



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2021-0127228
(43) 공개일자 2021년10월21일

(51) 국제특허분류(Int. Cl.)
G01S 5/14 (2006.01) G01S 13/76 (2006.01)
G01S 13/87 (2006.01) G01S 5/02 (2010.01)
H04W 4/02 (2018.01) H04W 64/00 (2009.01)
(52) CPC특허분류
G01S 5/14 (2013.01)
G01S 13/765 (2013.01)
(21) 출원번호 10-2021-7029737
(22) 출원일자(국제) 2020년02월17일
심사청구일자 없음
(85) 번역문제출일자 2021년09월15일
(86) 국제출원번호 PCT/EP2020/054029
(87) 국제공개번호 WO 2020/169505
국제공개일자 2020년08월27일
(30) 우선권주장
19158080.2 2019년02월19일
유럽특허청(EPO)(EP)

(71) 출원인
코닌클리케 필립스 엔.브이.
네덜란드 아인트호벤 5656 에이지 하이 테크 캠퍼스 52
(72) 발명자
베른센 요하네스 아놀두스 코넬리스
네덜란드 아인트호벤 5656 에이지 하이 테크 캠퍼스 5
(74) 대리인
장훈

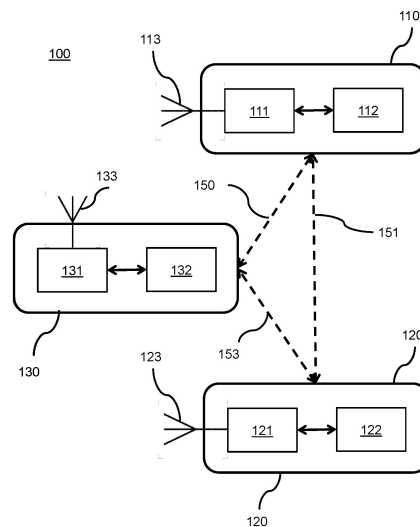
전체 청구항 수 : 총 15 항

(54) 발명의 명칭 신뢰성있는 거리 측정 시스템

(57) 요약

디바이스는 제2 디바이스로부터의 측정 메시지를 사용하여 레인징 프로토콜에 따라 거리 측정을 하도록 배열된다. 측정 메시지의 제1 도달 시간에 기초하여, 제1 디바이스(110)와 제2 디바이스(120) 사이의 제1 거리(151)가 결정된다. 제3 디바이스(130)는 신뢰된 거리(150)에 위치되는 협력 디바이스로서 동작한다. 협력 디바이스는 동일한 측정 메시지의 제3 도달 시간을 결정하고, 제3 도달 시간에 기초하는 지원 데이터를 제1 디바이스로 전달한다. 제1 디바이스는 지원 데이터를 사용하여 제3 디바이스와 제2 디바이스 사이의 제3 거리(153)를 획득한다. 이어서, 제1 거리(151), 신뢰된 거리(150) 및 제3 거리(153)에 대해 검증 테스트가 수행된다. 제1 거리는 상기 거리들이 디바이스들의 실행가능한 공간 콘스텔레이션(100)에 대응할 때 신뢰성이 있다.

대표도 - 도1



(52) CPC특허분류

G01S 13/876 (2013.01)

G01S 5/0244 (2020.05)

H04W 4/023 (2020.05)

H04W 64/006 (2013.01)

명세서

청구범위

청구항 1

제1 디바이스(110)로서 동작하여 무선 통신을 위한 제2 디바이스(120)와의 사이의 무선 통신을 통한 거리 측정을 위한 디바이스로서,

상기 무선 통신은 상기 제1 디바이스에서의 측정 메시지의 도달 시간에 기초하여 상기 제1 디바이스와 상기 제2 디바이스 사이의 거리를 결정하기 위한 레인징 프로토콜(ranging protocol)을 포함하고, 상기 프로토콜은 상기 제2 디바이스에 의해 상기 측정 메시지를 송신하는 것을 포함하고;

상기 디바이스는

- 메시지들의 송신 및 수신을 위한 제1 송수신기(111),
- 제1 메시지 프로세서(112)를 포함하고, 상기 제1 메시지 프로세서(112)는
- 상기 레인징 프로토콜에 따라 상기 메시지들을 프로세싱하고,
- 상기 제1 디바이스에서의 상기 측정 메시지의 제1 도달 시간을 결정하고,
- 상기 제1 도달 시간에 기초하여 상기 제1 디바이스와 상기 제2 디바이스 사이의 제1 거리(151)를 결정하도록 배열되고;

상기 제1 메시지 프로세서(112)는 상기 제1 디바이스로부터 신뢰된 거리(150)에 위치되는 협력 디바이스로서 동작하는 제3 디바이스(130)와 통신하도록 배열되고,

상기 결정된 거리를 평가하기 위해,

- 상기 협력 디바이스에서 상기 제1 메시지의 제3 도달 시간에 기초하는 지원 데이터를 상기 협력 디바이스로부터 수신하고,
- 상기 지원 데이터를 사용하여 상기 제3 디바이스와 상기 제2 디바이스 사이의 제3 거리(153)를 획득하고,
- 상기 제1 거리(151), 상기 신뢰된 거리(150), 및 상기 제3 거리(153)에 대한 검증 테스트를 수행하도록 배열되고, 상기 검증 테스트는 상기 거리들이 상기 제1 디바이스, 상기 제2 디바이스, 및 상기 협력 디바이스의 실행가능한 공간 콘스텔레이션(100)에 대응할 때 상기 제1 거리를 신뢰성있는 것으로서 수용하는, 디바이스.

청구항 2

제1항에 있어서, 상기 검증 테스트는 상기 실행가능한 공간 콘스텔레이션에 대한 코사인 법칙 검사 또는 삼각 부등식 검사를 포함하는, 디바이스.

청구항 3

제1항 또는 제2항에 있어서, 상기 레인징 프로토콜은 키 데이터에 기초하여 암호로 보호되는 교환 메시지들을 포함하고, 상기 제1 메시지 프로세서(112)는 상기 협력 디바이스와 상기 키 데이터를 공유하도록 배열되어 상기 제3 메시지 프로세서(132)로 하여금 상기 레인징 프로토콜에 따라 상기 메시지들을 암호로 프로세싱할 수 있게 하는, 디바이스.

청구항 4

제1항 내지 제3항 중 어느 한 항에 있어서, 상기 제1 메시지 프로세서(112)는 상기 레인징 프로토콜에 따라 상기 신뢰된 거리를 결정하도록 배열되는, 디바이스.

청구항 5

제1항 내지 제4항 중 어느 한 항에 있어서, 상기 디바이스는 상기 도달 시간들을 결정하기 위해 시간 기준을 제

공하기 위한 클록 유닛을 포함하고, 상기 제1 메시지 프로세서(112)는 상기 시간 기준을 상기 협력 디바이스 내의 대응하는 클록 유닛과 동기화시키도록 배열되는, 디바이스.

청구항 6

제1항 내지 제5항 중 어느 한 항에 있어서, 상기 레인징 프로토콜은 상기 제1 디바이스를 포함하고, 상기 제1 디바이스는 개시 디바이스로서 동작하고 개시 메시지를 상기 제2 디바이스로 전송하는 한편, 상기 개시 메시지의 수신 시, 상기 제2 디바이스는 상기 측정 메시지를 전송해야 하고, 상기 제1 메시지 프로세서(112)는,

- 상기 제3 디바이스와 역할-변경 데이터를 교환하여 상기 제3 디바이스로 하여금 거리 측정을 위해 상기 개시 디바이스로서 동작할 수 있게 하도록 배열되고;

상기 제3 디바이스는, 상기 역할-변경 데이터를 수신할 때,

- 제2 측정 메시지에 기초하여 상기 레인징 프로토콜에 따라 상기 제3 디바이스와 상기 제2 디바이스 사이의 제3 거리를 획득하고,

- 상기 제3 거리를 나타내는 제3 지원 데이터를 상기 제1 디바이스로 전달하도록 배열되며;

한편 상기 제1 메시지 프로세서(112)는

- 상기 제1 디바이스에서 상기 제2 측정 메시지를 수신할 때 상기 제1 디바이스와 상기 제2 디바이스 사이의 제2 거리를 결정하고,

- 상기 제3 디바이스로부터 상기 제3 지원 데이터를 수신하고,

- 상기 제2 거리 및 상기 제3 지원 데이터를 또한 사용하여 상기 검증 테스트를 수행하도록 배열되는, 디바이스.

청구항 7

제1항 내지 제6항 중 어느 한 항에 있어서,

상기 제3 메시지 프로세서(132)는

- 상기 제2 디바이스로부터 수신된 적어도 하나의 메시지의 제3 신호 강도를 결정하고,
- 상기 제1 디바이스에 대한 상기 지원 데이터에 제3 신호 강도 데이터를 포함시키도록 배열되고,

상기 제1 메시지 프로세서(112)는

- 상기 제2 디바이스로부터 수신된 적어도 하나의 메시지의 제1 신호 강도를 결정하고,
- 상기 결정된 거리들에서 상기 제1 신호 강도 및 상기 제3 신호 강도를 각자의 예상 신호 강도들과 비교함으로써 상기 결정된 거리들이 신뢰성이 있는지 여부를 검증하도록 배열되는, 디바이스.

청구항 8

제1항 내지 제7항 중 어느 한 항에 있어서, 상기 제1 메시지 프로세서(112)는, 상기 결정된 거리가 신뢰성이 없는 것으로 평가할 때,

- 상기 제2 디바이스에 의해 상이한 보안 프로토콜을 실행할 것을 요구하는 것;
- 상이한 레인징 프로토콜 및/또는 상이한 유형의 무선 통신을 사용하여 추가 거리 측정을 요청하는 것;
- 상기 제1 디바이스에서 적어도 몇몇 데이터에 대한 그리고/또는 적어도 하나의 기능에 대한 액세스를 거부하거나 제한하는 것 중 적어도 하나를 수행하도록 배열되는, 디바이스.

청구항 9

제1항 내지 제8항 중 어느 한 항에 기재된 디바이스, 제1항에 기재된 제3 디바이스 및 상기 제1 디바이스로부터 또는 상기 제3 디바이스로부터 제2 신뢰된 거리에 위치되는 제2 협력 디바이스로서 동작하는 제4 디바이스를 포함하는, 신뢰성있는 거리 측정 시스템으로서,

상기 제4 디바이스는,

- 메시지들을 수신하기 위한 제4 무선 수신기(141),
- 제4 메시지 프로세서(142)를 포함하고, 상기 제4 메시지 프로세서(142)는
- 상기 제4 디바이스에서의 상기 측정 메시지의 제4 도달 시간을 결정하고,
- 상기 제4 도달 시간에 기초하는 제4 지원 데이터를 상기 제1 디바이스로 전달하도록 배열되고;

상기 제1 메시지 프로세서(112)는

- 상기 제2 협력 디바이스로부터 상기 제4 지원 데이터를 수신하고,
- 상기 제4 지원 데이터를 사용하여 상기 제4 디바이스와 상기 제2 디바이스 사이의 제4 거리를 획득하고,
- 상기 제2 신뢰된 거리 및 상기 제4 거리를 또한 사용하여 상기 검증 테스트를 수행하도록 배열되는, 시스템.

청구항 10

제9항에 있어서, 상기 제1 메시지 프로세서(112)는

- 상기 제1 디바이스, 상기 제2 디바이스 및 상기 제3 디바이스의 제1 공간 콘스텔레이션에 대한 제1 삼각 부등식, 및 상기 제1 디바이스, 상기 제2 디바이스 및 상기 제4 디바이스의 제2 공간 콘스텔레이션에 대한 제2 삼각 부등식의 결합을 사용하여 상기 검증 테스트를 수행하거나; 또는
- 상기 제1 공간 콘스텔레이션에 따른 상기 제2 디바이스의 제1 위치가 상기 제2 공간 콘스텔레이션에 따른 상기 제2 디바이스의 제2 위치에 대응하는지 여부를 검증하거나; 또는
- 모든 결정된 거리들이 0보다 더 큰지 여부를 검출하기 위한 불일치 검사를 사용하여 상기 검증 테스트를 수행하거나; 또는
- 상기 제3 디바이스 및 상기 제4 디바이스는, 제3 디바이스로부터 제1 디바이스로의 라인과 제4 디바이스로부터 제1 디바이스로의 라인 사이의 신뢰된 각도가 적어도 90도이도록 배열되는 셋업에 기초하여 상기 검증 테스트를 수행하거나; 또는
- 상기 제3 디바이스 및 상기 제4 디바이스는 상기 제1 디바이스에 대해 서로 반대편에 배열되는 셋업에 기초하여 상기 검증 테스트를 수행하거나; 또는
- 상기 제2 신뢰된 거리가 상기 신뢰된 거리에 대응하는 셋업에 기초하여 상기 검증 테스트를 수행하도록 배열되는, 시스템.

청구항 11

제9항 또는 제10항에 있어서, 상기 시스템은 추가 협력 디바이스로서 동작하는 적어도 하나의 추가 디바이스를 포함하고, 상기 제3 디바이스, 상기 제4 디바이스 및 상기 적어도 하나의 추가 디바이스는 다각형의 에지들에서의 평면 내에 배열되고, 상기 제1 디바이스는 상기 다각형 내부에 있고, 상기 제1 메시지 프로세서(112)는

- 적어도 2개의 공간 콘스텔레이션들에 대한 삼각 부등식들의 결합을 사용하여 상기 검증 테스트를 수행하도록 배열되며, 각각의 콘스텔레이션은 상기 제2 디바이스와 상기 제1 디바이스 및 상기 협력 디바이스들의 세트 중 2개의 디바이스들을 포함하는, 시스템.

청구항 12

제1 디바이스(110)와 제2 디바이스(120) 사이의 무선 통신을 통한 거리 측정을 위한 방법으로서,

상기 무선 통신은 상기 제1 디바이스에서의 측정 메시지의 도달 시간에 기초하여 상기 제1 디바이스와 상기 제2 디바이스 사이의 거리(140)를 결정하기 위한 레인징 프로토콜을 포함하고, 상기 프로토콜은 상기 제2 디바이스에 의해 상기 측정 메시지를 송신하는 것을 포함하고;

상기 방법은,

- 상기 제1 디바이스에서의 상기 측정 메시지의 제1 도달 시간에 기초하여 상기 제1 디바이스와 상기 제2 디바

이스 사이의 제1 거리를 획득하는 단계,

- 제3 디바이스(130)와 통신하는 단계를 포함하고, 상기 제3 디바이스는 상기 제1 디바이스로부터 신뢰된 거리에 위치되는 협력 디바이스로서 동작하며,

상기 제3 디바이스는

- 상기 제3 디바이스에서의 상기 측정 메시지의 제3 도달 시간을 결정하고,
- 상기 제3 도달 시간에 기초하는 지원 데이터를 제공하도록 배열되고;

상기 방법은, 상기 결정된 거리를 평가하기 위해,

- 상기 지원 데이터를 사용하여 상기 제3 디바이스와 상기 제2 디바이스 사이의 제3 거리를 획득하는 단계,
- 상기 제1 거리, 상기 신뢰된 거리 및 상기 제3 거리에 대한 검증 테스트를 수행하는 단계를 포함하고, 상기 검증 테스트는 상기 거리들이 상기 제1 디바이스, 상기 제2 디바이스, 및 상기 협력 디바이스의 실행가능한 공간 콘스텔레이션에 대응할 때 상기 제1 거리를 신뢰성있는 것으로서 수용하는, 방법.

청구항 13

제12항에 있어서, 상기 방법은,

- 상기 제1 도달 시간 또는 상기 제1 거리를 제공하기 위해 개시 디바이스로서 동작할 것을 상기 제1 디바이스에 지시하는 단계, 또는
- 상기 제3 도달 시간에 기초하는 상기 지원 데이터를 제공하기 위해 상기 협력 디바이스로서 동작할 것을 상기 제3 디바이스에 지시하는 단계를 포함하는, 방법.

청구항 14

제1 디바이스(110)와 제2 디바이스(120) 사이의 무선 통신을 통한 거리 측정에서 협력 디바이스로서 동작하기 위한 방법으로서,

상기 협력 디바이스는 상기 제1 디바이스로부터 신뢰된 거리에 위치되고,

상기 무선 통신은 상기 제1 디바이스에서의 측정 메시지의 도달 시간에 기초하여 상기 제1 디바이스와 상기 제2 디바이스 사이의 거리를 결정하기 위한 레인징 프로토콜을 포함하고, 상기 프로토콜은 상기 제2 디바이스에 의해 상기 측정 메시지를 송신하는 것을 포함하고;

상기 제1 디바이스는

- 상기 제1 디바이스에서의 상기 측정 메시지의 제1 도달 시간에 기초하여 상기 제1 디바이스와 상기 제2 디바이스 사이의 제1 거리를 획득하도록 배열되고,

상기 방법은,

- 상기 협력 디바이스에서의 상기 측정 메시지의 제3 도달 시간을 결정하는 단계, 및
- 상기 제3 도달 시간에 기초하는 지원 데이터를 제공하는 단계를 포함하고;

상기 제1 디바이스는, 상기 결정된 거리를 평가하기 위해,

- 상기 지원 데이터를 사용하여 상기 협력 디바이스와 상기 제2 디바이스 사이의 제3 거리를 획득하고,
- 상기 제1 거리, 상기 신뢰된 거리 및 상기 제3 거리에 대한 검증 테스트를 수행하도록 배열되고, 상기 검증 테스트는 상기 거리들이 상기 제1 디바이스, 상기 제2 디바이스, 및 상기 협력 디바이스의 실행가능한 공간 콘스텔레이션에 대응할 때 상기 제1 거리를 신뢰성있는 것으로서 수용하는, 방법.

청구항 15

네트워크로부터 다운로드 가능하고/하거나 컴퓨터 판독 가능 매체 및/또는 마이크로프로세서 실행 가능 매체에 저장된 컴퓨터 프로그램 제품으로서, 상기 제품은 컴퓨터 상에서 실행될 때 제12항 내지 제14항 중 어느 한 항에 따른 방법을 구현하기 위한 프로그램 코드 명령어들을 포함하는, 컴퓨터 프로그램 제품.

발명의 설명

기술 분야

- [0001] 본 발명은, 제1 디바이스로서 동작하여 무선 통신을 위한 제2 디바이스와의 사이의 무선 통신을 통한 거리 측정을 위한 디바이스에 관한 것이고, 무선 통신은 제1 디바이스에서의 측정 메시지의 도달 시간에 기초하여 제1 디바이스와 제2 디바이스 사이의 거리를 결정하기 위한 레인징 프로토콜(ranging protocol)을 포함하고, 프로토콜은 제2 디바이스에 의해 측정 메시지를 송신하는 것을 포함한다. 본 발명은 또한 디바이스 또는 서버에서 사용하기 위한 거리 측정 방법 및 컴퓨터 프로그램 제품들에 관한 것이다.
- [0002] 본 발명은 대체적으로 위치 시스템들의 분야에 관한 것으로, 더 구체적으로는 거리 측정을 검증하기 위한 다양한 디바이스들 및 방법들뿐만 아니라 대응하는 컴퓨터 프로그램 제품들을 제공한다.

배경 기술

- [0003] 위치 인식 서비스들에 대한 필요성이 실내 영역들에 존재할 수 있다. 예를 들어, 병원, 대학교, 주차장, 쇼핑몰, 및/또는 사무실과 같은 대규모 실내 단지 내에서 근거리에는 있는 모바일 디바이스들에 무선 서비스들이 제공될 수 있다. 실내 위치 시스템은 소비자들(이하 최종 사용자들)에게 서비스; 최종 사용자들이 궁극적으로 의존하게 될 서비스를 제공할 수 있다. 그러한 위치 기반 서비스들은 가까이 있는 디바이스들, 즉 서비스 제공 디바이스에 대해 제한된 거리에 있는 디바이스들에만 제공될 수 있다. 추가 예에서, 전자식 무선 자동차 도어 키는 문을 열 수 있기 전에 자동차에 가까이 있어야 한다. 치팅(cheating) 도어 키는 거리 측정 프로토콜을 이용하여 탬퍼링(tamper)할 수 있어서 키가 있어야 하는 거리보다 자동차에서 훨씬 멀리 떨어져 있을 때 도어를 열 수 있다.
- [0004] 따라서, 거리 측정은 신뢰성이 중요하다. 이러한 문맥에서 신뢰성이란, 거리 또는 도달 시간 데이터가 탬퍼링되었거나 위조되어 응답 디바이스에 대해 실제 거리와 상이한 거리를 의도적으로 발생시켰던 것과는 대조적으로, 응답 디바이스가 측정된 대로 신뢰성있고 정확한 거리 또는 도달 데이터를 제공한다는 것을 의미한다.
- [0005] 알려진 거리 측정 시스템은 IEEE 802.11에 정의된 무선 통신용 프로토콜의 버전으로 최근에 개발되었는데, 참조 문헌 [802.11]을 참조한다. 버전은 2개의 디바이스들 사이의 거리를 결정하기 위한 레인징 프로토콜을 포함하고, 정확한 거리 측정과, 최대 1 미터 또는 심지어 더 낮은 리졸루션까지 디바이스들의 위치를 결정하는 것을 가능하게 한다. 미세 타이밍 측정(Fine Timing Measurement, FTM) 절차로 지칭되는 레인징 프로토콜은 [802.11] 챕터 10.24.6에 정의되어 있으며, 측정 메시지들의 도달 시간을 정확하게 측정하여 신호의 왕복시간(Round-Trip Time, RTT)을 결정하고, 송신 타이밍과 결합한 메시지들의 측정된 도달 시간들에 기초하여 거리를 도출한다. 예를 들어, 무선 신호가 실질적으로 빛의 속도로 자유 공간에서 전파된다고 가정하면, 방사선이 1미터의 거리를 커버하는 데 3.3ns가 걸리는 반면 Wi-Fi 스테이션은 약 0.1ns의 시간 세분성(time granularity)에 도달할 수 있다.
- [0006] 이 응용은 레인징 프로토콜들의 분야임을 주목한다. 이들은 전자기 방사선이 송신기와 수신기 사이에서 이동하는 데 걸리는 시간을 측정하는 비행 시간 측정들로 알려진 것에 대응할 수 있다. 이들은 IP 데이터 패킷이 네트워크에서 소스 디바이스로부터 싱크 디바이스로 송신되는 데 걸리는 시간을 측정하는 핑 시간(ping times)으로 알려진 IP/HTTP 프로토콜에서 수행되는 거리 측정과는 근본적으로 상이하며, 그러한 송신은 다수의 중간 디바이스들을 포함할 수 있다.
- [0007] 2개의 디바이스들이 도달 시간 측정들에 기초하여 서로 간의 거리를 결정하기 위해서, 이들은 레인징 프로토콜에 따라 동작할 필요가 있다. 예를 들어, 개시 무선 디바이스는 왕복 시간 측정을 시작하라는 요청을 개시할 수 있다. 응답 디바이스는 메시지를 전송하는 것과 요청을 수신하는 것 사이의 간격을 결정하고, 시간 간격을 개시 디바이스로 전송할 수 있다.
- [0008] 그러나, 잘못된 데이터를 전송함으로써, 디바이스가 실제로는, 그것이 실제로 있는 것보다 더 가깝거나 더 멀리 있는 것으로 주장할 수 있다. 또한, 측정 메시지는, 예컨대 타이밍 그리드에 따라, 미리 결정된 시간에 송신되어야 할 수 있다. 악성 디바이스는 의도적으로 측정 메시지를 상이한 시간에 전송할 수 있다. 그러한 악성 거동은, 개시 디바이스가 결정된 거리/위치 정보를 정확한 것으로 신뢰할 경우 위치 기반 서비스의 가능한 남용으로 이어질 수 있다. 예를 들어, 위치 기반 서비스는 자동으로 몇몇 트랜잭션을 시작할 수 있다.

