(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2015-0106901
(43) 공개일자 2015년09월22일

(51) 국제특허분류(Int. Cl.)
*H04W 12/06* (2009.01) *H04L 29/06* (2006.01)
*H04W 12/04* (2009.01) *H04W 76/02* (2009.01)
*H04W 8/00* (2009.01)
(52) CPC특허분류
*H04W 12/06* (2013.01)
*H04L 63/0414* (2013.01)
(21) 출원번호 10-2015-7021329
(22) 출원일자(국제) 2014년01월23일
심사청구일자 2015년08월06일
(85) 번역문제출일자 2015년08월06일
(86) 국제출원번호 PCT/EP2014/051318
(87) 국제공개번호 WO 2014/114711
국제공개일자 2014년07월31일
(30) 우선권주장
13152725.1 2013년01월25일
유럽특허청(EPO)(EP)

(71) 출원인
**코닌클리즈케 케이피엔 엔.브이.**
네덜란드, 엔엘-2516 씨케이 더 하그, 만플레인 55
**네덜란제 오르가니자티에 포오르 토에게파스트-나투우르베텐샤펠리즈크 온데르조에크 테엔오**
네덜란드 엔엘-2595 디에이 ' 에스-그라벤헤이그 안나 반 뷰렌플레인 1
(72) 발명자
**프란센, 프랑크**
네덜란드, 엔엘-9801 지씨 주이드혼, 브릴웨그 21
**베우겐, 피터**
네덜란드, 엔엘-2272 더블유엔 브어버그, 호르스트 12
*(뒷면에 계속)*
(74) 대리인
**김윤배, 강철중**

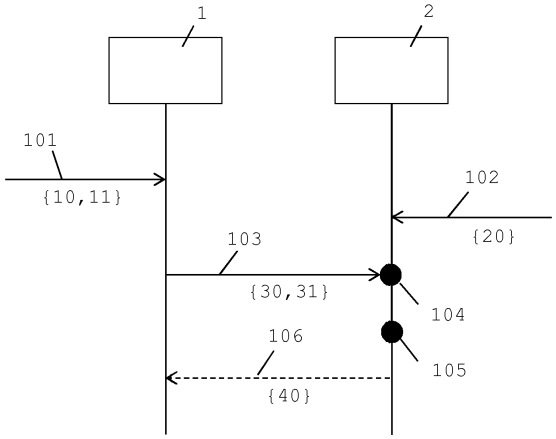
전체 청구항 수 : 총 14 항

(54) 발명의 명칭 **3GPP LTE에서 모바일 통신 디바이스 간의 근접성 발견, 인증 및 링크 설정**

## (57) 요 약

본 발명은 디바이스로 하여금 디투디 통신 모드를 위한 범위 내에 있는 하나 이상의 디바이스를 발견할 수 있도록 한다. 이러한 근접성 발견은 타겟 디바이스가, 예를 들어 소스 디바이스로부터 시그널 청취를 시작하는 것 또는 예를 들어 톨 게이트에서의 청구와 같은 근접성 발견에 기초한 임의의 다른 액션을 수행하는 것을 촉발시킬 수 있다. 발견되기를 원하는 소스 디바이스는 식별자 또는 식별자의 표현을 포함하는 메시지를 브로드캐스트한다. 이 식별자는 연결되길 원하는 타겟 디바이스 또는 소스 디바이스의 식별자이거나, 그것의 유도형이거나 피어들의 집합에 의해 사용되는 공통 보안 연계일 수 있다. 타겟 디바이스는 근접성 발견을 수립하기 위해 알려진 식별자와 브로드캐스트 식별자를 비교한다.

*대 표 도* - 도1



(52) CPC특허분류
*H04W 12/04* (2013.01)
*H04W 76/023* (2013.01)
*H04W 8/005* (2013.01)
(72) 발명자
**드 키에비트, 샌더**
네덜란드, 엔엘-2317 에이지 라이덴, 라벤호르스트 61
**에버츠, 마틴**
네덜란드, 엔엘-9714 에이치티 흐로닝언, 그라타마스트라트 42비

# 명 세 서

## 청구범위

### 청구항 1

식별자(12)를 포함하는 제1 데이터(11)를 소스 디바이스(1)에서 수신하는 단계(101);

식별자(12)의 제1 표현(21)을 포함하는 제2 데이터(20)를 타겟 디바이스(2)에서 수신하는 단계(102);

식별자의 제2 표현(31)을 포함하는 시그널(30)을 소스 디바이스(1)에 의해 브로드캐스팅하는 단계(103);

시그널(30)을 타겟 디바이스(2)에서 수신하는 단계(104); 및

성공적인 근접성 발견(proximity discovery)을 수립하기 위한 비교 결과를 얻기 위하여 식별자(12)의 제1 표현(21)과 식별자(12)의 제2 표현(31)을 타겟 디바이스에서 비교하는 단계(105)를 포함하는, 소스 디바이스(1)와 하나 이상의 타겟 디바이스(2) 간의 근접성 발견을 위한 방법.

### 청구항 2

청구항 1에 있어서,

상기 비교 결과에 따라 승인 메시지(acknowledgement message)(40)를 타겟 디바이스(2)에서 소스 디바이스(1)로 전송하는 단계(106)를 더 포함하는, 소스 디바이스(1)와 하나 이상의 타겟 디바이스(2) 간의 근접성 발견을 위한 방법.

### 청구항 3

청구항 1 또는 청구항 2에 있어서,

식별자(12)는,

타겟 디바이스(2)를 고유하게 식별시키는 임시의 브로드캐스트 식별자이고,

식별자(12)는,

타겟 디바이스(2)에 의해 소스 디바이스(1)와 관련될 수 있는, 소스 디바이스(1)와 하나 이상의 타겟 디바이스(2) 간의 근접성 발견을 위한 방법.

### 청구항 4

청구항 1 또는 청구항 2에 있어서,

소스 디바이스(1) 및 하나 이상의 타겟 디바이스(2)는,

디바이스들의 그룹을 형성하고,

식별자(12)는,

상기 디바이스들의 그룹을 식별시키는, 소스 디바이스(1)와 하나 이상의 타겟 디바이스(2) 간의 근접성 발견을 위한 방법.

### 청구항 5

청구항 3 또는 청구항 4에 있어서,

식별자(12), 식별자(12)의 제1 표현(21) 및 식별자(12)의 제2 표현(31)은,

동일한, 소스 디바이스(1)와 하나 이상의 타겟 디바이스(2) 간의 근접성 발견을 위한 방법.

### 청구항 6

청구항 1 내지 청구항 5 중의 어느 하나의 항에 있어서,

소스 디바이스(1) 및 하나 이상의 타겟 디바이스(2)는,

네트워크에 통신 가능하게 연결되고, 제1 데이터(11) 및 제2 데이터(20)는, 네트워크 내의 서버(3)로부터 수신(101, 102)되거나;

제1 데이터(11) 및 제2 데이터(20)는,

소스 디바이스(1)로부터 수신(101, 102)되는, 소스 디바이스(1)와 하나 이상의 타겟 디바이스(2) 간의 근접성 발견을 위한 방법.

**청구항 7**

청구항 6에 있어서,

식별자(12)의 제3 표현(51)을 포함하는 제3 데이터(50)를 타겟 디바이스(2)에서 수신하는 단계(107)를 더 포함하되,

식별자(21)의 제1 표현은,

식별자의 유도형을 연산하기 위해 식별자(12) 및 난수(random number)를 입력으로서 사용하는 제1 수학적 함수에 의해 얻어지는 식별자의 유도형이고,

식별자(12)의 제3 표현(51)은,

난수이고,

비교하는 단계(105)는,

입력으로서 식별자(12)의 제2 표현(31) 및 식별자(12)의 제3 표현(51)을 이용하여 상기 제1 수학적 함수와 동일한 제2 수학적 함수를 이용하는 식별자의 유도형을 연산하는 단계(108); 및

연산된 상기 식별자의 유도형과 식별자(12)의 제1 표현(21)을 비교하는 단계(109)를 포함하고,

난수는,

서버 또는 소스 디바이스(1)에서 생성되는 난수;

서버(3) 또는 소스 디바이스(1)에서 생성되는 솔트(salt);

서버(3) 또는 소스 디바이스(1)에서, 입력으로서 난수의 유도형을 계산하기 위해, 추가적인 난수 및 소스 디바이스(1)를 식별시키는 소스 식별자를 이용하는 제3 수학적 함수에 의해 획득되는 추가적인(further) 난수의 유도형(derivation); 중에서 하나인, 소스 디바이스(1)와 하나 이상의 타겟 디바이스(2) 간의 근접성 발견을 위한 방법.

**청구항 8**

청구항 6 또는 청구항 7에 있어서,

제2 데이터(20)는,

티켓 식별자(22)를 더 포함하고,

상기 방법은,

소스 디바이스(1)에서 서버(3)로부터 티켓 식별자(22), 제1 데이터(11) 및 제4 데이터(13)를 포함하는 티켓 데이터(10)를 수신하는 단계(110);

티켓 식별자와 관련된 제4 데이터(13)의 복사본(41)을 획득하기 위해 타겟 디바이스(2)에서 서버(3)로 티켓 식별자(22)를 전송하는 단계(111); 및

타겟 디바이스(2)에서 서버(3)로부터 제4 데이터(13)의 복사본(41)을 수신하는 단계(112)를 더 포함하되,

승인 메세지(40)는,

소스 디바이스(1)에서 제4 데이터(13)에 의한 확인을 위한 제4 데이터(13)의 복사본(41)을 포함하는, 소스 디바

이스(1)와 하나 이상의 타겟 디바이스(2) 간의 근접성 발견을 위한 방법.

**청구항 9**

청구항 6 내지 청구항 8 중의 어느 한 항에 있어서,

소스 디바이스(1) 또는 타겟 디바이스(2)로부터의 제1 데이터(11), 제2 데이터(20) 및/또는 티켓 데이터(10)에 대한 요청을 서버(3)의 오퍼레이터에 의해 청구(charging)하는 단계를 더 포함하는, 소스 디바이스(1)와 하나 이상의 타겟 디바이스(2) 간의 근접성 발견을 위한 방법.

**청구항 10**

청구항 8 또는 청구항 9에 있어서,

타겟 디바이스(2)에서 소스 디바이스(1)로부터 제1 챌린지 데이터(32)를 수신하는 단계(113); 및

타겟 디바이스(2)에서 제1 챌린지 데이터(32)에 대해 제 4 수학적 함수, 예를 들어 해쉬(hash) 함수를 이용하는 유도된 제1 챌린지 데이터(42)를 연산하는 단계(114)를 더 포함하되,

승인 메세지(40)가 유도된 제1 챌린지 데이터(42) 및 제2 챌린지 데이터(43)를 더 포함하고,

상기 방법은,

소스 디바이스(1)에서 수신된 유도된 제1 챌린지 데이터(42)와의 비교를 위한 제1 챌린지 데이터(32)에 대해, 제 4 수학적 함수와 동일한 제5 수학적 함수를 이용하는 유도된 제1 챌린지 데이터(42)를 연산하는 단계(15);

소스 디바이스(1)에서 제2 챌린지 데이터에 대해, 제6 수학적 함수를 이용하는 유도된 제2 챌린지 데이터(33)를 연산하는 단계(116);

유도된 제2 챌린지 데이터(33)를 타겟 디바이스(1)에 전송하는 단계(117); 및

타겟 디바이스(2)에서 수신된 유도된 제2 챌린지 데이터(33)와의 비교를 위해 제2 챌린지 데이터(43)에 대해 제 6 수학적 함수와 동일한 제7 수학적 함수를 이용하는 유도된 제2 챌린지 데이터(33)를 연산하는 단계(118)를 더 포함하는, 소스 디바이스(1)와 하나 이상의 타겟 디바이스(2) 간의 근접성 발견을 위한 방법.

**청구항 11**

청구항 10에 있어서,

티켓 데이터(10)는 암호화 키(14)를 더 포함하고,

상기 방법은,

타겟 디바이스(1)에서 서버(3)로부터 서버(3)에서 티켓 식별자(22)와 관련된 암호화 키(14)를 수신하는 단계(119)를 더 포함하고,

제4, 제5, 제6 및 제7 수학적 함수는 암호화 키(14)를 이용하는 암호 함수를 포함하는, 소스 디바이스(1)와 하나 이상의 타겟 디바이스(2) 간의 근접성 발견을 위한 방법.

