(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2022년08월12일
(11) 등록번호 10-2432545
(24) 등록일자 2022년08월10일

(51) 국제특허분류(Int. Cl.)
H04W 12/63 (2021.01) *H04W 12/069* (2021.01)
H04W 12/122 (2021.01) *H04W 12/69* (2021.01)
H04W 4/02 (2018.01) *H04W 4/06* (2018.01)
(52) CPC특허분류
H04W 12/63 (2022.08)
H04W 12/069 (2021.01)
(21) 출원번호 10-2021-0103369
(22) 출원일자 2021년08월05일
심사청구일자 2021년08월05일
(56) 선행기술조사문헌
KR1020170056098 A*
KR102088716 B1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
세종대학교산학협력단
서울특별시 광진구 능동로 209 (군자동, 세종대학교)
(72) 발명자
신지선
서울특별시 광진구 능동로 209 세종대학교 대양AI센터 708호
이신철
서울특별시 광진구 뚝섬로49길 68, 203호(자양동, 연준빌)
(74) 대리인
두호특허법인

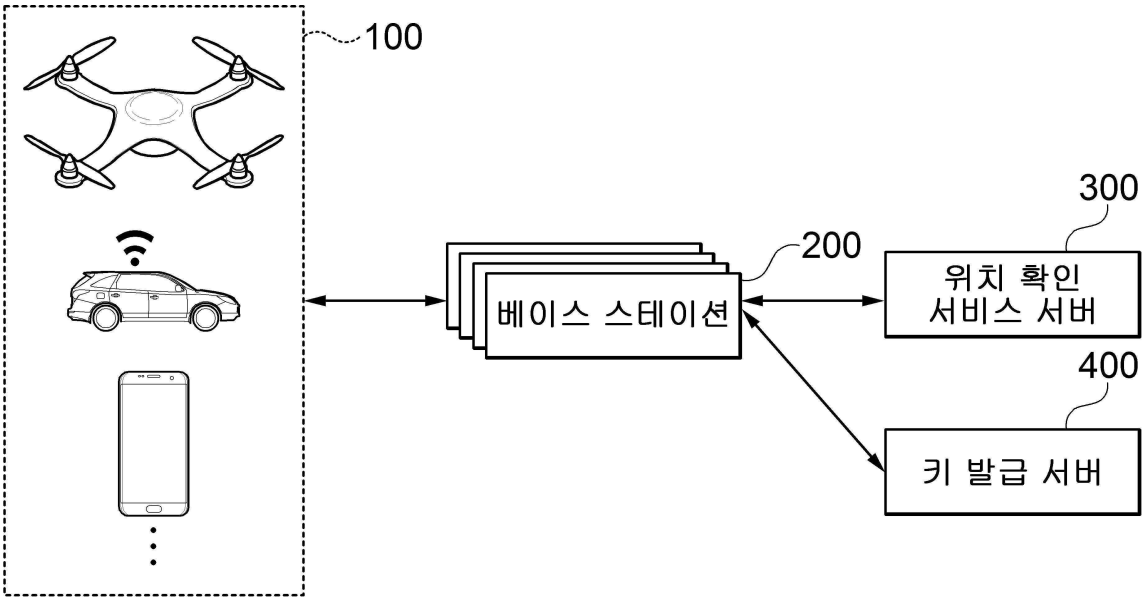
전체 청구항 수 : 총 12 항 심사관 : 이준석

(54) 발명의 명칭 **스마트 시티를 위한 위치 확인 방법 및 시스템과 이를 위한 이동통신 기기**

(57) 요 약

스마트 시티를 위한 위치 확인 방법 및 시스템, 이동통신 기기가 개시된다. 본 발명의 일 실시예에 따른 위치 확인 시스템은 기 설정된 영역별로 각각 위치하여, 인접한 이동통신 기기로 자신의 GPS 정보를 비밀키로 서명한 위치 확인 정보를 전송하는 복수의 베이스 스테이션을 포함한다.

대 표 도 - 도1



(52) CPC특허분류
H04W 12/122 (2021.01)
H04W 12/69 (2021.01)
H04W 4/023 (2020.05)
H04W 4/06 (2022.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 1711126109
과제번호 2018-0-01423-004
부처명 과학기술정보통신부
과제관리(전문)기관명 정보통신기획평가원
연구사업명 대학ICT연구센터육성지원사업
연구과제명 지능형 비행로봇 융합 기술 연구
기 여 율 1/2
과제수행기관명 세종대학교 산학협력단
연구기간 2021.01.01 ~ 2021.12.31
이 발명을 지원한 국가연구개발사업
과제고유번호 1711117818
과제번호 2020R1F1A1072275
부처명 과학기술정보통신부
과제관리(전문)기관명 한국연구재단
연구사업명 개인기초연구(과기정통부)(R&D)
연구과제명 무인항공기를 위한 블록체인 기반 보안 강화 기술 개발
기 여 율 1/2
과제수행기관명 세종대학교 산학협력단
연구기간 2021.03.01 ~ 2022.02.28

명 세 서

청구범위

청구항 1

이동통신 기기가 목적지에 도착한 후, 이동통신 기기측 난수값, 모빌리티 아이디 및 위치 확인 메시지를 포함하는 위치 확인 요청을 브로드캐스팅하는 단계;

상기 위치 확인 요청을 수신한 베이스 스테이션이 상기 이동통신 기기측 난수값, 상기 모빌리티 아이디, 공개키, 베이스 스테이션의 GPS 정보 및 베이스 스테이션측 현재시간 중 적어도 하나 이상을 포함하여 위치 확인 메시지를 생성하는 단계;

상기 위치 확인 메시지를 비밀키로 서명 처리하여 서명값을 생성하는 단계;

상기 위치 확인 메시지, 상기 서명값 및 상기 공개키를 포함하는 위치 확인 정보를 상기 이동통신 기기로 전송하는 단계; 및

상기 이동통신 기기가 기 저장된 공개키 중 상기 공개키와 일치하는 공개키가 존재하는 경우 상기 일치하는 공개키를 이용하여 상기 서명값의 유효성을 검증하고 상기 베이스 스테이션의 GPS 정보를 확인하여 자신의 위치 확인 절차를 수행하는 단계를 포함하며,

상기 베이스 스테이션이 복수 개인 경우 기 설정된 영역별로 각각 위치하며,

상기 위치 확인 요청을 브로드캐스팅하는 단계 이전에,

상기 복수의 베이스 스테이션 각각이 공개키 및 비밀키를 발급받는 단계;

상기 이동통신 기기가 자신을 식별할 수 있는 상기 모빌리티 아이디를 생성하는 단계; 및

상기 이동통신 기기가 상기 목적지에 위치하는 유효한 복수의 베이스 스테이션으로부터 공개키들을 수신하여 저장하는 단계를 더 포함하며,

상기 공개키들을 수신하여 저장하는 단계에서,

상기 이동통신 기기의 메모리 사용 제한이 제1 타입인 경우, 상기 공개키들을 블룸 필터(bloom filter)로 구성하여 관리하는 스마트 시티를 위한 위치 확인 방법.

청구항 2

삭제

청구항 3

삭제

청구항 4

이동통신 기기가 목적지에 도착한 후, 이동통신 기기측 난수값, 모빌리티 아이디 및 위치 확인 메시지를 포함하는 위치 확인 요청을 브로드캐스팅하는 단계;

상기 위치 확인 요청을 수신한 베이스 스테이션이 상기 이동통신 기기측 난수값, 상기 모빌리티 아이디, 공개키, 베이스 스테이션의 GPS 정보 및 베이스 스테이션측 현재시간 중 적어도 하나 이상을 포함하여 위치 확인 메시지를 생성하는 단계;

상기 위치 확인 메시지를 비밀키로 서명 처리하여 서명값을 생성하는 단계;

상기 위치 확인 메시지, 상기 서명값 및 상기 공개키를 포함하는 위치 확인 정보를 상기 이동통신 기기로 전송하는 단계; 및

상기 이동통신 기기가 기 저장된 공개키 중 상기 공개키와 일치하는 공개키가 존재하는 경우 상기 일치하는 공개키를 이용하여 상기 서명값의 유효성을 검증하고 상기 베이스 스테이션의 GPS 정보를 확인하여 자신의 위치 확인 절차를 수행하는 단계를 포함하며,

상기 베이스 스테이션이 복수 개인 경우 기 설정된 영역별로 각각 위치하며,

상기 위치 확인 요청을 브로드캐스팅하는 단계 이전에,

상기 복수의 베이스 스테이션 각각이 공개키 및 비밀키를 발급받는 단계;

상기 이동통신 기기가 자신을 식별할 수 있는 상기 모빌리티 아이디를 생성하는 단계; 및

상기 이동통신 기기가 상기 목적지에 위치하는 유효한 복수의 베이스 스테이션으로부터 공개키들을 수신하여 저장하는 단계를 더 포함하며,

상기 공개키들을 수신하여 저장하는 단계에서,

상기 이동통신 기기의 메모리 사용 제한이 제2 타입인 경우, 상기 공개키들을 테이블 형태로 관리하는 스마트 시티를 위한 위치 확인 방법.