[0009] 따라서, 공지된 시스템들에서, 측정들 또는 수신된 거리 데이터가 탬퍼링될 수 있고, 따라서 완전히 신뢰될 수 없다.

발명의 내용

[0010] 802.11의 시간 측정(Time Measurement, TM) 또는 미세 타이밍 측정(FTM) 방법들을 사용하여 제2 디바이스까지의 거리를 측정하는 제1 디바이스는 악성 디바이스들에 의한 위조된 도달 시간(time of arrival, TOA) 및 위조된 출발 시간(time of departure, TOD) 데이터로부터 자신을 보호하려고 시도할 수 있으며, 악성 디바이스들은 그렇게 함으로써 상이한 거리로, 특히 그들이 실제로 있는 것보다 더 짧은 거리로 나타내어지길 원한다.

[0011] 그러한 거동과 반대로, 거리 측정 시스템은 제3 디바이스를 수반할 수 있으며, 제3 디바이스 또한 잠재적으로 악성인 제2 디바이스와 제3 디바이스 사이의 제2 거리를 결정하기 위한 거리 측정을 수행한다. 둘 모두의 거리들을 비교하고 제1 디바이스와 협력 디바이스 사이의 거리를 알고 신뢰함으로써, 결정된 거리들 둘 모두에 대해 검증 테스트가 수행될 수 있다. 그러나, 악성 디바이스가 거리 측정들 둘 모두가 검증 테스트를 통과하도록 이들을 탬퍼링하는 것이 더 복잡할 수 있지만, 여전히 가능할 수 있다.

[0012] 본 발명의 목적은 도달 시간 기반 거리 측정을 더 신뢰할 수 있게 하는 시스템을 제공하는 것이다. 이러한 목적을 위해, 첨부된 청구항들에서 정의되는 바와 같은 디바이스들 및 방법들이 제공된다.

[0013] 본 발명의 제1 태양에 따르면, 제1 디바이스로서 동작하여 무선 통신을 위한 제2 디바이스와의 사이의 무선 통신을 통한 거리 측정을 위한 디바이스가 제공되고, 무선 통신은 제1 디바이스에서의 측정 메시지의 도달 시간에 기초하여 제1 디바이스와 제2 디바이스 사이의 거리를 결정하기 위한 레인징 프로토콜을 포함하고, 프로토콜은 제2 디바이스에 의해 측정 메시지를 송신하는 것을 포함하고;

[0014] 디바이스는,

[0015] - 메시지들의 송신 및 수신을 위한 제1 송수신기,

[0016] - 제1 메시지 프로세서를 포함하고, 제1 메시지 프로세서는

[0017] - 레인징 프로토콜에 따라 메시지들을 프로세싱하고;

[0018] - 제1 디바이스에서의 측정 메시지의 제1 도달 시간을 결정하고,

[0019] - 제1 도달 시간에 기초하여 제1 디바이스와 제2 디바이스 사이의 제1 거리를 결정하도록 배열되고;

[0020] 제1 메시지 프로세서는 제1 디바이스로부터 신뢰된 거리에 위치되는 협력 디바이스로서 동작하는 제3 디바이스와 통신하도록 배열되고,

[0021] 결정된 거리를 평가하기 위해,

[0022] - 협력 디바이스에서의 제1 메시지의 제3 도달 시간에 기초하는 지원 데이터를 협력 디바이스로부터 수신하고,

[0023] - 지원 데이터를 사용하여 제3 디바이스와 제2 디바이스 사이의 제3 거리를 획득하고,

[0024] - 제1 거리, 신뢰된 거리, 및 제3 거리에 대한 검증 테스트를 수행하도록 배열되고, 검증 테스트는 상기 거리들이 제1 디바이스, 제2 디바이스 및 협력 디바이스의 실행가능한 공간 콘스텔레이션에 대응할 때 제1 거리를 신뢰성있는 것으로서 수용한다.

[0025] 추가의 태양에 따르면, 제1 디바이스와 제2 디바이스 사이의 무선 통신을 통한 거리 측정을 위한 방법이 제공되며, 본 방법은

[0026] - 제1 디바이스에서의 측정 메시지의 제1 도달 시간에 기초하여 제1 디바이스와 제2 디바이스 사이의 제1 거리를 획득하는 단계,

[0027] - 제1 디바이스로부터 신뢰된 거리에 위치되는 협력 디바이스로서 동작하는 제3 디바이스와 통신하는 단계를 포함하고,

[0028] 제3 디바이스는

[0029] - 제3 디바이스에서의 측정 메시지의 제3 도달 시간을 결정하고,

[0030] - 제3 도달 시간에 기초하는 지원 데이터를 제공하도록 배열되며;

- [0031] 본 방법은, 결정된 거리를 평가하기 위해,
- [0032] - 지원 데이터를 사용하여 제3 디바이스와 제2 디바이스 사이의 제3 거리를 획득하는 단계,
- [0033] - 제1 거리, 신뢰된 거리, 및 제3 거리에 대한 검증 테스트를 수행하는 단계를 포함하고, 검증 테스트는 상기 거리들이 제1 디바이스, 제2 디바이스, 및 협력 디바이스의 실행가능한 공간 콘스텔레이션에 대응할 때 제1 거리를 신뢰성있는 것으로서 수용한다.
- [0034] 추가의 태양에 따르면, 제1 디바이스와 제2 디바이스 사이의 무선 통신을 통한 거리 측정에서 협력 디바이스로서 동작시키기 위한 방법이 제공되며, 협력 디바이스는 제1 디바이스로부터 신뢰된 거리에 위치된다. 무선 통신은 제1 디바이스에서의 측정 메시지의 도달 시간에 기초하여 제1 디바이스와 제2 디바이스 사이의 거리를 결정하기 위한 레인징 프로토콜을 포함하고, 프로토콜은 제2 디바이스에 의해 측정 메시지를 송신하는 것을 포함한다. 제1 디바이스는 제1 디바이스에서의 측정 메시지의 제1 도달 시간에 기초하여 제1 디바이스와 제2 디바이스 사이의 제1 거리를 획득하도록 배열된다. 본 방법은,
- [0035] - 협력 디바이스에서의 측정 메시지의 제3 도달 시간을 결정하는 단계, 및
- [0036] - 제3 도달 시간에 기초하는 지원 데이터를 제공하는 단계를 포함한다. 제1 디바이스는 결정된 거리를 평가하기 위해, 지원 데이터를 사용하여 협력 디바이스와 제2 디바이스 사이의 제3 거리를 획득하고, 제1 거리, 신뢰된 거리 및 제3 거리에 대한 검증 테스트를 수행하도록 배열되고, 검증 테스트는 상기 거리들이 제1 디바이스, 제2 디바이스 및 협력 디바이스의 실행가능한 공간 콘스텔레이션에 대응할 때 제1 거리를 신뢰성있는 것으로서 수용한다.
- [0037] 상기 특징들은, 제2 디바이스가 레인징 프로토콜에 참여할 때, 제1 디바이스가 제2 디바이스에 의해 송신된 바와 같은 측정 메시지의 제1 도달 시간에 기초하여 레인징 프로토콜에 따라 거리를 결정할 수 있는 효과를 갖는다. 또한, 제3 디바이스는 제3 디바이스에서의 동일한 측정 메시지의 제3 도달 시간을 결정한다. 제3 디바이스는 제1 디바이스로부터 일정 거리에 위치되고, 일정 거리는 제1 디바이스에게 알려져 있고 신뢰성있는 것으로서 신뢰된다. 그러한 거리는 본 명세서에서 신뢰된 거리로 지칭된다. 신뢰된 거리는 미리결정될 수 있거나, 별도로 측정될 수 있거나 또는 사용자에게 의해 입력될 수 있다. 그러한 제3 디바이스는 본 명세서에서 협력 디바이스로 지칭될 수 있다.
- [0038] 협력 디바이스로 동작하는 제3 디바이스는 몇몇 추가 측정 메시지들을 사용하여 레인징 프로토콜에 따른 추가 거리 측정을 수행하지 않는다는 것을 주목한다. 대신에, 제3 디바이스는 제3 디바이스에서의 상기 동일한 측정 메시지의 제3 도달 시간을 결정하고, 제3 도달 시간에 기초하는 지원 데이터를 제1 디바이스로 전달하도록 협력한다. 예를 들어, 지원 데이터는 기준 클록 또는 타이밍 그리드에 대한, 또는 제1 디바이스에 의해 또한 수신된 몇몇 다른 메시지의 수신에 대한 제3 도달 시간 데이터를 포함할 수 있다. 대안적으로 또는 추가적으로, 지원 데이터는 제3 거리 데이터를 포함할 수 있고, 제3 디바이스는 추가 수신 메시지들 및 신뢰된 거리를 사용함으로써 제3 디바이스와 제2 디바이스 사이의 제3 거리를 결정할 수 있다.
- [0039] 지원 데이터를 수신할 때, 프로세서는 지원 데이터를 사용하여 제3 디바이스와 제2 디바이스 사이의 제3 거리를 획득할 수 있게 된다. 후속적으로, 제1 거리, 신뢰된 거리 및 제3 거리에 대해 검증 테스트가 수행된다. 유리하게는, 검증 테스트는 상기 거리들이 제1 디바이스, 제2 디바이스 및 협력 디바이스의 실행가능한 공간 콘스텔레이션에 대응할 때 제1 거리를 신뢰성있는 것으로서 수용할 수 있다.
- [0040] 일 실시예에서, 검증 테스트는 실행가능한 공간 콘스텔레이션에 대한 코사인 법칙 검사 또는 삼각 부등식 검사를 포함한다. 유리하게는, 검사는 삼각형의 공간 콘스텔레이션이 변들의 각자의 길이들을 가질 수 있는지 여부를 증명한다.
- [0041] 일 실시예에서, 레인징 프로토콜은 키 데이터에 기초하여 암호로 보호되는 교환 메시지들을 포함하고, 제1 메시지 프로세서는 협력 디바이스와 키 데이터를 공유하도록 배열되어 제3 메시지 프로세서로 하여금 레인징 프로토콜에 따라 메시지들을 암호로 프로세싱할 수 있게 된다. 유리하게는, 제1 디바이스와 제3 디바이스 사이의 메시지들을 암호화하는 것은 그러한 메시지들이 잠재적으로 악성 제2 디바이스에 의해 탭핑되는 것으로부터 보호한다.
- [0042] 일 실시예에서, 제1 메시지 프로세서는 레인징 프로토콜에 따라 신뢰된 거리를 결정하도록 배열된다. 유리하게는, 제2 디바이스에 대한 실제 측정들에 앞서, 신뢰된 거리는 동일한 레인징 프로토콜을 사용하여 결정된다.
- [0043] 일 실시예에서, 디바이스는 상기 도달 시간들을 결정하기 위해 시간 기준을 제공하기 위한 클록 유닛을 포함하

고, 제1 메시지 프로세서는 시간 기준을 협력 디바이스 내의 대응하는 클록 유닛과 동기화시키도록 배열된다. 유리하게는, 시간 기준이 제1 디바이스와 제3 디바이스 사이에 공유된다. 제3 도달 시간은 시간 기준과 관련하여 결정될 수 있는데, 이는 지원 데이터가 그렇게 결정된 제3 도달 시간을 포함할 수 있게 하고 제1 디바이스에 의해 그와 같이 사용가능하다.

- [0044] 일 실시예에서, 라인징 프로토콜은 제1 디바이스를 포함하고, 제1 디바이스는 개시 디바이스로서 동작하고 개시 메시지를 제2 디바이스로 전송하는 한편, 개시 메시지의 수신 시, 제2 디바이스는 측정 메시지를 전송해야 한다. 제1 메시지 프로세서는 제3 디바이스와 역할-변경 데이터를 교환하여, 제3 디바이스가 거리 측정을 위해 개시 디바이스로서 동작할 수 있게 하도록 배열된다. 제3 디바이스는, 역할-변경 데이터를 수신할 때,
- [0045] - 제2 측정 메시지에 기초하여 라인징 프로토콜에 따라 제3 디바이스와 제2 디바이스 사이의 제3 거리를 획득하고,
- [0046] - 제3 거리를 나타내는 제3 지원 데이터를 제1 디바이스로 전달하도록 배열된다. 제1 메시지 프로세서는
- [0047] - 제1 디바이스에서 제2 측정 메시지를 수신할 때 제1 디바이스와 제2 디바이스 사이의 제2 거리를 결정하고,
- [0048] - 제3 디바이스로부터 제3 지원 데이터를 수신하고,
- [0049] - 제2 거리 및 제3 지원 데이터를 또한 사용하여 검증 테스트를 수행하도록 배열된다. 유리하게는, 상기 제2 거리를 결정하고 거리들 둘 모두를 결합하여 검증함으로써, 제2 디바이스가 거리 측정들 둘 모두를 일관되게 템퍼링하는 것이 더욱 곤란해진다.
- [0050] 일 실시예에서, 제3 메시지 프로세서는 제2 디바이스로부터 수신된 적어도 하나의 메시지의 제3 신호 강도를 결정하도록 배열되고, 제1 디바이스에 대한 지원 데이터에 제3 신호 강도 데이터를 포함시키도록 배열된다. 제1 메시지 프로세서는 제2 디바이스로부터 수신된 적어도 하나의 메시지의 제1 신호 강도를 결정하고, 결정된 거리들에서 제1 신호 강도 및 제3 신호 강도를 각자의 예상 신호 강도들과 비교함으로써 결정된 거리들이 신뢰성이 있는지 여부를 검증하도록 배열된다. 선택적으로, 제1 디바이스 및 제3 디바이스 둘 모두는 제2 디바이스로부터의 동일한 메시지의 신호 강도를 측정할 수 있다. 유리하게는, 결정된 거리들의 검증을 가능하게 하는 추가의 독립적인 메커니즘이 추가된다.
- [0051] 일 실시예에서, 제1 메시지 프로세서는, 결정된 거리가 신뢰성이 없는 것으로 평가될 때, 제2 디바이스에 의해 상이한 보안 프로토콜을 실행할 것을 요구하도록 배열된다. 유리하게는, 대안적으로 또는 추가적으로, 제1 메시지 프로세서는, 결정된 거리가 신뢰성이 없는 것으로 평가될 때, 상이한 라인징 프로토콜 및/또는 상이한 유형의 무선 통신을 사용하여 추가 거리 측정을 요청하도록 배열된다. 대안적으로 또는 추가적으로, 제1 메시지 프로세서는, 결정된 거리가 신뢰성이 없는 것으로 평가될 때, 제1 디바이스에서의 적어도 몇몇 데이터 및/또는 적어도 하나의 기능에 대한 액세스를 거부하거나 제한하도록 배열된다. 유리하게는, 제1 디바이스에서의 임의의 기능 또는 데이터에 대한 악성 액세스 또는 그의 사용이 방지된다.
- [0052] 본 발명의 추가의 태양에 따르면, 신뢰성있는 거리 측정을 위한 시스템은 전술된 바와 같이 디바이스 및 제3 디바이스, 및 제4 디바이스를 포함하며, 제2 협력 디바이스로서 동작하는 제4 디바이스는 제1 디바이스로부터 제2 신뢰된 거리에 위치되고 제3 디바이스로부터 제3 신뢰된 거리에 위치된다. 제4 디바이스는 메시지들을 수신하기 위한 제4 무선 수신기,
- [0053] 제4 디바이스에서 측정 메시지의 제4 도달 시간을 결정하고, 제4 도달 시간에 기초하는 제4 지원 데이터를 제1 디바이스로 전달하도록 배열된 제4 메시지 프로세서를 포함한다. 제1 메시지 프로세서는 제2 협력 디바이스로부터 제4 지원 데이터를 수신하고, 제4 지원 데이터를 사용하여 제4 디바이스와 제2 디바이스 사이의 제4 거리를 획득하고, 제2 신뢰된 거리 및 제4 거리를 사용하여 검증 테스트를 수행하도록 배열된다. 유리하게는, 상기 추가 거리를 결정하고 모든 거리들을 결합하여 검증함으로써, 제2 디바이스가 상기 거리들을 일관되게 조작하는 것이 더욱 곤란해진다.
- [0054] 선택적으로, 검증 테스트는 적어도 2개의 공간 콘스텔레이션들에 대한 삼각 부등식의 결합을 사용할 수 있으며, 각각의 콘스텔레이션은 제2 디바이스와 제1 디바이스 및 협력 디바이스들의 세트 중 2개의 디바이스들을 포함한다. 선택적으로, 제1 메시지 프로세서는, 제1 공간 콘스텔레이션에 따른 제2 디바이스의 제1 위치가 제2 공간 콘스텔레이션에 따른 제2 디바이스의 제2 위치에 대응하는지 여부를 검증하도록 배열될 수 있다.
- [0055] 선택적으로, 제1 메시지 프로세서는 모든 결정된 거리들이 0보다 더 큰지 여부를 검출하기 위한 불일치 검사를

사용하여 검증 테스트를 수행하도록 배열될 수 있다.

- [0056] 선택적으로, 제1 메시지 프로세서는, 제3 디바이스로부터 제1 디바이스로의 라인과 제4 디바이스로부터 제1 디바이스로의 라인 사이의 신뢰된 각도가 적어도 90도이도록 제3 디바이스 및 제4 디바이스가 배열되는 셋업에 기초하여 검증 테스트를 수행하도록 배열될 수 있다.
- [0057] 선택적으로, 제1 메시지 프로세서는, 제3 디바이스 및 제4 디바이스가 제1 디바이스에 대해 서로 반대편에 배열되는 셋업에 기초하여 검증 테스트를 수행하도록 배열될 수 있다.
- [0058] 선택적으로, 제1 메시지 프로세서는, 제2 신뢰된 거리가 신뢰된 거리에 대응하는 셋업에 기초하여 검증 테스트를 수행하도록 배열될 수 있다.
- [0059] 일 실시예에서, 시스템은 추가 협력 디바이스로서 동작하는 적어도 하나의 추가 디바이스를 포함하고, 제3 디바이스는, 제4 디바이스 및 적어도 하나의 추가 디바이스는 다각형의 에지들에서의 평면 내에 배열되고, 제1 디바이스는 다각형 내부에 있고, 제1 메시지 프로세서는
- [0060] - 적어도 2개의 공간 컨스텔레이션들에 대한 삼각 부등식들의 결합을 사용하여 검증 테스트를 수행하도록 배열되며, 각각의 컨스텔레이션은 제2 디바이스와 제1 디바이스 및 협력 디바이스들의 세트 중 2개의 디바이스들을 포함한다. 유리하게는, 상기 추가 거리를 결정하고 모든 거리들을 결합하여 검증함으로써, 제2 디바이스가 상기 거리들을 일관되게 조작하는 것이 더욱 곤란해진다.
- [0061] 일 실시예에서, 본 방법은 제1 도달 시간 또는 제1 거리를 제공하기 위해 개시 디바이스로서 동작할 것을 제1 디바이스에 지시하는 단계를 포함한다. 대안적으로 또는 추가적으로, 본 방법은 제3 도달 시간에 기초하는 지원 데이터를 제공하기 위해 협력 디바이스로서 동작할 것을 제3 디바이스에 지시하는 단계를 포함한다. 효과적으로, 거리 측정의 제어가 이제 상기 지시에 의해 수행된다.
- [0062] 위에서, 명료성의 이유들로 인해, 거리 측정 및 거리 신뢰성 검증을 수행하는 제1 디바이스가 기술되었음을 주목한다. 그러나, 제1 디바이스, 제3 디바이스 및/또는 추가의 협력 디바이스들이 모든 요구되는 정보를 거리 측정 및 거리 신뢰성 검증을 수행하는 제어 디바이스에 제공하는 것이 또한 가능하다.
- [0063] 본 발명에 따른 방법은 컴퓨터 구현 방법으로서 컴퓨터 상에서, 또는 전용 하드웨어에서, 또는 이들 둘 모두의 결합으로 구현될 수 있다. 본 발명에 따른 방법을 위한 실행 가능 코드는 컴퓨터 프로그램 제품에 저장될 수 있다. 컴퓨터 프로그램 제품들의 예들은 메모리 스틱과 같은 메모리 디바이스들, 광학 디스크와 같은 광학 저장 디바이스들, 집적 회로들, 서버들, 온라인 소프트웨어 등을 포함한다. 컴퓨터 프로그램 제품은, 상기 프로그램 제품이 컴퓨터에서 실행될 때 본 발명에 따른 방법을 수행하기 위해 컴퓨터 판독가능 매체에 저장된 비일시적 프로그램 코드 수단을 포함할 수 있다. 실시예에서, 컴퓨터 프로그램은 컴퓨터 프로그램이 컴퓨터 상에서 실행될 때 본 발명에 따른 방법의 모든 단계들 또는 스테이지들을 수행하도록 적응되는 컴퓨터 프로그램 코드 수단을 포함한다. 바람직하게는, 컴퓨터 프로그램은 컴퓨터 판독 가능 매체 상에 구현된다. 네트워크로부터 다운로드 가능하고/하거나 컴퓨터 판독 가능 매체 및/또는 마이크로프로세서 실행 가능 매체에 저장된 컴퓨터 프로그램 제품이 제공되며, 제품은 컴퓨터 상에서 실행될 때 전송된 바와 같은 방법을 구현하기 위한 프로그램 코드 명령어들을 포함한다.
- [0064] 본 발명의 다른 태양은 컴퓨터 프로그램을, 예를 들어 위치 기반 애플리케이션에 포함되는 다운로드에 사용할 수 있게 하는 방법을 제공한다. 이 태양은 컴퓨터 프로그램이 예를 들어 애플(Apple)의 앱 스토어(App Store), 구글(Google)의 플레이 스토어(Play Store), 또는 마이크로소프트(Microsoft)의 윈도우 스토어(Windows Store)에 업로드될 때, 그리고 컴퓨터 프로그램이 그러한 스토어로부터 다운로드가 가능할 때 사용된다.
- [0065] 본 발명에 따른 디바이스들 및 방법들의 추가의 바람직한 실시예들이 첨부된 청구항들에서 주어지며, 그 개시 내용은 본 명세서에 참고로 포함된다.