**청구항 12**

청구항 1 내지 청구항 11 중의 어느 한 항에 따른 소스 디바이스와 하나 이상의 타겟 디바이스 간의 근접성 발견을 위한 방법을 이용해서 하나 이상의 타겟 디바이스(2)와의 근접성 발견 과정을 수행하도록 구비된 소스 디바이스(1).

**청구항 13**

청구항 1 내지 청구항 11 중의 어느 한 항에 따른 소스 디바이스와 하나 이상의 타겟 디바이스 간의 근접성 발견을 위한 방법을 이용해서 소스 디바이스(1)와의 근접성 발견 과정을 수행하도록 구비된 타겟 디바이스(2).

**청구항 14**

청구항 12에 따른 소스 디바이스(1) 및 청구항 13에 따른 하나 이상의 타겟 디바이스(2)를 포함하는 네트워크.

## 발명의 설명

### 기 술 분 야

[0001] 본 발명은 통신 디바이스의 근접성 발견에 관한 것으로 더욱 상세하게는 디바이스 간에 디투디 통신 세션 세팅을 야기하는 디바이스의 근접성 발견(proximity discovery)에 관한 것이다.

### 배 경 기 술

[0002] 3GPP(3rd Generation Partnership Project) 표준에서의 최근의 발전은 롱텀 레볼루션(Long Term Evolution: LTE) 네트워크 및 디바이스에 관한 것이다. 또한 4G(즉, 제4 세대) 모바일 통신 표준으로 알려진, LTE는 모바일 전화 및 데이터 단말기를 대상으로 하는 고속 데이터 무선 통신을 위한 표준이다. 이는 GSM/EDGE(또한 2G 또는 2.5G로 알려진) 및 UMTS/HSPA(또한 3G로 알려진) 네트워크 기술들의 계승자로서, 코어 네트워크 향상과 함께 다른 라디오 인터페이스를 이용하여 용량과 속도를 증가시킨다. 최근의 LTE 확장은, 주로 베이스 스테이션과 모바일 디바이스 간의 전통적인 통신 다음으로, 직접적으로 또는 릴레이로 근처의 베이스 스테이션을 사용하는 디투디(device-to-device: D2D) 통신을 가능하게 한다. LTE에서 디투디 통신은 또한 LTE-Direct 통신으로 알려져 있다.

[0003] LTE-Direct 통신에 관한 사용 예들(use cases)은 3GPP 기술 보고(technical report) TR 22.803으로부터 알려졌다. 제1 사용 예에서 알리스는 컨퍼런스에 참석 중이고 그녀의 친구인 밥의 근접성을 감지하려 한다. 알리스는 그녀의 친구 밥을 발견하기 위해 직접 모드를 턴온 한다. 여기서 알리스의 폰은 그녀가 직접 모드 사용을 원하고 특히 밥에게 발견되기 원하는 것을 알리기 위해 그녀의 모바일 오퍼레이터(mobile operator)에게 메세지를 보낸다. 모바일 오퍼레이터의 직접 모드 서버(direct mode server)는 알리스와 밥을 짝(pair)으로 리스트(list)한다. 그리고, 네트워크가 밥과 알리스가 가까이 있음을 감지(예를 들어, 그들이 같은 네트워크 셀에 위치하거나 다른 메카니즘에 의해)하는 경우, 네트워크는 알리스와 밥에게 알리고, 그들이 그들의 사생활 공개 없이 서로를 신뢰하며 식별할 수 있도록 하는 정보를 전송한다. 제2 사용 예는, 소방대(fire brigade), 경찰 및 구급차 서비스와 같은 공공 안전 서비스(public safety services)에 관한 것이다. 예를 들면, 보호 장비 없이 빌딩에 들어간 소방대원은 자신의 동료에게 전할 말이 있을 수 있다. 이러한 예에서 디바이스는 서로를 발견할 수 있고 안전하고 인증된 커넥션을 구축할 수 있다.

[0004] 유선 및/또는 모바일의 디바이스, 예를 들어 전화 및 머신 타입 통신(machine type communication: MTC) 디바이스들 각각이 서로 근접해 있는 경우, 디투디 통신 세션(D2D communication session)은, LTE 모바일 디바이스 경우에서의 LTE-Direct 또는, IEEE 802.11, IEEE 802.16, IEEE 802.20, 블루투스(Bluetooth), Wi-Fi 또는 WiMAX에 기초하는 다른 디투디 통신 표준을 이용하여 디바이스 간에 구축될 수 있다. 여기서 디바이스들은 전형적으로 서로의 존재를 감지하고 사용자에게 다른 디바이스의 근접성을 알린다.

[0005] 일반적으로 네트워크는 디바이스의 근접성의 발견에 도움을 줄 수 있다. 여기서, 네트워크는 두 디바이스가 서로 간에 근접될 수 있는지 판단하고 서로 상대 디바이스에 근접될 수 있는지에 관한 정보를 알려 준다. 네트워크는 디바이스들이 도달 가능한 범위에 있음을 판단하지 못할 수 있다. 이러한 경우 디바이스들은, 예를 들어 다른 근접한 디바이스에 의해 픽업될 수 있는 식별자(identifier)를 브로드캐스팅(broadcasting)하는 것과 같은 추가적인 근접성 테스트를 수행하여야 한다. 선택적으로, 근접성의 발견은 디바이스에 의해 직접적으로 수행된다. 이러한 경우, 디바이스는 전형적으로 식별자를 브로드캐스트(broadcast)하고 브로드캐스트 식별자(broadcast identifiers)에서 다른 디바이스를 발견한다. 블루투스 디바이스들은 이러한 근접성 발견 능력들을 가지는 것으로 알려져 있다.

[0006] 두 개 중 어느 하나의 솔루션(네트워크가 조력하는 경우 또는 근접성의 직접 발견)에서, 각각의 디바이스들의 식별자들은 브로드캐스트되거나 그렇지 않은 경우 각각의 디바이스들에 의해 전송된다. 전형적으로 식별자들은 정적이고, 일정한 인터벌로 브로드캐스트 식별자를 단순히 경청함으로써 각각의 디바이스의 자취 추적을 가능하게 할 수 있다. 이러한 사용자의 사생활 침범은 상당히 바람직하지 못하다.

[0007] 알려진 근접성 발견 솔루션들에 관한 다른 단점은 솔루션들이 개인 디바이스의 발견에 사용된다는 점이다. 개인 디바이스의 근접성 발견 및 디바이스 그룹의 근접성 발견을 가능하게 하는 선택적인 발견에 관한 솔루션에 관한 요구가 존재한다. 그리하여, 사용자는 예를 들어, 자신의 디바이스의 발견 가능성을 조정하여, 자신의 디바이스가 제한된 수의 디바이스에게만 자신을 식별시키도록, 예를 들어 회의에서 자신의 동료의 디바이스 또는 팝 콘서트에서 친구의 디바이스에게만 자신을 식별시키도록 할 수 있다. 디투디 통신 범위에 있는 다른 디바이스들은

바람직하게는 그룹 내의 디바이스의 근접성에 관하여 모르는 것이 좋다.

[0008] 사생활을 존중하는 제어되는(controlled) 라디오 네트워크(radio network)에서 디바이스의 근접성 발견을 가능하게 하고, 선택적인 발견 가능성(selective discoverability)을 허용하고 네트워크 부하(network load) 및 필요한 컴퓨팅 파워(computing power) 차원에서 바람직하게는 낮은 프로파일(low profile)을 가지는 솔루션에 대한 요구가 존재한다.

## *발명의 내용*

### *해결하려는 과제*

[0009] 본 발명은 사생활을 존중하는 제어된 라디오 네트워크에서 디바이스의 근접성 발견을 가능하게 하고, 선택적인 발견 가능성을 허용하고 네트워크 부하 및 필요한 컴퓨팅 파워 차원에서 바람직하게는 낮은 프로파일을 가지는 솔루션을 제공하는 것을 목적으로 한다.

### *과제의 해결 수단*

[0010] 본 발명의 하나의 실시예에 따르면 소스 디바이스와 하나 이상의 타겟 디바이스 사이의 근접성 발견을 위한 방법(이하, 본 방법)이 개시된다. 본 방법은, 식별자를 포함하는 제1 데이터를 소스 디바이스에서 수신하는 단계를 포함한다. 본 방법은 식별자의 제1 표현(representation)을 포함하는 제2 데이터를 타겟 디바이스에서 수신하는 단계를 더 포함할 수 있다. 본 방법은 식별자의 제2 표현(representation)을 포함하는 시그널을 소스 디바이스에 의해 브로드캐스팅하는 단계를 더 포함할 수 있다. 본 방법은 성공적인 근접성 발견 수립을 위한 비교 결과를 얻기 위하여 식별자의 제1 표현 및 식별자의 제2 표현을 타겟 디바이스에서 비교하는 단계를 더 포함할 수 있다.

[0011] 이와 같이 얻어진 비교 결과는 전형적으로 식별자의 제1 표현 및 제2 표현이 매치될 수 있는가를 알려준다. 이것이 그러한 경우라면 근접성 발견은 성공적일 수 있다.

[0012] 식별자 대신에, 소스 디바이스는, 특정의 타겟 디바이스 또는 타겟 디바이스의 그룹(group) 만이 소스 디바이스와 연관될 수 있는 식별자의 유도형(derivation of the identifier)을 유리하게 브로드캐스트할 수 있다. 그렇게 함으로써 타겟 디바이스는 누가 브로드캐스팅 하는지 알 수 있다. 예를 들어, 타겟 디바이스는 소스 디바이스가 가까운 범위, 예를 들어, 디투디 통신 세션 범위에 있다는 결론을 내리거나, 또는 가까운 범위에 있는 소스 디바이스에 기반하여 임의의 액션의 유발, 예를 들어 톨 게이트(toll gate)에서 청구(charging)를 할 수 있다. 한편, 소스 디바이스의 신원은 추적이 불가능하다.

[0013] 본 발명의 하나의 실시예에 있어서 본 방법은 비교 결과에 따른 승인 메시지(acknowledgement message)를 타겟 디바이스로부터 소스 디바이스로 전송하는 단계를 더 포함할 수 있다. 이것은 유리하게도 타겟 디바이스가 가까운 범위에 있다는 것을 소스 디바이스에게 학습시킬 수 있다.

[0014] 본 발명의 다른 실시예에 있어서 식별자는 타겟 디바이스를 고유하게 식별시키는 임시의 브로드캐스트 식별자일 수 있다. 그리고 식별자는 타겟 디바이스에 의해 소스 디바이스와 관련될 수 있다. 이는 유리하게도 소스 디바이스가 식별자를 전송하도록 할 수 있는데, 여기서 식별자는, 소스 디바이스 추적을 불가능하게 하여 식별자가 소스 디바이스에 연결되지 않은 것처럼 감청자에게 보여진다. 타겟 디바이스는 식별자를 소스 디바이스에 연계(associate)시킬 수 있다.

[0015] 본 발명의 다른 실시예에서 소스 디바이스 및 하나 이상의 타겟 디바이스는 디바이스들의 그룹을 생성할 수 있다. 그리고 식별자는 그룹을 식별시킬 수 있다. 이는 유리하게도 단지 하나의 타겟 디바이스보다는 디바이스들의 그룹에 대한 근접성 발견을 가능하게 할 수 있다.

[0016] 본 발명의 다른 실시예에서 식별자, 식별자의 제1 표현 및 식별자의 제2 표현은 동일할 수 있다.

[0017] 본 발명의 다른 실시예에서 소스 디바이스 및 하나 이상의 타겟 디바이스는 네트워크에 통신 가능하게 연결되고 제1 데이터 및 제2 데이터는 네트워크 내의 서버로부터 수신될 수 있다. 선택적으로, 제1 데이터 및 제2 데이터는 소스 디바이스로부터 수신될 수 있다. 이는 네트워크가 관여되는 것을 가능하게 하거나 네트워크 없이 독립(standalone) 모드에서의 동작을 가능하게 할 수 있다.