청구항 5

이동통신 기기가 목적지에 도착한 후, 이동통신 기기측 난수값, 모빌리티 아이디 및 위치 확인 메시지를 포함하는 위치 확인 요청을 브로드캐스팅하는 단계;

상기 위치 확인 요청을 수신한 베이스 스테이션이 상기 이동통신 기기측 난수값, 상기 모빌리티 아이디, 공개키, 베이스 스테이션의 GPS 정보 및 베이스 스테이션측 현재시간 중 적어도 하나 이상을 포함하여 위치 확인 메시지를 생성하는 단계;

상기 위치 확인 메시지를 비밀키로 서명 처리하여 서명값을 생성하는 단계;

상기 위치 확인 메시지, 상기 서명값 및 상기 공개키를 포함하는 위치 확인 정보를 상기 이동통신 기기로 전송하는 단계; 및

상기 이동통신 기기가 기 저장된 공개키 중 상기 공개키와 일치하는 공개키가 존재하는 경우 상기 일치하는 공개키를 이용하여 상기 서명값의 유효성을 검증하고 상기 베이스 스테이션의 GPS 정보를 확인하여 자신의 위치 확인 절차를 수행하는 단계를 포함하며,

상기 베이스 스테이션이 복수 개인 경우 기 설정된 영역별로 각각 위치하며,

상기 위치 확인 요청을 브로드캐스팅하는 단계 이전에,

상기 복수의 베이스 스테이션 각각이 공개키 및 비밀키를 발급받는 단계;

상기 이동통신 기기가 자신을 식별할 수 있는 상기 모빌리티 아이디를 생성하는 단계; 및

상기 이동통신 기기가 상기 목적지에 위치하는 유효한 복수의 베이스 스테이션으로부터 공개키들을 수신하여 저장하는 단계를 더 포함하며,

상기 공개키들을 수신하여 저장하는 단계에서,

상기 목적지가 복수인 경우, 각각의 목적지에 아이디를 할당하여 상기 목적지별 아이디를 기준으로 상기 공개키들을 분류하여 저장 및 관리하는 스마트 시티를 위한 위치 확인 방법.

청구항 6

이동통신 기기가 목적지에 도착한 후, 이동통신 기기측 난수값, 모빌리티 아이디 및 위치 확인 메시지를 포함하는 위치 확인 요청을 브로드캐스팅하는 단계;

상기 위치 확인 요청을 수신한 베이스 스테이션이 상기 이동통신 기기측 난수값, 상기 모빌리티 아이디, 공개키, 베이스 스테이션의 GPS 정보 및 베이스 스테이션측 현재시간 중 적어도 하나 이상을 포함하여 위치 확

인 메시지를 생성하는 단계;

상기 위치 확인 메시지를 비밀키로 서명 처리하여 서명값을 생성하는 단계;

상기 위치 확인 메시지, 상기 서명값 및 상기 공개키를 포함하는 위치 확인 정보를 상기 이동통신 기기로 전송하는 단계; 및

상기 이동통신 기기가 기 저장된 공개키 중 상기 공개키와 일치하는 공개키가 존재하는 경우 상기 일치하는 공개키를 이용하여 상기 서명값의 유효성을 검증하고 상기 베이스 스테이션의 GPS 정보를 확인하여 자신의 위치 확인 절차를 수행하는 단계를 포함하며,

상기 위치 확인 절차를 수행하는 단계에서,

상기 위치 확인 절차가 기 설정된 횟수 이상으로 완료된 경우, 위치 재확인 절차가 성공한 것으로 판단하는 스마트 시티를 위한 위치 확인 방법.

청구항 7

삭제

청구항 8

베이스 스테이션이 위치 확인 메시지, 주소 아이디 및 서명값 중 적어도 하나 이상을 포함하는 위치 확인 정보를 브로드캐스팅 하는 단계;

특정 목적지로 이동한 이동통신 기기가 해당 목적지에 위치하는 상기 베이스 스테이션으로부터 상기 위치 확인 정보를 수신하는 단계; 및

상기 이동통신 기기가 상기 목적지에 대응되는 주소 아이디 및 서명값을 기초로 상기 위치 확인 정보를 확인하여 자신의 현재 위치를 확인하는 단계를 포함하며,

상기 위치 확인 정보를 브로드캐스팅 하는 단계 이전에,

상기 베이스 스테이션이 자신을 식별할 수 있는 주소 아이디를 설정하는 단계; 및

상기 베이스 스테이션이 상기 주소 아이디에 대한 비밀키를 발급받는 단계를 더 포함하며,

상기 위치 확인 메시지는, 베이스 스테이션의 GPS 정보, 베이스 스테이션측 현재 시간 및 상기 주소 아이디를 포함하며,

상기 위치 확인 정보를 브로드캐스팅 하는 단계에서,

상기 베이스 스테이션이 상기 베이스 스테이션의 GPS 정보, 상기 베이스 스테이션측 현재 시간을 상기 비밀키로 서명하여 상기 서명값을 생성하는 스마트 시티를 위한 위치 확인 방법.

청구항 9

삭제

청구항 10

삭제

청구항 11

삭제

청구항 12

기 설정된 영역별로 각각 위치하여, 인접한 이동통신 기기로 자신의 GPS 정보를 비밀키로 서명한 위치 확인 정

보를 전송하는 복수의 베이스 스테이션을 포함하며,

상기 베이스 스테이션은,

베이스 스테이션의 GPS 정보, 베이스 스테이션측 현재 시간 및 주소 아이디를 포함하는 위치 확인 메시지를 생성하는 위치 생성부; 및

상기 베이스 스테이션의 GPS 정보 및 상기 베이스 스테이션측 현재 시간을 상기 주소 아이디에 대해 발급받은 비밀키로 서명하여 서명값을 생성하고, 상기 위치 확인 메시지, 상기 주소 아이디 및 상기 서명값 중 적어도 하나 이상을 포함하는 상기 위치 확인 정보를 브로드캐스팅 하도록 하는 서명 처리부를 포함하는 스마트 시티를 위한 위치 확인 시스템.

청구항 13

청구항 12에 있어서,

상기 베이스 스테이션은,

상기 이동통신 기기로부터 전송되는 위치 확인 요청을 수신하면, 상기 이동통신 기기측 난수값, 모빌리티 아이디, 공개키, 베이스 스테이션의 GPS 정보 및 베이스 스테이션측 현재시간 중 적어도 하나 이상을 포함하는 위치 확인 메시지를 생성하는 위치 생성부; 및

상기 위치 확인 메시지를 비밀키로 서명 처리하여 생성한 서명값, 상기 위치 확인 메시지 및 공개키를 포함하는 상기 위치 확인 정보를 상기 이동통신 기기로 전송하도록 하는 서명 처리부를 포함하는 스마트 시티를 위한 위치 확인 시스템.

청구항 14

청구항 13에 있어서,

상기 베이스 스테이션은,

키 발급 서버를 통해 자신의 상기 공개키 및 상기 비밀키를 발급받기 위한 키 생성부를 더 포함하는 스마트 시티를 위한 위치 확인 시스템.

청구항 15

삭제

청구항 16

청구항 12에 있어서,

상기 베이스 스테이션은, 상기 위치 확인 정보를 기 설정된 주기로 브로드캐스팅하는 스마트 시티를 위한 위치 확인 시스템.

청구항 17

자신을 식별할 수 있는 모빌리티 아이디를 생성하기 위한 아이디 생성부;

사전에 목적지에 위치한 유효한 복수의 베이스 스테이션의 공개키들을 수신하여 관리하기 위한 키 관리부; 및

상기 목적지에 도착한 후, 난수값, 상기 모빌리티 아이디 및 위치 확인 요청 메시지를 포함하는 위치 확인 요청을 브로드캐스팅하고, 복수의 베이스 스테이션으로부터 전송되는 위치 확인 정보를 기초로 자신의 현재 위치를 재확인하는 위치 확인부를 포함하며,

상기 키 관리부는, 이동통신 기기의 메모리 사용 제한이 제1 타입인 경우, 상기 공개키들을 블룸 필터(bloom filter)로 구성하여 관리하고,

상기 이동통신 기기의 메모리 사용 제한이 제2 타입인 경우, 상기 공개키들을 테이블 형태로 관리하는 이동통신 기기.

청구항 18

삭제

청구항 19

자신을 식별할 수 있는 모빌리티 아이디를 생성하기 위한 아이디 생성부;

사전에 목적지에 위치한 유효한 복수의 베이스 스테이션의 공개키들을 수신하여 관리하기 위한 키 관리부; 및

상기 목적지에 도착한 후, 난수값, 상기 모빌리티 아이디 및 위치 확인 요청 메시지를 포함하는 위치 확인 요청을 브로드캐스팅하고, 복수의 베이스 스테이션으로부터 전송되는 위치 확인 정보를 기초로 자신의 현재 위치를 재확인하는 위치 확인부를 포함하며,

상기 키 관리부는,

상기 목적지가 복수인 경우, 각각의 목적지에 아이디를 할당하여 상기 목적지별 아이디를 기준으로 상기 공개키들을 분류하여 저장 및 관리하는 이동통신 기기.

청구항 20

자신을 식별할 수 있는 모빌리티 아이디를 생성하기 위한 아이디 생성부;

사전에 목적지에 위치한 유효한 복수의 베이스 스테이션의 공개키들을 수신하여 관리하기 위한 키 관리부; 및

상기 목적지에 도착한 후, 난수값, 상기 모빌리티 아이디 및 위치 확인 요청 메시지를 포함하는 위치 확인 요청을 브로드캐스팅하고, 복수의 베이스 스테이션으로부터 전송되는 위치 확인 정보를 기초로 자신의 현재 위치를 재확인하는 위치 확인부를 포함하며,

상기 위치 확인부는,

상기 위치 확인 정보를 기초한 위치 확인 절차가 기 설정된 횟수 이상으로 완료된 경우, 위치 재확인 절차가 성공한 것으로 판단하는 이동통신 기기.

발명의 설명

기 술 분 야

[0001] 본 발명의 실시예들은 스마트 시티를 위한 위치 확인 방법 및 시스템과 이를 위한 이동통신 기기와 관련된다.

배 경 기 술

[0002] 드론 또는 스마트 카 등과 같이 GPS(global positioning system) 정보를 기초하여 목적지로 이동하는 기술이 다양한 분야에서 활용되고 있다. 이러한 이유로, GPS 신호에 대한 신뢰성이 중요한 이슈로 대두되고 있는 실정이다.