도면의 간단한 설명

- [0066] 본 발명의 이들 및 다른 태양이 다음 설명에서 그리고 첨부 도면을 참조하여 예로서 기술되는 실시예로부터 명백할 것이고 그러한 실시예를 참조하여 추가로 설명될 것이다.

도 1은 무선 통신 및 거리 측정을 위한 디바이스들을 도시한다.

도 2는 무선 통신을 위한 디바이스 및 협력 디바이스의 공간 컨스텔레이션을 도시한다.

도 3은 무선 통신을 위한 2개의 디바이스들의 공간 콘스텔레이션을 도시한다.

도 4는 무선 통신을 위한 2개의 디바이스들의 추가의 공간 콘스텔레이션을 도시한다.

도 5는 2개의 협력 디바이스들을 갖는 공간 콘스텔레이션을 도시한다.

도 6은 2개의 협력 디바이스들을 갖는 제2 공간 콘스텔레이션을 도시한다.

도 7은 2개의 협력 디바이스들을 갖는 추가의 공간 콘스텔레이션을 도시한다.

도 8은 거리 측정을 위한 방법을 도시한다.

도 9는 거리 측정에서 협력 디바이스로서 동작을 하는 방법을 도시한다.

도 10a는 컴퓨터 판독가능 매체를 도시한다.

도 10b는 프로세서 시스템의 개략도를 도시한다.

도면은 전적으로 도식적인 것이며, 일정한 축척으로 작성된 것은 아니다. 도면에서, 이미 기술된 요소에 대응하는 요소는 동일한 도면 부호를 가질 수 있다.

발명을 실시하기 위한 구체적인 내용

[0067] 후술되는 무선 통신을 사용하는 거리 측정 방법들 및 디바이스들은, 적어도 기본 기능을 제공하는데, 즉, 모바일 디바이스와 예컨대, 고정된 포지션 상의 다른 디바이스 사이의 현재 거리에 대한 정보를 제공한다. 다양한 프로토콜들이 측정 메시지들의 도달 시간들을 사용하는 적절한 레인징 프로토콜들의 예들로서 이제 설명되며, 이는 이후에 기술되는 실시예들을 사용하여 향상될 수 있다.

[0068] 거리 측정의 제1 예가 [802.11]에 기술된다. 조항 11.24.6은 미세 타이밍 측정(FTM) 절차를 명시한다. FTM 메커니즘은, RF 파들이 빛의 속도로 일 디바이스에서 다른 디바이스로 이동하는 데 걸리는 시간을 또한 보상할 수 있도록 2개의 디바이스들의 클럭들 사이의 절대 시간의 차를 측정하기 위한 것이다. FTM 절차에서, 2개의 디바이스 사이의 왕복 시간(RTT)을 다른 디바이스가 측정할 수 있는 것과 같은 방식으로 디바이스들 중 하나는 그 클럭의 타임 스탬프들을 다른 디바이스로 전송한다(추후 설명됨). 802.11(Wi-Fi)를 사용하는 2개의 디바이스들 사이의 거리 측정은 [802.11]의 조항 11.24.6에 명시된 미세 타이밍 측정(FTM) 절차를 사용하여 왕복 시간(RTT)을 측정하고, RTT를 빛의 속도로 곱하고 2로 나눔으로써 수행된다.

[0069] 다음은 [802.11]에서의 FTM의 설명이며, 예컨대, 도 11 내지 도 35, 도 11 내지 도 36, 도 11 내지 도 37 및 주변 텍스트를 참조한다. 아래의 타임 스탬프들의 넘버링은 도 11 내지 도 36에 따른다. 개시 STA(station)는, 다른 STA인 응답 STA에 대한 거리 또는 RTT를 알기 원한다. 이를 달성하기 위해서, 개시 STA는 초기 FTM 요청을 응답 STA에 전송한다. 응답 STA는 FTM₁(0, 0) 메시지를 개시 STA로 전송하고, 정확한 송신 시간을 측정한다. 응답 STA는 이 시간을 t_{1_1}로 저장한다. 개시 STA는 FTM₁(0, 0) 메시지의 수신을 t_{2_1}로서 측정한다. 이는 결과 ACK의 송신 시간을 t_{3_1}로서 측정한다. 그러나, 개시 STA는 아직 값들 t_{2_1} 및 t_{3_1}을 사용할 수 없다.

[0070] 응답 STA는 FTM₁(0, 0)에 대한 응답으로서 수신된 ACK의 수신 시간을 측정하여 이를 t_{4_1}로 저장한다. 잠시(적어도 Min Delta FTM 초) 후, 응답 STA는 FTM₂(t_{1_1}, t_{4_1})를 송신하고 송신 시간을 t_{1_2}로 기록한다. 이러한 개시 STA는 전송된 것과 동일한 루틴, 즉 FTM₂(t_{1_1}, t_{4_1})의 수신 시간을 t_{2_2}로 그리고 ACK의 송신 시간을 t_{3_2}로 측정하는 동일한 루틴을 거치게 된다. 그러나, 이 때, 개시 STA는 [802.11]로부터의 다음 수학적(11-5)에 따라 RTT를 측정할 수 있다.

[0071]
$$RTT = [(t_{4_1} - t_{1_1}) - (t_{3_1} - t_{2_1})] \quad (1)$$

[0072] 상기 식의 우변을 재정렬하면 다음 식과 같다.

[0073]
$$RTT = (t_{2_1} - t_{1_1}) + (t_{4_1} - t_{3_1}) \quad (2)$$

[0074] 여기서, (t_{2_1} - t_{1_1})은 FTM 프레임을 전달하는 동안 FTM 프레임이 RF 매체를 통해 요청 STA에서 개시 STA로 이동하는 시간이고 (t_{4_1} - t_{3_1})은 ACK 프레임이 RF 매체를 통해 개시 STA로부터 응답 STA로 이동하는 시간이므로, 그들의 합은 실제로 왕복 시간이라는 것을 용이하게 알 수 있다.

[0075] 정확도를 증가시키기 위하여, 상기의 것이 반복될 수 있고 RTT가 모든 측정들의 평균으로서 계산될 수 있다.

- [0076] $t1_X$ 는 출발 시간(TOD)이다. TOD는, "TOD [...]는 마지막으로 송신된 미세 타이밍 측정 프레임의 프리앰블의 시작이 송신 안테나 커넥터에 나타난 시간을 시간 기반으로 나타낸다."는 것으로 [802.11]에서 정의된다. 프리앰블은 PHY 프레임의 맨 처음 부분이고, 이는 무엇보다도 송신기가 프리앰블 직전에 어떠한 RF 에너지도 송신하지 않는다는 것을 의미한다. 따라서, 개시 STA는 동일한 방식으로 $t3_X$ 를 측정해야 하는데, 즉 $t3_X$ 는 수신된 미세 타이밍 측정 프레임에 대한 응답으로 마지막으로 송신된 ACK 프레임의 프리앰블의 시작이 송신 안테나 커넥터에 나타난 시간을 시간 기반으로 나타낸다.
- [0077] $t4_x$ 는 도달 시간이다. TOA는, "TOA [...]는 마지막으로 송신된 미세 타이밍 측정 프레임에 대해 Ack 프레임의 프리앰블의 시작이 수신 안테나 커넥터에 도달한 시간을 시간 기반으로 나타낸다."는 것으로 [802.11]에서 정의된다. 따라서, 개시 STA는 동일한 방식으로 $t2_X$ 를 측정해야 하는데, 즉 $t2_X$ 는 마지막으로 수신된 미세 타이밍 측정 프레임의 프리앰블의 시작이 수신 안테나 커넥터에 도달한 시간을 시간 기반으로 나타낸다.
- [0078] 따라서, 최소 시간 $t3 - t2$ 는 수신된 FTM(,) 프레임 + SIFS의 길이와 같고 최대 시간 $t3 - t2$ 는 수신된 FTM(,) 프레임 + DIFS의 길이와 같다. FTM(,) 프레임들의 길이는 변할 수 있다. 본 명세서의 나머지 부분에서, 다음 정의를 사용한다:
- [0079] - 개시 STA가 $t2$ 와 $t3$ 를 측정한 결과로 물리적 FTM 프레임의 시간 길이를 나타내도록 L_{ftm} 을 사용하고;
- [0080] - 개시 STA가 물리적 FTM 프레임의 마지막 심볼(즉, CRC 검사의 마지막 심볼)이 그의 수신 안테나 커넥터에 도달한 직후부터 FTM 프레임에 대한 응답으로 개시 STA가 보낸 ACK 프레임의 TOD까지 걸리는 시간으로서, 용어, 반응 시간 또는 개시 STA의 반응 시간 및 심볼, R을 사용한다. ACK 프레임을 전송하는 것은 다소 단순한 동작이기 때문에 하드웨어에서 수행될 가능성이 높으므로 일정할 수 있다.
- [0081] [802.11]의 조항 11.24.5는 타이밍 측정(TM) 절차를 명시한다. FTM 절차와 몇 가지 차이점들이 있지만, 가장 눈에 띄는 것은 타임 스탬프들의 더 양호한 레졸루션이며, 이는 원칙적으로 더 정확한 거리 측정을 가능하게 한다. 하기 실시예들은 FTM에 대해 본 명세서에 기술된 바와 같이 TM에 대해 동일한 방식으로 사용될 수 있다.
- [0082] FTM과 유사한 거리 측정 시스템의 추가 예가 미국 특허 제8762727B2호에 기술되어 있다. 차이점은, 개시자 STA를 소스 노드로 지칭하고 응답자 STA를 타깃 노드로 지칭하며 소스 노드가 $t1$ 및 $t4$ 를 측정하고 타깃 노드가 $t2$ 및 $t3$ 를 측정하여 이들을 소스 노드로 전송한다는 것이다.
- [0083] 거리 측정 시스템의 추가 예는, OTDOA(Observed Time Difference Of Arrival)로 지칭되는 3GPP에 기술되어 있으며, rel9 E-UTRA(LTE 라디오)에 도입된 포지셔닝 특징인 [OTDOA]를 참조하고, 아래에 설명된 바와 같이 참조 문헌들 [36.nnn]을 참조한다. 그것은 UE(User Equipment)가 여러 개의 eNodeB들(즉 기지국들)로부터 몇몇 특정 신호들인 PRS(Positioning Reference Signal)들 사이의 시간 차를 측정하고 이러한 시간 차들을 네트워크의 특정 디바이스, 위치 서버(the Evolved Serving Mobile Location Center - E-SMLC)에 보고하는 다각적 방법이다. 이들 시간 차들 및 eNodeB들 위치들에 대한 지식에 기초한다. E-SMLC는 UE들의 포지션을 계산한다. LPP(LTE 포지셔닝 프로토콜)의 설명은[36.355]사양에서 찾을 수 있다. PRS 신호들의 정확한 세부사항들은 [36.211]의 섹션 6.10.4에서 찾을 수 있으며, 단순한 OTDOA 절차는 [37.571-1] 사양의 섹션 9에 있는 RAN5 OTDOA 테스트 케이스들의 설명들에서 찾을 수 있다. Wi-Fi의 현지화에 대한 측정들과 마찬가지로, 모바일 디바이스는 이러한 OTDOA 보고서들을 위조하여 원하는 곳이면 어디든지 네트워크에 나타낼 수 있다. 아래의 이들 실시예들은 이러한 유형의 치팅에 대해 보호하기 위해 사용될 수 있다. UE에 의해 OTDOA에서 수행되는 동일한 측정들에 대한 다른 용어는 RSTD(Reference Signal Time Difference)이다. RSTD 측정 정확도 요건들은 [36.133]에 명시되어 있다.
- [0084] 3GPP에서의 거리 측정의 추가 예는 시간 그리드와 관련하여 메시지들의 도달 시간들에 기초하며 향상된 셀 ID 기반(Enhanced cell ID based) 또는 E-CID로 지칭된다. 셀 ID 기반 방법들은 이미 rel9 이전에 가능하였다. 향상된 셀 ID는 몇몇 이미 이용가능한 측정들을 함께 집성하며, 그들 중 몇몇은 포지셔닝 정확도 능력들을 개선하기 위해 정확도 요건들이 증가했다. 향상된 셀 ID, E-CellID, 또는 E-CID는 rel9 E-UTRA (LTE 라디오)에 도입된 포지셔닝 특징이다. UE는 서빙 셀 ID, 서빙 셀과의 타이밍 어드밴스(그의 송신과 수신 시간의 차), 기준(협대역) 신호 수신 전력(reference (narrowband) signal received power, RSRP/NRSRP), (협대역) 기준 신호 수신 품질((narrowband) reference signal received quality, RSRQ/RSRQ)을 네트워크에 (서빙 셀 또는 eNodeB를 통해 위치 서버, 진화된 서빙 모바일 위치 센터(Evolved Serving Mobile Location Center, E-SMLC)로) 보고한다. RSRP/NRSRP, 및 RSRQ/RSRQ는 임의의 이웃 셀로부터 측정 및 보고될 수 있지만, 타이밍 어드밴스는 프라이머리 셀(서빙 셀)에 대해서만 측정된다. 서빙 셀 또는 eNodeB는 도달 각도와 같은 추가 정보를 E-SMLC에 보고

할 수 있다. ESMC는 이러한 정보 및 셀들의 포지션들에 대한 그의 지식에 기초하여 UE 포지션을 추정한다.

[0085] 타이밍 어드밴스를 측정하는 것은 다음과 같다. LTE 또는 GSM에서, 셀은 전송 또는 수신 기회들의 주파수-시간 그리드를 고정된 타이밍으로 전송한다. LTE의 경우, 개별 주파수들은 OFDM 서브캐리어들의 주파수들이고, 보통 15 kHz 이격되어 있다. 시간 영역은 10ms의 연속 프레임들로 구성되며, 각각의 프레임은 10개의 서브프레임들로 구성되고 각각의 서브프레임은 0.5ms의 2개의 슬롯들로 구성된다. 이러한 주파수-시간 그리드는 셀에 의해 매우 엄격한 타이밍으로 유지된다. 그리드 요소 별로, 셀은 범위 내의 모든 모바일 디바이스들로 송신(브로드캐스트)하거나 하나의 특정 디바이스로 송신할 수 있다. 그리드 요소들(주파수, 서브프레임 결합 또는 때때로 주파수-슬롯 결합) 중 몇몇에서, 셀은 3GPP 사양들에 정의된 바와 같이 항상 송신할 것이다. 따라서, 이러한 그리드 요소들은, 유연하게 사용될 수 있는 그리드 요소들 각각의 목적과 같이, 시스템 정보를 셀 내의 모바일 디바이스들로 송신하는 데 이상적으로 적합하다. 다른 그리드 요소들, 따라서 더 유연하게 사용될 수 있는 요소들 각각에서, 셀이 범위 내의 모든 모바일 디바이스들에 브로드캐스팅하고 있을 수 있거나, 특정 모바일 디바이스로 송신하고 있을 수 있거나, 또는 셀 또는 셀 내의 다른 모바일 디바이스로 송신할 권한을 특정 모바일 디바이스에 부여했을 수 있다.

[0086] RF 파들이 셀로부터 모바일 디바이스(마이크로초당 약 300 미터)로 이동하는 데 시간이 걸리기 때문에, 그리드는 이러한 이동 시간만큼 모바일 디바이스로 지연되는 것처럼 나타날 것이다. 이 이동 시간이 t 초라고 가정한다. 모바일 디바이스가, 송신이 허용된 서브프레임의 시작부터 정확히 송신을 시작할 때, 그것은 셀에서의 서브프레임의 시작보다 t 초 늦게 송신을 시작한다. 모바일 디바이스에 의해 송신된 신호가 셀에 도달하는 데 다시 t 초가 걸린다. 따라서, 셀은, 그것에 할당된 서브프레임의 시작에서 정확히 시작하지 않고 $2t$ 초 후에 모바일 디바이스로부터의 송신을 수신한다. 이러한 지연을 측정함으로써, 셀은 모바일 디바이스까지의 거리를 결정할 수 있다.

[0087] 모바일 디바이스가 셀로부터 멀리 떨어져 있는 경우, 서브프레임에서의 모바일 디바이스의 송신의 끝이 다음 서브프레임의 시작보다 늦게 도달할 수 있으므로, 간섭이 발생할 수 있다. 이러한 문제를 극복하기 위해, 셀은 특정 모바일 디바이스로 어드레싱되는 타이밍 어드밴스 커맨드에서 소위 TA 값으로 코딩되는, 소정 양의 타이밍 어드밴스를 사용할 것을 모바일 디바이스에 요청할 수 있다. 이어서, 모바일 디바이스는 모바일 디바이스에 의해 결정된 바와 같이 서브프레임의 시작보다 먼저 그의 송신 TA를 시작한다. 타이밍 어드밴스에 대해 가능한 최대값은 0.67ms이며, 모바일 디바이스에서 셀까지의 거리가 100km를 약간 초과하는 것에 해당한다. 기술 사양 3GPP TS 36.321 [36.321], 섹션 6.1.3.5 "타이밍 어드밴스 커맨드 MAC 제어 요소"는 LTE에 대한 TA 값 조정 절차들을 기술한다.

[0088] 상이한 거리로 나타나길 원하는 모바일 디바이스는, 셀에 더 가깝게 있는 것으로 나타나길 원할 때에는 주파수-시간 그리드와 셀로부터 수신된 TA 값만큼 예상보다 일찍 송신을 시작할 수 있거나, 실제보다 셀에서 더 멀리 있는 것으로 나타나길 원할 때에는 예상보다 늦게 송신을 시작할 수 있다.

[0089] 정밀하고 정확한 거리 측정이 여러 응용들에서 중요하다. 예컨대, Wi-Fi FTM을 사용하여 Wi-Fi로 자동차에서 열쇠 고리까지의 거리를 측정하여 측정된 거리가 소위 5미터 미만일 때 자동차가 그 문들을 열 것을 결정할 수 있을 때 열쇠 고리까지의 실제 거리가 실제로 5미터 미만이라는 것이 중요하다. 다른 예는 다른 디바이스가 소정 거리보다 멀리 떨어져 있지 않은 경우에 디바이스가 단지 저작권이 있는 콘텐츠를 다른 디바이스로 스트리밍하도록 허용되는 경우일 수 있다. 정밀하고 정확한 거리 측정이 또한 보안 인증된 채널을 셋업할 때 중간자 공격들을 방지하는 데 사용될 수 있다. 이는 다음 단락들에서 설명된다.

[0090] 2개의 디바이스들이 그들의 유선 또는 무선 통신을 보안해야 할 때, 그들은 그들의 통신을 암호화할 수 있다. 그러나, 이는 무선 디바이스들 둘 모두가 동일한 키를 알 것을 요구한다. Diffie-Hellman(DH)은 두 당사자들 사이에 비밀 키를 확립하는 잘 알려진 기술이며, 비밀 키를 확립하기 위한 당사자들 사이의 통신은 확립된 비밀 키에 대한 어떠한 정보도 제3자들에게 공개하지 않는다. 두 당사자들은 각각 자신의 공개/개인 키 쌍을 사용하고 공개 키를 서로 교환한다. 각각의 당사자는 그 자신의 개인 키 및 다른 당사자의 공개 키 및 가능하게는 몇몇 다른 정보, 예컨대 각각의 당사자로부터의 임시값(난수)을 사용하여 비밀 키를 계산할 수 있다. 각각의 당사자는 Diffie-Hellman을 수행하거나 이전 키 쌍을 재사용할 때마다 키 쌍을 새로 생성할 수 있다.

[0091] 네트워크를 통해 Diffie-Hellman을 수행할 때, Diffie-Hellman을 수행하기 위한 공개 키를 수신한 디바이스는 이 공개 키가 어느 디바이스로부터 온 것인지 알지 못한다. 이는 소위 중간자 공격으로 공격자에 의해 활용될 수 있다. 공격자 E는 디바이스 A가 접속하려는 실제 디바이스 B로 가장할 수 있다. 공격자 E는 디바이스 A와 Diffie-Hellman을 수행하고 디바이스 A와 비밀 키 K_{AE} 를 확립한다. 마찬가지로 공격자는 디바이스 B에 대해 디

바이스 A로 가장하고 디바이스 B와 비밀 키 Kbe를 확립한다. 디바이스 A 또는 B 중 하나로부터 메시지가 수신되면, 공격자는 하나의 비밀 키를 이용하여 메시지를 암호해제하고, 다른 비밀 키를 이용하여 메시지를 암호화하고 이를 다른 디바이스로 포워딩한다. 이러한 방식으로, 디바이스들(A 및 B)은 약간의 추가 지연을 제외하고는 그들의 통신에서 어떠한 이상한 점도 알아차리지 못한다. 그들이 다른 통신 방법을 사용하여 동일한 정보를 전송하고 그 결과들을 비교함으로써 그들의 통신을 검사할 때, 그들은 그들의 통신에서 어떠한 탬퍼링도 알아차리지 못할 것이다. 그러나 공격자는 그들이 통신한 것에 대한 완전한 지식을 가지고 있다.

[0092] DPP(Device Provisioning Protocol)에서, 제1 단계는 DPP 부트스트래핑을 수행하는 것으로서, 즉 다른 디바이스의 공개 부트스트래핑 키의 신뢰를 얻고 이것이 중간자 디바이스의 공개 키가 아니라는 신뢰를 얻기 위한 절차이다. 부트스트래핑 방법들 중 하나는 다른 디바이스에 의해 디스플레이되거나 다른 디바이스 상에 인쇄된 바와 같이 다른 디바이스의 공개 부트스트래핑 키를 포함하는 QR 코드를 스캔하는 것이다. 다른 디바이스는 또한 제1 디바이스의 QR 코드(상호 인증)를 스캔할 수 있다. 그 후에, 부트스트래핑 키(들)는 DPP 인증 프로토콜에서 사용되며, 여기서 다른 디바이스가 또한 공개 부트스트래핑 키에 속하는 개인 키를 소유하는지 여부가 검사된다. DPP 내의 공개 부트스트래핑 키들이 Wi-Fi(임의의 형태의 Wi-Fi, 예컨대, NAN(Neighbor Awareness Network))를 통해 교환되었던 경우, 그들이 RF 범위 내의 어떠한 디바이스에 의해서 전송되었을 수 있으므로 그들은 신뢰될 수 없다. DPP를 계속 사용하면 DPP 인증 프로토콜은 공통 공유 키 Ke의 확립으로 이어질 것이지만, 디바이스는, 그들이 이 키를 의도된 디바이스와 또는 중간자 디바이스와 공유하고 있는지 여부를 알지 못한다. 유사하게, OWE(Opportunistic Wireless Encryption)를 사용할 때, 공개 키들이 Wi-Fi를 통해 그리고 Diffie-Hellman을 사용함으로써 교환되고, 2개의 디바이스들 사이의 후속 통신들의 암호화를 위해 공통 공유 키가 확립된다.