[0018] 본 발명의 다른 실시예에서 본 방법은 타겟 디바이스에서 식별자의 제3 표현을 포함하는 제3 데이터를 수신하는 단계를 더 포함할 수 있다. 식별자의 제1 표현은 식별자의 유도형을 연산하기 위해 식별자 및 난수(random

number)를 입력으로 사용하는 제1 수학적 함수에 의해 얻어지는 식별자의 유도형일 수 있다. 식별자의 제3 표현은 난수일 수 있다. 비교하는 단계는, 입력으로서 식별자의 제2 표현 및 식별자의 제3 표현을 이용하는 제1 수학적 함수와 동일한 제2 수학적 함수를 이용하여 식별자의 유도형을 연산하는 단계를 포함할 수 있다. 비교하는 단계는 식별자의 연산된 유도형과 식별자의 제1 표현을 비교하는 단계를 더 포함할 수 있다. 난수는 서버 또는 소스 디바이스에서 생성되는 난수일 수 있다. 선택적으로 난수는 서버 또는 소스 디바이스에서 생성되는 솔트(salt)일 수 있다. 선택적으로 난수는, 난수의 유도형을 연산하기 위해 소스 디바이스를 식별시키는 소스 식별자 및 추가적인 난수를 입력으로 이용하는 제3 수학적 함수에 의해 서버 또는 소스 디바이스에서 얻어지는 추가적인 난수의 유도형일 수 있다.

[0019] 이는 유리하게도, 디바이스 추적을 더욱 어렵게 하면서 교환된 식별자에 대해 모호성(obscurity) 레벨을 추가시킨다.

[0020] 다른 실시예에서 제2 데이터는 티켓 식별자(ticket identifier)를 더 포함할 수 있다. 본 방법은 티켓 식별자, 제1 데이터 및 제4 데이터를 포함하는 티켓 데이터를 소스 디바이스에서 서버로부터 수신하는 단계를 더 포함할 수 있다. 본 방법은 티켓 식별자와 연관된 제4 데이터의 복사본을 획득하기 위해 티켓 식별자를 타겟 디바이스에서 서버로 전송하는 단계를 더 포함할 수 있다. 본 방법은 제4 데이터의 복사본을 타겟 디바이스에서 서버로부터 수신하는 단계를 더 포함할 수 있다. 승인 메시지는 소스 디바이스에서 제4 데이터에 의한 확인(verification)을 위한 제4 데이터의 복사본을 포함할 수 있다.

[0021] 티켓팅은 유리하게도 근접성 발견 시도들을 추적하는 것을 가능하게 한다. 예를 들어, 추적(tracking)은 근접성 발견 시도들을 위한 로그(log) 또는 청구(charge)에 이용될 수 있다.

[0022] 다른 실시예에서 본 방법은, 제1 데이터, 제2 데이터 및/또는 티켓 데이터에 대한 요청을 서버의 오퍼레이터에 의해 소스 디바이스 또는 타겟 디바이스로부터 청구(charging)하는 단계를 더 포함할 수 있다. 이는 유리하게도 근접성 발견 시도, 가능하게는 성공적인 근접성 발견 시도만에 대한 청구(charging)를 가능하게 한다.

[0023] 다른 실시예에서 본 방법은 제1 챌린지 데이터를 타겟 디바이스에서 소스 디바이스로부터 수신하는 단계를 더 포함할 수 있다. 본 방법은 제4 수학적 함수, 예를 들어 해시 함수(hash function)를 제1 챌린지 데이터에 사용하여 유도된 제1 챌린지 데이터를 타겟 디바이스에서 연산하는 단계를 더 포함할 수 있다. 승인 메시지는 유도된 제1 챌린지 데이터 및 제2 챌린지 데이터를 더 포함할 수 있다. 본 방법은, 수신된 유도된 제1 챌린지 데이터와의 비교를 위해, 제4 수학적 함수와 동일한 제5 수학적 함수를 제1 챌린지 데이터에 이용하여 유도된 제1 챌린지 데이터를 소스 디바이스에서 연산하는 단계를 더 포함할 수 있다. 본 방법은 제6 수학적 함수를 제2 챌린지 데이터에 사용하여, 유도된 제2 챌린지 데이터를 소스 디바이스에서 연산하는 단계를 더 포함할 수 있다. 본 방법은 유도된 제2 챌린지 데이터를 타겟 디바이스에 전송하는 단계를 더 포함할 수 있다. 본 방법은, 수신된 유도된 제2 챌린지 데이터와 비교하기 위해 제2 챌린지 데이터에 제6 수학적 함수와 동일한 제7 수학적 함수를 사용하여, 유도된 제2 챌린지 데이터를 타겟 디바이스에서 연산하는 단계를 더 포함할 수 있다.

[0024] 이는 유리하게도 챌린지-응답 인증(challenge-response authentication)의 형태로 식별자 교환에 보안 레벨을 추가한다.

[0025] 다른 실시예에서 티켓 데이터는 암호화 키(encryption key)를 더 포함할 수 있다. 본 방법은 티켓 식별자에 대해 서버에서 연관된 암호화 키를 타겟 디바이스에서 서버로부터 수신하는 단계를 더 포함할 수 있다.

[0026] 이는 유리하게도 식별자 교환에 보안 레벨(level of security)을 추가할 수 있다.

[0027] 본 발명의 일 실시예에 따르면 상기 기술된 방법의 하나 이상의 단계를 이용하여 하나 이상의 타겟 디바이스와 근접성 발견 과정 수행을 위해 구성되는 소스 디바이스가 개시된다.

[0028] 본 발명의 일 실시예에 따르면 상기 기술된 방법의 하나 이상의 단계를 이용하는 소스 디바이스와 근접성 발견 과정을 수행을 위해 구성되는 타겟 디바이스가 개시된다.

[0029] 본 발명의 일 실시예에 따르면 상기 기술된 소스 디바이스 및 상기 기술된 하나 이상의 타겟 디바이스를 포함하는 네트워크가 개시된다.

[0030] 이하, 본 발명의 실시예는 더욱 자세히 기술될 것이다. 그러나 이러한 실시예는 본 발명의 권리 범위를 제한하는 것으로 이해되는 것이 아님을 주목하여야 한다.

## *발명의 효과*

[0031] 본 발명은 특히 디투디 통신을 할 수 있고 디투디 통신 세션을 위한 인근의 디바이스를 발견하려는 디바이스에 유용하고, 그렇다고 이에 한정되는 것은 아니다.

## 도면의 간단한 설명

[0032] 본 발명의 태양들은 도면에 나타낸 실시예를 참조함으로써 보다 상세하게 설명될 것이다.

도 1 내지 도 6은 소스 디바이스, 타겟 디바이스 및 선택적으로 서버 간에서 시계열적 다이어그램으로 묘사되는 본 발명의 실시예에 따른 근접성 발견 과정에 관한 것이다.

## 발명을 실시하기 위한 구체적인 내용

[0033] 다음의 기술에서 디바이스(device), 터미널(terminal) 및 사용자 장비(user equipment: UE)는 유선(fixed) 또는 모바일 엔드-유저(end-user) 또는 MTC 디바이스의 동의어로 이해될 수 있다. 피어(peer)는 디투디 통신에 관여될 수 있는 임의의 유선 또는 모바일 엔드-유저 디바이스로 이해될 수 있다.

[0034] 디투디 통신 모드에서 디바이스들은 직접적으로, 즉 유선 또는 무선의 네트워크 없이 통신한다. 디바이스 간의 시그널 릴레이를 위해서 디투디 통신 링크는 베이스 스테이션(base station)을 사용할 수 있다. 그러나 베이스 스테이션 네트워크의 추가적인 네트워크 기능은 사용되지 않을 것이다. 피어들(peers)은 디투디 통신 모드 다음으로 무선 또는 유선 네트워크에 연결될 수 있다.

[0035] 본 발명은 디바이스가 디투디 통신 범위 내에서 하나 이상의 다른 디바이스를 발견하도록 할 수 있다. 이러한 근접성 발견(proximity discovery)은 타겟 디바이스로 하여금, 예를 들어 소스 디바이스로부터의 시그널 청취를 시작하게 하거나 톨 게이트에서의 청구(charging)와 같은 근접성 발견에 기초한 임의의 다른 액션을 수행하도록 할 수 있다. 근접성 발견은 소스 디바이스와 타겟 디바이스 사이의 디투디(device-to-device) 통신 세팅하는 것을 야기할 수 있다.

[0036] 디바이스들의 신원(identity) 또는 신원의 표현(representation)은 근접성 발견을 가능하게 하도록 서로 교환될 수 있다. 디바이스들의 전송을 청취하거나 엿듣는 것 및 전송되는 식별자를 픽업하는 것에 의해 디바이스들이 추적될 수 없도록 하는 방식으로 식별자들의 이러한 교환은 이루어진다.

[0037] 네트워크에 대해 유선 또는 무선 연결을 갖는 둘 이상의 디바이스 간의 디투디 통신 세션을 수립하기 위해, 디바이스는 근접성 발견 과정을 시작하기에 앞서 자신이 발견되거나 임의의 피어(들)(의 집합)를 발견할 의향이 있음을 네트워크 내의 서버에 알림으로써 다른 디바이스들을 선택적으로 촉발시킬 수 있다. 근접성 발견 과정에 앞서, 네트워크, 서드 파티(third party)(예를 들어, 최상의(over-the-top) 공급자 또는 다른 서드 파티) 또는 디바이스 자신들은 전형적으로 피어들이 인근에 있음을 감지한다.

[0038] 근접성 발견 과정의 일부로서, 발견되길 원하는 소스 디바이스는 식별자 또는 식별자의 표현을 포함하는 메시지를 브로드캐스트한다. 식별자는 연결될 타겟 디바이스 또는 소스 디바이스의 식별자이거나 그것의 유도형 또는 피어의 집합(set of peers)에 의해 사용되는 공통(common) 보안 연계(security association)의 식별자일 수 있다. 바람직하게는 디바이스는 디바이스의 추적가능성(traceability)을 배제하기 위하여 자기 자신의 식별자를 평문으로(in the clear) 브로드캐스트하지 않는다.

[0039] 식별자는 임시 브로드캐스트 식별자(temporary broadcast identifier: T-BID)일 수 있으며 시간에 따라 변할 수 있다. T-BID는 다른 파티, 예를 들어 새로운 식별자를 디바이스에 공급하는 네트워크에 의하거나 또는 최상의(over-the-top) 서비스, 즉 새로운 식별자를 공급하는 페이스북(Facebook), 구글플러스(Google+) 또는 와츠앱(Whatsapp)과 같은 네트워크 외부의 파티에 의한 권한설정(provisioning)에 의해 변할 수 있다. T-BID는 네트워크(즉, 디투디 통신 모드를 사용하지 않는), 또는 와이파이(Wi-Fi), 블루투스(Bluetooth), NFC와 같은 다른 연결 또는 카메라와 스크린의 통신에 전해지는 두 디바이스 간의 통신 세션이라는 수단에 의해, 예를 들어 디바이스로 하여금 새로운 임시 식별자 및 새로운 임시 식별자 연산을 위한 램덤/알고리즘을 교환하게 함으로써 변할 수 있다. T-BID는 예를 들어, 시간 두 개의(또는 이상의) 디바이스 간에 디투디 커넥션이 셋업된 회수, 네트워크 오퍼레이터 또는 최상의 서비스 공급자와 같은 서드 파티에 의해 공급되는 랜덤(random) 또는 솔트(salt) 및/또는 암호화된/해시된(hashed) 식별자와 동시에 전송되는 램덤을 포함하는 알고리즘에 의해 변할 수 있다.

[0040] 근접성 발견 과정의 일부로서, 타겟 디바이스는 브로드캐스트 메시지(예를 들어, 복호화(deciphering), 리해싱(rehashing) 또는 알려진 신원(identities)을 리스트와의 단순 비교)로부터 필요한 정보를 추출한다. 소스 디바이스는 특정의 타겟 디바이스만이 누가 브로드캐스팅하고 있는지를 알 수 있는 방법으로 자신의 신원(identit

y)을 브로드캐스트한다.

[0041] 선택적으로 타겟 디바이스는 승인 메시지를 소스 디바이스에 전송함으로써 그것이 다른 디바이스를 들었다(hear)는 것과 그것이 디투디 통신에 준비되어 있다는 것을 응답한다. 선택적인 승인 메시지(optional acknowledgement message)는 초기 브로드캐스트에 포함될 수 있는 챌린지에 대한 응답(response)을 포함할 수 있다. 선택적인 승인 메시지는 데이터를 포함할 수 있는데, 이 데이터로부터 인증 목적의 소스 디바이스 및 타겟 디바이스에 의해 공통 시크리트(common secret)가 알려지는 것이 수립될 수 있다.