[0003] 한편, GPS 스푸핑(Spoofing) 공격은 무선 간섭을 통해 위성 신호 손실 및 위치 손실 가능성을 유발하여, 수신기가 잘못된 위치에 있다고 믿게 만드는 간섭이다. GPS 스푸핑 공격 중에는 주변에 있는 무선 송신기가 가짜 GPS 신호를 대상 수신기, 예를 들어, 드론으로 송부하여 원래 목표하는 방향과 다른 방향으로 가도록 유도하거나 또는 현재 위치를 착각하도록 할 수 있다.

[0004] 이에, 운용자는 드론과 같은 이동통신 기기의 GPS 정보에 대한 신뢰성을 확보하기 위한 기술에 대한 연구의 필

요성을 인식하게 되었다.

선행기술문헌

특허문헌

[0006] (특허문헌 0001) 대한민국 공개특허공보 제10-2016-0045283호 (2016. 04. 27.)

발명의 내용

해결하려는 과제

[0007] 본 발명의 실시예들은 이동통신 기기가 GPS 정보를 기초로 목적지로 이동한 경우 목적지의 위치를 재확인할 수 있도록 하기 위한 스마트 시티를 위한 위치 확인 방법 및 시스템과 이를 위한 이동통신 기기를 제공하기 위한 것이다.

과제의 해결 수단

[0009] 본 발명의 예시적인 실시예에 따르면, 스마트 시티를 위한 위치 확인 방법은, 이동통신 기기가 목적지에 도착한 후, 이동통신 기기측 난수값, 모빌리티 아이디 및 위치 확인 메시지를 포함하는 위치 확인 요청을 브로드캐스팅하는 단계; 상기 위치 확인 요청을 수신한 베이스 스테이션이 상기 이동통신 기기측 난수값, 상기 모빌리티 아이디, 공개키, 베이스 스테이션의 GPS 정보 및 베이스 스테이션측 현재시간 중 적어도 하나 이상을 포함하여 위치 확인 메시지를 생성하는 단계; 상기 위치 확인 메시지를 비밀키로 서명 처리하여 서명값을 생성하는 단계; 상기 위치 확인 메시지, 상기 서명값 및 상기 공개키를 포함하는 위치 확인 정보를 상기 이동통신 기기로 전송하는 단계; 상기 이동통신 기기가 기 저장된 공개키 중 상기 공개키와 일치하는 공개키가 존재하는 경우 상기 일치하는 공개키를 이용하여 상기 서명값의 유효성을 검증하고 상기 베이스 스테이션의 GPS 정보를 확인하여 자신의 위치 확인 절차를 수행하는 단계를 포함한다.

[0010] 상기 베이스 스테이션이 복수 개인 경우 기 설정된 영역별로 각각 위치하며, 스마트 시티를 위한 위치 확인 방법은, 상기 위치 확인 요청을 브로드캐스팅하는 단계 이전에, 상기 복수의 베이스 스테이션 각각이 공개키 및 비밀키를 발급받는 단계; 상기 이동통신 기기가 자신을 식별할 수 있는 상기 모빌리티 아이디를 생성하는 단계; 및 상기 이동통신 기기가 상기 목적지에 위치하는 유효한 복수의 베이스 스테이션으로부터 공개키들을 수신하여 저장하는 단계를 더 포함할 수 있다.

[0011] 또한, 스마트 시티를 위한 위치 확인 방법은, 상기 공개키들을 수신하여 저장하는 단계에서, 상기 이동통신 기기의 메모리 사용 제한이 제1 타입인 경우, 상기 공개키들을 블룸 필터(bloom filter)로 구성하여 관리할 수 있다.

[0012] 또한, 스마트 시티를 위한 위치 확인 방법은, 상기 공개키들을 수신하여 저장하는 단계에서, 상기 이동통신 기기의 메모리 사용 제한이 제2 타입인 경우, 상기 공개키들을 테이블 형태로 관리할 수 있다.

[0013] 또한, 스마트 시티를 위한 위치 확인 방법은, 상기 공개키들을 수신하여 저장하는 단계에서, 상기 목적지가 복수인 경우, 각각의 목적지에 아이디를 할당하여 상기 목적지별 아이디를 기준으로 상기 공개키들을 분류하여 저장 및 관리할 수 있다.

[0014] 또한, 스마트 시티를 위한 위치 확인 방법은, 상기 위치 확인 절차를 수행하는 단계에서, 상기 위치 확인 절차가 기 설정된 횟수 이상으로 완료된 경우, 위치 재확인 절차가 성공한 것으로 판단할 수 있다.

[0015] 또한, 스마트 시티를 위한 위치 확인 방법은, 상기 위치 확인 절차를 수행하는 단계에서, 상기 이동통신 기기가 위치 확인 정보 회신시간 기준, GPS 정보 및 현재 시간 및 이들의 조합 중 어느 하나를 통해 상기 위치 확인 정보에 대한 교란 방지 검증 절차를 수행할 수 있다.

[0016] 본 발명의 다른 예시적인 실시예에 따르면, 스마트 시티를 위한 위치 확인 방법은, 베이스 스테이션이 위치 확인 메시지, 주소 아이디 및 서명값 중 적어도 하나 이상을 포함하는 위치 확인 정보를 브로드캐스팅 하는 단계; 특정 목적지로 이동한 이동통신 기기가 해당 목적지에 위치하는 상기 베이스 스테이션으로부터 상기 위치 확인 정보를 수신하는 단계; 상기 이동통신 기기가 상기 목적지에 대응되는 주소 아이디 및 서명값을 기초로 상기 위

치 확인 정보를 확인하여 자신의 현재 위치를 확인하는 단계를 포함한다.

[0017] 또한, 스마트 시티를 위한 위치 확인 방법은, 상기 위치 확인 정보를 브로드캐스팅 하는 단계 이전에, 상기 베이스 스테이션이 자신을 식별할 수 있는 주소 아이디를 설정하는 단계; 및 상기 베이스 스테이션이 상기 주소 아이디에 대한 비밀키를 발급받는 단계를 더 포함할 수 있다.

[0018] 상기 위치 확인 메시지는, 베이스 스테이션의 GPS 정보, 베이스 스테이션측 현재 시간 및 상기 주소 아이디를 포함할 수 있다.

[0019] 또한, 스마트 시티를 위한 위치 확인 방법은, 상기 위치 확인 정보를 브로드캐스팅 하는 단계에서, 상기 베이스 스테이션이 상기 베이스 스테이션의 GPS 정보, 상기 베이스 스테이션측 현재 시간을 상기 비밀키로 서명하여 상기 서명값을 생성할 수 있다.

[0020] 본 발명의 다른 예시적인 실시예에 따르면, 스마트 시티를 위한 위치 확인 시스템은, 기 설정된 영역별로 각각 위치하여, 인접한 이동통신 기기로 자신의 GPS 정보를 비밀키로 서명한 위치 확인 정보를 전송하는 복수의 베이스 스테이션을 포함한다.

[0021] 또한, 상기 베이스 스테이션은, 상기 이동통신 기기로부터 전송되는 위치 확인 요청을 수신하면, 상기 이동통신 기기측 난수값, 모빌리티 아이디, 공개키, 베이스 스테이션의 GPS 정보 및 베이스 스테이션측 현재시간 중 적어도 하나 이상을 포함하는 위치 확인 메시지를 생성하는 위치 생성부; 및 상기 위치 확인 메시지를 비밀키로 서명 처리하여 생성한 서명값, 상기 위치 확인 메시지 및 공개키를 포함하는 상기 위치 확인 정보를 상기 이동통신 기기로 전송하도록 하는 서명 처리부를 포함할 수 있다.

[0022] 상기 베이스 스테이션은, 키 발급 서버를 통해 자신의 상기 공개키 및 상기 비밀키를 발급받기 위한 키 생성부를 더 포함할 수 있다.

[0023] 상기 베이스 스테이션은, 베이스 스테이션의 GPS 정보, 베이스 스테이션측 현재 시간 및 주소 아이디를 포함하는 위치 확인 메시지를 생성하는 위치 생성부; 상기 베이스 스테이션의 GPS 정보 및 상기 베이스 스테이션측 현재 시간을 상기 주소 아이디에 대해 발급받은 비밀키로 서명하여 서명값을 생성하고, 상기 위치 확인 메시지, 상기 주소 아이디 및 상기 서명값 중 적어도 하나 이상을 포함하는 상기 위치 확인 정보를 브로드캐스팅 하도록 하는 서명 처리부를 포함할 수 있다.

[0024] 상기 베이스 스테이션은, 상기 위치 확인 정보를 기 설정된 주기로 브로드캐스팅할 수 있다.

[0025] 본 발명의 다른 예시적인 실시예에 따르면, 이동통신 기기는, 자신을 식별할 수 있는 모빌리티 아이디를 생성하기 위한 아이디 생성부; 사전에 목적지에 위치한 유효한 복수의 베이스 스테이션의 공개키들을 수신하여 관리하기 위한 키 관리부; 및 상기 목적지에 도착한 후, 난수값, 상기 모빌리티 아이디 및 위치 확인 요청 메시지를 포함하는 위치 확인 요청을 브로드캐스팅하고, 복수의 베이스 스테이션으로부터 전송되는 위치 확인 정보를 기초로 자신의 현재 위치를 재확인하는 위치 확인부를 포함한다.

[0026] 상기 키 관리부는, 상기 이동통신 기기의 메모리 사용 제한이 제1 타입인 경우, 상기 공개키들을 블룸 필터(bloom filter)로 구성하여 관리하고, 상기 이동통신 기기의 메모리 사용 제한이 제2 타입인 경우, 상기 공개키들을 테이블 형태로 관리할 수 있다.

[0027] 상기 키 관리부는, 상기 목적지가 복수인 경우, 각각의 목적지에 아이디를 할당하여 상기 목적지별 아이디를 기준으로 상기 공개키들을 분류하여 저장 및 관리할 수 있다.