[0093] 그러나, 중간자 디바이스와 공통 공유 키를 셋업할 확률을 제한하는 방법은 디바이스들이 다른 디바이스까지의 거리를 측정하는 것이고 그 거리가 디바이스의 규칙에 의해 또는 그의 사용자에게 의해 결정된 바와 같이 소정 거리, 예컨대 몇 미터 미만인 경우 그들은 다른 디바이스로부터 수신된 공개 키를 신뢰한다. 이 경우 사용자는 Wi-Fi를 통해 공개 키를 전송한 디바이스, 즉 의도한 디바이스 또는 중간자 디바이스가 거리 제한 미만으로 떨어져 있음을 알 것이다. 이어서, 사용자는 의도한 디바이스 외에 이 범위 내에 어떤 다른 디바이스들이 있는지 여부를 판단할 수 있다.

[0094] 거리 측정을 사용하여 중간자 디바이스와 공통 공유 키를 셋업할 확률을 제한하는 것은 먼저 공개 키들을 Wi-Fi를 통해 교환하고 이어서, 예컨대 OWE 또는 DPP의 DPP 인증 프로토콜 부분(여기서 DPP 부트스트래핑이 Wi-Fi를 통해, 예컨대 Wi-Fi 인식으로 수행됨)에 의해 공유 세션 키를 계산함으로써 그리고 OWE(Opportunistic Wireless Encryption) 또는 DPP 또는 몇몇 다른 방법에 의해 또는 FTM_X 프레임들에서 t1 및 t4 값들을 포함하는 필드들을 적어도 암호화함으로써 결정된 공유 세션 키를 사용하여 암호화된 FTM_X 프레임들을 사용하여 FTM 절차를 후속적으로 실행함으로써 수행될 수 있다. 이렇게 측정된 요청 STA까지의 거리가 x미터 미만인 경우, 개시 STA는 수신된 공개 키를 신뢰할 수 있고 합의된 세션 키를 사용하여 다른 디바이스와 추가로 통신을 진행할 수 있다. DPP의 경우에, 추가 통신은 DPP 구성 프로토콜일 것이다. OWE의 경우에, 그것은 AP와 STA 사이의 암호화된 WAN 접속일 것이다. 개시 STA는 또한, 응답 STA까지 측정된 거리 내에 하나의 Wi-Fi 디바이스만이 있다는 것을 사용자가 확신하는지 여부를 사용자에게 질문할 수 있으며, 사용자가 이를 확인하면, 개시 STA는 공유 세션 키를 사용하여 진행한다.

[0095] 전송된 바와 같이, 응답 STA는, 개시 STA로 하여금 이것이 실제로 있는 거리가 아닌 또 다른 거리에 있는 것으로 믿게 만드는 이유를 가질 수 있다. 특히, 응답 STA는, 개시 STA로 하여금, t4_X 값들을 감소시킴으로써 그리고/또는 t1_x 값들을 증가시킴으로써 이것이 실제로 있는 것보다 더 가까이 있는 것으로 믿게 만들 수 있다. 이는 [802.11]로부터 식 (11-5)로부터 용이하게 명백하다.

[0096]
$$RTT = [(t4_X - t1_X) - (t3_X - t2_X)] \quad (3)$$

[0097] 2개의 디바이스들 사이의 거리는 다음과 같다:

[0098]
$$d = c * RTT / 2 \quad (4)$$

[0099] 여기서, c는 빛의 속도(약 3×10^8 m/s)이다.

[0100] 개시 STA에 의해 측정된 바와 같은 거리를 1 미터만큼 감소시키기 위해, 응답 STA는, 그들의 측정된 값들에서 t4_Z와 t1_X의 차를 약

- [0101] $\Delta t = 2 * 1 \text{ m} / 3 * 10^8 \text{ m/s} = 2 * 3.33 * 10^{-9} \text{ s} = 6.66 \text{ ns}$ (5)
- [0102] 만큼 감소시켜야 한다.
- [0103] 그러나, 응답 STA는, 개시 STA에 측정된 값들을 보고할 때 그들의 측정된 값들에서 $t4_X$ 와 $t1_X$ 의 차를 너무 많이 감소시키지 않도록 주의해야 하는데, 이는 이어서 개시 STA가 네거티브 RTT를 측정할 것이기 때문이다. 보고된 $t4_Z$ 와 $t1_X$ 의 차가 개시 STA의 반응 시간, 즉 $t3_X$ 와 $t2_X$ 사이의 차와 같을 때 개시 STA는 0의 왕복 시간을 측정할 것이다. 따라서, 성공적인 치팅을 위해서는 응답 STA가 개시 STA의 $t3_X$ 와 $t2_X$ 의 차를 아는 것이 중요하다.
- [0104] 전술한 바와 같이, 개시 STA의 $t3_X$ 와 $t2_X$ 의 차는 전송된 FTM PHY 프레임의 길이(L_{ftm})와 반응 시간 R의 2개의 부분들로 구성된다. 응답 STA는 FTM 프레임 자체를 전송했으므로, 프레임의 시간 길이(L_{ftm})를 알고 있다. 반응 시간 R은 다양한 방식으로 응답 STA에 알려질 수 있다.
- [0105] 치팅 디바이스가 개시 STA까지의 실제 거리를 어떻게든 알고 있으므로 보고된 $t1$ 및 $t4$ 를 적응시킴으로써 개시 STA가 측정할 거리를 정확하게 위조할 수 있는 것으로 가정한다. 따라서, 전술된 바와 같이 FTM을 사용하여 측정들을 수행할 때의 문제는 악성 응답 STA가 그의 보고된 도달 시간들 $t1$ 및 $t4$ 를 조작하여 이것이 실제보다 개시 STA에 더 가깝거나 더 멀리있는 것으로 나타날 수 있다는 것이다.
- [0106] 거리를 성공적으로 위조하는 것을 방지하기 위해서, 개시 디바이스는 개시 디바이스에 대해 알려진 포지션에 있는 하나 이상의 협력 디바이스들을 수반할 수 있다. 협력 디바이스는 개시 디바이스의 클록과 동기화된 클록들을 사용할 수 있거나 몇몇 다른 시간 기준을 공유할 수 있다. 협력 디바이스(들)는 측정 메시지들의 도달 시간(들)을 독립적으로 측정하고 이들을 개시 디바이스에 보고한다. 개시 디바이스는 삼각형들로부터의 속성들을 사용하여 치팅 응답 디바이스에 의해 조작된 도달 시간 측정들을 시도하고 검출한다. 3GPP 기반 시스템들의 경우, 개시 디바이스 및 하나 이상의 협력 디바이스들은 기지국들에 의해 구현될 수 있고 응답 디바이스는 사용자 장비 UE에 의해 구현된다.
- [0107] 거리 기반 측정을 더 신뢰할 수 있게 함으로써, 그것은 신뢰성있는 근접 기반 서비스들을 위한 실행가능한 도구가 된다. 몇몇 예시적인 사용 경우들은:
- [0108] - 당신이 근처에 있는 무선 키보드, 근처에 있는 무선 저장 디바이스, 근처에 있는 센서 또는 근처에 있는 무선 웹캠에 접속하는 경우, 당신은, 당신이 하고 있는 일을 모니터링하거나, 복사하거나 또는 추적하기 원하는 몇몇 중간자 디바이스에 접속하는 것이 아니라 정확한 디바이스에 접속했는지 확인하기 원한다.
- [0109] - 당신이 당신의 친구를 만나고 당신의 친구의 휴대폰에 접속하여 몇몇 사진들을 교환하기 원한다면, 당신은 중간자 디바이스가 아닌 당신 친구의 휴대폰에 확실히 접속하고 있는지 확인하기 원한다.
- [0110] - 집이나 상점에서 당신이 몇몇 디바이스들을 자동으로 켜고, 몇몇 문을 열거나 사람이 가까이 있을 때 그의 모바일 디바이스로 몇몇 서비스에 접속할 수 있게 하길 원한다면, 당신은 그 모바일 디바이스의 위치가 정확하고 근처에 있는 것으로 주장하는 가짜 디바이스가 아닌지 확인하기 원한다.
- [0111] - 상점에서 당신이 거래를 개시하려는 경우, 예를 들어, 레지스터에 가까울 때, 당신이 "피싱(phishing)" 공격을 받고 있지 않은지 확인하기 원하는데, 피싱 공격에 의해서 사용자가 인식하지 못한 채로 상점에서 제공하는 공식 서비스 대신 더 멀리 위치되어 있는 피싱 디바이스에 접속할 수 있다.
- [0112] 도 1은 무선 통신 및 거리 측정을 위한 디바이스들을 도시한다. 무선 통신을 위한 디바이스들의 공간 콘스텔레이션(100)은 제1 디바이스(110) 및 제2 디바이스(120)를 포함하며, 디바이스들은 거리(151)에서 물리적으로 떨어져 있다. 제1 디바이스는 메시지들의 송신 및 수신을 위한 제1 송수신기(111) 및 제1 메시지 프로세서(112)를 갖는다. 제2 디바이스는 무선 수신기(121), 또는 제2 송수신기 및 제2 메시지 프로세서(122)를 갖는다. 또한, 제3 디바이스는 제3 송수신기(131) 및 제3 메시지 프로세서(132)를 갖는다. 디바이스들은 송수신기들(111, 121, 131)에 접속된 안테나들(113, 123, 133)에 의해 개략적으로 나타내어진 바와 같이 무선 통신을 위해 장착된다.
- [0113] 디바이스들은, 아래에서 더 상세히 설명되는 바와 같이, 제1 디바이스와 제2 디바이스 사이의 거리를 결정하기 위해 제1 디바이스와 제2 디바이스 사이의 레인징 프로토콜에 따라 무선 통신을 통한 거리 측정을 위해 배열된다. 무선 통신은 제1 디바이스에서의 측정 메시지들의 도달 시간에 기초하여 제1 디바이스와 제2 디바이스 사이의 거리를 결정하기 위한 레인징 프로토콜을 포함한다. 프로토콜은 제2 디바이스에 의해 측정 메시지를 송신하는 것을 포함할 수 있다. 예들에서, 무선 통신 및 레인징 프로토콜은 [802.11]에 따르지만, 다른 무선 프로토

콜들, 예컨대 블루투스가 또한 사용될 수 있는데, 이는 도달 시간 측정에 기초하여 적절한 레인징 프로토콜을 제공한다.

- [0114] 제1 메시지 프로세서(112)는 레인징 프로토콜에 따라 메시지들을 프로세싱하고 제1 디바이스에서의 측정 메시지의 제1 도달 시간을 결정하고 제1 도달 시간에 기초하여 제1 디바이스와 제2 디바이스 사이의 제1 거리(151)를 결정하도록 배열된다. 또한, 제1 메시지 프로세서는 제3 디바이스(130)와 통신하도록 배열된다. 제3 디바이스는 협력 디바이스로서 동작하고, 제1 디바이스로부터 신뢰된 거리(150)에 위치된다. 신뢰된 거리는 제1 디바이스에 알려져 있고 신뢰성있는 것으로 신뢰된다. 신뢰된 거리는 미리결정될 수 있거나, 별도로 측정될 수 있거나 또는 사용자에게 의해 입력될 수 있다. 선택적으로, 제1 메시지 프로세서는 제3 디바이스에 의해 실행되는 레인징 프로토콜에 따라 신뢰된 거리를 결정하도록 배열된다. 제2 디바이스에 대한 실제 측정들에 앞서, 신뢰된 거리는 동일하거나 다른 레인징 프로토콜을 사용하여 결정될 수 있다.
- [0115] 협력 디바이스로서 지칭되는 제3 디바이스에서, 제3 메시지 프로세서(132)는 제3 디바이스에서의 측정 메시지의 제3 도달 시간을 결정하도록 배열된다. 특히, 제3 디바이스는 제3 디바이스에서 상기 동일한 측정 메시지의 제3 도달 시간을 결정함으로써 그리고 제3 도달 시간에 기초하는 지원 데이터를 제1 디바이스로 전달함으로써 제1 디바이스와 협력한다. 예를 들어, 지원 데이터는 기준 클럭 또는 타이밍 그리드에 대한, 또는 제1 디바이스에 의해 또한 수신된 몇몇 다른 메시지의 수신에 대한 제3 도달 시간 데이터를 포함할 수 있다. 대안적으로 또는 추가적으로, 지원 데이터는 제3 거리 데이터를 포함할 수 있다. 그에 대해, 제3 디바이스는, 예컨대 추가 수신 메시지들 및 신뢰된 거리를 사용함으로써 제3 디바이스와 제2 디바이스 사이의 제3 거리를 결정할 수 있다.
- [0116] 제1 메시지 프로세서는, 결정된 거리를 평가하기 위해, 협력 디바이스로부터 지원 데이터를 수신하고, 지원 데이터를 사용하여 제3 디바이스와 제2 디바이스 사이의 제3 거리(153)를 획득하도록 배열된다. 제1 메시지 프로세서는 후속하여 제1 거리(151), 신뢰된 거리(150) 및 제3 거리(153)에 대한 검증 테스트를 수행하도록 배열된다. 검증 테스트는 상기 거리들이 제1 디바이스, 제2 디바이스 및 협력 디바이스의 실행가능한 공간 콘스텔레이션에 대응할 때 제1 거리를 신뢰성있는 것으로서 수용할 수 있다. 예를 들어, 검증 테스트는 아래에서 추가로 설명될 바와 같이 실행가능한 공간 콘스텔레이션에 대한 코사인 법칙 검사 또는 삼각 부등식 검사를 포함한다. 검사는 삼각형의 실제 공간 콘스텔레이션이 결정된 거리들에 따라 변들의 각자의 길이들을 가질 수 있는지 여부를 증명하는 것을 목표로 한다.
- [0117] 레인징 프로토콜은 키 데이터에 기초하여 암호로 보호되는 메시지들을 교환하는 것을 포함할 수 있다. 선택적으로, 제1 메시지 프로세서는 협력 디바이스와 키 데이터를 공유하도록 배열되어 제3 메시지 프로세서가 레인징 프로토콜에 따라 메시지들을 암호로 프로세싱할 수 있게 된다. 이와 같이 알려진, 무선 통신 프로토콜에 따라 제1 디바이스와 제3 디바이스 사이의 메시지들을 암호화하는 것은 그러한 메시지들이 잠재적으로 악성 제2 디바이스에 의해 탭핑되는 것으로부터 보호한다.
- [0118] 선택적으로, 디바이스는 상기 도달 시간들을 결정하기 위한 시간 기준을 제공하는 클럭 유닛을 가질 수 있다. 제1 메시지 프로세서는 시간 기준을 협력 디바이스 내의 대응하는 클럭 유닛과 동기화하도록 배열될 수 있는데, 예컨대 [802.1AS]로부터의 프로토콜과 동기화될 수 있다. 효과적으로, 시간 기준이 제1 디바이스와 제3 디바이스 사이에서 공유될 수 있다. 제3 도달 시간은 시간 기준에 대해 결정될 수 있는데, 이는 지원 데이터가 그렇게 결정된 제3 도달 시간을 포함할 수 있게 하고 제1 디바이스에 의해 그와 같이 사용가능하게 한다.
- [0119] 다음에서, 하나 이상의 협력 STA들의 추가는 응답 STA들이 그들이 실제로 있는 것보다 개시 STA에 더 가까이 있는 것으로 나타나기를 원하는 것을 검출하는 데 도움이 될 수 있는 방법 및 그에 대한 범위가 설명된다. 다음 가정들이 적용될 수 있다:
- [0120] • 응답 STA는, 이것이 개시 STA에 대해 어떤 거리에 나타나도록 개시 STA에 보고하는 측정들을 조정하는 방법을 알고 있고;
- [0121] • 개시 STA 및 협력 STA(들)은 802.1AS 프로토콜[802.1AS]과 동기화된 물리적 프레임들의 도달 시간 및 출발 시간을 타이밍(time)하는 그들의 클럭들을 가질 수 있거나, 또는 다른 방식으로 통신하여, 개시 STA는 대응하는 STA(들)의 어느 측정들이 그 자신의 어느 측정들과 결합할지를 알게 되고;
- [0122] • 개시 STA 및 협력 STA(들)는 협력 STA들이 응답 STA로부터 FTM(,) 메시지들을 수신, 식별 및 필요한 경우 암호해제할 수 있도록 협력 STA(들)에 필요한 정보를 공유하고, 따라서, 협력 STA(들)는 응답 STA로부터의 FTM(,) 메시지들의 도달 시간을 측정하고 이들을 개시 STA에 보고할 수 있으므로, 개시 STA는 이러한 도달 시간들을 동

일한 메시지들에 대한 그 자신의 측정들과 결합할 수 있다;

- [0123] • FTM 측정들은 2회 이상 수행될 수 있고 모든 STA들의 측정 및 보고된 시간들 t_1 , t_2 , t_3 및 t_4 는 이들이 거리 및 위치 계산들에 사용되기 전에 먼저 평균화될 수 있으므로, 측정 정확도는 결과들을 신뢰할 수 있도록 충분히 양호하다.
- [0124] 타이밍 측정들만을 수행할 수 있는 STA들에 대한 강력한 공격에 대한 양호한 방어가 아래에 설명된다. 그러한 방어에서, 개시 STA는 하나 이상의 협력 STA들과 함께 작동하며, 도시된 바와 같이 삼각 부등식을 적용하고, 2개 이상의 협력 STA들의 경우에는, 계산된 포지션들에서 불일치 검사들을 적용한다. 상세한 예들은[802.11]의 FTM 프로토콜을 사용하여 주어진다. 그러나, 그것은 Wi-Fi, Bluetooth 또는 다른 무선(또한 광학) 기술을 사용하는 범위 측정 기술과도 잘 작동하며, 여기서 하나의 디바이스가 프로토콜 메시지들의 출발 시간, 도달 시간, 또는 이들의 차를 다른 디바이스에 보고한다.
- [0125] 도 2는 무선 통신을 위한 디바이스 및 협력 디바이스의 공간 콘스텔레이션을 도시한다. 콘스텔레이션(200)은, 도 1을 참조하여 기술된 디바이스들과 유사하게, 개시 STA로 지칭되는 제1 디바이스(210), 응답 STA로 지칭되는 제2 디바이스(220), 및 협력 STA로 지칭되는 제3 디바이스(230)를 포함한다. 제1 거리 d_{1c} 가 실제 거리 d_1 (또는 d)에 있는 제1 디바이스(210)와 제2 디바이스(220) 사이에서 결정된다. 제3 거리 d_{2c} 가 제3 디바이스(230)와 제2 디바이스(220) 사이에서 결정된다. 신뢰된 거리 L 은, 실제 거리 d_2 에 있는 제1 디바이스(210)와 제3 디바이스(230) 사이에 있다.
- [0126] 예에서, 치팅 응답 STA로부터 개시 STA까지의 실제 거리는 d 이고, 이는 또한, 치팅 응답 STA로부터 협력 STA까지의 거리이다. 개시 STA는 전술된 방법들 중 임의의 것을 이용하여 치팅 응답 STA에 대한 거리 측정을 수행한다. 나머지에서, FTM 프로토콜을 가정한다.
- [0127] 각각의 거리 측정의 경우, 개시 STA는, 치팅 응답 STA가 전송한 FTM(t_{1X} , t_{4X}) 물리적 프레임의 도달 시간(t_{2X})으로서 협력 STA가 측정한 것을 협력 STA에게 요청한다. $_c$ 가 첨부되어 있는 거리들은 디바이스가 계산한 대응하는 거리들이다.
- [0128] 이어서, 개시 STA는 통상적으로 거리 d 를 계산한다:
- [0129]
$$RTT = [(t_{4X} - t_{1X}) - (t_{3X} - t_{2X})] \quad (6)$$
- [0130] 2개의 디바이스들 사이의 거리는 다음과 같다:
- [0131]
$$dL_c = c * RTT / 2 = c * [(t_{4X} - t_{1X}) - (t_{3X} - t_{2X})] / 2 \quad (7)$$
- [0132] 여기서, c 는 빛의 속도(약 3×10^8 m/s)이다. 모든 측정들이 정확하게 수행되고 보고되었다면, 계산된 dL_c 는 측정 정확도 내에서 실제 거리 d 에 대응할 것이다.
- [0133] 치팅 응답 STA가, 이것이 d 대신 위조된 거리 f 에 있는 것으로 개시 STA가 간주하기를 원한다고 가정한다. 치팅 응답 STA는 t_{4X} 및 t_{1X} 를 측정했다. 이를 위해, 응답 STA는 t_{4rX} 와 t_{1rX} 의 값들을 변경하여 그 차이가 $2 * (d - f) / c$ 인 것으로 보고하는데, 이는 실제로 측정된 t_{4X} 와 t_{1X} 의 차보다 작다. 따라서, 치팅 응답 STA가 개시 STA에 보고한 시간들은 다음과 같다:
- [0134]
$$(t_{4rX}, t_{1rX}) = (t_{4X} - (1 - \alpha) * (2 * (d - f) / c), t_{1X} + \alpha * (2 * (d - f) / c)) \quad (8)$$
- [0135] 여기서, α 는 자유롭게 선택될 수 있다.
- [0136] 응답 STA에 의해 보고된 바와 같은 (t_{4rX} , t_{1rX})를 사용하여, 개시 STA는 응답 STA와 그 자신 사이의 거리 dL_c 를 다음과 같이 계산할 수 있다.
- [0137]
$$dL_c = c * RTT / 2$$
- [0138]
$$= c * [(t_{4X} - (1 - \alpha) * (2 * (d - f) / c) - (t_{1X} + \alpha * (2 * (d - f) / c))) - (t_{3X} - t_{2X})] / 2$$
- [0139]
$$= c * [(t_{4X} - t_{1X}) - (t_{3X} - t_{2X}) - (2 * (d - f) / c)] / 2$$
- [0140]
$$= c * [(t_{4X} - t_{1X}) - (t_{3X} - t_{2X})] / 2 - c * (2 * (d - f) / c) / 2$$
- [0141]
$$= d - (d - f)$$
- [0142]
$$= f \quad (9)$$