[0042] 성공적인 근접성 발견 후에, 디투디 연결이 디바이스 간에 셋업될 수 있다.

[0043] 근접성 발견 과정은 안전한 디투디 연결을 셋업하는데 사용될 수 있다. 두 디바이스들이 서로를 인증할 수 있다는 것(예를 들어 중간 공격에서 어느 사람을 막는 행위)과 네트워크가 연결 셋업 방법에 관한 제어 능력을 가지고 있다는 것을 확인하는 것이 바람직하다. 근접성 발견은 다음과 같이 구현될 수 있는 3가지 방식의 핸드셰이크(handshake) 과정을 포함할 수 있다:

[0044] 1. 소스 디바이스는 T-BID와 동일한 브로드캐스트에서 타겟 디바이스에 랜덤(챌린지)을 전송한다;

[0045] 2. 타겟 디바이스는 hash(challenge||common secret)를 연산한다. 여기서, 공통 시크리트(common secret)는, 예를 들어 램덤, 솔트(salt) 또는 일반적인 T-BID일 수 있다. 타겟 디바이스는 추가적인 random||hash(challenge||common secret)을 포함하는 메시지와 함께 추가적인 랜덤 리플라이(further random replies)를 생성한다;

[0046] 3. 소스 디바이스는 hash(challenge||common secret)를 확인할 수 있고, hash(further random||common secret)를 포함하는 메시지와 함께 응답한다;

[0047] 4. 타겟 디바이스는 hash(further random||common secret)를 확인할 수 있고, 현재 소스 디바이스 및 타겟 디바이스는 둘이 동일한 공통 시크리트(common secret)를 가지고 있고 서로를 인증했음을 안다.

[0048] 다음의 본 발명에 따른 예시적인 실시예에서는, 앞서 대략적으로 설명된 근접성 발견 과정이 보다 상세히 설명될 것이다.

[0049] 다른 종류의 식별자들이 근접성 발견 과정에 사용될 수 있다. 예를 들어, 브로드캐스트 식별자(BID), 임시 브로드캐스트 식별자(T-BID), 그룹 특정 브로드캐스트 식별자(G T-BID), 친구 특정 (임시) 브로드캐스트 식별자(F(T)-BID) 그리고 보안 연계 (임시) 브로드캐스트 식별자(SA(T)-BID)이다. 브로드캐스트 식별자는 세계적으로 고유한 식별자로서 누군가를 호출하거나 자신의 존재를 알리기 위해 공유 매체(shared medium)를 통해 브로드캐스트된다. 디바이스는 BID의 유도형 또는 호출될 친구(friend)/다른 디바이스의 BID를 브로드캐스트 할 수 있다. 임시 브로드캐스트 식별자는 한정된 시간 또는 용례 또는 지리적인 위치를 위해서만 사용되는 브로드캐스트 식별자다. 이러한 룰의 예외는 소위 원타임 T-BID(one time T-BIT)가 T-BID로부터 유도되고 대신 브로드캐스트된다. 그룹 특정 (T-)BID는 그룹에 관한 브로드캐스트 식별자다. 이는 그룹 내의 모든 디바이스들이 이러한 BID를 청취함을 뜻한다. 친구 특정 (T-)BID는 두 개의 친구/디바이스들 간에만 공유되는 브로드캐스트 식별자다. 보안 연계 (T-)BID는 보안 연계에 관한 브로드캐스트 식별자다. 이는 두 디바이스가 보안 연계를 공유하면, 그들은 같은 브로드캐스트 식별자를 청취한다.

[0050] 전형적으로 근접성 감지(proximity detection)는 근접성 발견 과정(proximity discovery procedure)에 선행한다. 근접성 감지 과정에서 디바이스들은 그들이 가까이 있다는 정보를 수신한다. 근접성 발견 과정에서 자신들이 근접하다는 정보를 수신한 하나 이상의 디바이스들은 디투디 통신이 가능한지 여부를 판단한다. 근접성 감지를 수행하는 복수의 방법이 존재한다. 예를 들어, 네트워크가 두 피어들이 근접함을 감지하고 알려줄 수 있다. 이는 장점일 수 있는데, 그 이유로서 첫째, 네트워크가 알려 주면, 디바이스는 식별자를 브로드캐스트하면 되는데, 이는 낮은 베터리 소모 및 낮은 브로드캐스트 채널 사용의 결과를 야기한다. 그리고 둘째, 네트워크는 (동일 메시지에서) 식별자 그리고 (선택적으로) 암호화 재료를 공급할 수 있다. 추가적으로 또는 택일적으로, 최상의 서비스 공급자 또는 제3 파티는 피어들에게 그들이 근접해 있음을 알려줄 수 있다. 추가적으로 또는 택일적으로, 사용자들은 서로간 근접해 있는 디바이스들을 활성화할 수 있다. 이는 네트워크 커버리지가 없는 상황 그리고 사용자가 디투디 연결을 셋업하려는 상황에서 바람직할 수 있다. 네트워크 커버리지가 있는 경우에도 이 방법은, 예를 들어 서로간에 모르는 피어들에 대해 여전히 바람직할 수 있는데, 예를 들어 당신이 새로운 사람을 만나는데 전화번호를 교환하려는 경우이다.

[0051] 도 1 내지 도 6은 네트워크 내의 소스 디바이스(1), 타겟 디바이스(2) 및 선택적인 서버(3) 간에서 시계열적 다

이어그램으로 근접성 발견 과정(proximity discovery procedure)이 그려지는 경우의 본 발명에 관한 예시적인 실시예를 보여주고 있다. 여러 개의 타겟 디바이스(2)가 존재하는 것으로 이해될 수 있다. 화살표는 데이터 흐름들을 나타낸다. 검은색 도트는 디바이스에서 수행되는 액션을 나타낸다. 중괄호 안의 참조 번호는 데이터 요소들을 나타낸다. 대시 라인들은 선택적인 단계를 나타낸다.

[0052] 도 1에서 식별자(12)를 포함하는 제1 데이터(11)는 소스 디바이스(1)에서 수신된다(101). 제1 데이터(11)는 외부 서버 또는 소스 디바이스(1) 자체로부터 기원할 수 있다. 후자의 경우에 소스 디바이스(1)는 식별자(12)를 생성한다. 식별자(12)의 제1 표현(21)을 포함하는 제2 데이터(20)는 타겟 디바이스(2)에서 수신된다(102). 제2 데이터(20)는 외부 서버 또는 소스 디바이스(1)로부터 기원할 수 있다. 다음으로, 소스 디바이스(1)는 식별자(12)의 제2 표현(31)을 포함하는 시그널(30)을 브로드캐스트 하는데(103), 이것은 타겟 디바이스(2)에서 수신된다. 타겟 디바이스(2)는 식별자(12)의 제1 표현(21)을 식별자(12)의 제2 표현(31)과 비교한다(105). 그리하여 얻어진 비교 결과는 식별자의 제1 표현 및 제2 표현에서 식별자가 매치될 수 있는지 여부를 나타낸다. 만약 이것이 그러한 경우라면 근접성 발견이 성공적으로 귀결될 수 있는데, 이는 선택적으로 인증 메시지(40)에서 소스 디바이스(1)에게 보고될 수 있다(106).

[0053] 도 2는 티켓에 기초하고 네트워크가 조력하는 실시예를 나타내는데, 이 실시예는 티켓의 이용을 탐지함으로써 근접성 발견의 네트워크 오퍼레이터에 의한 청구(charging)를 가능하게 한다.

[0054] 근접성 발견 전에, 소스 디바이스(1)는 네트워크 내에 있거나 서드 파티에 속하는 서버(3)에게 소스 디바이스(1)가 하나 이상의 타겟 디바이스(2)를 발견하겠다는 것을 통지한다. 예를 들어, 디바이스들은 네트워크 또는 서드 파티(third party)에 가입하고 위치가 추적되기 때문에, 또는 디바이스들이 네트워크 또는 서드 파티(third party)에 알렸기 때문에, 네트워크 또는 서드 파티는 이러한 언급된 타겟 디바이스들(2) 중 어느 것이 발견될 수 있거나 발견할 수 있는지 알 수 있어서, 이들을 피어들(peers)로서 리스트(list)한다. 예를 들어, 디바이스들은 네트워크 또는 서드 파티에 가입하고, 위치가 추적되거나 또는 디바이스들이 네트워크 또는 서드 파티에 알렸기 때문이다.

[0055] 서버(3)는 소스 디바이스(1)에 티켓 데이터(10) 형태로 티켓을 공급하는데(101), 티켓 데이터에서 소스 디바이스(1)는 피어들(2) 서로 간에 도달하기 위하여 브로드캐스트하는 식별자(12)를 제공 받는다. 네트워크(3)는 또한, 소스 디바이스(1)의 피어들(2)에게 이들이 귀기울어야 하는 식별자(21)에 대해 알려 준다. 이 식별자(21)는 식별자(12) 또는 식별자(12)의 제1 표현형(21)과 동일할 수 있다.

[0056] 네트워크는 선택적으로 티켓(10)에서 보안 연계(14), 예를 들어 소스 디바이스(1)가 자신의 피어들(2) 중의 하나에 대한 연결을 안전하게 셋업하기 위해 이용할 수 있는 암호화 키를 포함할 수 있다. 비슷하게, 네트워크(3)는 이미 보안 연계(140)를 타겟 디바이스(2)에 전송할 수 있다. 그러나 청구(charging) 관점에서, 타겟 디바이스(2)가 이를 요청하면 전체 티켓을 전송하는 것이 바람직할 수 있다. 그 이유는, 이러한 경우 네트워크는 성공적인 발견을 확신할 수 있는데, 이는 네트워크가 청구(charging)를 허용함을 뜻한다. 선택적으로, 네트워크는, 네트워크(3)가 두 피어들(1, 2)이 가까이 있음을 감지한 때에, 키(14)를 전송할 수 있다. 이러한 경우 네트워크(3)는 근접성 감지 또는 연결 셋업과 관련될 수 있다. 이것은 키 신선도(key freshness)를 위해서 유익하다. 더욱이 네트워크(3)는, 동료인 모든 디바이스를 위한 키(key)에 대해 레지스트리(registry)를 유지할 필요가 없다.

[0057] 네트워크(3)는 근접성 감지 시점에 식별자(12) 또는/및 식별자(12)의 유도형(21)을 전송할 수 있다.

[0058] 피어들(2) 각각을 위해 소스 디바이스(1)는 이제 다음과 같은 정보를 포함하는 티켓(10)을 가지고 있다: 티켓 식별자(22); 선택적으로 선택적인 챌린지 응답 시스템에서 사용될 공통 시크리트(common secret) 또는 랜덤; 제1 디바이스(1)가 타겟 디바이스(2)에 도달하기 위해 사용할 수 있는 T-BID와 같은 식별자(12, 21); 선택적으로 타겟 디바이스(2)가 제1 디바이스(1)에 닿기 위해 응답에서 사용할 수 있는 T-BID와 같은 추가적인 식별자(13). 추가적인 식별자(13)는 또한 본 발명의 실시예에서 제4 데이터로 알려져 있다.

[0059] 선택적으로(optionally), 다른 키들이 파생될 수 있는 마스터 암호화 키 또는 키들의 집합(암호 키들 및 통합 보호 키들)은 티켓 데이터(10)에 포함될 수 있다.

[0060] 피어들(1, 2) 각각은 이제 메모리에 다음과 같은 정보를 현재 가지고 있다: 소스 디바이스(1)를 청취하고 연관되기 위한 T-BID(12, 21)(또는 그들의 표현); 선택적으로(optionally) 동일한 공통 시크리트(common secret) 또는 랜덤; 티켓 식별자(22); 옵션으로 다른 키들이 파생되는 마스터 암호 키(master cryptographic key) 또는 키들의 집합(암호(cypher) 키들 및 통합 보호(integrity protection) 키들)

[0061] 약간의 시간이 흐른 시점에, 네트워크 또는 서드 파티/최상의 공급자는 소스 디바이스 및 타겟 디바이스가 인근에 있음을 감지할 수 있다(그리고 여전히 서로간에 발견될 수 있다, 즉 어떠한 사용자들도 그들의 세팅을 변경하지 않는다). 네트워크 또는 서드 파티는 제1 디바이스에 그들이 가까이 있음을 알린다.