[0028] 상기 위치 확인부는, 상기 위치 확인 정보를 기초한 위치 확인 절차가 기 설정된 횟수 이상으로 완료된 경우, 위치 재확인 절차가 성공한 것으로 판단할 수 있다.

발명의 효과

[0030] 본 발명의 실시예들에 따르면, 드론 또는 스마트 카 등의 이동통신 기기가 GPS 정보를 기초로 목적지로 이동한 경우 목적지에서 자신의 위치를 재 확인할 수 있다는 효과를 기대할 수 있다.

[0031] 또한, 본 발명의 실시예들에 따르면, 이동통신 기기가 목적지에 위치하는 베이스 스테이션으로부터 위치 재 확인을 위해 전달받은 위치 확인 정보에 대해 GPS 스푸핑 교란 방지 검증을 수행하기 때문에, 위치 확인 정보에 대한 신뢰성이 향상될 수 있다는 것이다.

도면의 간단한 설명

[0033] 도 1은 본 발명의 일 실시예에 따른 스마트 시티를 위한 위치 확인 시스템을 설명하기 위한 블록도

도 2는 도 1의 베이스 스테이션을 설명하기 위한 블록도

도 3은 도 1의 이동통신 기기를 설명하기 위한 블록도

도 4는 본 발명의 일 실시예에 따른 위치 확인 방법의 일 예를 설명하기 위한 예시도

도 5는 본 발명의 일 실시예에 따른 위치 확인 방법의 다른 예를 설명하기 위한 예시도

도 6은 본 발명의 일 실시예에 따른 스마트 시티를 위한 위치 확인 방법의 일 예를 설명하기 위한 흐름도

도 7은 본 발명의 일 실시예에 따른 스마트 시티를 위한 위치 확인 방법의 다른 예를 설명하기 위한 흐름도

도 8은 본 발명의 일 실시예에 따른 컴퓨팅 장치를 포함하는 컴퓨팅 환경을 예시하여 설명하기 위한 블록도

발명을 실시하기 위한 구체적인 내용

[0034] 이하, 도면을 참조하여 본 발명의 구체적인 실시형태를 설명하기로 한다. 이하의 상세한 설명은 본 명세서에서 기술된 방법, 장치 및/또는 시스템에 대한 포괄적인 이해를 돕기 위해 제공된다. 그러나 이는 예시에 불과하며 본 발명은 이에 제한되지 않는다.

[0035] 본 발명의 실시예들을 설명함에 있어서, 본 발명과 관련된 공지기술에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략하기로 한다. 그리고, 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다. 상세한 설명에서 사용되는 용어는 단지 본 발명의 실시예들을 기술하기 위한 것이며, 결코 제한적이어서는 안 된다. 명확하게 달리 사용되지 않는 한, 단수 형태의 표현은 복수 형태의 의미를 포함한다. 본 설명에서, "포함" 또는 "구비"와 같은 표현은 어떤 특성들, 숫자들, 단계들, 동작들, 요소들, 이들의 일부 또는 조합을 가리키기 위한 것이며, 기술된 것 이외에 하나 또는 그 이상의 다른 특성, 숫자, 단계, 동작, 요소, 이들의 일부 또는 조합의 존재 또는 가능성을 배제하도록 해석되어서는 안 된다.

[0037] 이하에서 개시하는 스마트 시티는 다양한 유형의 전자 데이터 수집 센서를 사용하여 자산과 자원을 효율적으로 관리하는데 필요한 정보를 제공하는 도시 지역으로, 액세스 포인트(AP) 등 통신 네트워크 인프라가 구역마다 존재하는 지역을 의미할 수 있다. 이때, 액세스 포인트는 이하에서 개시하는 베이스 스테이션과 동일 구성일 수 있다.

[0038] 도 1은 본 발명의 일 실시예에 따른 스마트 시티를 위한 위치 확인 시스템을 설명하기 위한 블록도이고, 도 2는 베이스 스테이션을 설명하기 위한 블록도이다.

[0039] 이하에서는, 본 발명의 일 실시예에 따른 위치 확인 방법의 일 예를 설명하기 위한 예시도인 도 4 및 본 발명의 일 실시예에 따른 위치 확인 방법의 다른 예를 설명하기 위한 예시도인 도 5를 참조하여 설명하기로 한다.

[0040] 도 1을 참고하면, 위치 확인 시스템은 기 설정된 영역별로 각각 위치하여, 인접한 이동통신 기기(100)로 자신의 GPS 정보를 비밀키로 서명한 위치 확인 정보를 전송하는 복수의 베이스 스테이션(200)을 포함한다.

[0041] 상술한 위치 확인 시스템은 목적지 이동에 따라 자신의 현재 위치를 확인 요청하는 이동통신 기기(100), 복수의 베이스 스테이션(200)의 GPS 정보 등을 관리하는 위치 확인 서비스 서버(300) 및 베이스 스테이션(200)의 비밀키 및 공개키를 발급 처리하기 위한 키 발급 서버(key generation server)(400)를 추가로 포함할 수 있다.

[0042] 도 2를 참고하면, 베이스 스테이션(200)은 키 생성부(210), 위치 생성부(230) 및 서명 처리부(250)를 포함할 수 있다.

[0043] 이때, 베이스 스테이션(200)의 각 구성은 위치 확인 정보를 제공하는 방식에 따라 2가지 경우로 분류하여 설명할 수 있다.

[0044] 일 예로, 베이스 스테이션(200)이 이동통신 기기(100)와 서로 정보를 송수신하는 양방향 통신을 통해 위치 확인 절차를 수행하는 경우를 예로 들어 설명하기로 한다.

[0045] 키 생성부(210)는 키 발급 서버(400)를 통해 자신의 공개키(pk_N) 및 비밀키(sk_N)를 발급받을 수 있다.

[0046] 위치 생성부(210)는 이동통신 기기(100)로부터 전송되는 위치 확인 요청을 수신하면, 이동통신 기기측 난수값, 모빌리티 아이디(M_ID), 공개키, 베이스 스테이션의 GPS 정보 및 베이스 스테이션측 현재시간 중 적어도 하나 이상을 포함하는 위치 확인 메시지를 생성할 수 있다. 이때, 베이스 스테이션측 현재시간은 GPS 스푸핑(spoofing) 등의 교란을 방지하기 위한 검증 정보로 활용될 수 있다.

[0047] 서명 처리부(250)는 위치 확인 메시지를 비밀키로 서명 처리하여 생성한 서명값(σ), 상기 위치 확인 메시지 및 공개키를 포함하는 위치 확인 정보를 이동통신 기기(100)로 전송하도록 할 수 있다. 이때, 서명 처리부(250)는 도 8의 네트워크 통신 인터페이스(26)를 통해 위치 확인 정보를 이동통신 기기(100)로 전송할 수 있다. 이때, 서명 처리부(250)는 ESDSA(elliptic curve digital signature algorithm) 알고리즘 기반의 디지털 서명을 수행할 수 있다.

[0048] 도 4를 참고하면, A 영역에 위치하는 복수의 베이스 스테이션(200a, 200b, 200c)은 이동통신 기기(100)가 A 영역에 진입함에 따라, 이동통신 기기(100)로부터 브로드캐스팅된 위치 확인 요청을 수신할 수 있다. 이후, 복수의 베이스 스테이션(200a, 200b, 200c)은 상술한 위치 확인 정보를 이동통신 기기(100)로 전송하여 이동통신 기기(100)가 자신의 GPS 정보를 재확인할 수 있도록 하는 것이다.

[0049] 다른 예로, 베이스 스테이션(200)이 기 설정된 주기로 위치 확인 정보를 송신하는 방식으로 위치 확인 절차를 수행하는 경우를 예로 들어 설명하기로 한다.

[0050] 키 생성부(210)는 자신을 식별할 수 있는 주소 아이디를 설정할 수 있다.

[0051] 또한, 키 생성부(210)는 주소 아이디에 대한 비밀키를 발급받을 수 있다.

[0052] 예를 들어, 스마트 시티에서 베이스 스테이션(200)들은 자신의 주소(예를 들어, street 정보)인 "서울시 광진구 능동로 XX", "광진구 능동로 XX", 또는 "능동로 XX"를 자신의 아이디(ID)로 설정하고, 아이디 기반 서명을 위해 키 발급 서버(400)로부터 해당 아이디에 대한 비밀키를 발급받을 수 있다.

[0053] 이때, 아이디 기반 서명방식은 키 발급 서버(400)의 비밀키 관리가 중요하므로, 키 발급 서버(400)를 각 구별로 구비하거나, 각 구 단위 보다 더 작은 영역 단위로 구비하거나, 또는 키 발급 서버(400) 내에서 비밀키 및 공개키를 주기적으로 업데이트 할 수 있다. 드론이나 스마트 카와 같은 이동통신 기기(100)가 위치 기반 서비스를 받기 위해서는 공개키의 무결성이 중요한데, 이를 위해 위치 확인 서비스를 제공하는 앱이나 서비스 소프트웨어를 주기적으로 업데이트하여 최신 파라미터값을 유지하도록 할 수 있다.

[0054] 위치 생성부(230)는 베이스 스테이션의 GPS 정보, 베이스 스테이션측 현재 시간 및 주소 아이디를 포함하는 위치 확인 메시지를 생성할 수 있다.

[0055] 서명 처리부(250)는 베이스 스테이션의 GPS 정보 및 베이스 스테이션측 현재 시간을 주소 아이디에 대해 발급받은 비밀키로 서명하여 서명값을 생성하고, 상기 위치 확인 메시지, 상기 주소 아이디 및 상기 서명값 중 적어도 하나 이상을 포함하는 상기 위치 확인 정보를 브로드캐스팅 하도록 할 수 있다.

[0056] 이때, 베이스 스테이션(250)은 도 8의 네트워크 통신 인터페이스(26)를 통해 위치 확인 정보를 기 설정된 주기로 브로드캐스팅할 수 있다.