- [0143] 이러한 계산된 거리는 실제로, 치팅 응답 STA가, 개시 STA가 계산하기 원했던 것이다.
- [0144] 응답 STA에 의해 보고된 ($t4_r_X$, $t1_r_X$) 및 협력 STA로부터 획득된 $t2c_X$ 를 사용하여, 개시 STA는 응답 STA와 협력 STA 사이의 거리 $d2_c$ 를 다음과 같이 계산할 수 있다.
- [0145]
$$d2_c = d1_c + c * (t2c_X - t2_X) \quad (10)$$
- [0146] 변들 A, B 및 C를 가진 임의의 삼각형의 경우, 다음 부등식이 성립되어야 한다(삼각 부등식).
- [0147]
$$|C| \leq |A| + |B| \quad (11)$$
- [0148] 따라서, 도 2의 콘스텔레이션에서, 다음 2개의 부등식들은 개시 STA에 의해 측정된 거리들에 대해서 뿐만 아니라 실제 거리들에 대해서도 참이어야 한다.
- [0149]
$$L \leq d1 + d2 \quad (12)$$
- [0150]
$$L \leq 2 * d1 + c * (t2c_X - t2_X) \quad (13)$$
- [0151] 개시 STA는 위의 2개의 부등식들이 측정된 거리들 $d1_c$ 및 $d2_c$ 에 대해 성립되는지 여부를 검사할 수 있다.
- [0152]
$$L \leq d1_c + d2_c \quad (14)$$
- [0153]
$$L \leq d1_c + d1_c + c * (t2c_X - t2_X) \quad (15)$$
- [0154]
$$L \leq 2 * f + c * (t2c_X - t2_X) \quad (16)$$
- [0155] 도 2의 콘스텔레이션에서, $d1$ 및 $d2$ 가 동일하므로, $t2c_X$ 및 $t2_X$ 가 동일하다. 그것은 치팅 응답 STA가 다음과 같이 f 를 선택하면 부등식 (16)이 더 이상 성립되지 않을 것을 뜻한다:
- [0156]
$$f < L / 2 \quad (17)$$
- [0157] 이는, 도 2의 콘스텔레이션에서, 개시 STA가, 응답 STA가 개시 STA에 대해 $L / 2$ 보다 더 가까이 있는 것으로 나타나도록 그의 측정들을 위조했음을 검출할 수 있음을 뜻한다
- [0158] 도 3은 무선 통신을 위한 2개의 디바이스들의 공간 콘스텔레이션을 도시한다. 콘스텔레이션(300)은, 도 1을 참조하여 기술된 디바이스들과 유사하게, 개시 STA로 지칭되는 제1 디바이스(310), 응답 STA로 지칭되는 제2 디바이스(320), 및 협력 STA로 지칭되는 제3 디바이스(330)를 포함한다. 제1 거리 $d1_c$ 가 실제 거리 $d1$ (또는 d)에 있는 제1 디바이스(310)와 제2 디바이스(320) 사이에서 결정된다. 제3 거리 $d2_c$ 가 실제 거리 $d2$ 에 있는 제3 디바이스(330)와 제2 디바이스(320) 사이에서 결정된다. 신뢰된 거리(L)는 제1 디바이스(310)와 제3 디바이스(330) 사이에 있다.
- [0159] 이 예에서, 개시 STA는 치팅 응답 STA까지의 거리로서 f 를 측정할 것이고 협력 STA와 치팅 응답 STA 사이의 거리로서 $f - L$ 을 결정할 것이다.
- [0160] 이제, 부등식(14)은 다음과 같을 것이다.
- [0161]
$$L \leq d1_c + d2_c \quad (18)$$
- [0162]
$$L \leq 2 * f - L \quad (19)$$
- [0163]
$$L \leq f(20)$$
- [0164] 이는 f 가 L 보다 더 크거나 같은 경우에만 성립한다. 따라서, 제안된 방어는 도 3의 콘스텔레이션에서 작동하며, 개시 STA가, 응답 STA가 개시 STA에 대해 L 보다 더 가까이 있는 것으로 나타나도록 그의 측정들을 위조했음을 검출할 수 있다.
- [0165] 도 4는 무선 통신을 위한 2개의 디바이스들의 추가의 공간 콘스텔레이션을 도시한다. 콘스텔레이션(400)은, 도 1을 참조하여 기술된 디바이스들과 유사하게, 개시 STA로 지칭되는 제1 디바이스(410), 응답 STA로 지칭되는 제2 디바이스(420), 및 협력 STA로 지칭되는 제3 디바이스(430)를 포함한다. 제1 거리 $d1_c$ 가 실제 거리 $d1$ (또는 d)에 있는 제1 디바이스(410)와 제2 디바이스(420) 사이에서 결정된다. 제3 거리 $d2_c$ 가 실제 거리 $d2$ 에 있는

제3 디바이스(430)와 제2 디바이스(420) 사이에서 결정된다. 신뢰된 거리(L)는 제1 디바이스(410)와 제3 디바이스(430) 사이에 있다.

[0166] 예에서, 코사인 법칙이 사용된다. $d2$ 는 다음과 같이 계산된다:

$$d2^2 = d1^2 + L^2 - 2 * d1 * L * \cos(\phi) \quad (21)$$

[0168] 다음과 같은 방식으로 a 를 사용하여 $d1$ 과 L 을 관련시킨다.

$$d1 = a * L \quad (22)$$

[0170] 다음 식을 얻는다.

$$d2 = \sqrt{(a * L)^2 + L^2 - 2 * a * L * L * \cos(\phi)}$$

$$= L * \sqrt{a^2 + 1 - 2 * a * \cos(\phi)} \quad (23)$$

[0173] 그러나, 치팅 응답 STA는 그가 개시 STA에게 전송하는 정보를 변경하여 거리들 $d1_c$ 및 $d2_c$ 는 다음과 같을 것이다.

$$d1_c = d1 - (d1 - f) \quad (24)$$

$$d2_c = d2 - (d1 - f) \quad (25)$$

[0176] 개시 STA는, 부등식 (14)가 그것이 측정되었던 거리들에 대해 성립하는지 여부를 검사한다.

$$L \leq d1_c + d2_c \quad (26)$$

$$L \leq f + L * \sqrt{a^2 + 1 - 2 * a * \cos(\phi)} - a * L + f \quad (27)$$

$$L \leq 2 * f + L * \{ \sqrt{a^2 + 1 - 2 * a * \cos(\phi)} - a \} \quad (28)$$

$$f \geq 0.5 * L * \{ 1 + a - \sqrt{a^2 + 1 - 2 * a * \cos(\phi)} \} \quad (29)$$

[0181] 따라서, 개시 STA는, 다음 부등식에서와 같이 응답 STA가 f 를 선택할 때 그의 보고된 측정들을 위조하는 응답 STA를 검출할 것이다.

$$f / L < 0.5 * \{ 1 + a - \sqrt{a^2 + 1 - 2 * a * \cos(\phi)} \} = TI \quad (30)$$

[0183] 테이블 1은 $\alpha \geq 0$ 와 $0 \leq \phi \leq 90$ 도의 결합들에 대한 TI 의 값들을 나타낸다.

$\alpha \backslash \phi$	0.0	10.0	20.0	30.0	40.0	50.0	60.0	70.0	80.0	90.0
0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
0.10	0.10	0.10	0.10	0.09	0.09	0.08	0.07	0.06	0.06	0.05
0.20	0.20	0.20	0.19	0.18	0.17	0.16	0.14	0.12	0.11	0.09
0.30	0.30	0.30	0.29	0.27	0.25	0.23	0.21	0.18	0.15	0.13
0.40	0.40	0.39	0.38	0.36	0.33	0.30	0.26	0.23	0.19	0.16
0.50	0.50	0.49	0.47	0.44	0.40	0.36	0.32	0.27	0.23	0.19
0.51	0.51	0.50	0.48	0.45	0.41	0.37	0.32	0.28	0.23	0.19
0.55	0.55	0.54	0.52	0.48	0.44	0.39	0.34	0.29	0.25	0.20
0.60	0.60	0.59	0.56	0.52	0.47	0.42	0.36	0.31	0.26	0.22
0.70	0.70	0.68	0.64	0.59	0.53	0.47	0.41	0.35	0.29	0.24
0.80	0.80	0.77	0.72	0.65	0.58	0.51	0.44	0.38	0.32	0.26
0.90	0.90	0.85	0.78	0.70	0.62	0.55	0.47	0.40	0.34	0.28
1.00	1.00	0.91	0.83	0.74	0.66	0.58	0.50	0.43	0.36	0.29
1.10	1.00	0.95	0.86	0.77	0.69	0.60	0.52	0.45	0.37	0.31
1.20	1.00	0.96	0.89	0.80	0.71	0.63	0.54	0.46	0.39	0.32
1.30	1.00	0.97	0.90	0.82	0.73	0.65	0.56	0.48	0.40	0.33
1.40	1.00	0.97	0.91	0.83	0.75	0.66	0.58	0.49	0.41	0.34
1.50	1.00	0.98	0.92	0.85	0.76	0.68	0.59	0.50	0.42	0.35
1.60	1.00	0.98	0.93	0.86	0.77	0.69	0.60	0.51	0.43	0.36
1.70	1.00	0.98	0.93	0.86	0.78	0.70	0.61	0.52	0.44	0.36
1.80	1.00	0.98	0.94	0.87	0.79	0.71	0.62	0.53	0.45	0.37
1.90	1.00	0.98	0.94	0.88	0.80	0.71	0.63	0.54	0.46	0.38
2.00	1.00	0.99	0.94	0.88	0.80	0.72	0.63	0.55	0.46	0.38
3.00	1.00	0.99	0.96	0.90	0.84	0.76	0.68	0.59	0.50	0.42
4.00	1.00	0.99	0.96	0.91	0.85	0.78	0.70	0.61	0.52	0.44
5.00	1.00	0.99	0.96	0.92	0.86	0.79	0.71	0.62	0.54	0.45
6.00	1.00	0.99	0.96	0.92	0.86	0.79	0.72	0.63	0.55	0.46
7.00	1.00	0.99	0.97	0.92	0.87	0.80	0.72	0.64	0.55	0.46
8.00	1.00	0.99	0.97	0.92	0.87	0.80	0.73	0.64	0.56	0.47
9.00	1.00	0.99	0.97	0.93	0.87	0.80	0.73	0.65	0.56	0.47
10.00	1.00	0.99	0.97	0.93	0.87	0.81	0.73	0.65	0.56	0.48
100.00	1.00	0.99	0.97	0.93	0.88	0.82	0.75	0.67	0.58	0.50
1000.00	1.00	0.99	0.97	0.93	0.88	0.82	0.75	0.67	0.59	0.50

[0184]

[0185] 테이블 2는 $\alpha \geq 0$ 와 $90 \leq \phi \leq 180$ 도의 결합들에 대한 TI 의 값들을 나타낸다.

$\alpha \backslash \phi$	90.0	100.0	110.0	120.0	130.0	140.0	150.0	160.0	170.0	180.0
0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
0.10	0.05	0.04	0.03	0.02	0.02	0.01	0.01	0.00	0.00	0.00
0.20	0.09	0.07	0.06	0.04	0.03	0.02	0.01	0.01	0.00	0.00
0.30	0.13	0.10	0.08	0.06	0.04	0.03	0.02	0.01	0.00	0.00
0.40	0.16	0.13	0.10	0.08	0.05	0.03	0.02	0.01	0.00	0.00
0.50	0.19	0.15	0.12	0.09	0.06	0.04	0.02	0.01	0.00	0.00
0.60	0.22	0.17	0.13	0.10	0.07	0.05	0.03	0.01	0.00	0.00
0.70	0.24	0.19	0.15	0.11	0.08	0.05	0.03	0.01	0.00	0.00
0.80	0.26	0.21	0.16	0.12	0.08	0.05	0.03	0.01	0.00	0.00
0.90	0.28	0.22	0.17	0.13	0.09	0.06	0.03	0.01	0.00	0.00
1.00	0.29	0.23	0.18	0.13	0.09	0.06	0.03	0.02	0.00	0.00
1.10	0.31	0.25	0.19	0.14	0.10	0.06	0.04	0.02	0.00	0.00
1.20	0.32	0.25	0.20	0.15	0.10	0.07	0.04	0.02	0.00	0.00
1.30	0.33	0.26	0.20	0.15	0.11	0.07	0.04	0.02	0.00	0.00
1.40	0.34	0.27	0.21	0.16	0.11	0.07	0.04	0.02	0.00	0.00
1.50	0.35	0.28	0.22	0.16	0.11	0.07	0.04	0.02	0.00	0.00
1.60	0.36	0.29	0.22	0.16	0.11	0.07	0.04	0.02	0.00	0.00
1.70	0.36	0.29	0.23	0.17	0.12	0.08	0.04	0.02	0.00	0.00
1.80	0.37	0.30	0.23	0.17	0.12	0.08	0.04	0.02	0.00	0.00
1.90	0.38	0.30	0.23	0.17	0.12	0.08	0.04	0.02	0.00	0.00
2.00	0.38	0.31	0.24	0.18	0.12	0.08	0.05	0.02	0.01	0.00
3.00	0.42	0.34	0.26	0.20	0.14	0.09	0.05	0.02	0.01	0.00
4.00	0.44	0.36	0.28	0.21	0.15	0.10	0.05	0.02	0.01	0.00
5.00	0.45	0.37	0.29	0.22	0.15	0.10	0.06	0.03	0.01	0.00
6.00	0.46	0.37	0.29	0.22	0.16	0.10	0.06	0.03	0.01	0.00
7.00	0.46	0.38	0.30	0.23	0.16	0.10	0.06	0.03	0.01	0.00
8.00	0.47	0.38	0.30	0.23	0.16	0.11	0.06	0.03	0.01	0.00
9.00	0.47	0.39	0.31	0.23	0.16	0.11	0.06	0.03	0.01	0.00
10.00	0.48	0.39	0.31	0.23	0.16	0.11	0.06	0.03	0.01	0.00
100.00	0.50	0.41	0.33	0.25	0.18	0.12	0.07	0.03	0.01	0.00
1000.00	0.50	0.41	0.33	0.25	0.18	0.12	0.07	0.03	0.01	0.00

[0186]

[0187] 응답 STA가 그것이 거리 $0.5 \cdot L$ 또는 더 가까운 거리에 있는 것처럼 위조하길 원한다는 것을 검출하는 것에 관심이 있는 것을 가정한다. 따라서, ($0.5 \cdot L$ 더 멀리 있는) 위조 STA가 $0.5 \cdot L$ 더 가깝게 나타내어지길 원하는 경우, 이는 위조 STA가 비음영 영역 내에 있는 경우 검출될 수 있다. 따라서, 이러한 위조 STA들에 대한 측정된 거리가 $0.5 \cdot L$ 미만일 것인데, 그 거리가 그의 의도이기 때문이다.

[0188] STA가 실제로 $0.5 \cdot L$ 이내에 있는 경우, 이를 위조할 필요가 없으므로, 테이블 1에서 $\alpha \leq 0.5$ 인 경우의 영역에는 음영이 없다.

[0189] 테이블 1과 테이블 2의 회색 음영 영역은 응답 STA와 개시 STA 사이의 실제 거리가 $0.5 \cdot L$ 보다 먼 경우(따라서 $\alpha > 0.5$), 및 개시 STA는, 응답 STA가 $0.5 \cdot L$ 이하의 거리로 나타내어지길 원한다는 것을 검출할 수 없는 경우이다. 제안된 방법은 $0 \leq \phi \leq 90$ 도인 경우의 넓은 영역에 존재하는 치팅 응답 STA로부터 보호한다. 그러나, 방법은 $90 < \phi \leq 180$ 도인 경우의 영역에서는 치팅 응답 STA들에 대해 보호하지 못한다. 이에 대해, 추가의 협력 디바이스를 사용하는 것이 제안된다. 따라서, 거리 측정을 위한 시스템은 제1 디바이스 및 적어도 2개의 협력 디바이스들을 포함할 수 있다. 다양한 예들이 아래에서 논의된다. 그러한 시스템에서, 제2 협력 디바이스로서 동작하는 제4 디바이스는 제4 디바이스에서의 측정 메시지의 제4 도달 시간을 결정하고 제4 도달 시간에 기초하는 제4 지원 데이터를 제1 디바이스로 전달하도록 배열된 제4 메시지 프로세서를 가질 수 있다. 제1 메시지 프로세서는 제2 협력 디바이스로부터 제4 지원 데이터를 수신하고, 제4 지원 데이터를 사용하여 제4 디바이스와 제2 디바이스 사이의 제4 거리를 획득하고, 제2 신뢰된 거리 및 제4 거리를 또한 사용하여 검증 테스트를 수행하도록 배열된다.

[0190] 일 실시예에서, 검증 테스트는 제1 디바이스, 제2 디바이스 및 제3 디바이스의 제1 공간 콘스텔레이션에 대한 제1 삼각 부등식, 및 제1 디바이스, 제2 디바이스 및 제4 디바이스의 제2 공간 콘스텔레이션에 대한 제2 삼각 부등식의 결합을 사용한다. 검증 테스트는 아래의 삼각 부등식 및 2개의 협력 STA들을 사용하는 것에 대한 단락에서 논의된 테스트들을 포함할 수 있다. 대안적으로, 검증 테스트는 더 나은 방식으로 삼각 부등식 및 2개의 협력 STA들을 사용하여 이후의 섹션에 기술된 바와 같이 2개의 협력 STA들을 사용할 수 있다. 이를 위해, 2

개의 협력 디바이스들 사이의 거리는 제1 디바이스에 의해 알려질 수 있다.

- [0191] 일 실시예에서, 검증 테스트는, 제1 공간 콘스텔레이션에 따른 제2 디바이스의 제1 위치가 제2 공간 콘스텔레이션에 따른 제2 디바이스의 제2 위치에 대응하는지 여부를 검증할 수 있다. 선택적으로, 검증 테스트는 모든 결정된 거리들이 0보다 더 큰지 여부를 검출하기 위한 불일치 검사를 사용할 수 있다.
- [0192] 또한, 검증 테스트는 제1 및 제2 신뢰된 거리를 초과하여, 즉 제1, 제3 및 제4 디바이스의 전체 콘스텔레이션에 기초할 수 있다. 예를 들어, 이는 개시 디바이스와 협력 디바이스들 둘 모두 사이의 접속 라인들 사이의 신뢰된 각도를 사용함으로써 수행될 수 있다. 선택적으로, 검증 테스트는, 제3 디바이스 및 제4 디바이스가, 제3 디바이스로부터 제1 디바이스로의 라인과 제4 디바이스로부터 제1 디바이스로의 라인 사이의 신뢰된 각도가 적어도 90도이도록 배열되는 셋업에 기초할 수 있다. 선택적으로, 검증 테스트는, 제3 디바이스 및 제4 디바이스는 제1 디바이스에 대해 서로 반대편에 배열되는 셋업에 기초할 수 있다. 선택적으로, 검증 테스트는, 제2 신뢰된 거리는 신뢰된 거리에 대응하는 셋업에 기초할 수 있다. 검증 테스트에 대한 다양한 상황들 및 계산들이 다음 섹션들에서 논의된다. 다음 예는 삼각 부등식 및 2개의 협력 STA들을 사용한다.
- [0193] 도 5는 2개의 협력 디바이스들을 갖는 공간 콘스텔레이션을 도시한다. 콘스텔레이션(500)은, 도 1을 참조하여 기술된 디바이스들과 유사하게, '개시 STA'로 마킹되는 제1 디바이스, 및 2개의 '협력 STA들'을 포함한다. 제1 신뢰된 거리(L)는 제1 디바이스와 제1 협력 STA 사이에 있는 반면, 제2 신뢰된 거리(L)는 제1 디바이스와 제2 협력 STA 사이에 있다.
- [0194] 예시적인 콘스텔레이션을 사용하여, 제1 협력 STA와 정확히 반대편에 있는 제2 협력 STA를 사용함으로써, $90 < \phi \leq 180$ 의 경우에 더 나은 성능이 달성된다. 그 경우에, 개시 STA는 $0.5 \cdot L$ 보다 더 가까이 있는 것으로 나타나길 원하는 모든 치팅 응답 STA들은 아니더라도 많은 것을 검출할 수 있다. 이러한 콘스텔레이션의 경우, 응답 STA가 그것이 거리 $0.5 L$ 또는 그보다 더 가까이 있는 것처럼 위조하길 원하는 영역은 도 5에서 회색으로 도시된다. 이러한 영역은 웨지형 단면을 갖는 링과 유사하다.
- [0195] 도 6은 2개의 협력 디바이스들을 갖는 제2 공간 콘스텔레이션을 도시한다. 콘스텔레이션(600)은, 도 1을 참조하여 기술된 디바이스들과 유사하게, 개시 STA로 지칭되는 제1 디바이스, 및 2개의 협력 STA들을 포함한다. 제1 신뢰된 거리(L)는 제1 디바이스와 제1 협력 STA 사이에 있는 반면, 제2 신뢰된 거리(L)는 제1 디바이스와 제2 협력 STA 사이에 있다.
- [0196] 예시적인 콘스텔레이션을 사용하여, 개시 STA는 전술된 바와 같이 2개의 협력 STA들을 사용하고 응답 STA가 그것이 $0.3 L$ 또는 그보다 더 가까운 거리에 있는 것처럼 위조하길 원한다는 점에 관심이 있다. 그러한 경우, 테이블 1로부터, 적어도 $1.1L$ 떨어져 있는 모든 응답 STA들이 발견되고 $1.1L$ 보다 더 가까이 있는 많은 STA들이 발견되는 것을 알 수 있다.
- [0197] 도 7은 2개의 협력 디바이스들을 갖는 추가의 공간 콘스텔레이션을 도시한다. 콘스텔레이션(700)은, 도 1을 참조하여 기술된 디바이스들과 유사하게, 개시 STA로 지칭되는 제1 디바이스(710), 응답 디바이스로 지칭되는 제2 디바이스(720), 및 2개의 협력 STA들(730, 731)을 포함한다. 제1 신뢰된 거리(L)는 제1 디바이스와 제1 협력 STA 사이에 있는 반면, 제2 신뢰된 거리(L)는 제1 디바이스와 제2 협력 STA 사이에 있다. 이러한 특정 콘스텔레이션에서, 제2 디바이스(720)는 제1, 제3 및 제4 디바이스를 연결하는 라인 상에 그 중심이 있는 원의 3d 내 어딘가에 있을 수 있다는 것을 주목한다. 이 때문에, 여기서는 제1, 제2, 제3 및 제4 디바이스를 연결하는 평면의 2d 좌표로만 제2 디바이스의 위치를 계산한다.
- [0198] 예시적인 콘스텔레이션에서, 삼각 부등식 및 2개의 협력 STA들이 사용된다. 삼각 부등식은 협력 STA 1 및 2를 통한 측정에 사용된다. 코사인 법칙을 사용하여, 다음과 같이 $d2_1$ 을 계산할 수 있다.
- [0199]
$$d2_1^2 = L * \text{sqrt}(a^2 + 1 - 2 * a * \cos(\phi)) \quad (31)$$
- [0200] 그리고 $d2_2$ 를 계산할 수 있다.
- [0201]
$$d2_2^2 = L * \text{sqrt}(a^2 + 1 - 2 * a * \cos(180 - \phi))$$
- [0202]
$$= L * \text{sqrt}(a^2 + 1 + 2 * a * \cos(\phi)) \quad (32)$$
- [0203] 치팅 응답 STA는, 개시 STA가 다음 식과 같이 되는 거리들 $d1_c$, $d2_1_c$ 및 $d2_2_c$ 가 되도록 개시 STA에 전송하는 정보를 변경한다.