[0062] 여기서 티켓에 기초하는 시스템의 장점이 명확해 진다: 근접성 발견을 하는 것이 네트워크일 필요는 없는데, 이는 일단 네트워크가 키들(1)을 포함하는 티켓(10)을 발행하기만 하면, 네트워크는 타겟 디바이스(2)에 키들(14)을 공급할 수 있고 소스 디바이스(1)에 빌링(bill)을 요구할 수 있다는 것을 의미한다.

[0063] 제1 디바이스는 전에 수신된 임시 브로드캐스트 식별자 또는 타겟 디바이스(2)에 의해 수신된(104) 그의 제2 표현(31)을 포함하는 시그널(30)을 브로드캐스트한다(103).

[0064] 선택적으로(optionally) 이러한 메커니즘은 챌린지 응답 시스템을 가지고 확장될 수 있다. 이러한 경우 식별자(31)의 브로드캐스트(103)는 (또한, 본 발명의 실시예에서 제1 챌린지 데이터(32)로 불리는) 챌린지(32) 와 함께 수행될 수 있는데, 타겟 디바이스(2)는 챌린지(32)에 올바른 해답(correct answer)을 제공할 수 있다.

[0065] 타겟 디바이스(2)는, 브로드캐스트를 수신한 후에, 인증 메시지(106)를 사용하여 메시지를 받았음을 타겟 디바이스(1)에 선택적으로 응답한다. 선택적으로(optionally), 상기 설명한 것처럼 타겟 디바이스(2)는, 브로드캐스트 메시지(103)를 받으면 (키들을 포함하는) 전체 티켓을 네트워크로부터 회수한다. 선택적으로(optionally), 타겟 디바이스(102)는 챌린지(32)에 대한 해답을 연산하는데(114), 선택적으로(optionally) 해답을 암호화하고 제1 디바이스(1)에 응답한다(106).

[0066] 챌린지(32)에 대한 해답(106)은 hash(challenge(32)||common secret) 형태 일 수 있다. 수신 후에 소스 디바이스(1)는 상기와 같은 연산을 수행할 수 있고 응답이 동일함을 확인할 수 있다(115).

[0067] 응답(reply)을 암호화하는 것의 장점은 응답이 해시 함수에 관한 무차별 공격(brute force) 또는 레인보우 공격(rainbow attack)에 대해 취약하지 않다는 점이다. 그럼에도 불구하고, 암호화(encryption) 없이도 솔루션은 여전히 안전하다.

[0068] 타겟 디바이스(2)는 또한 (본 발명의 실시예에서 제2 챌린지 데이터(43)로 불리는) 챌린지(43)를 그의 응답에 포함할 수 있다. 이는 타겟 디바이스(2)에 의해 생성되는 다른 랜덤(random)일 수 있다.

[0069] 소스 디바이스는 선택적으로(optionally) hash(challenge(43)||common secret)를 연산하고(116), 그리고 소스 디바이스(1)가 hash(challenge(43)||common secret)를 올바르게 연산했음을 결론적으로 확인할 수 있는, 타겟 디바이스(2)에 대한 유도된 제2 챌린지 데이터 값(33)을 가지고 응답한다(117). 현재 양측이 갖는 보안 연계에 기초하여, 안전하고(secured) 인증된(authenticated) 연결(202)이 선택적으로(optionally) 셋업될 수 있다.

[0070] 싱글 티켓(10)은 여러 번 사용될 수 있다. 그러나 브로드캐스트 T-BID의 추적을 피하기 위해서는 적은 회수로 사용을 제한하는 것이 바람직하다. 이것은 또한 성공적이지 못한, (예를 들어 피어들이 도달하지 못하는) T-BID의 브로드캐스트 후에 새로운 티켓(10)이 발행되어야 함을 의미한다.

[0071] 추적을 당하지 않고, 사용자가 같은 티켓을 재사용하길 원함을 상상할 수 있다. 여기에 도 4 및 도 6에 개시되는 솔루션이 있다. 그리고 아래에 기술되는 그룹 어드레싱(group addressing)을 위한 솔루션은 도 2에 추가적으로 사용될 수 있다.

[0072] 도 3 및 도4에 나타낸 네트워크 조력의 실시예에서, 식별자들이 피어들(1, 2)에게 미리 로드되고 네트워크는 소스 디바이스(1) 및 타겟 디바이스(2)가 피어들에 해당함을 통지받는다.

[0073] 도 2를 참조하면 근접성 발견 전에 소스 디바이스(1)는 네트워크(3)에 하나 이상의 타겟 디바이스(2)를 발견하길 원한다는 것을 통지한다. 네트워크(3)는 언급된 타겟 디바이스(2) 중에 어느 것이 발견될 수 있거나 발견할 수 있는지 인지하고, 피어들로서 이들을 리스트(list)한다. 네트워크는 따라서 소스 디바이스(1) 및 타겟 디바이스(2)가 가까이 있다는 것을 감지할 수 있고 그들에게 알릴 수 있음을 감지할 수 있다.

[0074] 근접성 발견에 선행하는 이러한 단계는 블록(203)으로 나타낼 수 있다.

[0075] 임의의 일정 구간에(예를 들어 야간 또는 다른 시간 구간 동안), 피어들(1, 2)은 디바이스(1, 2) 각각을 위한 근접성 발견에 이용될 수 있는 T-BID의 집합(set)(12, 21)(또는 다른 식별자 12, 21)를 부여 받는다(101, 102). 여기에 식별자(12)들은 소스 디바이스(1)가 있는 네트워크로부터 제1 데이터(11)에서 수신되고, 본 예에서 식별자(12)와 동일할 수 있는 식별자(21)는 타겟 디바이스(들)(2)가 있는 네트워크로부터 제2 데이터에서 수신된다(102). 본 예에서 T-BID들(12, 21)은 피어 특정 T-BID들이다. 또한, 피어들(1, 2)은 다른 디바이스가 사

용할 T-BID(12, 21)를 제공받는다. 선택적으로(optionally) 피어들(1, 2)은 또한 디바이스들의 그룹의 발견 가능성을 위해 사용될 수 있는 제너럴(General) T-BID(12, 21)(Gen T-BID)를 수신한다(101, 102). Gen T-BID(12, 21)는 또한 각각의 쌍을 이룬 디바이스들에 배포된다. 각각의 피어(1, 2)는 이제 다음 표와 같은 레지스트리를 가진다(본 예는 소스 디바이스(1)에 대해 유효하다):

표 1

[0076]

| | Broadcast | Receive | |
|---|---|---|---|
| | T-BID | Gen T-BID | T-BID |
| 제너럴(General) T-BID | a | | |
| 제1 타겟 디바이스를 위한 T-BID | b | f | j |
| 제2 타겟 디바이스를 위한 T-BID | c | g | k |
| 제3 타겟 디바이스를 위한 T-BID | d | h | m |
| 제4 타겟 디바이스를 위한 T-BID | e | i | n |

[0077] 표 1의 Broadcast 쪽에는, 소스 디바이스(1)가 임의의 특정의 타겟 디바이스(2)와 접촉을 원하는 경우 또는 소스디바이스(1)가 제너럴 T-BID(31)(즉, "a"를 사용하는 누군가를 위해 발견되어지길 원하는 경우에, 소스 디바이스(1)로부터 브로드캐스트되고 타겟 디바이스(2)에서 수신되는 T-BID들(31)(즉, "b", "c", "d" 및 "e")이 존재한다. 표의 Receive 쪽에는 피어 발견의 경우 소스 디바이스(1)가 귀기울어야할 브로드캐스트가 존재한다. 그래서, 소스 디바이스(1)가 제1 타겟 디바이스(2)에 도달하려면, 소스 디바이스(1)는 "b"를 브로드캐스트해야 한다(103). Receive 쪽에서, 소스 디바이스(1)는 마지막 두개 컬럼에 대해 귀를 기울여야 한다. 마지막 컬럼("j", "k", "m", "n")의 값들 중의 임의의 것이 브로드캐스드되면, 피어들(2) 중의 하나는 근접해 있고 소스 디바이스(1)에 연결하려고 시도중이라는 결론을 얻을 수 있다. 중간 컬럼의 값("f", "g", "h", "i") 중의 임의의 값이 브로드캐스트되면 소스 디바이스(1)는 피어들(2) 중의 하나가 근접해 있음을 그리고 피어들은 단지 그들이 존재하고 있다는 것을 알리기 위해 그들의 제너럴 T-BID를 브로드캐스트함을 안다.

[0078] 레지스트리(registry)를 저장하는 방식이 임의적이다는 것이 이해될 수 있다. 표 1의 형식은 단지 예시에 불과하고, 값을 저장하는 임의의 다른 형태가 사용될 수 있다. 식별자(12, 21)는 알파벳 글자로 표현된다. 식별자는 임의의 2진수값, 10진수값, 16진수값, 워드값, 디워드값(dword value), 스트링값 및 기타의 길이를 가질 수 있다는 것이 이해될 수 있다.

[0079] 도 3의 실시예는 근처에 누가 있는지에 관한 사전 지식이 없이 Gen T-BID(31) 또는 많은 수의 특정 T-BID들(31)을 단순히 브로드캐스트하는 것을 허용한다. 피어(1, 2)가 현재 네트워크 커버리지 또는 제어 범위에 없는 경우, 예를 들어 (가능하다면 임시로) 애드혹 모드에서 동작하는 때에도 이것이 또한 적용될 것이다.

[0080] 디투디 연결(20)의 시점에서 보안 연계가 알려져 있지 않고 이러한 보안 연계(204)가 요구된다면, 네트워크(3)는 바람직하게는 보안 회선(secure line)을 통해 디바이스(1, 2)에 암호화 키들(14)을 선택적으로 제공할 수 있다. 바람직하게도 네트워크는 발견이 성공적임을 통보 받고(205), 이는 바람직하게 청구(charging)를 가능하게 한다.

[0081] 제너럴 BID(12, 21) 또는 피어 특정 T-BID(12, 21)를 변경하는 메커니즘을 갖는 것도 바람직할 수 있다. 예를 들어, T-BID(31)가 브로드캐스트 되면(103)(그리고 디투디 세션(206)이 성공적으로 셋업되었는지에 무관하게) 악성 사용자가 T-BID를 저장하고 나중에도 계속 찾는 것이 가능할 수도 있다. 특정 시점에서 동일한 T-BID가 다시 브로드캐스트되면, 악성 사용자는 특정 디바이스가 인근에 있는 것으로 결정할 수 있다. 따라서 소스 디바이스(1)가 네트워크(3)에 그들의 T-BID(12)를 업데이트 할 것을 요청(101a)하는 것이 선택적으로 가능할 수 있다. 네트워크(3)는 그리고 나서 새로운 T-BID(12)를 할당하고 피어들(1, 2)에게 새로운 T-BID(12)를 알려준다(101b, 102b).

[0082] 네트워크는 브로드캐스트에서 T-BID(12, 21)가 사용되는 모든 때를 위해 T-BID들(12, 21)을 재할당하고 모든 피어들(1, 2)에게 이들을 재분배(101b, 102a)하는 것이 가능하다.

[0083] BID 및 피어 특정 T-BID 다음으로, 네트워크는 친구들/디바이스들의 특정 그룹에만 발견되기 위해서 선택적으로

특정의 T-BID를 공급할 수 있다. 따라서 가까운 사용자 그룹 특정 T-BID(CUG T-BID)는 더 큰 그룹으로 정의될 수 있다. 이러한 CUG T-BID 식별자들은 또한 바람직하게 그룹 내의 모두에게 공급된다. 이는 정적인 그룹들, 예를 들어 동료들(colleagues) 또는 경찰 및 소방대 같은 사회 안전 서비스를 위해서는 바람직하다.

[0084] 피어 특정 T-BID는 디투디 연결 중에 네트워크에 연관되거나 네트워크에 통지없이 선택적으로 리플레시(refresh) 될 수 있다. 이는 증가된 정도의 프라이버시(네트워크는 식별자(12, 21) 조차도 모른다)를 제공하고 네트워크가 T-BID들을 생성하는 임무를 덜어준다.

[0085] 도 4의 실시예에서 식별자들(12)은 미리 로드되고 정적이다. 그러나, 소스 디바이스(1)가, 예를 들어 식별자의 암호화 또는 해싱함으로써 식별자의 유도형을 연산(103a)하기 위해 사용하는, 그리고 타겟 디바이스(2)가 암호를 풀고 식별자를 확인(109a)하기 위해 사용하는 랜덤(51)을 소스 디바이스(1) 및 타겟 디바이스(2)에 공급하는 예를 들어 네트워크(3)에 의해 브로드캐스트 T-BID들(31)이 변경될 수 있다(브로드캐스팅이 발생하기 전에).