[0057] 도 5를 참고하면, A 영역에 위치하는 복수의 베이스 스테이션(200a, 200b, 200c)은 기 설정된 주기로 위치 확인 정보를 브로드캐스팅하고, A 영역에 진입한 이동통신 기기(100)가 복수의 베이스 스테이션(200a, 200b, 200c)으로부터 수신한 위치 확인 정보를 기초로 자신의 GPS 정보를 재확인할 수 있는 것이다.

[0058] 이러한 경우, 이동통신 기기(100)는 목적지(예를 들어, A 영역)로 이동하기 전에 목적지에 위치하는 베이스 스테이션(200a, 200b, 200c)의 공개키를 획득 및 저장하는 절차를 생략할 수 있다. 이에 따라, 이동통신 기기(100) 측면에서 효율성이 상대적으로 높을 수 있다는 효과를 기대할 수 있다.

[0060] 도 3은 도 1의 이동통신 기기를 설명하기 위한 블록도이다.

[0061] 도 3을 참고하면, 이동통신 기기(100)는 아이디 생성부(110), 키 관리부(130) 및 위치 확인부(150)를 포함한다.

[0062] 아이디 생성부(110)는 자신을 식별할 수 있는 모빌리티 아이디를 생성하기 위한 구성일 수 있다. 이때, 모빌리티 아이디는 모빌리티명 및 모빌리티 정보를 포함할 수 있으며, 이에 한정되지 않는다.

[0063] 키 관리부(130)는 사전에 목적지에 위치한 유효한 복수의 베이스 스테이션(200)의 공개키들을 수신하여 관리하기 위한 구성일 수 있다.

[0064] 키 관리부(130)는 이동통신 기기(100)의 메모리 사용 제한이 제1 타입인 경우, 공개키들을 블룸 필터(bloom filter)로 구성하여 관리할 수 있다. 이때, 메모리 사용 제한이 제1 타입인 것은 메모리 사용이 기준치 이하로 제한된 타입을 의미하는 것으로서, 드론과 같이 메모리 사용이 상대적으로 제한된 디바이스에 적용될 수 있다.

[0065] 키 관리부(130)는 이동통신 기기(100)의 메모리 사용 제한이 제2 타입인 경우, 공개키들을 테이블 형태로 관리할 수 있다. 메모리 사용 제한이 제2 타입인 것은 메모리 사용이 제1 타입에 비해 제한적이지 않은 타입을 의미하는 것으로서, 스마트 카와 같이 메모리 사용이 상대적으로 제한적이지 않은 대상에 적용될 수 있다.

[0066] 상술한 제1 타입은 제2 타입에 비해 메모리 사용 기준이 작을 수 있다.

[0067] 키 관리부(130)는 목적지가 복수인 경우, 각각의 목적지에 아이디를 할당하여 목적지별 아이디를 기준으로 공개키들을 분류하여 저장 및 관리할 수 있다.

[0068] 예를 들어, 이동통신 기기(100)가 드론과 같이 제1 타입을 적용한 경우, BF 목적지ID1, BF 목적지ID2, BF 목적지ID3 등과 같은 형태로 공개키들을 분류하여 저장 및 관리할 수 있다. 이동통신 기기(100)가 스마트 카와 같이 제2 타입을 적용한 경우, T 목적지ID1, T 목적지ID2, T 목적지ID3 등과 같은 형태로 공개키들을 분류하여 저장 및 관리할 수 있다.

[0069] 이동통신 기기(100)는 목적지로 이동하기 전에 상술한 목적지의 공개키들을 구비하여 주행할 수 있는 것이다. 이때, 이동통신 기기(100)의 메모리 사용 제한이 제1 타입인 경우, 공개키들의 블룸 필터(bloom filter)만을 보관하여 목적지로 이동할 수 있다.

[0070] 상술한 목적지 이동 전에 목적지의 베이스 스테이션(200)들의 공개키들을 저장하는 것은 베이스 스테이션(200)이 이동통신 기기(100)와 양방향 통신을 통해 위치 확인 정보를 제공하는 경우에 적용되는 방식일 수 있다.

[0071] 만약, 상술한 도 5의 복수의 베이스 스테이션(200)들이 위치 확인 정보를 기 설정된 주기마다 브로드 캐스팅하는 방식이 적용되는 경우라면, 키 관리부(130)는 목적지 이동 전에 공개키를 획득 및 저장하는 절차를 생략할 수 있다.

[0072] 위치 확인부(150)는 목적지에 도착한 후, 난수값, 모빌리티 아이디 및 위치 확인 요청 메시지를 포함하는 위치 확인 요청을 브로드캐스팅하고, 복수의 베이스 스테이션(200)으로부터 전송되는 위치 확인 정보를 기초로 자신의 현재 위치를 재확인하는 구성일 수 있다.

[0073] 위치 확인부(150)는 위치 확인 정보를 기초한 위치 확인 절차가 기 설정된 횟수 이상으로 완료된 경우, 위치 재확인 절차가 성공한 것으로 판단할 수 있다.

[0074] 만약, 상술한 도 5의 복수의 베이스 스테이션(200)들이 위치 확인 정보를 기 설정된 주기마다 브로드 캐스팅하는 방식이 적용되는 경우라면, 위치 확인부(150)는 유효한 주소 아이디를 기반으로 위치 재확인 절차를 수행할 수 있다.

[0075] 한편, 상술한 이동통신 기기(100)는 통신 네트워크(미도시)를 통해 복수의 베이스 스테이션(200)과 통신 가능하게 연결될 수 있다. 몇몇 실시예들에서, 통신 네트워크는 인터넷, 하나 이상의 로컬 영역 네트워크(local area networks), 광역 네트워크(wide area networks), 셀룰러 네트워크, 모바일 네트워크, 그 밖에 다른 종류의 네트워크들, 또는 이러한 네트워크들의 조합을 포함할 수 있다.

[0076] 본 실시예들에서, 이동통신 기기(100)는 원격 조정 기술 또는 자율 주행 기술에 의해 이동 가능한 이동 수단을 포함할 수 있다. 또한, 이동통신 기기(100)는 근거리 무선 통신을 포함하는 이동통신 기능을 포함한 이동통신 단말기를 포함할 수도 있다.

[0077] 예를 들어, 이동통신 기기(100)는 드론과 같은 무인 항공기 또는 스마트 카와 같은 자율 주행 차 또는 자율 주행 로봇 또는 PDA(personal digital assistant) 및 셀룰러 폰(*cellular* phone)과 같은 이동통신 단말기 등이 포함될 수 있으나, 이에 한정되는 것은 아니다.

[0079] 도 6은 본 발명의 일 실시예에 따른 스마트 시티를 위한 위치 확인 방법의 일 예를 설명하기 위한 흐름도이다. 도 6에 도시된 방법은 예를 들어, 전술한 이동통신 기기(100) 및 베이스 스테이션(200)에 의해 수행될 수 있다. 도시된 흐름도에서는 상기 방법을 복수 개의 단계로 나누어 기재하였으나, 적어도 일부의 단계들은 순서를 바꾸

어 수행되거나, 다른 단계와 결합되어 함께 수행되거나, 생략되거나, 세부 단계들로 나뉘어 수행되거나, 또는 도시되지 않은 하나 이상의 단계가 부가되어 수행될 수 있다.

[0080] 101 단계에서, 복수의 베이스 스테이션(200) 각각은 공개키 및 비밀키를 발급받을 수 있다. 상기 베이스 스테이션(200)이 복수 개인 경우 기 설정된 영역별로 각각 위치할 수 있다.

[0081] 103 단계에서, 이동통신 기기(100)는 자신을 식별할 수 있는 모빌리티 아이디를 생성할 수 있다.

[0082] 105 단계에서, 이동통신 기기(100)는 목적지에 위치하는 유효한 복수의 베이스 스테이션(200)으로부터 공개키들을 수신하여 저장할 수 있다.

[0083] 이동통신 기기(100)의 메모리 사용 제한이 제1 타입인 경우, 이동통신 기기(100)는 공개키들을 블룸 필터(boom filter)로 구성하여 관리할 수 있다.

[0084] 이동통신 기기(100)의 메모리 사용 제한이 제2 타입인 경우, 이동통신 기기(100)는 공개키들을 테이블 형태로 관리할 수 있다.

[0085] 만약, 목적지가 복수인 경우, 이동통신 기기(100)는 각각의 목적지에 아이디를 할당하여 상기 목적지별 아이디를 기준으로 상기 공개키들을 분류하여 저장 및 관리할 수 있다.

[0086] 107 단계 및 109 단계에서, 이동통신 기기(100)는 목적지에 도착한 후, 이동통신 기기측 난수값, 모빌리티 아이디 및 위치확인요청 메시지를 포함하는 위치 확인 요청을 생성하여 브로드캐스팅할 수 있다.

[0087] 111 단계에서, 위치 확인 요청을 수신한 베이스 스테이션(200)이 이동통신 기기측 난수값, 모빌리티 아이디, 공개키, 베이스 스테이션의 GPS 정보 및 베이스 스테이션측 현재시간 중 적어도 하나 이상을 포함하여 위치 확인 메시지를 생성할 수 있다. 또한, 베이스 스테이션(200)은 위치 확인 메시지를 비밀키로 서명 처리하여 서명값을 생성할 수 있다.

[0088] 113 단계에서, 베이스 스테이션(200)은 위치 확인 메시지, 서명값 및 공개키를 포함하는 위치 확인 정보를 이동통신 기기(100)로 전송할 수 있다.

[0089] 115 단계에서, 이동통신 기기(100)는 기 저장된 공개키 중 상기 공개키와 일치하는 공개키가 존재하는 경우 상기 일치하는 공개키를 이용하여 상기 서명값의 유효성을 검증하고 상기 베이스 스테이션의 GPS 정보를 확인하여 자신의 위치 확인 절차를 수행할 수 있다.

