 한다.

선행기술문헌

특허문헌

[0005] (특허문헌 0001) 대한민국 공개특허 제2020-0005477호 (2020.01.15. 공개)

발명의 내용

해결하려는 과제

[0006] 본 발명이 이루고자 하는 기술적인 과제는, UWB HRP 모드에서의 채널 특성 분석 기반 거리 측정 시스템 및 그 방법을 제공하는 것이다.

과제의 해결 수단

[0007] 본 발명의 일 실시예에 따른 거리 위조 공격 탐지 방법은 UWB(Ultra-Wide Band)의 HRP(High Rate Pulse) 모드에서 동작하는 수신 장치에 의해 수행되는 거리 위조 공격 탐지 방법으로서, 수신되는 RF 신호의 STS(Secure Training Sequence, 보안 훈련 시퀀스) 필드 신호로부터 특징을 추출하는 단계, 및 추출된 특징을 사전학습된 탐지 모델에 입력하여 거리 위조 공격을 탐지하는 단계를 포함하고, 상기 특징을 추출하는 단계는, 리딩 엣지(leading edge)를 탐지하기 위한 임계치, 최대 피크(maximum peak)의 크기와 시간 중 적어도 하나, 및 리딩 엣지의 크기와 시간 중 적어도 하나를 포함한다.

[0008] 실시예에 따라, 상기 탐지 모델은 추출된 특징을 학습 데이터로 활용하여 사전학습된 OC-SVM(One-Class Support Vector Machine) 또는 LOF(Local Outlier Factor)일 수 있다.

[0009] 실시예에 따라, 상기 탐지 모델은 정상 신호만을 이용하여 학습될 수 있다.

[0010] 실시예에 따라, 상기 특징을 추출하는 단계는, 채널 임펄스 응답(Channel Impulse Response, CIR)을 생성하는 단계, 상기 CIR에 기초하여 최대 피크를 도출하는 단계, 및 백-서치 알고리즘(back-search algorithm)을 이용하여 리딩 엣지를 도출하는 단계를 포함할 수 있다.

발명의 효과

[0011] 본 발명의 실시예에 따른, UWB HRP 모드에서의 채널 특성 분석 기반 거리 측정 시스템 및 그 방법에 의할 경우, HRP 모드를 대상으로 하는 거리 위조 공격을 효과적으로 방어할 수 있는 효과가 있다.

도면의 간단한 설명

[0012] 본 발명의 상세한 설명에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 상세한 설명이 제공된다.

도 1은 NLoS로 인한 전파 지연 상황과 이에 따른 상관관계 결과를 도시한다.

도 2는 공격자가 거리 위조 공격을 수행하는 과정을 설명하기 위한 도면이다.

도 3은 본 발명의 일 실시예에 따른 거리 위조 공격 탐지 장치를 설명하기 위한 도면이다.

도 4는 I/Q 수신기를 통한 채널 임펄스 응답(CIR) 생성 과정을 도시한다.

발명을 실시하기 위한 구체적인 내용

[0013] 본 명세서에 개시되어 있는 본 발명의 개념에 따른 실시예들에 대해서 특정한 구조적 또는 기능적 설명들은 단지 본 발명의 개념에 따른 실시예들을 설명하기 위한 목적으로 예시된 것으로서, 본 발명의 개념에 따른 실시예들은 다양한 형태들로 실시될 수 있으며 본 명세서에 설명된 실시예들에 한정되지 않는다.

[0014] 본 발명의 개념에 따른 실시예들은 다양한 변경들을 가할 수 있고 여러 가지 형태들을 가질 수 있으므로 실시예들을 도면에 예시하고 본 명세서에서 상세하게 설명하고자 한다. 그러나, 이는 본 발명의 개념에 따른 실시예들을 특정한 개시 형태들에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물, 또는 대체물을 포함한다.

[0015] 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.

[0016] 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.

[0017] 본 명세서에서 사용한 용어는 단지 특정한 실시예를 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.

[0018] 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.

[0019] 이하, 본 명세서에 첨부된 도면들을 참조하여 본 발명의 실시예들을 상세히 설명한다. 그러나, 특허출원의 범위가 이러한 실시예들에 의해 제한되거나 한정되는 것은 아니다. 각 도면에 제시된 동일한 참조 부호는 동일한 부재를 나타낸다.