[0204] $d1_c = d1 - (d1 - f) \quad (33)$

[0205] $d2_1_c = d2_1 - (d1 - f) \quad (34)$

[0206] $d2_2_c = d2_2 - (d1 - f) \quad (35)$

[0207] 개시 STA는, 부등식(14)이 협력 STA 1 및 2로부터 수신한 거리들에 대해 성립되는지 여부를 검사한다.

[0208] $2*L \leq d2_1_c + d2_2_c \quad (36)$

[0209] $2*L \leq L * \sqrt{a^2 + 1 - 2 * a * \cos(\phi)} + L * \sqrt{a^2 + 1 + 2 * a * \cos(\phi)} - 2 * (a * L - f) \quad (37)$

[0210] $L \leq f + L * \{ \sqrt{a^2 + 1 - 2 * a * \cos(\phi)} + \sqrt{a^2 + 1 + 2 * a * \cos(\phi)} - 2 * a \} / 2 \quad (38)$

[0211] $f \geq 0.5 * L * \{ 2 + 2 * a - \sqrt{a^2 + 1 - 2 * a * \cos(\phi)} - \sqrt{a^2 + 1 + 2 * a * \cos(\phi)} \} \quad (39)$

[0212] 따라서, 개시 STA는, 다음 부등식에서와 같이 응답 STA가 f 를 선택할 때 그의 보고된 측정들을 위조하는 응답 STA를 검출할 것이다.

[0213] $f / L < 0.5 * \{ 2 + 2 * a - \sqrt{a^2 + 1 - 2 * a * \cos(\phi)} - \sqrt{a^2 + 1 + 2 * a * \cos(\phi)} \} = T3(40)$

[0214] 테이블 3은 $a \geq 0$ 와 $0 \leq \phi \leq 180$ 도의 결합들에 대해 T3의 값들을 나타낸다. T3의 값들의 테이블은 $\phi = 90$ 도를 중심으로 대칭이다.

ϕ a	0.0	10.0	20.0	30.0	40.0	50.0	60.0	70.0	80.0	90.0
180.0	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
170.0	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10
160.0	0.20	0.20	0.20	0.19	0.19	0.19	0.18	0.18	0.18	0.18
150.0	0.30	0.30	0.30	0.29	0.29	0.28	0.27	0.26	0.26	0.26
140.0	0.40	0.40	0.40	0.39	0.38	0.36	0.35	0.34	0.33	0.32
130.0	0.50	0.50	0.50	0.48	0.46	0.44	0.42	0.41	0.39	0.38
120.0	0.51	0.51	0.50	0.49	0.47	0.45	0.43	0.41	0.40	0.39
110.0	0.55	0.55	0.54	0.53	0.50	0.48	0.46	0.44	0.42	0.41
100.0	0.60	0.60	0.59	0.57	0.54	0.51	0.49	0.46	0.45	0.44
90.0	0.70	0.70	0.69	0.65	0.61	0.58	0.54	0.52	0.50	0.48
80.0	0.80	0.80	0.78	0.73	0.68	0.63	0.59	0.56	0.54	0.52
70.0	0.90	0.90	0.86	0.79	0.73	0.68	0.63	0.60	0.57	0.56
60.0	1.00	1.00	0.92	0.84	0.78	0.72	0.67	0.63	0.61	0.59
50.0	1.10	1.00	0.95	0.88	0.81	0.75	0.70	0.66	0.64	0.62
40.0	1.20	1.00	0.97	0.90	0.84	0.78	0.73	0.69	0.66	0.64
30.0	1.30	1.00	0.97	0.92	0.86	0.80	0.75	0.71	0.68	0.67
20.0	1.40	1.00	0.98	0.93	0.87	0.82	0.77	0.73	0.70	0.69
10.0	1.50	1.00	0.98	0.94	0.89	0.83	0.79	0.75	0.72	0.70
0.0	1.60	1.00	0.99	0.95	0.90	0.85	0.80	0.76	0.74	0.72
	1.70	1.00	0.99	0.95	0.91	0.86	0.81	0.78	0.75	0.73
	1.80	1.00	0.99	0.96	0.91	0.87	0.83	0.79	0.76	0.74
	1.90	1.00	0.99	0.96	0.92	0.88	0.84	0.80	0.77	0.76
	2.00	1.00	0.99	0.96	0.93	0.88	0.84	0.81	0.79	0.77
	3.00	1.00	0.99	0.98	0.96	0.93	0.90	0.87	0.85	0.84
	4.00	1.00	1.00	0.98	0.97	0.95	0.93	0.91	0.89	0.88
	5.00	1.00	1.00	0.99	0.97	0.96	0.94	0.92	0.91	0.90
	6.00	1.00	1.00	0.99	0.98	0.97	0.95	0.94	0.93	0.92
	7.00	1.00	1.00	0.99	0.98	0.97	0.96	0.95	0.94	0.93
	8.00	1.00	1.00	0.99	0.98	0.97	0.96	0.95	0.94	0.94
	9.00	1.00	1.00	0.99	0.99	0.98	0.97	0.96	0.95	0.94
	10.00	1.00	1.00	0.99	0.99	0.98	0.97	0.96	0.95	0.95
	100.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
	1000.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00

[0215]

[0216] 응답 STA가 그것이 $0.5*L$ 또는 더 가까운 거리에 있는 것처럼 위조하길 원한다는 것을 검출하는 것에 관심이 있다고 가정한다. STA가 실제로 $0.5*L$ 이내에 있는 경우, 이를 위조할 필요가 없으므로, 테이블 3에서 $a \leq 0.5$ 인 경우의 영역에는 음영이 없다.

- [0217] 테이블 3의 회색 음영 영역은 응답 STA와 개시 STA 사이의 실제 거리가 $0.5*L$ 보다 더 먼 경우(따라서 $\alpha > 0.5$), 및 개시 STA는, 응답 STA가 $0.5*L$ 이하의 거리로 나타내어지길 원한다는 것을 검출할 수 없는 경우이다. 제안된 방법은 $0 \leq \phi \leq 90$ 도인 경우의 넓은 영역에 존재하는 치팅 응답 STA들로부터 보호하고 그것이 보호하지 않는 영역(회색 음영 영역)은 테이블 1의 영역보다 명백히 훨씬 더 작다는 것이 명백하다.
- [0218] 도 7의 콘스텔레이션에서, 4개의 디바이스들을 연결하는 평면 내의 포지션(x, y)을 여러 방식으로 계산할 수 있다. 응답 STA가 그의 측정들을 충실히 보고하는 경우, 이들 계산된 포지션들은 측정 에러들을 제외하고는 일치할 것이다. 그러나, 응답 STA가 그의 측정들을 위조하고 있는 경우, 특히 실제로 있는 것보다 더 가까이 있는 것으로 나타나길 원할 때에는 그렇지 않을 것이다.
- [0219] 개시 STA가 $(x, y) = (0, 0)$ 에 있고, 협력 STA 1이 $(L, 0)$ 에 있고 협력 STA 2가 $(-L, 0)$ 에 있다고 가정한다. 이들 STA들 및 응답 STA는 물론 3-d 세계에 위치된다는 점을 주목한다. 평면 (x, y) 는 3-d 내의 임의의 평면일 수 있으며, 여기에, 개시 STA 및 2개의 협력 STA들을 연결하는 라인이 놓인다. 이 섹션에서 y-좌표에 대한 계산들은 2개의 값들 $\pm y$ 를 산출해야 한다. 포지티브 솔루션만 유지하는 것은 개시 STA와 2개의 협력 STA들을 연결하는 라인을 중심으로 평면을 180도 회전시킬 때 y에 대한 다른 솔루션이 획득되기 때문에 어떠한 문제도 없다.
- [0220] 먼저 아래의 "코사인 법칙 검사와 삼각 부등식 검사 사이의 관계" 섹션에서 설명된 바와 같이, 개시 STA에 의해 결정된 거리들이 0보다 큰지 여부를 검사한다.
- [0221] $d1_c > 0$ (41)
- [0222] $d2_1_c > 0$ (42)
- [0223] $d2_2_c > 0$ (43)
- [0224] 위의 3개의 부등식들 중 어느 것이라도 성립하지 않는 경우 치팅 응답 STA를 가정한다.
- [0225] 이들 3개의 부등식들이 성립하면, 응답 STA의 포지션을 계산하기 위해 4개의 에지들의 결합들에 대해 코사인 법칙을 사용한다.
- [0226] $\cos(\angle ACB) = (|A|^2 + |B|^2 - |C|^2) / (2 * |A| * |B|)$ (44)
- [0227] 본 발명자들은 항상 포인트 b를 응답 STA의 포지션으로 사용한다.
- [0228] 포인트 $a=(L, 0)$ 및 $c=(0, 0)$ 을 사용하여, 응답 STA를 $b1=(x1, y1)$ 에 있는 것으로 측정할 수 있다.
- [0229] $\cos_c1 = (d1_c^2 + L^2 - d2_1_c^2) / (2 * d1_c * L)$ (45)
- [0230] 포인트 $a=(-L, 0)$ 및 $c=(0, 0)$ 을 사용하여, 응답 STA를 $b=(x2, y2)$ 에 있는 것으로 측정할 수 있다.
- [0231] $\cos_c2 = (d1_c^2 + L^2 - d2_2_c^2) / (2 * d1_c * L)$ (46)
- [0232] 포인트 $a=(L, 0)$ 및 $c=(-L, 0)$ 을 사용하여, 응답 STA를 $b=(x3, y3)$ 에 있는 것으로 측정할 수 있다.
- [0233] $\cos_c3 = (d2_1_c^2 + 4L^2 - d2_2_c^2) / (2 * d2_1_c * 2L)$ (47)
- [0234] 포인트 $a=(-L, 0)$ 및 $c=(L, 0)$ 을 사용하여, 응답 STA를 $b=(x4, y4)$ 에 있는 것으로 측정할 수 있다.
- [0235] $\cos_c4 = (d2_2_c^2 + 4L^2 - d2_1_c^2) / (2 * d2_2_c * 2L)$ (48)
- [0236] 이어서, 계산된 코사인들 중 4개가 모두 구간 $[-1, 1]$ 에 있는지 여부를 검사한다. 아래의 "코사인 법칙 검사와 삼각 부등식 검사 사이의 관계" 섹션으로부터, 지금까지 삼각 부등식 테스트들과 동일한 테스트를 수행했음을 알고 있으므로, 지금까지의 검사와 함께, 위의 3개의 테이블들이 적용된다.
- [0237] 4개의 계산된 코사인들 모두가 구간 $[-1, 1]$ 에 있다면, 다음과 같이 응답 STA의 포지션에 대해 4개의 포인트들 $b1, b2, b3$ 및 $b4$ 를 계산한다.
- [0238] $x1 = \cos_c1 * d1_c$ (49)

[0239] $y1 = \sqrt{1 - \cos_c I^2} * d1_c(50)$

[0240] $x2 = -\cos_c2 * d1_c(51)$

[0241] $y2 = \sqrt{1 - \cos_c2^2} * d1_c(52)$

[0242] $x3 = L - \cos_c3 * d2_1_c(53)$

[0243] $y3 = \sqrt{1 - \cos_c3^2} * d2_1_c(54)$

[0244] $x4 = -L + \cos_c4 * d2_2_c(55)$

[0245] $y4 = \sqrt{1 - \cos_c4^2} * d2_2_c(56)$

[0246] 응답 STA가 그의 시간 측정들을 충실히 보고했다면, 이들 4개의 포인트들은 타이밍 측정 에러들의 영향을 제외하고는 동일해야 한다. 다른 곳에서도 설명한 것처럼, 여러 번의 측정들을 수행하고 결과들을 평균화함으로써 측정 에러들이 더 작아지게 할 수 있다는 것을 주목한다. 그러나, 이들 4개의 포인트들은, 응답 STA가 그것이 실제로 있는 것보다 더 가까이 있는 것으로 나타나도록 그의 측정값들을 위조할 때와 응답 STA가 협력 STA 1 및 2를 연결하는 라인 상에 있지 않을 때 서로 상이하다.

[0247] 4개의 포인트들 $b1$ 과 $b2$ 와 $b3$ 와 $b4$ 사이의 거리들 모두의 최대치 $emax$ 를 계산한다.

[0248] $i \in \{1, 2, 3, 4\}$ 및 $j \in \{1, 2, 3, 4\}$ 의 경우, $emax = \max |bi - bj|$ (57)

[0249] $b3$ 와 $b4$ 는 수치적 에러들을 제외하고는 동일한 포인트로 계산될 것이므로 $b4$ 를 계산할 필요가 없다는 것을 주목한다.

[0250] 테이블 4는 코사인 검사들 중 임의의 것이 실패한 경우를 제외하고 $emax/L$ 의 값들을 도시하며, 이 경우 99의 값이 도시된다. 치팅 응답 STA가 나타내어지기 원하는 값 f 는 이러한 검사들의 경우 중요하다. f 를 테이블 4에서 0.9로 선택한다.

Φ α	0.0	10.0	20.0	30.0	40.0	50.0	60.0	70.0	80.0	90.0
180.0	180.0	170.0	160.0	150.0	140.0	130.0	120.0	110.0	100.0	90.0
0.00	1.85	1.85	1.85	1.85	1.85	1.85	1.85	1.85	1.85	1.85
0.10	1.65	1.59	1.55	1.53	1.50	1.48	1.47	1.46	1.45	1.45
0.20	1.46	1.38	1.31	1.27	1.23	1.20	1.18	1.16	1.15	1.15
0.30	1.26	1.16	1.09	1.03	0.99	0.95	0.93	0.91	0.90	0.89
0.40	1.07	0.96	0.87	0.81	0.77	0.73	0.71	0.69	0.68	0.68
0.50	0.87	0.76	0.67	0.61	0.57	0.54	0.52	0.50	0.50	0.49
0.51	0.85	0.74	0.65	0.59	0.55	0.52	0.50	0.49	0.48	0.48
0.55	0.77	0.66	0.57	0.51	0.48	0.45	0.43	0.42	0.42	0.41
0.60	0.68	0.56	0.48	0.42	0.39	0.37	0.36	0.35	0.34	0.34
0.70	0.48	0.36	0.30	0.26	0.24	0.23	0.22	0.21	0.21	0.21
0.80	0.28	0.18	0.14	0.12	0.11	0.10	0.10	0.10	0.10	0.10
0.90	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
1.00	99.00	99.00	0.11	0.10	0.09	0.09	0.09	0.08	0.08	0.08
1.10	99.00	99.00	0.21	0.18	0.17	0.16	0.16	0.16	0.16	0.15
1.20	99.00	99.00	99.00	0.25	0.23	0.22	0.22	0.22	0.22	0.22
1.30	99.00	99.00	99.00	0.31	0.29	0.28	0.28	0.27	0.27	0.27
1.40	99.00	99.00	99.00	0.36	0.34	0.33	0.32	0.32	0.32	0.32
1.50	99.00	99.00	99.00	0.41	0.38	0.37	0.36	0.36	0.36	0.36
1.60	99.00	99.00	99.00	0.47	0.42	0.41	0.40	0.40	0.40	0.40
1.70	99.00	99.00	99.00	99.00	0.46	0.44	0.43	0.43	0.44	0.44
1.80	99.00	99.00	99.00	99.00	0.49	0.47	0.46	0.46	0.47	0.47
1.90	99.00	99.00	99.00	99.00	0.52	0.50	0.49	0.49	0.49	0.49
2.00	99.00	99.00	99.00	99.00	0.56	0.53	0.51	0.52	0.52	0.52
3.00	99.00	99.00	99.00	99.00	99.00	0.80	0.72	0.68	0.68	0.68
4.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	0.84	0.78	0.76
5.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00
6.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00
7.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00
8.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00
9.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00
10.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00
100.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00
1000.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00

[0251]

- [0252] 이 테이블로부터 알 수 있는 바와 같이, $\alpha > 0.9$ 의 경우, 99를 나타내는 셀들은 테이블 3에서 0.9보다 큰 값을 갖는 셀들과 일치하며, 이는 아래의 "코사인 법칙 검사와 삼각 부등식 검사 사이의 관계" 섹션에서 논의된 등가성을 보여준다.
- [0253] 개시 STA로부터 실제로 $0.9 L$ 범위 내에 있는 응답 STA들은 그들이 이러한 범위 내에 있는 것으로 위조할 필요가 없으므로, 이 구역(region)은 테이블 4에서 음영으로 처리되지 않는다. 응답 STA의 포지션에 대한 측정들 b_1, b_2, b_3 및 b_4 에서의 최대 불일치에 대해 임계치로서 $0.25 L$ 을 사용하여, 셀들이 0.25 미만인 값을 갖고 $\alpha > 0.9$ 인 테이블 4의 영역을 음영으로 처리하였다.
- [0254] 이는, 음영 영역 내에서, 따라서 기본적으로 개시 STA로부터 $0.9 L$ 과 $1.2 L$ 사이의 거리에 있는 응답 STA들의 경우, 제안된 시스템이, 이러한 응답 STA들이 개시 STA로부터 $0.9 L$ 내에 위치되는 것으로 나타나도록 그들의 타이밍 측정들을 위조하고 있다고 결정할 수 없다는 것을 의미한다.
- [0255] 따라서, 개시 STA로부터 거리 L 에서 반대 위치들에 위치한 2개의 협력 STA들을 사용하여, 제안된 시스템은, 개시 STA로부터 $0.9 L$ 이내에 위치되는 것으로 나타나도록 그들의 타이밍 측정들을 위조하고 있는 응답 STA들로서 개시 STA로부터 $1.2 L$ 보다 더 먼 모든 거리들에 위치한 응답 STA들을 검출할 수 있다.
- [0256] 다음 섹션은 삼각 부등식 및 2개를 초과하는 협력 STA들을 사용한다. 개시 STA 주위에 2개 초과하는 협력 STA들을 배치함으로써 더 나은 성능을 얻을 수 있다. 개시 STA 주변에 가능한 한 많은 포지션들에 위치한 치팅 응답 STA들을 가장 잘 검출하기 위해서는, 3개의 협력 STA들을 사용할 때, 개시 STA와 협력 STA들을 일 평면에 배치시키는 것이 가장 좋다. 이것은, 개시 STA가 3개의 협력 STA들을 연결하는 평면 상에 없는 경우, 치팅 응답 STA가 항상 3개의 협력 STA들 중 어느 것보다 개시 STA에 더 가깝고, 따라서 제안된 방법이 작동하지 않는 불륨 일 것이기 때문이다(예컨대, 테이블 2 참조).
- [0257] 하나의 라인 상에 포지셔닝되어 있지 않지만 콘스텔레이션이 삼각형을 형성하는 2개의 협력 STA들과 개시 STA들을 사용하는 것도 가능하다. 거리들 d_1, d_{2_1}, d_{2_2} 및 2개의 협력 STA들 및 개시 STA에 의해 형성된 삼각형의 변들의 길이들을 사용하여, 개시 STA는 2개의 협력 STA들 및 개시 STA의 세트 중에서 제2 디바이스와 임의의 디바이스들의 쌍에 의해 형성된 삼각형들에 대한 코사인 법칙을 사용하여 검사들을 수행할 수 있다.
- [0258] 4개의 협력 STA들을 사용할 때, 이들은 이상적으로는 정사면체의 모서리들 상에 배치되어야 하고 개시 STA는 정사면체의 중심에 위치되어야 한다. 이러한 콘스텔레이션은 가능한 가장 대칭적인 것이므로 최상의 보호를 제공한다.
- [0259] 단위 구 상에 4개의 포인트들이 있고 원점이 중심이며 수평이고 낮은 면 수준을 갖는 정사면체의 꼭짓점들은 다음 식과 같다.
- [0260] $A = (\sqrt{8/9}, 0, -1/3)$
- [0261] $B = (-\sqrt{2/9}, \sqrt{2/3}, -1/3)$
- [0262] $C = (-\sqrt{2/9}, -\sqrt{2/3}, -1/3)$
- [0263] $D = (0, 0, 1)$
- [0264] 따라서, 이 경우 협력 STA들은 꼭짓점들의 포지션에 있고 개시 STA는 원점에 위치되며 거리 L 은 1과 같다. 임의의 2개의 STA들 사이의 가장 먼 거리는 임의의 2개의 협력 STA들 사이의 거리이므로, 정사면체의 모서리들 각각의 길이는 다음과 같다.
- [0265] $||A - D|| = ||(\sqrt{8/9}, 0, -1/3) - (0, 0, 1)||$
- [0266] $= ||(\sqrt{8/9}, 0, -4/3)||$
- [0267] $= \sqrt{8/3} \approx 1.63 \quad (58)$
- [0268] 임의의 협력 STA와 원점과 응답 STA 사이의 가장 큰 각도는 응답 STAA가 원점과 정사면체의 네 면들 중 어느 하나의 중심을 연결하는 라인에 있을 때이다. 면 ABD의 중심은 다음과 같다.
- [0269] $F = \{ (\sqrt{8/9}, 0, -1/3) + (-\sqrt{2/9}, \sqrt{2/3}, -1/3) + (0, 0, 1) \} / 3$
- [0270] $= (\sqrt{8/9} - \sqrt{2/9}, \sqrt{2/3}, 1/3) / 3 \quad (59)$

[0271] 각도들 $\angle AOF$, $\angle BOF$ 및 $\angle DOF$ 는 모두 동일하다. 이러한 각도는 코사인 법칙을 사용하여 계산될 수 있다.

$$\cos(\angle DOF) = (||D||^2 + ||F||^2 - ||D - F||^2) / (2 * ||D|| * ||F||) \quad (60)$$

$$||D||^2 = 1 \quad (61)$$

$$||F||^2 = \{ (\sqrt{8/9} - \sqrt{2/9})^2 + 2/3 + 1/9 \} / 9$$

$$= \{ 8/9 + 2/9 - 2 * \sqrt{16/81} + 7/9 \} / 9$$

$$= 1/9 \quad (62)$$

$$||D - F||^2 = \{ (\sqrt{8/9} - \sqrt{2/9})^2 + 2/3 \} / 9 + (8/9)^2$$

$$= \{ 8/9 + 2/9 - 2 * \sqrt{16/81} + 2/3 \} / 9 + 64/81$$

$$= \{ 2/9 + 6/9 \} / 9 + 64/81$$

$$= 72/81 = 8/9 \quad (63)$$

[0281] 따라서

$$\cos(\angle DOF) = (1 + 1/9 - 8/9) / (2 * 1 * 1/3)$$

$$= 3 * (2/9) / 2$$

$$= 1/3 \quad (64)$$

$$\angle DOF = \arccos(1/3) = 70.53 \text{ 도} \quad (65)$$

[0286] 따라서, 정사면체의 중심에 위치한 1개의 개시 STA와 개시 STA로부터 거리 L에 있는 그 사면체의 꼭짓점들에 위치한 4개의 협력 STA들로 구성된 콘스텔레이션을 이용하여, 개시 STA에 대해 0.5L보다 더 가까운 것으로 위조하길 원하는 모든 응답 STA들은 그들이 개시 STA로부터 1.5L보다 더 멀리 떨어져 있는 경우 검출될 수 있는데, 테이블 1을 참조한다. 0.5 L과 1.5 L 사이의 영역 내의 많은 그러한 STA들이 검출될 수 있다.