[0086] 도 4의 실시예는 빠르게 변하는 그룹들의 예에 있어서 특별히 바람직한데, 여기서에서 그룹 멤버들은 서로의 식별자를 갖지만, 모두 같은 랜덤을 갖는 것은 아니다.

[0087] 다음의 도 4를 참조하는 제1 예에서, 근접성 발견에 앞서 피어들(1, 2)은 $p_i$(소스 디바이스(1)에 관한 $p_1$, 제1 타겟 디바이스(2)에 관한 $p_2$, 제2 타겟 디바이스(2)에 관한 $p_3$, 기타) 라고 불리는 T-BID를 할당받는다(207).

[0088] 오퍼레이터(3)는 소스 디바이스(1)로부터 소스 디바이스가 제1, 제2, 제3 및 제4 타겟 디바이스(2)를 발견하기 원한다는 메시지를 받는다(101c). 오퍼레이터(3)는 제1, 제2 및 제4 타겟 디바이스(2)가 가까이 있음을 감지한다. 제5 및 제6 타겟 디바이스는 또한 가까이 있지만 소스 디바이스(1)의 리스트에 없을 수 있다. 제5 및 제6 타겟 디바이스는 따라서 발견되지 않는다.

[0089] 오퍼레이터(3)는 난수(random number) x를 취하는데, 이 난수의 길이는 $p_i^2$ 이고 제1 타겟 디바이스(2)를 위해 연산한다: $p_2$ 에 대해 $x_2=x \bmod p_2$이다; 그리고 제3 타겟 디바이스(2)에 대해서 동일하다(제2 및 제4 타겟 디바이스는, 본 예에서 가까이 있지 않아서 해당안됨). 선택적으로, 소스 디바이스(1)는 오퍼레이터(3)에 난수 x를 공급한다.

[0090] 오퍼레이터(3)는 x를 소스 디바이스(1)에 전송한다(102b). 오퍼레이터(3)는 $x_2$를 제1 타겟 디바이스(2)에 전송하고 $x_4$를 제3 타겟 디바이스(2)에 전송한다. 여기서 $x_2$ 및 $x_4$는 식별자(12)의 표현(21)이다.

[0091] 소스 디바이스(1)는 랜덤 x(31)를 브로드캐스트한다(103). 그리고 도달 범위의 모든 피어들(2)(바라건데 제1 타겟 디바이스(2) 및 제3 타겟 디바이스(2)를 포함)은 $x_i==x \bmod p_i$ 여부를 확인할 수 있다(109). 값 x(31)은, 그것이 타겟 디바이스(2)에서 신원(identity)을 확인하는데 사용될 수 있듯이, 이제 인식자의 제2 표현(representative)으로 기능한다,

[0092] 제1 및 제3 타겟 디바이스(2)는 메시지가 수신되었음을 응답할 수 있다. 그리고 가능하면 서버(3)에서 수신한 보안 연계를 이용하여 디바이스들은 디투디 통신 세션을 셋업할 수 있다.

[0093] 제5 및 제6 타겟 디바이스는 또한 랜덤 x(31)를 수신할 수 있다. 그러나 그들의 정보는 너무 제한적이므로(그들은 $x_i$ 값을 오퍼레이터(3)로부터 수신하지 않는다) 누가 호출하고 있는지 알아내지 못하거나 추적(tracking) 및 트레이싱(tracing)에 그것을 사용하지 못한다).

[0094] 소스 디바이스(1)가 차기 브로드캐스트(103)를 위해 변경된 버전의 r(31)을 재사용하는 것이 가능하다. 만약 제1 디바이스(1)가 타겟 디바이스(2)의 $p_i$ 값을 알고 있으면, 상기가 가능하다. 소스 디바이스가 알고 있으면, 소스 디바이스는 $x_i==x \bmod p_i$가 여전히 적용되는, 즉 $x'=x + k\ LCM(p_2, p_3, 등)$인 새로운 x를 얻기 위해 양쪽의 (복수의) 최소 공배수(least commn multiplier: LCM)를 이용할 수 있다. 여기서, 사용된 식별자의 LCM에 관한 너무 많은 정보를 누설하는 것을 방지하기 위해, k는 프라임(prime)으로 취해져서는 안 되고, 바람직하게는 복수의 프라임(primes)으로 취해져야 한다. 이러한 솔루션의 장점은 아무것도 변경되지 않는 타겟 디바이스들에 대해서 그들의 응답은 여전히 동일하다는 점이다.

[0095] 도 4를 참조하는 다음의 두 번째 예에서, 근접성 발견 전에 피어들(1, 2)은 $p_i$ 라고 불리는 T-BID를 할당받는다(소스 디바이스(1)에 대해서는 $p_1$, 제1 타겟 디바이스(2)에 대해서는 $p_2$, 제2 타겟 디바이스(2)에 대해서는 $p_3$,

등). 피어들(1, 2)은 서로의 신원(identity)에 관해 통지를 받는데, 예를 들어 소스 디바이스(1)는 제1 타겟 디바이스(2)의 T-BID를 알고, 제2 타겟 디바이스(2)는 소스 디바이스(1)의 T-BID를 안다.

[0096] 오퍼레이터(3)는 소스 디바이스로부터 소스 디바이스가 제1, 제2, 제3 및 제4 타겟 디바이스(2)를 발견하길 원한다는 메시지(101c)를 수신한다. 오퍼레이터(3)는 제1, 제2 및 제4 타겟 디바이스(2)가 가까이 있음을 감지한다. 제5 및 제 6 타겟 디바이스 또한 가까이 있지만, 소스 디바이스(1)의 리스트에 없을 수 있다. 제5 및 제6 타겟 디바이스는 따라서 발견되지 않을 것이다.

[0097] 오퍼레이터(3)는 난수 r을 취하고 $x=hash(T\text{-}BID_{source\ device1}||r)$, 그리고 다시 제2 및 제4 타겟 디바이스(2)를 위한 $x_i=x \bmod p_i$ 을 연산한다. 선택적으로, 소스 디바이스(1)는 오퍼레이터(3)에게 난수 r을 공급한다.

[0098] 오퍼레이터(3)는 난수 r을 소스 디바이스(1)에 전송한다(102b). 오퍼레이터(3)는 ($x_2$, r)을 제1 타겟 디바이스(2)에 전송하고, ($x_4$, r) 을 제3 타겟 디바이스(2)에 전송한다. 여기서 $x_2$ 및 $x_4$ 는 식별자(12)의 표현(21)이다.

[0099] 소스 디바이스(1)는 x(31)를 브로드캐스트하고(103), 지척에 있는(within reach) 모든 피어들(2)(바라건데 제1 타겟 디바이스(2) 및 제3 타겟 디바이스(2)를 포함)은 $x_i==x \bmod p_i$ 인지 여부를 확인할 수 있다(109). x(31) 값은, 타겟 디바이스(2)에서 신원(identity)을 확인하기 위해 사용될 수 있기 때문에, 현재 식별자의 제2 대표(representative)로 기능한다.

[0100] 제1 및 제3 타겟 디바이스(2)는 메시지가 수신되었다고 응답할 수 있고, 그리고 타겟 디바이스(2)에서 연산되는(108) $hash(p_i||r)$를 반환함으로써 그의 진위를 증명할 수 있다.

[0101] 이전의 실시예와 같이, 네트워크(3)는 추가적인 보안을 공급하고 성공적인 근접성 감지(successful proximity detection)를 청구(charging)하는 것을 가능케하는 암호화 키(14) 교환에 연관될 수 있다.

[0102] 도 4의 예는 또한 하나의 디바이스(1, 2)가 다른 하나(1, 2) 만을 발견하길 원하는 경우에 적용된다. 그러면 네트워크(3)는 이러한 특정의 피어들에게만 알린다.

[0103] 디바이이스들(1, 2) 자신들이 발견 가능성(discoverability)을 위해 무엇을 브로드캐스트할지를 정하는 경우인, 다음 실시예에 독립(standalone) 근접성 발견 과정(proximity discovery procedure)이 나타나 있다. 네트워크(3) 또는 서드 파티는 근접성(proximity)과 유사한 즉, 근접성 감지(proximity detection)를 디바이스(1, 2)에 통지하는 것에 여전히 관련될 수 있다. 독립 근접성 발견 과정(standalone proximity discovery)에서 과거 어느 시점에 연락(contact)이 있었거나, 식별자가 다른 수단, 예를 들어, 소스 디바이스(1) 및 타겟 디바이스(2)에서 주변장 칩(near field chip)을 이용하는 것(예를 들어, 디바이스들(1, 2)을 결합하거나 셰이킹 동작(shaking gesture)을 함으로써 유발되는), 상대 디바이스의 스크린의 바코드 또는 태그(tag)를 스캐닝, 식별자의 사용자 입력, 와이파이를 이용, 페이스북과 같은 서드 파티 어플리케이션을 이용 또는 임의의 다른 수단에 의해 교환되었다는 것을 전제로 할 수 있다.

[0104] 도 5는 오토-포겟 옵션(auto-forget option)을 갖는 인버스 해시 스택(inverse hash stack)에 기초하는 독립 근접성 발견 과정을 나타낸다. 도 5의 실시예는 다시 만날 확률이 높은 피어들(1, 2)이 많은 환경에 특히 유용하다. 피어들(1, 2)은 그들 자신이 무엇을 브로드캐스트할지(103) 그리고 어떻게 브로드캐스트 시그널에서의 식별자(21)의 제2 표현(31)을 암호화(encrypt) 또는 오퍼스케이트(obfuscate) 할 것인지를 결정한다. 추적(tracking) 및 트레이싱(tracing)을 어렵게 하도록 브로드캐스트인 T-BID 의 표현(31)은 시간에 따라 변할 수 있다.

[0105] 디투디 통신 세션 내에 있는 소스 디바이스(1) 및 타겟 디바이스(2)는 랜덤 T-BID(12) 및 솔트(salt)(51)를 생성할 수 있다. 디바이스(1, 2) 둘은 재귀적으로(recursively) 이전 해시 및 솔트(51)를 입력으로 취하는 해시 함수를 이용하는 n번째 해시(21)를 연산한다. 제1 해시는 그리고 나서 $hash_1=hash(T\text{-}BID, salt)$와 같이 연산되고 모든 후속의 해시들은 hash(previous_hash, salt)와 같이 연산된다. n번째 해시(21)를 연산하기 위해, 예를 들어 다음의 코드가 예를 들어 사용될 수 있다:

[0106] $hash_1=hash(T\text{-}BID, salt)$;

[0107] i=2;while i<=n do {

[0108] $hash_i=hash(hash_{i-1}, salt)$;

[0109] }

[0110] 여기서, T-BID(12)는 식별자(12)이다. T-BID의 n번째 해시는 식별자(12)의 제1 표현(21)이다. 그리고 솔트(salt)는 식별자(12)의 제3 표현이다.

[0111] 디바이스(1, 2)는 그들의 n번째 해시 및 솔트를 단계 102 및 107에서 교환한다.

[0112] 이 단계에서 소스 디바이스(1) 및 타겟 디바이스(2)는 네트워크(3) 또는 임의의 다른 서드 파티와의 연락 없이 다음 단계에서 서로 간에 연락할 수 있는 충분한 정보를 가진다.

[0113] 다음으로 그들은 서로 가까이 있는데, 이는 블록(209)에 의해 나타나는데, 소스 디바이스(1)는 T-BID의 제2 표현(31)으로 T-BID의 n-1번째 해시(31)를 브로드캐스트할 수 있다. 타겟 디바이스(2)는 그러면 hash($hash_{n-i}$, salt)=previous hash을 연산할 수 있다(108). 해시 함수를 알고 있는 감청자라도 솔트(51)를 알지는 못할 것이고 따라서 누가 호출되고 있는지 알아낼 수 없다.

[0114] 선택적으로 인근의 디바이스들(1, 2)은 근접성 발견 과정(proximity discovery procedure) 전의 근접성 감지 과정(proximity detection procedure)에서 근접성(proximity)에 대해 네트워크(3)로부터 통지받을 수 있다. 이러한 방법으로, 브로드캐스트 시그널 및 관련된 배터리 소모에 관한 꾸준한 모니터링을 할 필요가 없게 될 수 있다.