[0020] UWB(Ultra-Wide Band)의 HRP(High Rate Pulse) 모드에서는, 거리 측정을 위한 ToA(Time of Arrival)를 측정하기 위하여 RF 신호(또는 UWB 신호)의 STS(Secure Training Sequence, 보안 훈련 시퀀스) 필드를 사용하며, STS 필드는 거리를 측정하는 두 기기(initiator, responder)가 사전에 공유한 대칭키를 기반으로 생성된 의사 난수(pseudo random number) 값으로 구성되어 있다. 따라서, 이니시에이터(initiator, 송신기 등을 의미할 수 있음)의 신호를 수신한 리스폰더(responder, 응답기나 수신기 등을 의미할 수 있음)는 자신이 계산한 난수 값으로 이루어진 예상 신호(즉, 로컬 템플릿)와 수신된 STS 필드 신호와의 상관관계를 계산한다. 상관관계의 결과가 미리 정해진 일정 기준을 초과하면, 리스폰더는 유효한 STS 필드가 수신되었다고 판단하고 해당 시점에 동기화를 시작할 수 있다.

[0021] 그러나, 도 1의 (a)와 같은 NLoS(None-Line-of-Sight) 상황에서 장애물로 인하여 직접 경로(direct path)의 신호(즉, 직접 신호)가 감소되어 수신되면, 반사 경로(reflected path)의 신호(즉, 반사 신호)가 높은 상관관계 값을 가지게 된다. 이에 따라, 도 1의 (b)와 같이 최대 피크(maximum peak) 값을 생성한다. 따라서, 직접 경로를 찾기 위해 100 내지 300 ns의 이전 타임 윈도우에서 일정 기준을 초과하는 첫번째 신호인 리딩 엣지(leading edge)를 탐색하며, 이러한 과정을 백-서치 알고리즘(back-search algorithm)이라 한다.

[0022] 거리 위조 공격(또는 거리 감소 공격)을 수행하는 공격자는 STS 필드를 조작하여 리스폰더가 감소된 ToA를 측정

하도록 가짜 리딩 엣지를 생성하는 것을 목표로 한다. STS 필드를 조작하기 위해, 공격자는 도 2와 같이 정상적인 STS 필드를 더 강력한 새 펄스로 덮어쓴다.

[0023] 이에, 본 발명은 UWB 기술의 HRP 모드를 사용하는 기기의 측위 시스템에 대해 STS 필드가 정당한 STS 필드인지를 검증하여 거리 위조 공격(또는 거리 감소 공격)을 탐지하는 기법을 제안하고자 한다.

[0024] 도 3은 본 발명의 일 실시예에 따른 거리 위조 공격 탐지 장치를 설명하기 위한 도면이다.

[0025] 거리 위조 공격 탐지는 이니시에이터(송신기, 송신 장치 등을 의미할 수 있음)로부터 송신된 RF 신호(또는 UWB 신호)를 수신하는 수신기(수신 장치, 리스폰더, UWB 장치 등을 의미할 수 있음)에 의해 수행될 수 있다. 예시적인 수신기는 HWB 기술을 채용하여 측위 동작을 수행하는 차량, 차량에 탑재된 수신 장치(예컨대, UWB 통신을 수행하는 차량용 전자 제어 유닛(Electronic Control Unit, ECU)), 스마트키, 스마트폰 등으로 구현될 수 있다. 즉, 수신기는 UWB 기술을 활용하여 UWB 신호를 수신하는 임의의 기기를 의미할 수 있다. 또한, 수신기는 거리 위조 공격 탐지 장치로 명명될 수도 있다.

[0026] 거리 위조 공격 탐지 장치는 제어부(마이크로컨트롤러(Microcontroller, MCU) 등을 의미할 수 있음)를 포함하고, 거리 위조 공격 탐지 동작을 이루는 단계들 중 적어도 일부는 제어부에 의해 수행될 수 있다. 실시예에 따라, 제어부는 적어도 일부의 구성으로 탐지부(도 3의 UWB-CA)를 포함할 수 있고, 탐지부는 탐지 모델의 학습 및/또는 검증 동작을 수행할 수 있다.

[0027] 도 3의 예에서, 거리 위조 공격 탐지 장치가 학습을 통해 탐지 모델을 생성하거나, 및/또는 검증 동작을 수행하는 것으로 표현되어 있으나, 실시예에 따라, 탐지 모델의 생성 동작은 별도의 컴퓨팅 장치에 의해 수행되는 것도 가능하다. 이 경우, 탐지 모델은 적어도 프로세서(Processor) 또는 컨트롤러를 포함하는 컴퓨팅 장치에 의해 생성된 후, 거리 위조 공격 탐지 장치에 저장되고, 거리 위조 공격 탐지 장치는 사전 학습된 탐지 모델을 활용하여 거리 위조 공격을 탐지, 즉 STS 필드가 공격자에 의해 악의적으로 변조된 신호인지 여부를 검증할 수 있다. 컴퓨팅 장치는 PC(Personal Computer), 서버(Server), 랩탑 컴퓨터, 태블릿 PC, 스마트폰 등을 포함할 수 있다.