[0090] 이동통신 기기(100)는 상기 위치 확인 절차가 기 설정된 횟수 이상으로 완료된 경우, 위치 재확인 절차가 성공한 것으로 판단할 수 있다.

[0091] 또한, 이동통신 기기(100)는 위치 확인 정보 회신시간 기준, GPS 정보 및 현재 시간 및 이들의 조합 중 어느 하나를 통해 위치 확인 정보에 대한 교란 방지 검증 절차를 수행할 수 있다.

[0092] 구체적으로, 베이스 스테이션(200)과 이동통신 기기(100)의 메시지를 릴레잉(relaying)해서 이동통신 기기(100)가 실제 위치보다 먼 곳에 위치하는 베이스 스테이션(200)과 통신하도록 하여 이동통신 기기(100)가 자신의 위치를 잘못 알게 하는 공격이 발생할 수 있다. 이를 위해, 본 실시예에서는 이동통신 기기(100)가 시간 제한 기준(timeout)을 적용하여 자신이 위치 확인 요청을 송신한 시점과 베이스 스테이션(200)으로부터 위치 확인 정보를 수신한 시점 간의 시간을 위치 확인 정보 회신시간 기준과 비교하여, 위치 확인 정보에 대한 신뢰성을 검증하는 것이다.

[0093] 또한, 본 실시예는 베이스 스테이션(200)이 GPS 정보와 함께 베이스 스테이션측 현재 시간 정보를 함께 회신하도록 하고, 이동통신 기기(100)는 상술한 GPS 정보 및 베이스 스테이션측 현재 시간을 기초로 위치 확인 정보에 대한 신뢰성을 검증하는 것이다. 예를 들어, 이동통신 기기(100)가 베이스 스테이션의 현재 시간과 동기화된 현재 시간을 베이스 스테이션측 현재 시간과 비교하여 위치 확인 정보에 대한 신뢰성을 검증할 수 있다.

[0094] 추가로, 이동통신 기기(100)는 최소 기준 횟수 이상의 베이스 스테이션(200)으로부터 위치 확인 정보를 수신하여 위치 확인 절차를 수행함에 따라 보안성을 강화할 수 있다.

[0096] 도 7은 본 발명의 일 실시예에 따른 스마트 시티를 위한 위치 확인 방법의 다른 예를 설명하기 위한 흐름도이다. 도 7에 도시된 방법은 예를 들어, 전술한 이동통신 기기(100) 및 베이스 스테이션(200)에 의해 수행될 수 있다. 도시된 흐름도에서는 상기 방법을 복수 개의 단계로 나누어 기재하였으나, 적어도 일부의 단계들은 순서를 바꾸어 수행되거나, 다른 단계와 결합되어 함께 수행되거나, 생략되거나, 세부 단계들로 나뉘어 수행

되거나, 또는 도시되지 않은 하나 이상의 단계가 부가되어 수행될 수 있다.

[0097] 201 단계에서, 베이스 스테이션(200)은 자신을 식별할 수 있는 주소 아이디를 설정할 수 있다.

[0098] 203 단계에서, 베이스 스테이션(200)은 주소 아이디에 대한 비밀키를 발급받을 수 있다.

[0099] 예를 들어, 스마트 시티에서 베이스 스테이션(200)들은 자신의 주소(예를 들어, street 정보)인 "서울시 광진구 능동로 XX", "광진구 능동로 XX", 또는 "능동로 XX"를 자신의 아이디(ID)로 설정하고, 아이디 기반 서명을 위해 키 발급 서버(400)로부터 해당 아이디에 대한 비밀키를 발급받을 수 있다.

[0100] 이때, 아이디 기반 서명방식은 키 발급 서버(400)의 비밀키 관리가 중요하므로, 키 발급 서버(400)를 각 구별로 구비하거나, 각 구 단위 보다 더 작은 영역 단위로 구비하거나, 또는 키 발급 서버(400) 내에서 비밀키 및 공개키를 주기적으로 업데이트 할 수 있다. 드론이나 스마트 카와 같은 이동통신 기기(100)가 위치 기반 서비스를 받기 위해서는 공개키의 무결성이 중요한데, 이를 위해 위치 확인 서비스를 제공하는 앱이나 서비스 소프트웨어를 주기적으로 업데이트하여 최신 파라미터값을 유지하도록 할 수 있다.

[0101] 205 단계 및 207 단계에서, 베이스 스테이션(200)은 위치 확인 메시지, 주소 아이디 및 서명값 중 적어도 하나 이상을 포함하는 위치 확인 정보를 브로드캐스팅할 수 있다. 상기 위치 확인 메시지는 베이스 스테이션의 GPS 정보, 베이스 스테이션측 현재 시간 및 상기 주소 아이디를 포함할 수 있다.

[0102] 도 5를 참고하면, A 영역에 위치하는 복수의 베이스 스테이션(200a, 200b, 200c)은 기 설정된 주기로 위치 확인 정보를 브로드캐스팅하는 것이다.

[0103] 205 단계에서, 베이스 스테이션(200)은 베이스 스테이션의 GPS 정보, 베이스 스테이션측 현재 시간을 주소 아이디에 대해 발급받은 비밀키로 서명하여 상기 서명값을 생성할 수 있다. 본 실시예에서는 디지털 서명 방식 대신 주소 아이디 기반 서명방식을 적용하는 것이다.

[0104] 209 단계에서, 특정 목적지로 이동한 이동통신 기기(100)는 해당 목적지에 위치하는 베이스 스테이션(200)으로부터 위치 확인 정보를 수신할 수 있다.

[0105] 211 단계에서, 이동통신 기기(100)는 목적지에 대응되는 주소 아이디 및 서명값을 기초로 위치 확인 정보를 확인하여 자신의 현재 위치를 확인할 수 있다.

[0106] 도 5를 참고하면, A 영역에 진입한 이동통신 기기(100)가 복수의 베이스 스테이션(200a, 200b, 200c)으로부터 수신한 위치 확인 정보를 기초로 자신의 GPS 정보를 재확인할 수 있는 것이다.

[0107] 상술한 아이디 기반으로 스마트 시티의 베이스 스테이션(200)들이 자신의 주소 아이디를 공개키로 하여, 자신의 GPS 정보를 주기적으로 브로드캐스팅하면, 유효한 공개키를 가진 모든 이동통신 기기(100)는 해당 위치에서 브로드캐스팅 받은 GPS 정보를 통해 자신의 위치를 재확인할 수 있다.

[0108] 본 실시예에서는, 베이스 스테이션(200)이 위치 확인 정보를 브로드캐스팅할 때, GPS 정보와 함께 현재시간을 함께 전송하여 GPS 스푸핑 공격을 막을 수 있도록 할 수 있다. 이를 위해, 베이스 스테이션(200)과 이동통신 기기(100) 간에 현재시간이 정확히 일치 또는 동기화 되어야함은 당연하다 할 것이다. 도 7에서 개시하는 일방향 통신 방식의 위치 확인 방법은 이동통신 기기(100)가 사전에 목적지 베이스 스테이션의 공개키를 저장하여 이동할 필요가 없기 때문에 상대적으로 효율성이 높을 수 있다.

[0110] 도 8은 예시적인 실시예들에서 사용되기에 적합한 컴퓨팅 장치를 포함하는 컴퓨팅 환경(10)을 예시하여 설명하기 위한 블록도이다. 도시된 실시예에 서, 각 컴포넌트들은 이하에 기술된 것 이외에 상이한 기능 및 능력을 가질 수 있고, 이하에 기술된 것 이외에도 추가적인 컴포넌트를 포함할 수 있다.

[0111] 도시된 컴퓨팅 환경(10)은 컴퓨팅 장치(12)를 포함한다. 일 실시예에서, 컴퓨팅 장치(12)는 베이스 스테이션(200)일 수 있다. 또한, 컴퓨팅 장치(12)는 이동통신 기기(100) 또는 위치 확인 서비스 서버(300)일 수 있다.

[0112] 컴퓨팅 장치(12)는 적어도 하나의 프로세서(14), 컴퓨터 판독 가능 저장 매체(16) 및 통신 버스(18)를 포함한다. 프로세서(14)는 컴퓨팅 장치(12)로 하여금 앞서 언급된 예시적인 실시예에 따라 동작하도록 할 수 있다. 예컨대, 프로세서(14)는 컴퓨터 판독 가능 저장 매체(16)에 저장된 하나 이상의 프로그램들을 실행할 수 있다. 상기 하나 이상의 프로그램들은 하나 이상의 컴퓨터 실행 가능 명령어를 포함할 수 있으며, 상기 컴퓨터 실행 가능 명령어는 프로세서(14)에 의해 실행되는 경우 컴퓨팅 장치(12)로 하여금 예시적인 실시예에 따른 동작들을 수행하도록 구성될 수 있다.

[0113] 컴퓨터 판독 가능 저장 매체(16)는 컴퓨터 실행 가능 명령어 내지 프로그램 코드, 프로그램 데이터 및/또는 다른 적합한 형태의 정보를 저장하도록 구성된다. 컴퓨터 판독 가능 저장 매체(16)에 저장된 프로그램(20)은 프로세서(14)에 의해 실행 가능한 명령어의 집합을 포함한다. 일 실시예에서, 컴퓨터 판독 가능 저장 매체(16)는 메모리(랜덤 액세스 메모리와 같은 휘발성 메모리, 비휘발성 메모리, 또는 이들의 적절한 조합), 하나 이상의 자기 디스크 저장 디바이스들, 광학 디스크 저장 디바이스들, 플래시 메모리 디바이스들, 그 밖에 컴퓨팅 장치(12)에 의해 액세스되고 원하는 정보를 저장할 수 있는 다른 형태의 저장 매체, 또는 이들의 적합한 조합일 수 있다.

[0114] 통신 버스(18)는 프로세서(14), 컴퓨터 판독 가능 저장 매체(16)를 포함하여 컴퓨팅 장치(12)의 다른 다양한 컴포넌트들을 상호 연결한다.