[0115] 양 디바이스들(1, 2)은 많은 해시를 가지고 있어서, 그들은 예를 들어 매일 또는 그들이 근접하게 되는 매회마다 다른 해시를 사용할 것을 결정할 수 있다. 그래서 만약 그들이 T-BID의 제2 표현(31)을 해시로 브로드캐스트하면(103), 그들은 브로드캐스트 시그널(30)에 어떤 해시를 그들이 브로드캐스트 했는지를 알려주는 계수 값(counter value) k를 포함할 수 있다. 계수 값 k는 예를 들어 (n-k)번째 해시(n 마이너스 k 번째 해시)가 식별자의 제2 표현으로 브로드캐스트 시그널(30)에 포함되어 있음을 나타낼 수 있다.

[0116] 선택적으로, k는 예를 들어 마지막 디투디 통신 세션으로부터 지나간 날짜 및 시간에 기초하여 타이머에 의해 주어진다. 이는 적시에 해시 스택(hash stack)을 덜어주고(deplete) 결국 두 디바이스(1, 2)의 피어니스(peerness)를 깨는 종료 방법(expiry method)을 소개하기 위해 이용될 수 있다. 예를 들어, 디바이스(1, 2)가 그들의 초기 보안 연계(security association)가 만료한 후 다시 만나는 경우, 그들은 초기 근접성 발견 과정(proximity discovery procedure)을 다시 거쳐야 할 것이다.

[0117] 타겟 디바이스(2)가 모든 인커밍(incoming) 해시된 T-BID(31)에 대해 해시를 계산(108)해야 한다면, 도 5의 예시적인 실시예는 연산적으로 대규모(extensive)일 수 있다. 언제 브로드캐스트를 경청할지를 알려주는 네트워크(3)에 의존함으로써 이는 경감될 수 있다. 선택적으로, 이는 브로드캐스트 해시의 수를 결부시킴으로써(concatenating)(그래서 브로드캐스트에 n-k를 추가) 경감될 수도 있다. 이러한 방법으로, 타겟 디바이스(2)는 그가 그의 피어들 중의 하나로부터 (n-k)번째 해시를 기대하는지 여부를 체크할 수 있고 그리고 인커밍 브로드캐스트를 위한 (재귀적) 해시를 연산(108) 하는 것을 결정할 수 있다.

[0118] 도 5의 근접성 발견 과정은 유리하게도 네트워크 커버리지가 존재하지 않는 때에도 적용될 수 있다(네트워크는 반드시 관련될 필요가 없다). 더욱이, 이는 청구(charging) 또는 신청(subscription) 목적으로 사용될 수 있는, 시간이 경과한 후에 피어들을 망각하기 위한 메커니즘을 가지고 그리고 모든 인커밍 브로드캐스트(103)에 대한 재귀적인 해시 연산으로 인한 연산 부하(computational load)를 감소시키는 메커니즘을 갖는 것을 가능하게 한다.

[0119] 도 5의 변형된 실시예로서 디바이스(1, 2) 자신이 식별자(12)를 암호화하기 위해 어떠한 랜덤(random)을 이용할지를 결정하는 것이 가능하다. 식별자들이 변경된 경우, 예를 들어 이전의 근접성 감지 과정 또는 네트워크에 의해 제공되는 경우, 네트워크 또는 서드 파티는 디투디 통신 세션 구축에 연관될 필요가 없다. 이러한 선택적인 과정은 다음과 같이 동작할 수 있다.

[0120] 먼저, 소스 디바이스(1)는 랜덤(51)을 연산하고, hash(R||T-BID)를 연산하는데, R은 랜덤(51)이고 T-BIT는 식별자(12)다. T-BIT는 예를 들어, 누가 호출하는지 또는 누가 호출되는지를 특정할 수 있는 피어 특정 T-BID일 수 있다(예를 들어 도 2 예의 표 1에서와 같이 "b" 또는 "j"). 만약 하나가 특정되면 T-BID는 예를 들어 보안 연계 T-BIT(SA-T-BID)일 수 있다.

[0121] 다음으로, 소스 디바이스(1)는 R||hash(R||T-BID)를 브로드캐스트한다. 브로드캐스트를 수신하는 타겟 디바이스(들)(2)은 그들의 메모리(가능하면 자신의 것을 포함)에서 T-BID들을 위해 함수 hash(R||T-BID)을 연산하고 그

들이 매치하는지 여부를 결정한다. 만약 매치가 발견되면, 도출될 수 있는 결론은 어떤 T-BID가 브로드캐스트 되는지에 달려있다. 만약 소스 디바이스(1)가 자신의 신원(identity)을 표현하는 T-BID를 브로드캐스트 하면, 소스 디바이스(1)가 도달 범위 내에 있다는 결론이 타겟 디바이스(2)에 의해 도출될 수 있다. 만약 소스 디바이스(1)가 타겟 디바이스(2)의 신원(identity)을 표현하는 T-BID를 브로드캐스트 하면, 호출된 파티에 해당하는 타겟 디바이스(2)만이 그 자신의 신원(identity)과의 매치를 찾을 것이다. 악성 사용자들은 여전히 타겟 디바이스(2)가 호출되고 있음을 알 수 있다, 그러나 누가 호출하고 있는지를 알아내지 못한다. 만약 소스 디바이스(1)가 공통 보안 연계(common security association)(이는 소스 디바이스(1)의 T-BID들 및/또는 타겟 디바이스(들)(2) 및/또는 T-SA-BID를 포함할 수 있다)로부터 T-BID들을 브로드캐스트하면, 타겟 디바이스(2)는 그가 호출되고 있다고 결정할 수 있다.

[0122] 도 5의 실시예의 장점은 소스 디바이스(1) 자체가 자신을 알리는 방법을 결정할 수 있다는 점이고, 네트워크로 하여금 누가 브로드캐스트 하는지 발견하도록 하는 것을 허용하면서, 높은 정도의 프라이버시를 제공한다는 점이다. 후자는 예를 들어 청구 이유 또는 합법적인 도청(Legal Interception)에 대해 유리하다. 추가적인 장점은 네트워크가 관련될 필요가 없고 따라서 네트워크 커버리지 없이도 과정이 또한 잘 이루어진다.

[0123] 도 6의 실시예는 하이브리드 솔루션을 나타내는데, 이 경우 네트워크 또는 서드 파티는 해시 함수에 사용되는 솔트(salt)를 공급한다.

[0124] 도 6의 실시예는 도 4 및 도 5의 실시예의 변형이고, 특히 다시 만날 확률이 높은 많은 피어들(1, 2)의 경우에 유리하다. 피어들(1, 2)은 서로 간의 정보, 예를 들어 식별자(12)를 가지고 있는데, 그들은 이를 다음 세션에서 서로를 식별 하거나 다음(next)의 T-BID를 알기 위해 사용할 수 있다.

[0125] 도 6의 실시예에서 디투디 세션에서의 두 개의 디바이스(1, 2) 모두는 랜덤 T-BID를 생성한다. 그들은 선택된 T-BID(12)를 서로에게 알려준다(101). 미리 정해진 시점에, 예를 들어 매일 밤 또는 미리 정해진 시간 인터벌로, 네트워크(3)(또는 다른 서드 파티)는 솔트(51)를 디바이스(1, 2)에 배포한다(107). 선택적으로 또는 대안적으로, 네트워크(3)(또는 서드 파티)는, 두 개의 디바이스(1, 2)가 가까이 있고 서로 간에 채팅을 하려고 하는 경우를 탐지하면 솔트를 공급할 수 있다(107). 타겟 디바이스(들)(2)는, 즉, 알리는 단계(101)에서 수신된 것처럼, 모든 T-BID들에 대한 hash(T-BID, salt)를 연산함으로써, 디바이스(1, 2)의 알려진 T-BID들(12)의 제1 표현(21)을 획득한다(102). 소스 디바이스는 소스 디바이스(1)에 의해 사용되는 T-BID(31)의 제2 표현(31)을 연산함으로써 자신의 T-BID(12)을 위해 동일한 연산(210)을 수행한다. T-BID의 제2 표현(31)은 브로드캐스트(103)이고 타겟 디바이스(들)(2)에서 수신된다. 타겟 디바이스(들)(2)는 T-BID들의 연산된 제1 표현(21)과 T-BID(12)의 수신된 제2 표현을 비교하고(105, 108) 매치(match)가 발견되었는지를 확인한다(109).

[0126] 도 6의 실시예의 장점은 이것이, 빠르게 파라미터를 변경하는 것, 예를 들어 랜덤 수신, 그리고 랜덤이 수신될 때마다 해시를 연산하는 것에 의존하는 실시예와 비교하여 연산적으로 덜 집중적이라는 것이다. 이는 식별자(12)의 브로드캐스터(1)를 위해 여전히 충분한 프라이버시를 제공한다.

[0127] 도 1 내지 도 6은 본 발명의 서로 다른 실시예를 보여 준다. 본 발명은 상기 보인 실시예에 한정되지 않는다. 하나의 실시예에 보인 단계들은 예를 들어 비록 나타내진 않았지만 다른 실시예에서 사용될 수 있다. 이것의 예들은 식별자의 해싱, 티켓의 사용, 추가적인 챌린지 응답 확인, 그리고 암호화 키(14)를 사용하는 암호화 데이터이다. 승인 메시지를 전송하는 단계(106) 그리고 디투디 통신 세션을 수립하는 단계(206)와 같이, 나타나 있는 다른 단계들은 선택적일 수 있다.

[0128] 몇몇 예에서 식별자(12)의 유도형(21, 31)을 계산하기 위해 해시 함수가 사용되었다. 대신에 유도형(21, 31)을 만들기 위해 랜덤(51)을 사용하는 임의의 다른 수학적 함수가 사용될 수 있다는 것이 이해될 것이다. 랜덤(51)은 난수(random number) 또는 서버(3) 또는 소스 디바이스(1)에서 생성되는 그의 유도형(derivation), 서버(3) 또는 소스 디바이스(1)에서 생성되는 솔트(salt)일 수 있다.

[0129] 식별자(12)는 그룹 어드레싱에 사용될 수 있다. 예를 들어 T-BID는 디바이스들(1, 2)의 특정 그룹이 호출되고 있음을 나타내는데 사용될 수 있다. 그룹에 속하는 디바이스들(1, 2)은 그룹을 표현하는 식별자(12)를 수신한다. 다른 디바이스를 발견하기 위해, 예를 들어 현재 날짜 또는/및 시간 또는 랜덤(51) 교환 없이 디바이스(1, 2)에 의해 보편적으로 알려질 수 있는 다른 랜덤(51)에 의존하여, 디바이스들은 식별자(12)의 유도형을 연산한다. 식별자의 제2 유도형(31)은 따라서 x=hash(date||GroupIdentifier)와 같이 연산될 수 있다. 소스 디바이스(1)는 x를 브로드캐스트하고(103), 그룹의 타겟 디바이스(들)(2)는 x를 수신하고 동일한 연산 hash(date||GroupIdentifier)를 수행함으로써 식별자의 제1 유도형(21)을 연산할 수 있다. 제1 유도형(21)이

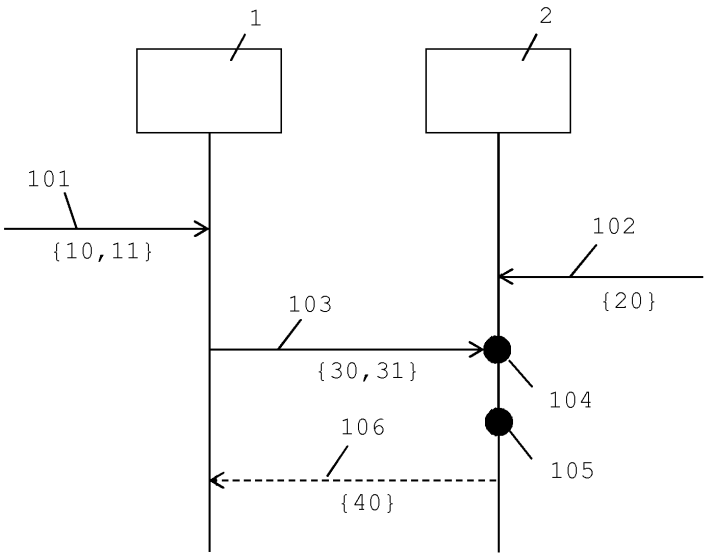
제3 유도형(31)과 매치하면 근접성 발견은 성공적이다.