[0287] 선택적으로, 이전 섹션에서 설명된 방어와 유사하게 개시 STA 및 협력 STA들을 사용하여 계산된 포지션들에서 불일치 검사들을 추가함으로써 방어가 개선될 수 있다.

[0288] 일 실시예에서, 레인징 프로토콜은 제1 디바이스를 포함할 수 있고, 제1 디바이스는 개시 디바이스로서 동작하고 개시 메시지를 제2 디바이스로 전송하는 한편, 개시 메시지의 수신 시, 제2 디바이스는 측정 메시지를 전송해야 한다. 제1 메시지 프로세서는 제3 디바이스와 역할-변경 데이터를 교환하여, 제3 디바이스가 거리 측정을 위해 개시 디바이스로서 동작할 수 있게 하도록 배열된다. 그에 대해, 제3 디바이스는, 역할-변경 데이터를 수신할 때, 제2 측정 메시지에 기초한 레인징 프로토콜에 따라 제3 디바이스와 제2 디바이스 사이의 제3 거리를 획득하고, 제3 거리를 나타내는 제3 지원 데이터를 제1 디바이스로 전달하도록 배열된다. 예를 들어, 제3 지원 데이터는 제3 디바이스가 측정했던 FTM 프로토콜의 t2 및 t3 값들을 포함할 수 있다. t1 및 t4 값들도 그 일부일 수 있지만, 제1 디바이스가 t1 및 t4를 포함하는 제2 디바이스로부터 원본 메시지를 수신하고 사용할 수 있기 때문에 이것이 필요하지 않다.

[0289] 또한, 제1 메시지 프로세서는 제1 디바이스에서 제2 측정 메시지를 수신할 때 제1 디바이스와 제2 디바이스 사이의 제2 거리를 결정하고, 제3 디바이스로부터 제3 지원 데이터를 수신하고, 제2 거리 및 제3 지원 데이터를 또한 사용하여 검증 테스트를 수행하도록 배열된다. 실시예에서, 개시 STA와 협력 STA는 역할들을 교환한다 - 즉 다른 말로 - 2개의 개시 STA들을 사용하여 포지션을 두 번 계산한다.

[0290] 도 4의 콘스텔레이션에서, 이제, 응답 STA까지의 거리를 결정하기 위해 함께 작동하는 제1 STA 1 및 제2 STA 2로 동작하는 2개의 디바이스들(410, 430)이 있다. 일련의 측정들에서, STA 1은 개시 STA로, STA 2는 협력 STA로 동작하고, 제2 일련의 측정들에서, 그들은 반대 역할들을 가정한다. 거리 측정 결과를 개선하기 위해서 거리가 계산되기 전에 각각의 일련의 개별 시간 측정들이 평균화된다. 제1 일련의 개별 측정들 모두는 역할들이 교환되어 제2 일련의 개별 측정들이 수행되기 전에 수행될 수 있다. 그러나, 역할 교환은 어떤 횟수의 개별 측

정들을 한 이후에라도 행해질 수 있다.

[0291] 제1 일련의 측정들로부터의 타이밍 측정들을 사용하여, STA 1이 개시 STA인 경우, 식 (49) 및 식 (50)을 사용하여 응답 STA의 포지션 $r1 = (x1, y1)$ 을 계산할 수 있다. 제2 일련의 측정들로부터의 타이밍 측정들을 사용하여, STA 2가 개시 STA인 경우, 유사한 식들을 사용하여 응답 STA의 포지션 $r2 = (x2, y2)$ 를 계산할 수 있다. 이러한 특정 컨스텔레이션에서, 제2 디바이스(420)는 제1 및 제3 디바이스를 연결하는 라인 상에 그 중심이 있는 원의 3d 내 어딘가에 있을 수 있다는 것을 주목한다. 이 때문에, 여기서는 제1, 제2 및 제3 디바이스를 연결하는 평면의 2d 좌표로만 제2 디바이스의 위치를 계산한다.

[0292] 응답 STA가 그의 타이밍 측정들을 충실히 보고한 경우, 계산된 포인트들($r1, r2$)은 측정 에러들을 제외하고는 동일해야 한다. 그러나, 이것은 응답 STA가 실제로 있는 것보다 더 가까이 있는 것으로 나타나길 원할 때 상이할 수 있다.

[0293] 이전 섹션들에서, 치팅 응답 STA는 개시 STA로부터 거리 f 에서 나타나도록 시도되었다. 응답 STA가, 2개의 STA들이 이따금 역할들을 교환한다는 것을 모르고 각각의 STA로부터 위조된 거리 f 에 나타나려고 시도한다고 가정한다. 이 경우, 특히 $f < 0.5 L$ 인 경우 $r1$ 및 $r2$ 는 명백히 상이할 것이다.

[0294] 따라서, 각각 개시 STA로 역할을 하는 2개 이상의 STA들을 사용하고 개시 STA들 각각에 의해 측정된 거리들을 사용하여 응답 STA의 위치를 계산하고 계산된 위치들의 차를 판단하는 것은 그들의 타이밍 측정들을 위조하는 응답 STA들을 검출하기 위한 좋은 아이디어이다.

[0295] 그러나, 전술된 공격은 이러한 상황에서 최상의 가능한 공격이 아니다. 더 양호한 공격은, 응답 STA가 그가 어떠한 개시 STA에 의해 FTM 프로토콜을 수행하고 있는지를 알고 있는 경우이고, 응답 STA가 컨스텔레이션의 파라미터들(즉 L 및 ϕ 또는 $d1$ 및 $d2$)을 알고 있는 것이다. 이는 실제로 알기 어려울 수 있지만 불가능한 것은 아니다. 비밀 암호 키들을 제외하고, 공격자가 모든 것을 알고 있다고 가정하는 것이 양호한 보안 관행이다. 따라서, 이전 섹션들에 기재된 바와 같은 방어가 바람직하게 사용된다.

[0296] 다음 섹션은 코사인 법칙 검사와 삼각 부등식 검사 사이의 관계를 논의한다. 삼각 부등식들이 3개의 길이들 $|A|, |B|$ 및 $|C|$ 에 대해 성립되는지 여부를 검사하는 것은

[0297] $|C| \leq |A| + |B| \quad (66)$

[0298] $|A| \leq |B| + |C| \quad (67)$

[0299] $|B| \leq |A| + |C| \quad (68)$

[0300] 다음 식의 성립 여부를 검사하는 것과 동일하다.

[0301] $-1 \leq \cos(\angle ACB) \leq 1 \quad (69)$

[0302] 각도 $\angle ACB$ 에 대한 코사인 법칙은 다음과 같다:

[0303] $\cos(\angle ACB) = (|A|^2 + |B|^2 - |C|^2) / (2 * |A| * |B|) \quad (70)$

[0304] 코사인이 -1 이상인지 여부를 검사하는 것은 다음과 같다.

[0305] $\cos(\angle ACB) \geq -1 \Leftrightarrow$

[0306] $(|A|^2 + |B|^2 - |C|^2) / (2 * |A| * |B|) \geq -1 \quad (71)$

[0307] $(|A| * |B|) > 0$ 인 경우에만 부등식 (71)에서 다음 부등식을 도출할 수 있다.

[0308] $(|A|^2 + |B|^2 - |C|^2) \geq -2 * |A| * |B| \Leftrightarrow$

[0309] $(|A|^2 + |B|^2 + 2 * |A| * |B| - |C|^2) \geq 0 \Leftrightarrow$

[0310] $(|A| + |B|)^2 - |C|^2 \geq 0 \Leftrightarrow$

- [0311] $(|A| + |B|)^2 \geq |C|^2$ ⇔
- [0312] $|C| \leq (|A| + |B|)$ (72)
- [0313] 이는 부등식 (66)과 동일하다.
- [0314] 유사하게, 코사인이 1 이하인지 여부를 검사하는 것은 다음과 같다.
- [0315] $\cos(\angle ACB) \leq 1$ ⇔
- [0316] $(|A| - |B|)^2 - |C|^2 \leq 0$ ⇔
- [0317] $(|A| - |B|)^2 \leq |C|^2$ ⇔
- [0318] $\text{abs}(|A| - |B|) \leq |C|$ ⇔
- [0319] $|A| \leq (|B| + |C|) \ \& \ |B| \leq (|A| + |C|)$ (73)
- [0320] 삼각형에 대해서도 2개의 부등식들이 성립해야 한다.
- [0321] 실제 거리들이 항상 0 이상이라는 것을 주목한다. 위의 추론은 포지티브 거리들의 경우에는 성립하지만 네거티브 거리들의 경우에는 성립하지 않는다. 응답 STA가 그의 측정들을 더 가까이 있는 것으로 위조할 때 개시 STA에 의해 획득된 거리들은 네거티브일 수 있다. 따라서, 3개의 삼각형 부등식들에 대해 검사하는 것은 측정된 3개의 거리들이 0 이상인지 여부를 검사하고 코사인 부등식(69)이 성립되는지 여부를 검사하는 것과 같다.
- [0322] 일 실시예에서, 제3 메시지 프로세서는 제2 디바이스로부터 수신된 적어도 하나의 메시지의 제3 신호 강도를 결정하도록 배열되고, 제1 디바이스에 대한 지원 데이터에 제3 신호 강도 데이터를 포함시키도록 배열된다. 제1 메시지 프로세서는 제2 디바이스로부터 수신된 적어도 하나의 메시지의 제1 신호 강도를 결정하고 결정된 거리들에서 제1 신호 강도 및 제3 신호 강도를 각자의 예상 신호 강도들과 비교함으로써 결정된 거리들이 신뢰성이 있는지 여부를 검증하도록 배열된다. 실시예에서, 신뢰도를 증가시키기 위해 신호 강도들에 기초한 거리 측정이 추가적으로 수행된다. 도달 시간 및 송신 시간에 더하여, 또한 수신 신호 강도를 거리의 측정으로 사용할 수 있다. 디바이스는 일 메시지가 다른 디바이스로 전송되게 하는 송신 전력을 해당 메시지에서 포함하고, 다른 디바이스는 수신 신호 강도를 측정하고 다른 디바이스는 송신기 안테나 속성들(예컨대, 전방향성인 것) 및 신호 강도가 거리에 대해 2의 거듭제곱으로 감소한다는 가정에 기초하여 거리를 결정할 수 있다. 적어도 하나의 협력 디바이스가 동일한 메시지의 신호 강도를 측정하고 이러한 데이터를 제1 디바이스로 전달된 바와 같이 지원 데이터에 포함시키는 경우, 제1 디바이스는 수신 신호 강도들에 기초하여 제2 디바이스로부터의 거리들의 비를 결정할 수 있다.
- [0323] 일 실시예에서, 제1 디바이스 및 제3 디바이스는 3GPP 네트워크에서 기지국들에 의해 구현될 수 있는 반면, 제2 디바이스는 UE에 의해 구현된다. 3GPP의 기지국들은 소위 리소스 요소들이라고 하는 시간-주파수 그리드에서 송신하고 수신한다. 시간-주파수 그리드의 포지션들 중 몇몇은 3GPP 표준에 의해 고정되며 기지국 범위 내의 모든 UE들에 시스템 정보를 브로드캐스트하는 데 사용되며, 시스템 정보는 예컨대, 언제 어떤 주파수들로, 기지국이 특정 UE에 어떤 것을 전송(다운링크)할 것인지와 언제 어떤 주파수들로, 특정 UE가 어떤 것을 기지국에 전송(업링크)할 수 있는지 또는 특정 다른 UE로 전송(사이드링크)할 수 있는지에 대한 정보이다. 기지국들이 본 발명에 따라 협력하고 있을 때, 그들의 시간-주파수 그리드들은 정렬 및 동기화되어야 하고 그들이 각각 그리드 내 동일한 시간-주파수 포지션들(리소스 요소들)이 사용가능해지게 해야 하므로 그들은 모두 동일한 UE로부터의 동일한 메시지의 도달 시간 또는 수신 신호 강도를 측정할 수 있다.
- [0324] 추가 실시예에서, 레인징 프로토콜은 자격증명(예컨대, 공개 키) 또는 자격증명의 해시 또는 암호화된 자격증명을 포함하는 [802.11]에 정의된 바와 같이 예를 들어 레인징 프로토콜에 추가될 수 있는 추가 속성 또는 추가 메시지를 포함한다. 이러한 메시지는 키 데이터에 기초하여 암호로 보호되는 메시지의 일례이다. 제2 디바이스는, 레인징 프로토콜에 대한 메시지 교환의 일부로서 이러한 자격증명 또는 자격증명의 해시 또는 암호화된 자격증명을 포함할 수 있다. 대칭이 되기 위해, 또한 제1 디바이스는 이러한 자격증명, 자격증명의 해시 또는 암호화된 자격증명을 추가 메시지에 포함시킬 수 있다. 레인징 프로토콜의 메시지에서 자격증명 또는 자격증명의 해시 또는 암호화된 자격증명을 포함하는 바람직한 필드는 해당 필드의 신호 또는 해당 필드를 전달하는 신

호의 적어도 일부가 메시지의 송신 또는 도달 시간을 측정하는 데 사용되는 필드이므로, 다른 디바이스가 제1 디바이스와 제2 디바이스 사이의 거리를 측정하는 데 사용되는 메시지에 그의 자격증명 또는 그의 자격증명의 해시 또는 그의 암호화된 자격증명을 삽입하는 것은 불가능하지는 않더라도 매우 어렵다. 자격증명 또는 자격증명의 해시 또는 암호화된 자격증명을 반송하는 신호가 범위를 측정하는 데 사용되는 신호에 (시간 상) 가까울수록, 또는 이러한 신호들 사이에 중첩이 많을수록 더 양호하다. 이러한 방식으로, 제1 디바이스는 레인징 프로토콜의 메시지 내의 자격증명 또는 자격증명의 해시 또는 암호화된 자격증명이 실제로 범위 측정 프로토콜을 실행하고 있는 제2 디바이스 중 하나라는 것을 확신할 수 있다. 일 실시예에서, 제1 메시지 프로세서는 이러한 자격증명 또는 자격증명의 해시 또는 암호화된 자격증명을 프로세싱하도록 배열되고, 예컨대, Wi-Fi 보호 셋업 프로토콜, 디바이스 프로비저닝 프로토콜, Diffie-Hellman 키 교환 및/또는 4-웨이 WPA2 핸드셰이크를 사용함에 의해 그것이 디바이스 인증을 성공적으로 수행했고 상호 신뢰를 확립한 디바이스에 의해 이전에 사용된 자격증명과 일치하는지 여부를 검증한다. 일치가 발견되는 경우, 제1 디바이스는 제1 디바이스와 제2 디바이스 사이의 거리 측정들이 신뢰될 수 있고 신뢰성있는 것으로 간주될 수 있는 것으로 가정할 수 있다. 어떠한 일치도 발견되지 않는 경우, 제1 디바이스는 제1 디바이스와 제2 디바이스 사이의 거리 측정들을 불신하고, 예컨대 다른 실시예들에 기술된 바와 같은 메커니즘들을 사용하여 거리 측정들의 신뢰성을 검증하기 위한 추가적인 단계들을 수행할 것이다. 다른 실시예에서, 측정된 값들(예컨대, 제1 시간 데이터 및/또는 제2 시간 데이터)은 제1 디바이스와 제2 디바이스 사이에서 수행된 이전 디바이스 인증 절차 동안에 확립되었던 것으로서 제1 디바이스와 제2 디바이스 사이에 합의되었거나 합의된 자격증명들로부터 도출되는 키를 사용하여 암호화된다.

[0325] 대안적인 실시예에서, 제2 디바이스는 이후의 접속 셋업 동안에 사용될 자격증명 또는 자격증명의 해시 또는 암호화된 자격증명을 포함할 수 있다. 제1 메시지 프로세서는 측정된 거리들을 그 자격증명과 접속하는 특정 디바이스와 안전하게 상관시키기 위해서, 수신된 자격증명 또는 자격증명의 해시 또는 암호화된 자격증명을 제1 디바이스와 제2 디바이스 사이의 측정된 거리와 함께 프로세싱하고 저장하도록 배열된다. 제1 디바이스와 제2 디바이스 사이의 접속을 셋업할 때, 제1 디바이스는 디바이스 인증의 수행 동안, 예컨대 Wi-Fi 보호 셋업 프로토콜, 디바이스 프로비저닝 프로토콜, Diffie-Hellman 키 교환을 수행하는 동안 그리고/또는 4-웨이 WPA2 핸드셰이크를 수행하는 동안 동일한 자격증명 또는 그 파생물이 사용되는지를 검증한다. 그렇게 함으로써, 제1 디바이스는 그것이 접속하고 있는 디바이스가 특정 거리 측정이 수행되었던 것과 동일한 디바이스라는 것을 결정할 수 있다. 특히, 자격증명이 공개 키였고, 제1 디바이스와 제2 디바이스 사이의 접속을 셋업하는 것이, 제2 디바이스가 범위 측정에서 자격증명으로 공개 키에 속하는 개인 키를 소유하고 있음을 디바이스 1에게 성공적으로 증명했음을 포함했다면, 제1 디바이스는 제2 디바이스가 범위를 측정한 디바이스이고 사기꾼이 아니라는 것을 확신할 수 있다.

[0326] 일 실시예에서, 제1 메시지 프로세서는, 결정된 거리가 신뢰성이 없는 것으로 평가될 때, 의도된 프로세스 대신 상이한 프로세스 또는 기능, 데이터 또는 기능에 대한 액세스 거부로 진행하도록 배열된다. 예를 들어, 정상 거리 기반 프로세스는 위치 기반 서비스 또는 로컬 주변기기에 대한 액세스를 허용하는 것일 수 있다. 또한, 다른 네트워크, 예컨대 이더넷, 인터넷, 3GPP 코어 네트워크를 통한 제1 디바이스로의 또는 그로부터의 라우팅은 거리 측정에 기초하여 제어되거나 거부될 수 있다. 결정된 거리가 신뢰성 없는 것으로 간주되는 경우, 모든 추가 통신 및/또는 액세스가 거부될 수 있고 그리고/또는 경고 메시지가 관리 시스템 또는 경비원에게 전송될 수 있다. 또한, 제1 메시지 프로세서는 임의의 정상 거리 기반의 프로세스를 진행하기 전에 추가 자격증명들 및/또는 사용자의 개인 식별을 요청하는 것과 같이, 제2 디바이스가 실행될 수 있는 상이한 보안 프로토콜을 관여시키도록 배열될 수 있다. 상이한 보안 프로토콜은 추가 프로세스 또는 메인 프로토콜의 더욱 향상된 실행일 수 있으며, 예컨대 일반 보안 프로세스에서 더 엄격하거나 어려운 단계를 발생시킬 수 있다. 선택적으로, 제1 메시지 프로세서는 상이한 레인징 프로토콜 및/또는 상이한 유형의 무선 통신, 예를 들어 매우 가까운 거리에서는 NFC를 사용하여 또는 지문과 같은 몇몇 식별 및/또는 생체 측정 데이터를 제공할 제2 디바이스의 인간 운영자에 의해 추가 거리 측정을 요청하도록 배열된다. 또한, 제1 메시지 프로세서는 임의의 정상 거리 기반 프로세스로 진행하기 전에 제1 디바이스의 적어도 몇몇 데이터 및/또는 적어도 하나의 애플리케이션에 대한 액세스를 거부하거나 제한하도록 배열될 수 있다. 예를 들어, 거리가 신뢰성없는 것으로 간주되는 경우에도 기본 서비스가 제공될 수 있는 반면, 거리가 신뢰성있는 것으로 간주되는 경우 확장된 서비스가 제공된다.

[0327] 도 8은 제1 디바이스와 제2 디바이스 사이의 무선 통신을 통한 거리 측정을 위한 방법을 도시하며, 무선 통신은 전술한 바와 같은 레인징 프로토콜을 포함한다. 제1 디바이스 및 제2 디바이스는 도 1을 참조하여 도시되고 추가로 설명된 바와 같은 제1 및 제2 디바이스와 유사하다. 제3 디바이스는 제1 디바이스로부터 신뢰된 거리에 위치되는 협력 디바이스로서 동작하고 있다. 방법은 제1 디바이스 내의 프로세서에 의해 실행될 수 있지만, 또한 수신된 도달 시간들 및 지원 데이터에 기초하여 상이한 디바이스 내의 프로세서에 의해 그리고/또는 상이한

시간에 프로세싱될 수 있다. 예를 들어, 방법은, 레인징 프로토콜에 능동적으로 참여하고 있지 않지만 모든 메시지들을 수신하고 신뢰된 거리를 인식하는 추가 디바이스에서 실행될 수 있다.

[0328] 방법은 노드 START(801)에서 시작한다. 제1 스테이지 RNGP(802)에서, 방법은 레인징 프로토콜을 실행하고 도 1을 참조하여 기술된 바와 같이 도달 시간 측정들을 수행할 수 있다. 본 방법은 제1 디바이스에서 측정 메시지의 제1 도달 시간에 기초하여 제1 디바이스와 제2 디바이스 사이의 제1 거리를 획득함으로써 스테이지 OD1(803)로 계속되고, 이어서 스테이지 CO_COP(804)에서 협력 디바이스와 통신한다. 협력 디바이스는 협력 디바이스에서 측정 메시지의 제3 도달 시간을 결정하고, 제3 도달 시간에 기초하는 지원 데이터를 제공하도록 배열된다. 이어서, 본 방법은, 결정된 거리를 평가하는 단계로 계속된다. 다음 스테이지 OD3(805)에서, 예컨대, 측정 메시지의 제3 도달 시간 및 송신 시간에 기초하여 계산된 지원 데이터를 사용하여 제3 디바이스와 제2 디바이스 사이의 제3 거리가 획득된다. 마지막으로, 스테이지 VERT(806)에서, 제1 거리, 신뢰된 거리 및 제3 거리에 대해 검증 테스트가 수행된다. 검증 테스트는 상기 거리들이 제1 디바이스, 제2 디바이스 및 협력 디바이스의 실행가능한 공간 콘스텔레이션에 대응할 때 제1 거리를 신뢰성있는 것으로서 수용한다. 테스트는 상기에 기재된 바와 같은 삼각 부등식 및 불일치 검사에 기초할 수 있다.