[0115] 컴퓨팅 장치(12)는 또한 하나 이상의 입출력 장치(24)를 위한 인터페이스를 제공하는 하나 이상의 입출력 인터페이스(22) 및 하나 이상의 네트워크 통신 인터페이스(26)를 포함할 수 있다. 입출력 인터페이스(22) 및 네트워크 통신 인터페이스(26)는 통신 버스(18)에 연결된다. 입출력 장치(24)는 입출력 인터페이스(22)를 통해 컴퓨팅 장치(12)의 다른 컴포넌트들에 연결될 수 있다. 예시적인 입출력 장치(24)는 포인팅 장치(마우스 또는 트랙패드 등), 키보드, 터치 입력 장치(터치패드 또는 터치스크린 등), 음성 또는 소리 입력 장치, 다양한 종류의 센서 장치 및/또는 촬영 장치와 같은 입력 장치, 및/또는 디스플레이 장치, 프린터, 스피커 및/또는 네트워크 카드와 같은 출력 장치를 포함할 수 있다. 예시적인 입출력 장치(24)는 컴퓨팅 장치(12)를 구성하는 일 컴포넌트로서 컴퓨팅 장치(12)의 내부에 포함될 수도 있고, 컴퓨팅 장치(12)와는 구별되는 별개의 장치로 컴퓨팅 장치(12)와 연결될 수도 있다.

[0116] 이상에서 본 발명의 대표적인 실시예들을 상세하게 설명하였으나, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자는 상술한 실시예에 대하여 본 발명의 범주에서 벗어나지 않는 한도 내에서 다양한 변형이 가능함을 이해할 것이다. 그러므로 본 발명의 권리범위는 설명된 실시예에 국한되어 정해져서는 안 되며, 후술하는 청구범위뿐만 아니라 이 청구범위와 균등한 것들에 의해 정해져야 한다.