[0130] 일반적으로, 랜덤(51)이 시간에 따라 변하는 파라미터이면, 랜덤(51)이 현재 날짜인 경우에 예를 들어 하루에 한 번씩, 느리게 변하도록 랜덤(51)이 선택될 수 있다. 이러한 경우에 hash(date||GroupIdentifier)에 관한 연산 또는 hash(date||identifier)에 관한 연산이 하루에 오직 한 번 수행될 수 있다. 연산이 수행되면 비교 절차(109) 만이 이루어져야 한다. 도 5 및 도 6의 예에서 이것은 바람직하게 다른 디바이스의 해시가 오직 하루에 한 번 연산되기 때문에 최소의 연산을 수행해야 하는 결과로 귀결된다.

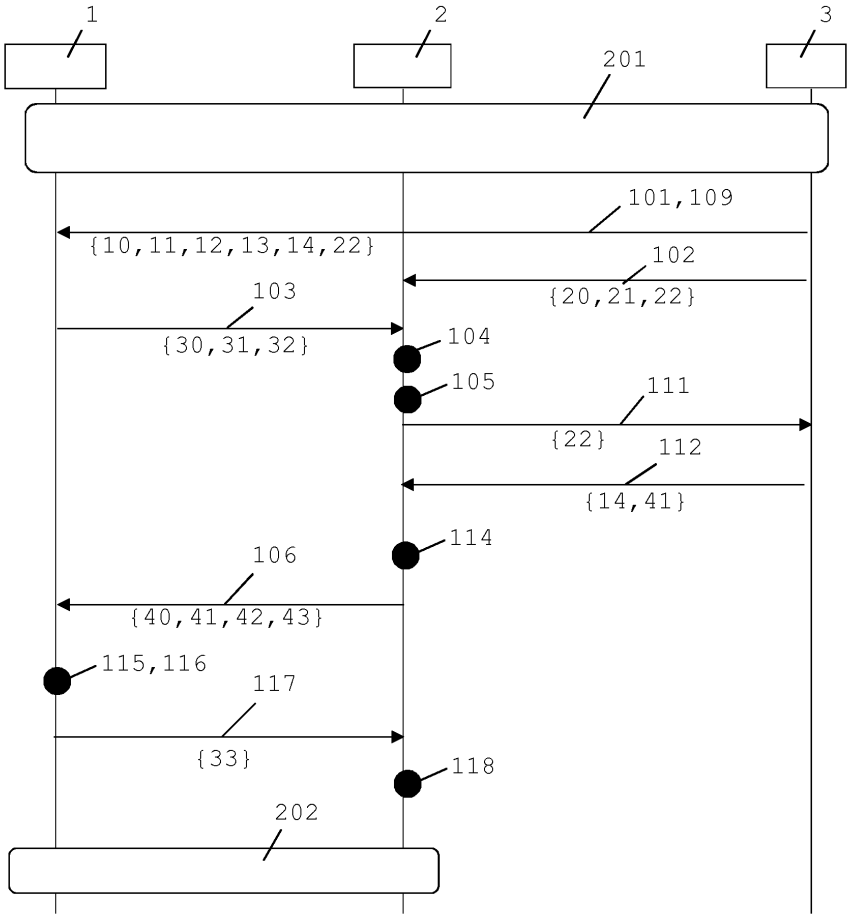
[0131] 본 발명의 하나의 실시에는 컴퓨터 시스템에서 사용되는 프로그램 생산품으로 구현될 수 있다. 프로그램 생산품의 프로그램은 실시예(여기에 설명된 방법을 포함)의 기능을 정의한다. 그리고 프로그램 생산품의 프로그램은 다양한 일시적이지 않은 컴퓨터가 읽을 수 있는 저장 매체에 포함될 수 있다. 예시적인 컴퓨터가 읽을 수 있는 저장 매체는, 다음을 포함하되 이에 한정되지 않는다: (ⅰ) 정보가 영구적으로 저장되는 쓸 수 없는 저장 매체(예를 들어, CD-ROM 드라이브에 읽힐 수 있는 CD-ROM 디스크와 같은 컴퓨터 내의 읽을 수만 있는 메모리 디바이스들, ROM 칩 또는 임의의 타입의 고체상태의 비휘발성 반도체 메모리) 그리고 (ii) 수정 가능한 정보가 저장되는 쓰기 가능한 저장 매체(예를 들어, 플래시 메모리, 디스켓 드라이브 내의 플로피 디스크 또는 하드-디스크 드라이브 또는 임의의 타입의 고체상태 랜덤-액세스 반도체 메모리).

## 도면

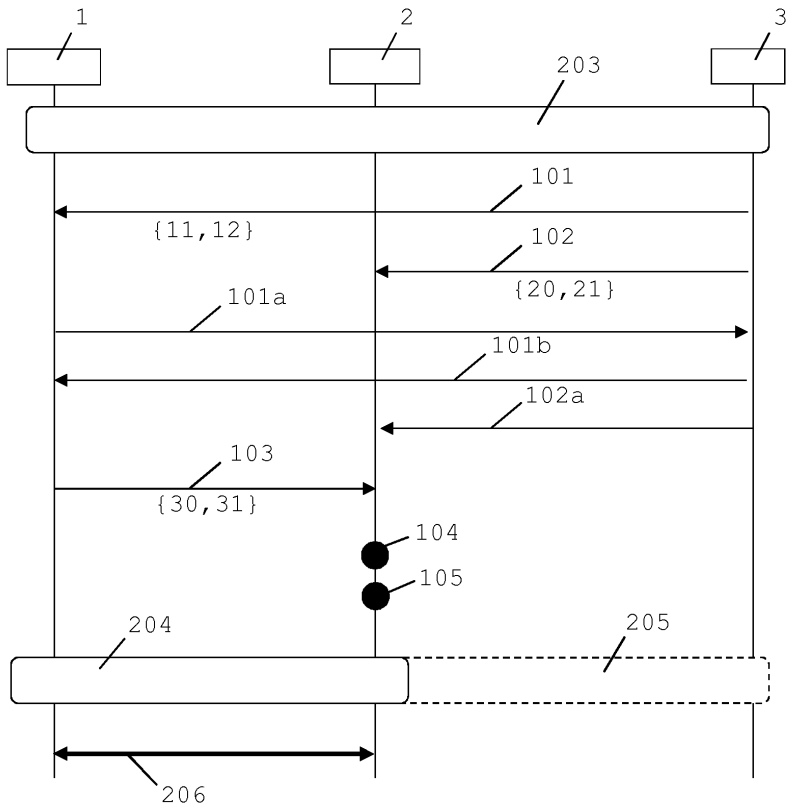
### 도면1



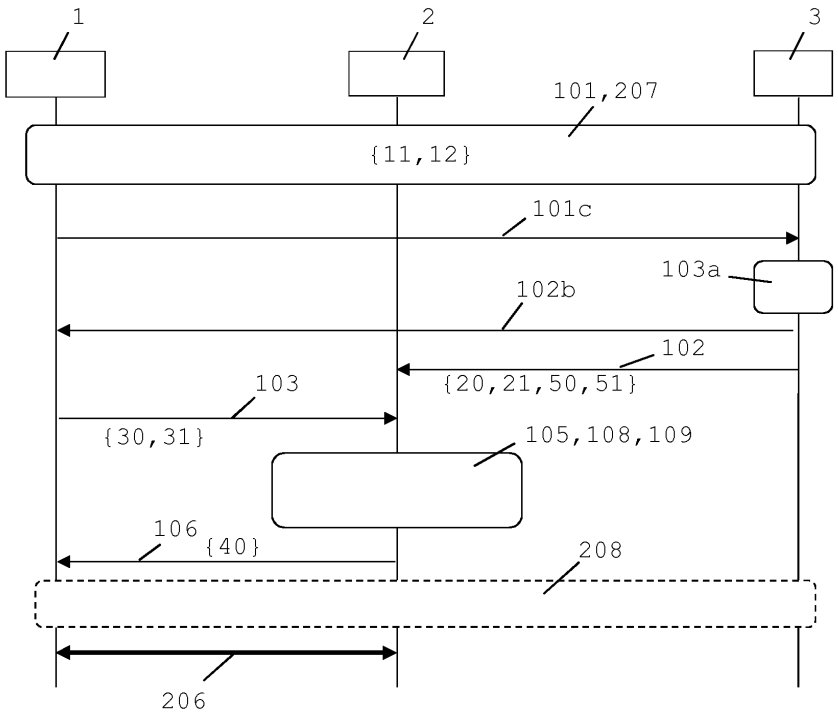
도면2


1
2
3
201
101,109
{10,11,12,13,14,22}
102
{20,21,22}
103
{30,31,32}
104
105
111
{22}
112
{14,41}
114
106
{40,41,42,43}
115,116
117
{33}
118
202

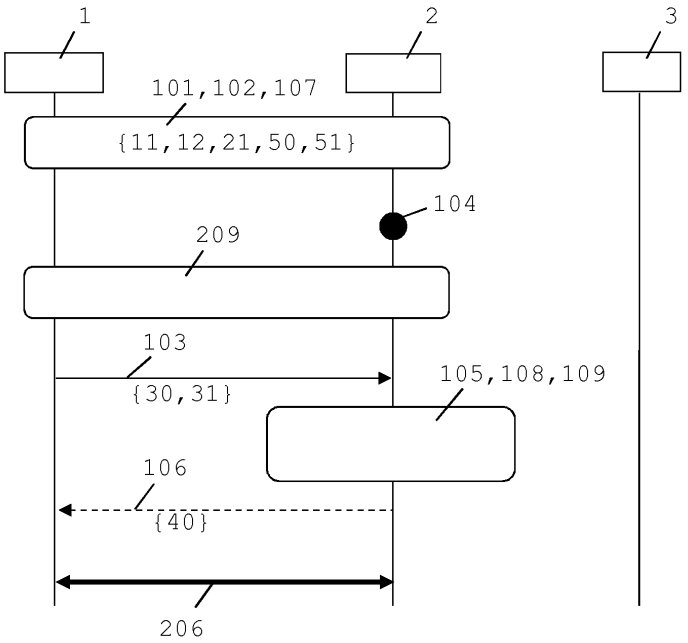
도면3


1
2
3
203
101
{11,12}
102
{20,21}
101a
101b
102a
103
{30,31}
104
105
204
205
206

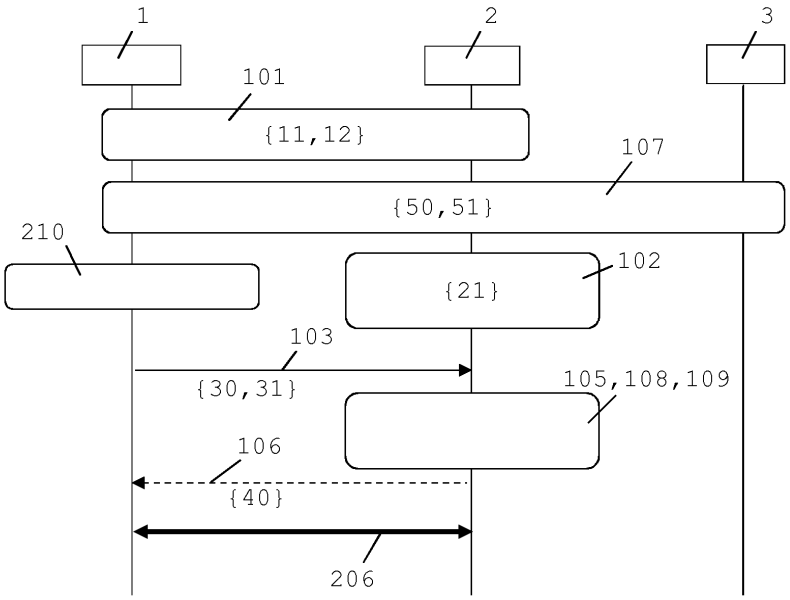
도면4


1
2
3
101,207
{11,12}
101c
103a
102b
102
{20,21,50,51}
103
{30,31}
105,108,109
106
{40}
208
206

도면5


1
2
3
101,102,107
{11,12,21,50,51}
104
209
103
{30,31}
105,108,109
106
{40}
206

도면6


1
2
3
101
{11,12}
107
{50,51}
210
102
{21}
103
{30,31}
105,108,109
106
{40}
206