[0028] 탐지 모델은 학습 과정을 통해 생성된다. 학습 과정에서는 RF 신호를 전처리(Preprocessing)하고, 학습에 적절한 특징(feature)을 추출한 후 모델을 학습시킴으로써 생성할 수 있다. 학습에 활용되는 머신 러닝 모델은 OC-SVM(One-Class Support Vector Machine) 또는 LOF(Local Outlier Factor)일 수 있다. 이 두 모델은 이상치 분류에 사용되는 모델이다.

[0029] 학습 과정은 신호 획득 단계, 전처리 단계, 특징 추출 단계, 및 학습 단계 중 적어도 하나를 포함할 수 있다. 이때, 획득되는 신호는 이상이 없는(즉, 공격에 의해 발생한 신호가 아닌) 정상적인 신호를 의미할 수 있다. 실시예에 따르면, 학습에 활용되는 신호는 미리 획득되어 거리 위조 공격 탐지 장치에 저장되어 있을 수도 있다.

[0030] 우선, 거리 위조 공격 탐지 장치는 RF 신호를 수신하고, 수신된 RF 신호를 I/Q 수신기(In-phase/Quadrature receiver)를 통해 변조하여 채널 임펄스 응답(Channel Impulse Response, CIR)을 생성한다. 이와 관련하여, I/Q 수신기(receiver)를 통한 CIR 생성 과정은 도 4에 도시되어 있다. 즉, 채널 임펄스 응답은 STS 필드에 대응하는 신호에 대한 채널 임펄스 응답을 의미할 수 있다.

[0031] 다음으로, 학습에 이용된 특징이 추출된다. 머신 러닝 모델의 학습에 사용될 특징은 제1 특징 및/또는 제2 특징을 포함할 수 있다. 여기서, 제1 특징은 CIR과 관련된 특징을, 제2 특징은 통계적 특징을 의미할 수 있다.

[0032] 제1 특징은 리딩 엣지를 탐지하기 위한 임계값 파라미터(threshold parameter, 리딩 엣지가 초과하여야 하는 기준을 의미할 수 있음), 최대 피크(최대 피크의 크기 및/또는 시간), 및 리딩 엣지(리딩 엣지의 크기 및/또는 시간)를 포함할 수 있다. 이때, 리딩 엣지는 백-서치 알고리즘을 통해 도출될 수 있다. 또한, 임계값 파라미터(또는 임계값)는 미리 정해진 값을 가질 수 있고, 최대 피크와 리딩 엣지는 생성된 CIR로부터 도출될 수 있다. 예시적으로, 가장 큰 값을 가진 피크가 최대 피크이고, 임계치 이상의 피크 중 가장 선행하는 피크가 리딩 엣지로 결정될 수 있다.

[0033] 제2 특징은 채널 또는 CIR의 통계적 특징으로써, 예시적인 특징은 CIR의 분산, 평균, 경로 손실(path loss), 채널 대역폭(channel bandwidth), 지터(Jitter), 드리프트(Drift), 수신 신호 강도, 신호 대 잡음비(Signal-to-Noise Ratio, SNR), 코히어런스 시간(Coherence Time), 및 코히어런스 대역폭(Coherence Bandwidth) 중 적어도 하나를 포함할 수 있다.

[0034] 학습 과정에서는, 정상적인 시나리오(장애물 등으로 인하여 반사 경로가 생성되는 경우를 포함할 수 있음)에서

수집한 신호, 즉 이상이 없는 정상적인 신호만을 이용하여 탐지 모델이 구축(또는 생성)될 수 있다.

[0035] 학습 과정이 완료되면, 학습이 완료된 머신 러닝 모델(즉, 탐지 모델)을 이용하여 실제 수신되는 STS 필드를 검증할 수 있다. 탐지 모델은 입력되는 특징에 대응하는 스코어를 출력하거나, 입력되는 특징에 대응하는 신호가 공격 신호(즉, 거리 위조 공격 신호)인지 여부를 출력할 수 있다. 탐지 모델이 입력되는 특징에 대한 스코어를 출력하는 경우, 해당 스코어는 수신 신호(수신된 STS 필드 신호)가 정상 신호일 확률 또는 비정상 신호일 확률을 나타낼 수 있다. 따라서, 미리 정해진 임계치와의 출력된 스코어의 비교를 통해 거리 위조 공격 여부가 판단될 수 있다. 예시적으로, 출력된 스코어가 미리 정해진 임계치를 초과하는 경우 정상적인 신호로(또는 공격 신호로) 판다될 수 있다.