부호의 설명

[0117] 10: 컴퓨팅 환경

12: 컴퓨팅 장치

14: 프로세서

16: 컴퓨터 판독 가능 저장 매체

18: 통신 버스

20: 프로그램

22: 입출력 인터페이스

24: 입출력 장치

26: 네트워크 통신 인터페이스

100: 이동통신 기기

110: 아이디 생성부

130: 키 관리부

150: 위치 확인부

200: 베이스 스테이션

210: 키 생성부

230: 위치 생성부

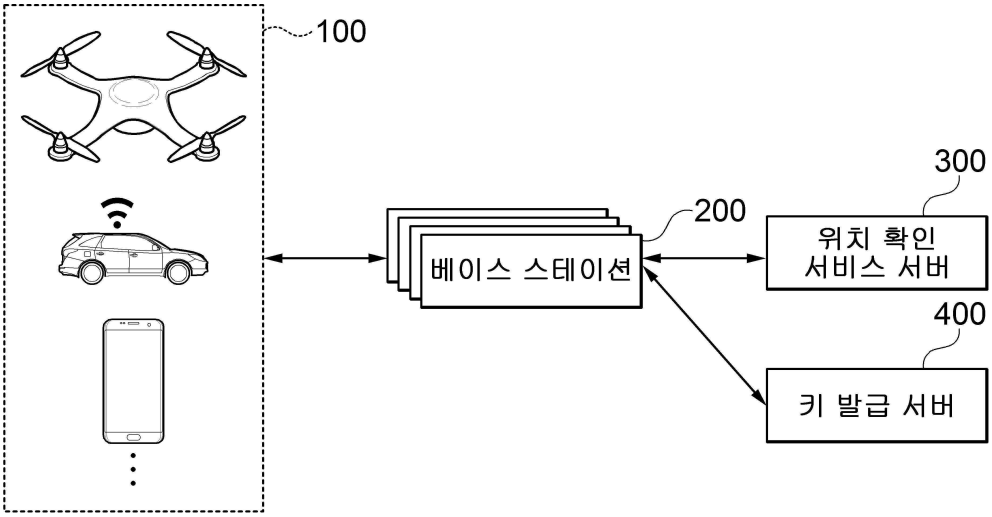
250: 서명 처리부

300: 위치 확인 서비스 서버

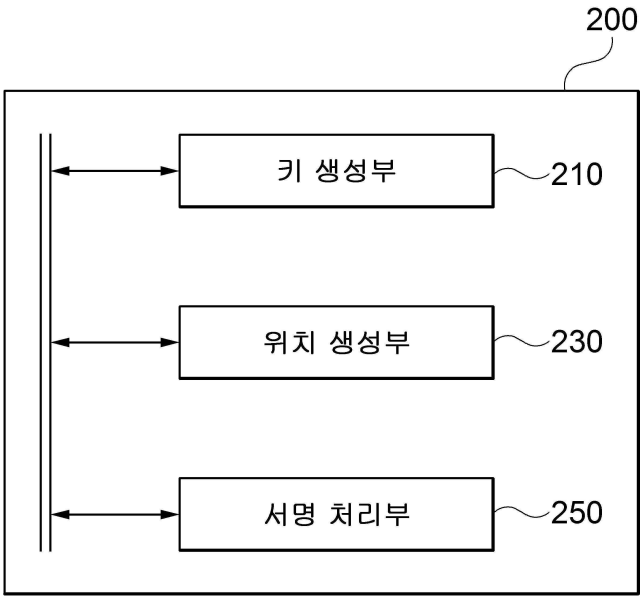
400: 키 발급 서버

도면

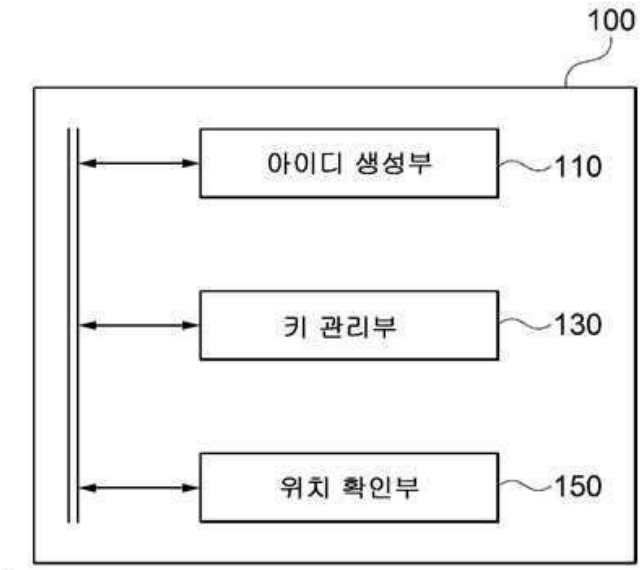
도면1



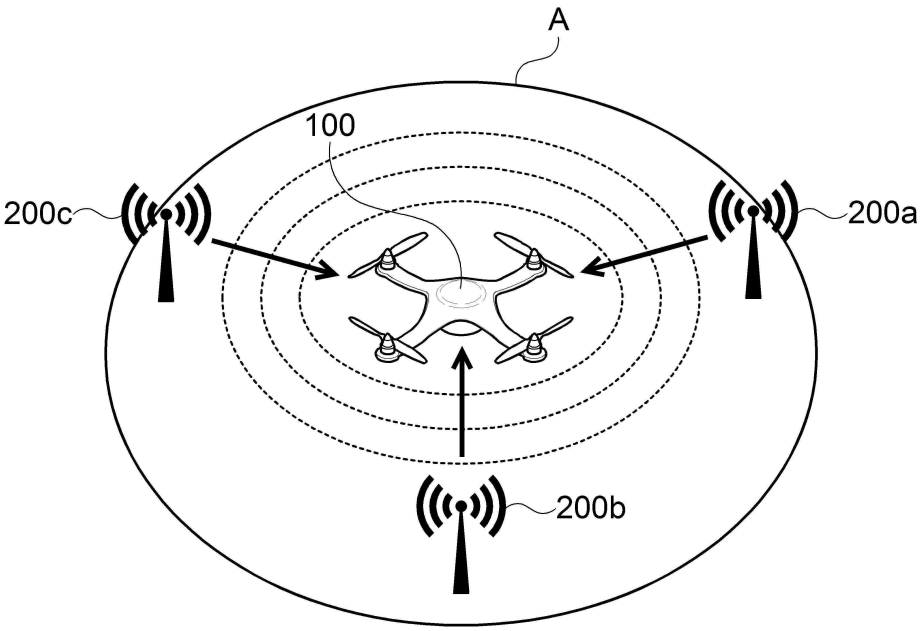
도면2



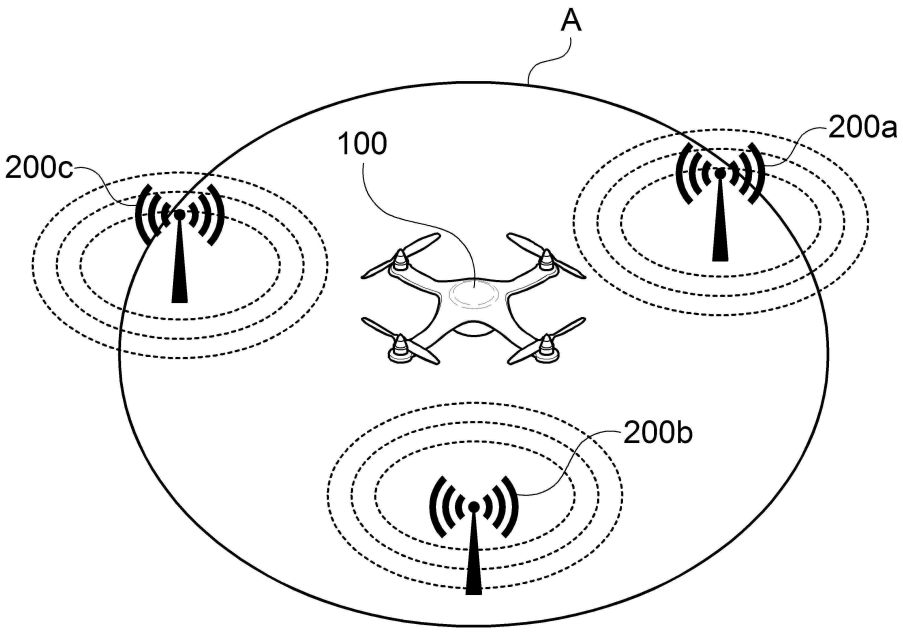
도면3



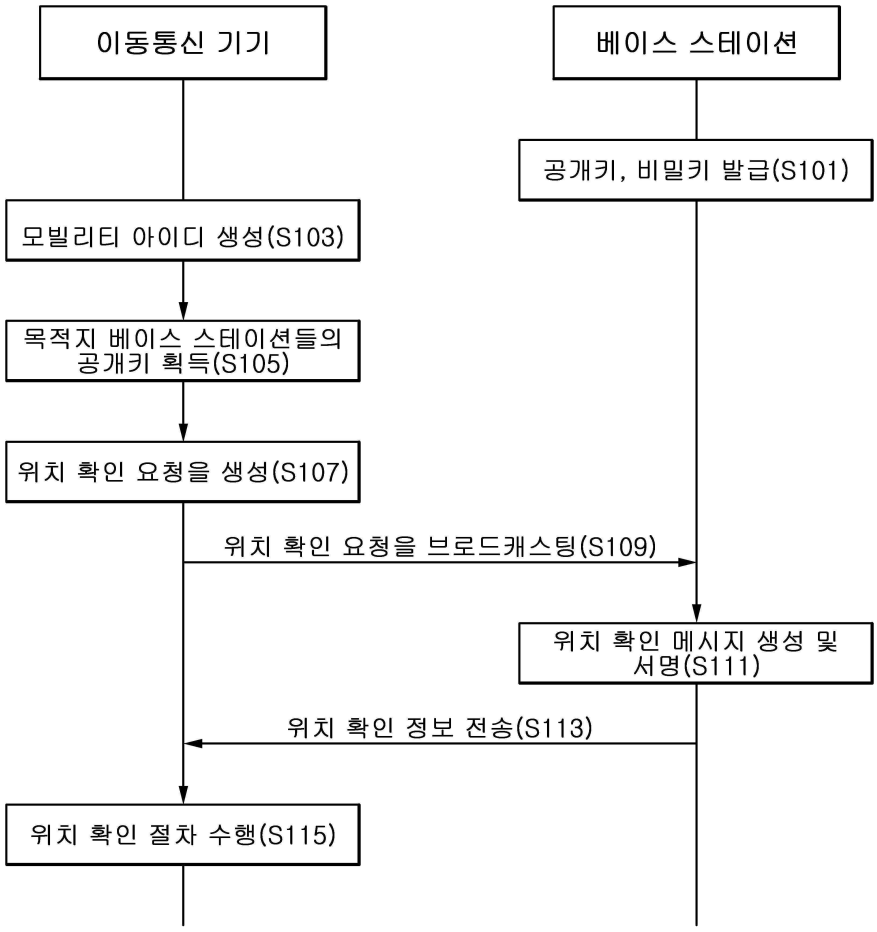
도면4



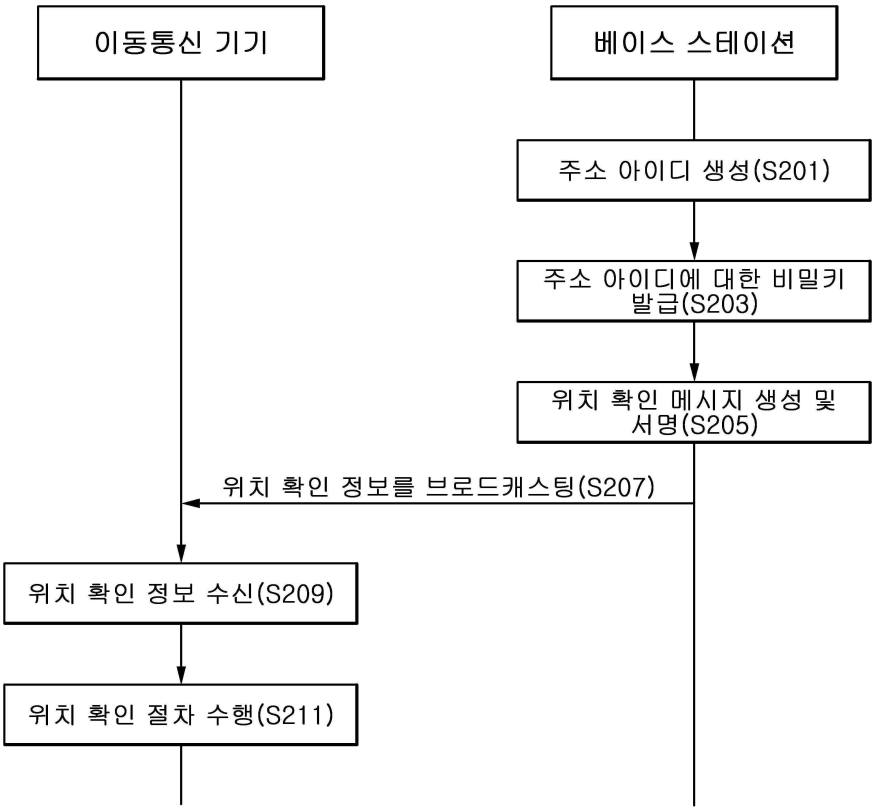
도면5


A
100
200a
200c
200b

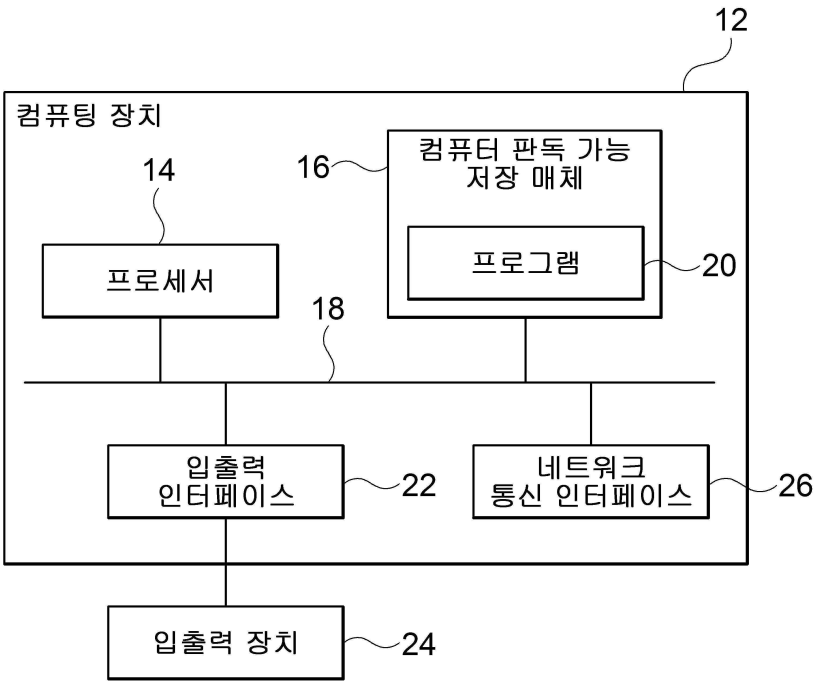
도면6


이동통신 기기
베이스 스테이션
공개키, 비밀키 발급(S101)
모빌리티 아이디 생성(S103)
목적지 베이스 스테이션들의 공개키 획득(S105)
위치 확인 요청을 생성(S107)
위치 확인 요청을 브로드캐스팅(S109)
위치 확인 메시지 생성 및 서명(S111)
위치 확인 정보 전송(S113)
위치 확인 절차 수행(S115)

도면7



도면8



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 청구항 17

【변경전】

자신을 식별할 수 있는 모빌리티 아이디를 생성하기 위한 아이디 생성부;

사전에 목적지에 위치한 유효한 복수의 베이스 스테이션의 공개키들을 수신하여 관리하기 위한 키 관리부; 및

상기 목적지에 도착한 후, 난수값, 상기 모빌리티 아이디 및 위치 확인 요청 메시지를 포함하는 위치 확인 요청을 브로드캐스팅하고, 복수의 베이스 스테이션으로부터 전송되는 위치 확인 정보를 기초로 자신의 현재 위치를 재확인하는 위치 확인부를 포함하며,

상기 키 관리부는, 상기 이동통신 기기의 메모리 사용 제한이 제1 타입인 경우, 상기 공개키들을 블룸 필터(bloom filter)로 구성하여 관리하고,

상기 이동통신 기기의 메모리 사용 제한이 제2 타입인 경우, 상기 공개키들을 테이블 형태로 관리하는 이동통신 기기.

【변경후】

자신을 식별할 수 있는 모빌리티 아이디를 생성하기 위한 아이디 생성부;

사전에 목적지에 위치한 유효한 복수의 베이스 스테이션의 공개키들을 수신하여 관리하기 위한 키 관리부; 및

상기 목적지에 도착한 후, 난수값, 상기 모빌리티 아이디 및 위치 확인 요청 메시지를 포함하는 위치 확인 요청을 브로드캐스팅하고, 복수의 베이스 스테이션으로부터 전송되는 위치 확인 정보를 기초로 자신의 현재 위치를 재확인하는 위치 확인부를 포함하며,

상기 키 관리부는, 이동통신 기기의 메모리 사용 제한이 제1 타입인 경우, 상기 공개키들을 블룸 필터(bloom filter)로 구성하여 관리하고,

상기 이동통신 기기의 메모리 사용 제한이 제2 타입인 경우, 상기 공개키들을 테이블 형태로 관리하는 이동통신 기기.