[0329] 일 실시예에서, 방법은 제1 디바이스가 제1 도달 시간 또는 제1 거리를 제공하기 위한 개시 디바이스로서 동작하도록 지시되는 준비 스테이지를 포함할 수 있다. 유사하게, 제3 디바이스는 제3 도달 시간에 기초하는 지원 데이터를 제공하기 위해 협력 디바이스로서 동작하도록 지시될 수 있다. 준비 스테이지는 별도의 제어 디바이스, 컴퓨터 또는 서버에 의해 실행될 수 있다. 대안적으로, 제1 디바이스 또는 제3 디바이스는 상기 지시를 실행할 수 있다.

[0330] 도 9는 상기도 8에 기술된 바와 같은 제1 디바이스와 제2 디바이스 사이의 무선 통신을 통한 거리 측정에서 협력 디바이스로서 동작하는 방법을 도시한다. 협력 디바이스는 제1 디바이스로부터 신뢰된 거리에 위치될 수 있다.

[0331] 방법은 노드 START(901)에서 시작한다. 제1 스테이지 RNGP(902)에서, 방법은 제1 및 제2 디바이스에 의해 수행되는 바와 같은 레인징 프로토콜을 모니터링할 수 있다. 본 방법은 협력 디바이스에서 측정 메시지의 제3 도달 시간을 결정함으로써 스테이지 ARR3(903)으로 계속된다. 후속적으로, 스테이지 CO_IN(904)에서, 협력 측은, 예컨대 무선 프로토콜을 사용하거나 유선 접속을 사용하여 제1 디바이스와 후속적으로 통신한다. 다음으로, 스테이지 SUP(905)에서, 방법은 제1 디바이스에 지원 데이터를 제공한다. 지원 데이터는 제3 도달 시간에 기초한다. 이어서, 협력 측에서의 방법은 노드 END(906)에서 종료된다. 전송된 바와 같이, 제1 디바이스는 지원 데이터를 사용하여 협력 디바이스와 제2 디바이스 사이의 상기 제3 거리를 획득하고, 제1 거리, 신뢰된 거리 및 제3 거리에 대한 검증 테스트를 수행하도록 배열된다.

[0332] 도 10a는 컴퓨터 프로그램(1020)을 포함하는 기록가능 부분(1010)을 갖는 컴퓨터 판독가능 매체(1000)를 도시하며, 컴퓨터 프로그램(1020)은 프로세서 시스템으로 하여금 도 9 및 도 10을 참조하여 설명된 바와 같은 시스템에서 상기 방법들 중 하나 이상을 수행하게 하는 명령어들을 포함한다. 컴퓨터 프로그램(1020)은 물리적 마크들로서 또는 컴퓨터 판독 가능 매체(1000)의 자화에 의해 컴퓨터 판독 가능 매체(1000) 상에 구현될 수 있다. 그러나, 임의의 다른 적합한 실시예가 또한 구상될 수 있다. 또한, 컴퓨터 판독 가능 매체(1000)가 광학 디스크로서 여기에 도시되지만, 컴퓨터 판독 가능 매체(1000)는 하드 디스크, 고체 상태 메모리, 플래시 메모리 등과 같은 임의의 적합한 컴퓨터 판독 가능 매체일 수 있고, 기록 불가 또는 기록 가능할 수 있다는 것이 인식될 것이다. 컴퓨터 프로그램(1020)은 프로세서 시스템으로 하여금 상기 방법들을 수행하게 하기 위한 명령어들을 포함한다.

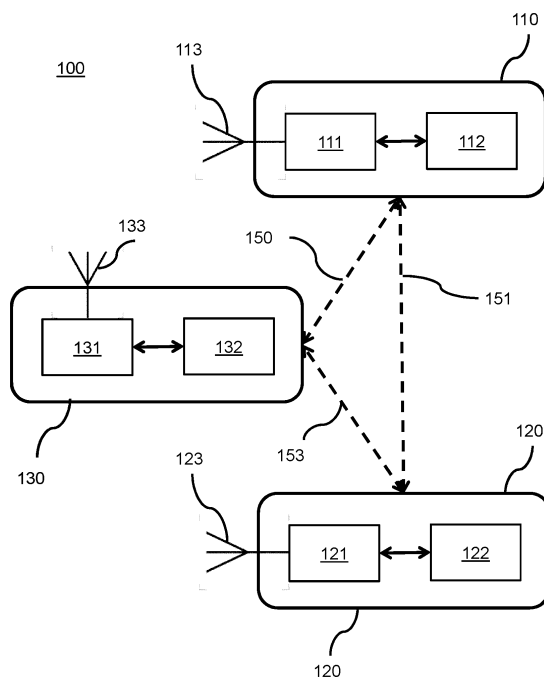
[0333] 도 10b는 도 9 및 도 10을 참조하여 설명된 바와 같은 디바이스 또는 서버의 실시예에 따른 프로세서 시스템(1100)의 개략도를 도시한다. 프로세서 시스템은 하나 이상의 집적 회로(1110)를 포함한다. 하나 이상의 집적 회로(1110)의 아키텍처가 도면에 개략적으로 도시되어 있다. 회로(1110)는 실시예에 따른 방법을 실행하고/하거나 그의 모듈들 또는 유닛들을 구현하기 위해 컴퓨터 프로그램 컴포넌트들을 실행하기 위한 처리 유닛(1120), 예를 들어 CPU를 포함한다. 회로(1110)는 프로그래밍 코드, 데이터 등을 저장하기 위한 메모리(1122)를 포함한다. 메모리(1122)의 일부는 읽기 전용일 수 있다. 회로(1110)는 통신 요소(1126), 예를 들어, 안테나, 커넥터 또는 이들 둘 모두 등을 포함할 수 있다. 회로(1110)는 방법에서 정의되는 처리의 일부 또는 전부를 수행하기 위한 전용 집적 회로(1124)를 포함할 수 있다. 프로세서(1120), 메모리(1122), 전용 IC(1124) 및 통신 요소(1126)는 상호연결부(1130), 즉 버스를 통해 서로 접속될 수 있다. 프로세서 시스템(1110)은 안테나 및/또는 커넥터들을 각각 사용한 접속 및/또는 비접촉 통신을 위해 배열될 수 있다.

- [0334] 네트워크로부터 다운로드 가능하고/하거나 컴퓨터 관독 가능 매체 및/또는 마이크로프로세서 실행 가능 매체에 저장된 컴퓨터 프로그램 제품들이 제공되며, 컴퓨터 프로그램 제품들은 아래에 추가로 설명되는 바와 같이 위치 정보를 보호하기 위해 컴퓨터 상에서 실행될 때 상기의 방법들을 구현하기 위한 프로그램 코드 명령어들을 포함한다.
- [0335] 본 발명에 따른 임의의 방법은 프로세서 시스템으로 하여금 각자의 방법을 수행하게 하기 위한 명령어들을 포함하는 소프트웨어를 사용하여 실행될 수 있다. 소프트웨어는 시스템의 특정 서브엔티티에 의해 취해지는 그러한 단계들만을 포함할 수 있다. 소프트웨어는 하드 디스크, 플로피, 메모리 등과 같은 적절한 저장 매체에 저장될 수 있다. 소프트웨어는 유선 또는 무선에 따라 또는 예컨대 인터넷과 같은 데이터 네트워크를 사용하여 신호로 전송될 수 있다. 소프트웨어는 다운로드 및/또는 서버 상의 원격 사용이 가능하게 될 수 있다. 본 발명에 따른 방법은 방법을 수행하기 위해, 프로그래머블 로직 예컨대 FPGA(field-programmable gate array)를 구성하도록 배열된 비트스트림을 사용하여 실행될 수 있다. 소프트웨어는 소스 코드, 객체 코드, 부분적으로 컴파일된 형태와 같은 코드 중간 소스 및 객체 코드의 형태, 또는 본 발명에 따른 방법의 구현에 사용하기에 적합한 임의의 다른 형태일 수 있다는 것이 인식될 것이다. 컴퓨터 프로그램 제품에 관한 실시예는 설명된 방법들 중 적어도 하나의 처리 단계들 각각에 대응하는 컴퓨터 실행 가능 명령어들을 포함한다. 이러한 명령어들은 서브루틴들로 세분되고/되거나, 정적 또는 동적으로 링크될 수 있는 하나 이상의 파일에 저장될 수 있다. 컴퓨터 프로그램 제품에 관한 다른 실시예는 설명된 시스템들 및/또는 제품들 중 적어도 하나의 수단들 각각에 대응하는 컴퓨터 실행 가능 명령어들을 포함한다.
- [0336] 명료함을 위해, 위의 설명은 상이한 기능 유닛들 및 프로세서들을 참조하여 본 발명의 실시예들을 설명한다는 것을 인식할 것이다. 그러나, 본 발명으로부터 벗어남이 없이 상이한 기능 유닛들 또는 프로세서들 사이의 기능의 임의의 적합한 분산이 사용될 수 있음이 명백할 것이다. 예를 들어, 별개의 유닛들, 프로세서들 또는 제어기들에 의해 수행되도록 예시된 기능이 동일한 프로세서 또는 제어기에 의해 수행될 수 있다. 따라서, 특정 기능 유닛들에 대한 참조들은 오로지 엄격한 논리적 또는 물리적 구조 또는 조직을 나타내기보다는 설명된 기능을 제공하기 위한 적합한 수단에 대한 참조들로 간주되어야 한다. 본 발명은 하드웨어, 소프트웨어, 펌웨어 또는 이들의 임의의 조합을 포함한 임의의 적합한 형태로 구현될 수 있다.
- [0337] 이 명세서에서 단어 '포함하는'은 열거된 것들 이외의 요소들 또는 단계들의 존재를 배제하지 않고, 요소에 선행하는 단어 'a' 또는 'an'은 복수의 그러한 요소의 존재를 배제하지 않으며, 임의의 도면 부호는 청구항들의 범위를 제한하지 않고, 본 발명은 하드웨어 및 소프트웨어 둘 모두에 의해 구현될 수 있으며, 여러 개의 '수단' 또는 '유닛'이 하드웨어 또는 소프트웨어의 동일한 아이템에 의해 표현될 수 있고, 프로세서는 아마도 하드웨어 요소들과 협력하여 하나 이상의 유닛의 기능을 수행할 수 있다는 점에 유의한다. 또한, 본 발명은 실시예들로 제한되지 않으며, 본 발명은 위에서 설명되거나 서로 상이한 종속 청구항들에 기재된 각각의 그리고 모든 신규한 특징 또는 특징들의 조합에 존재한다.
- [0338] 참조 문헌들:
- [0339] [36.133] 3GPP TS 36.133: "Evolved Universal Terrestrial Radio Access (E-UTRA); Requirements for support of radio resource management".
- [0340] [36.211] 3GPP TS 36.211: "Evolved Universal Terrestrial Radio Access (E-UTRA); Physical Channels and Modulation".
- [0341] [36.214] 3GPP TS 36.214: "Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer - Measurements".
- [0342] [36.321] 3GPP TS 36.321: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); Medium Access Control (MAC) protocol specification".
- [0343] [36.355] 3GPP TS 36.355: "Evolved Universal Terrestrial Radio Access (E-UTRA); LTE Positioning Protocol (LPP)".
- [0344] [37.571-1] 3GPP TS 37.571-1: "Universal Terrestrial Radio Access (UTRA) and Evolved UTRA (E-UTRA) and Evolved Packet Core (EPC); User Equipment (UE) conformance specification for UE positioning; Part 1: Conformance test specification"

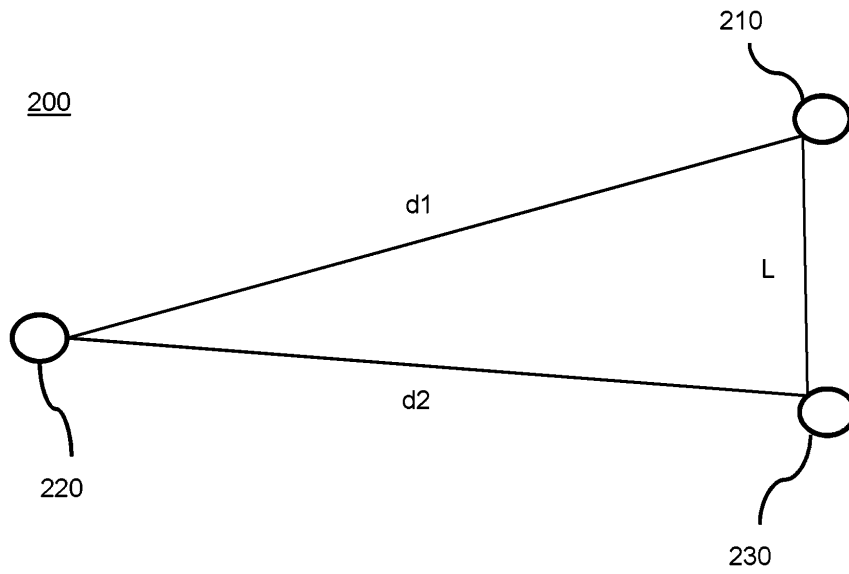
- [0345] [802.11] IEEE Computer Society, "IEEE Standard for Information Technology- telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," (IEEE Std. 802.11-2016), December 2016
- [0346] [802.1AS] Information technology - telecommunications and information exchange between systems - Local and metropolitan area networks - Part 1AS: Timing and synchronization for time sensitive applications in bridged local area networks, Reference number ISO/IEC/IEEE 8802-1AS:2014(E)
- [0347] [DH] Diffie, W.; Hellman, M. (1976), "New directions in cryptography", IEEE Transactions on Information Theory, 22 (6): 644-654
- [0348] [DPP] Device Provisioning Protocol - Technical Specification - Version 1.0, Wi-Fi Alliance, 2018, <https://www.wi-fi.org/file-member/device-provisioning-protocol-specification>.
- [0349] [NAN] Neighbor Awareness Networking - technical Specification - Version 2.0, Wi-Fi Alliance, 2017, <https://www.wi-fi.org/file-member/wi-fi-nan-technical-specification>.
- [0350] [OTDOA] Sven Fischer, "Observed Time Difference Of Arrival (OTDOA) Positioning in 3GPP LTE", Qualcomm Technologies, Inc., June 6, 2014.
- [0351] [OWE] Opportunistic Wireless Encryption - technical Specification - Version 1.0, Wi-Fi Alliance, 2018, <https://www.wi-fi.org/file-member/opportunistic-wireless-encryption-specification>.

도면

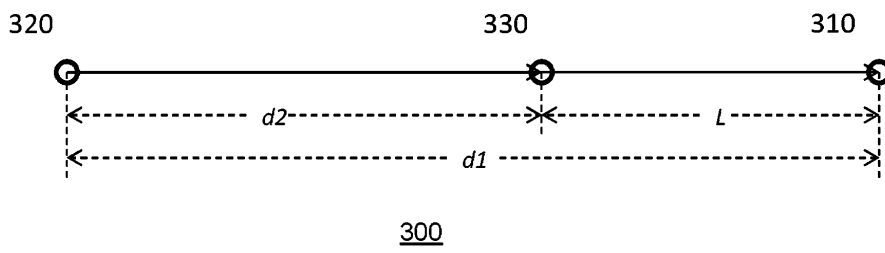
도면1



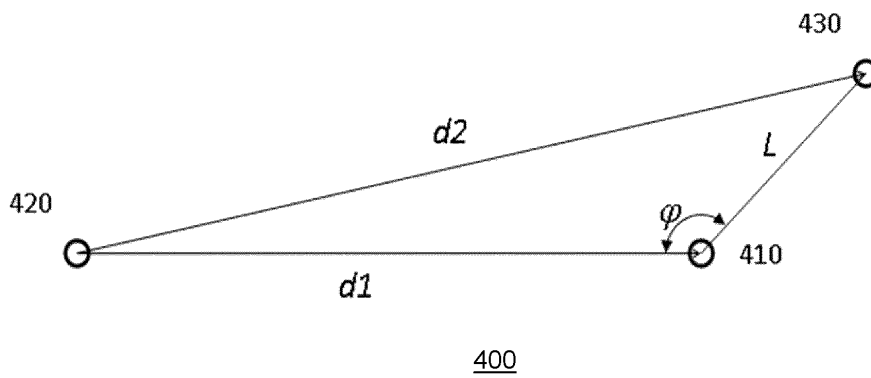
도면2



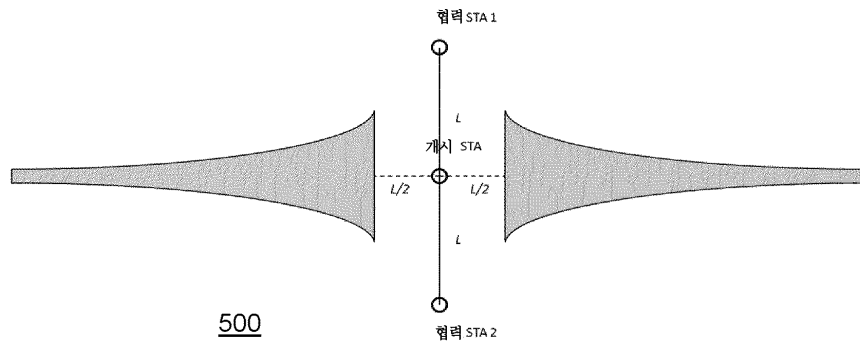
도면3



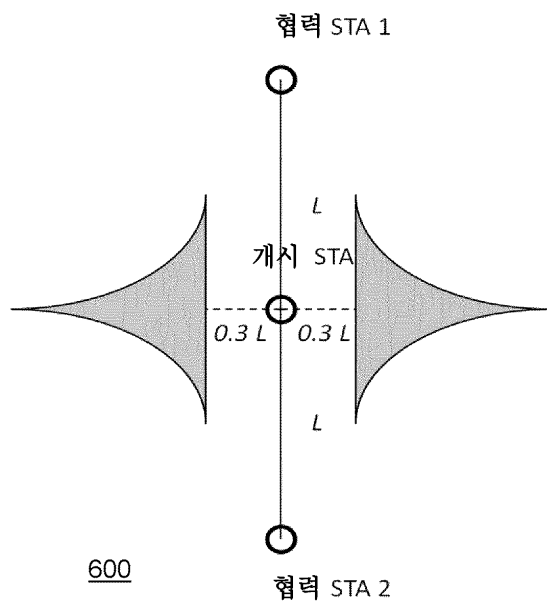
도면4



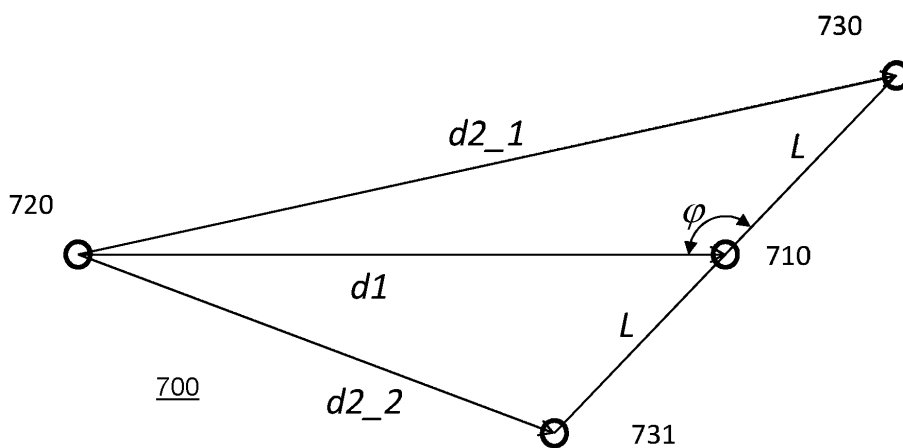
도면5



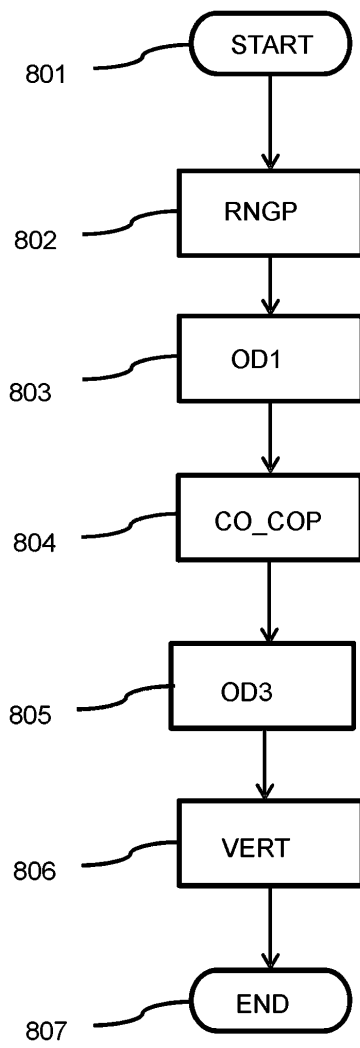
도면6



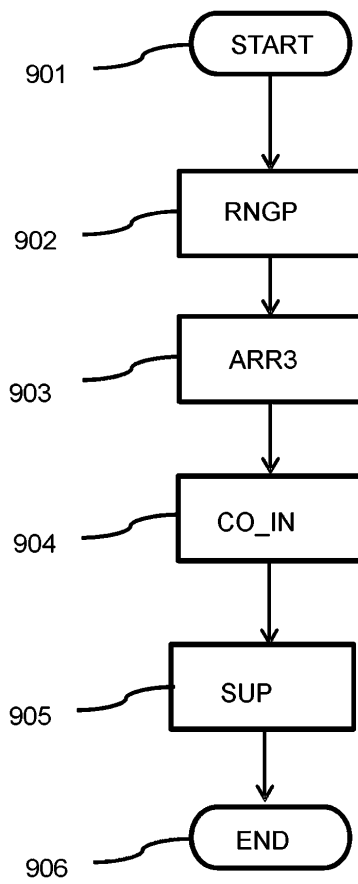
도면7



도면8

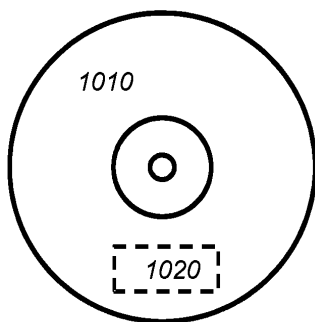


도면9



도면10a

1000



도면10b