[0036] 물론, 검증 과정에서는, 학습 과정에서와 동일하게, 수신된 신호에 대한 전처리 동작과 특징 추출 동작을 포함할 수 있다. 따라서, 학습에 활용된 특징과 동일한 특징이 추출되고, 이를 통해 수신된 신호의 이상 여부를 판단(또는 검증)할 수 있다.

[0037] 이상에서 설명된 장치는 하드웨어 구성 요소, 소프트웨어 구성 요소, 및/또는 하드웨어 구성 요소 및 소프트웨어 구성 요소의 집합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성 요소는, 예를 들어, 프로세서, 콘트롤러, 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 콘트롤러를 포함할 수 있다. 또한, 병렬 프로세서(Parallel Processor)와 같은, 다른 처리 구성(Processing Configuration)도 가능하다.

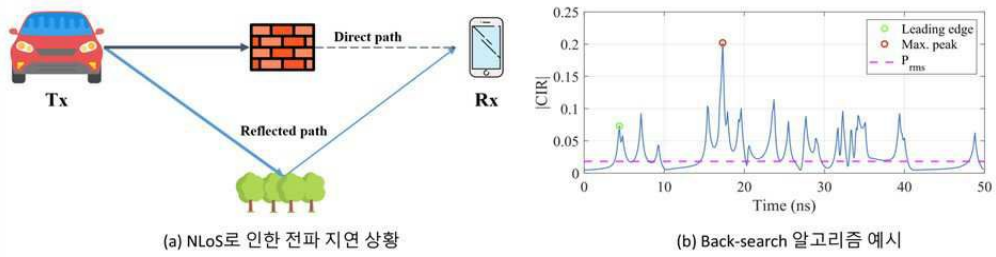
[0038] 소프트웨어는 컴퓨터 프로그램(Computer Program), 코드(Code), 명령(Instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(Collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성 요소(Component), 물리적 장치, 가상 장치(Virtual Equipment), 컴퓨터 저장 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.

[0039] 실시예에 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 실시예를 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 실시예의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0040] 본 발명은 도면에 도시된 실시예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 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.

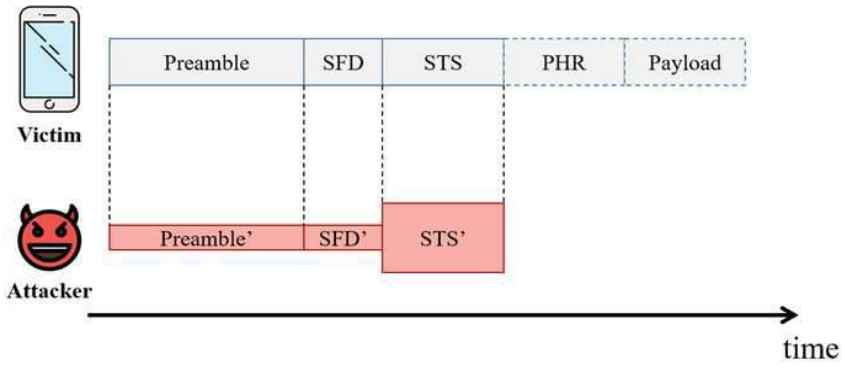
도면

도면1

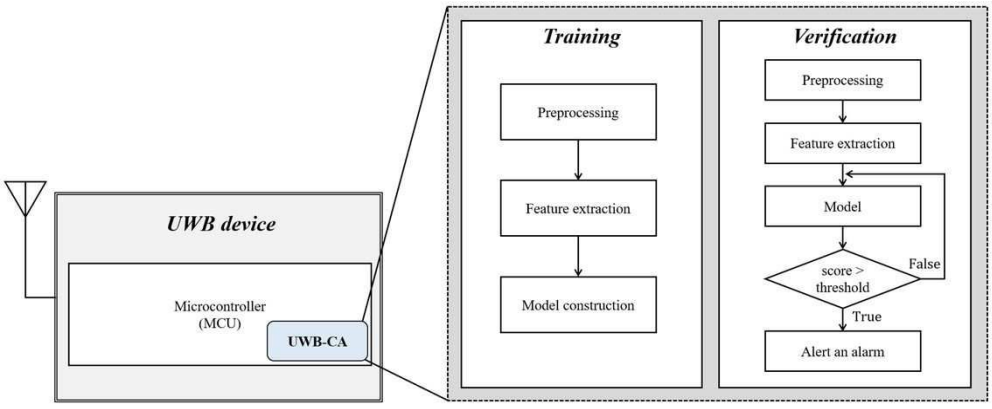


(a) NLoS로 인한 전파 지연 상황 (b) Back-search 알고리즘 예시

도면2



도면3



도면4