



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2018-0057468
(43) 공개일자 2018년05월30일

- (51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) H04L 9/08 (2006.01)
H04L 9/30 (2006.01)
(52) CPC특허분류
H04L 9/3263 (2013.01)
H04L 9/08 (2013.01)
(21) 출원번호 10-2017-0006909
(22) 출원일자 2017년01월16일
심사청구일자 2017년01월16일
(30) 우선권주장
1020160155078 2016년11월21일 대한민국(KR)

- (71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
이영경
서울특별시 동대문구 제기로11길 11 (제기동) 102호
이광수
서울특별시 성북구 길음로 119, 221동 902호 (길음동, 길음뉴타운 대우푸르지오아파트)
(74) 대리인
김등용, 김홍석

전체 청구항 수 : 총 9 항

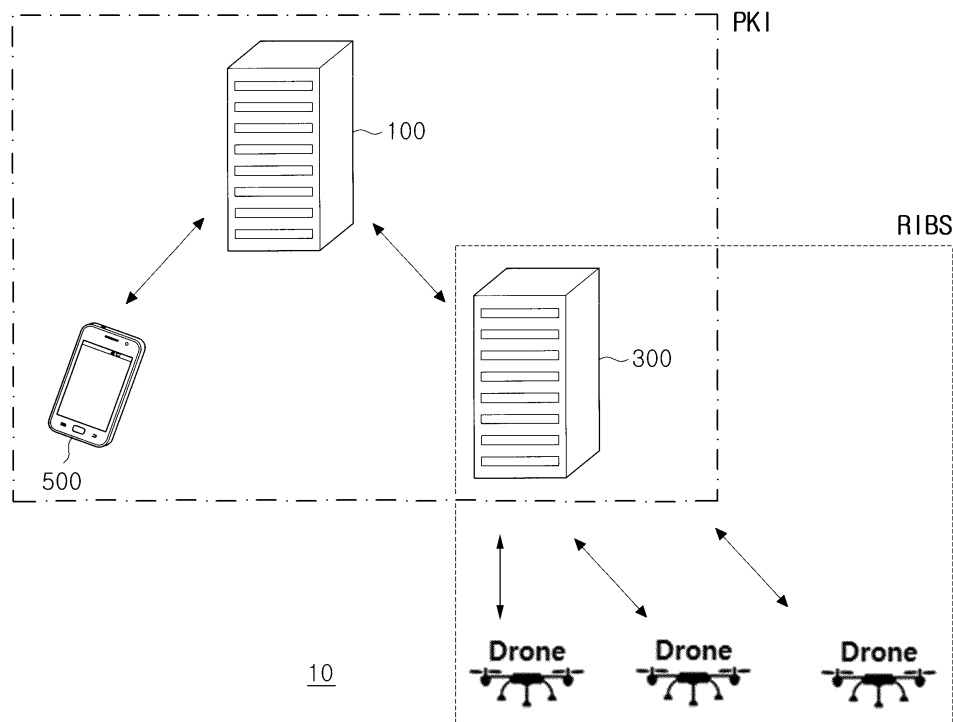
(54) 발명의 명칭 하이브리드 PKI 기반 드론 인증 시스템 및 드론 관리 서버

(57) 요약

드론 인증 시스템이 개시된다. 상기 드론 인증 시스템은 드론 관리 서버와 적어도 하나의 드론을 포함하고, 상기 드론 관리 서버는 상기 드론 관리 서버의 공개키와 서명키 쌍을 생성하고, 상기 공개키를 포함하는 인증서 발급 요청 메시지를 인증 서버로 송신하고, 상기 인증서 발급 요청 메시지에 대응하는 제1 인증서를 상기 서버로부터

(뒷면에 계속)

대표도 - 도1



수신하는 제1 인증서 수신부, 폐기 가능한 ID 기반 서명(Revocable ID-based Signature, RIBS)의 설정 알고리즘을 수행하여 상기 드론 관리 서버의 마스터키와 마스터 공개키 쌍을 생성하고, 상기 제1 인증서로부터 상기 마스터 공개키에 대응하는 제2 인증서를 생성하는 제2 인증서 생성부, RIBS의 개인키 추출 알고리즘을 수행하여 상기 적어도 하나의 드론의 ID에 대한 개인키를 생성하고, 상기 개인키를 상기 적어도 하나의 드론으로 송신하는 개인키 추출부, RIBS의 업데이트키 생성 알고리즘을 수행하여 현재 시간에 대한 업데이트키를 생성하고, 상기 업데이트키를 브로트캐스팅하는 업데이트키 생성부, 및 RIBS의 폐기 알고리즘을 수행하여 갱신된 폐기 리스트를 생성하는 폐기부를 포함한다.

(52) CPC특허분류

H04L 9/0891 (2013.01)

H04L 9/30 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	IITP-2016-R0992-16-1006
부처명	미래창조과학부
연구관리전문기관	정보통신기술진흥센터
연구사업명	대학ICT연구센터육성 지원사업
연구과제명	IoT 보안기술연구
기 여 율	1/1
주관기관	순천향대학교 산학협력단
연구기간	2016.01.01 ~ 2016.12.31

명세서

청구범위

청구항 1

드론 관리 서버와 적어도 하나의 드론을 포함하는 드론 인증 시스템에 있어서,

상기 드론 관리 서버는,

상기 드론 관리 서버의 공개키와 서명키 쌍을 생성하고, 상기 공개키를 포함하는 인증서 발급 요청 메시지를 인증 서버로 송신하고, 상기 인증서 발급 요청 메시지에 대응하는 제1 인증서를 상기 서버로부터 수신하는 제1 인증서 수신부;

폐기 가능한 ID 기반 서명(Revocable ID-based Signature, RIBS)의 설정 알고리즘을 수행하여 상기 드론 관리 서버의 마스터키와 마스터 공개키 쌍을 생성하고, 상기 제1 인증서로부터 상기 마스터 공개키에 대응하는 제2 인증서를 생성하는 제2 인증서 생성부;

RIBS의 개인키 추출 알고리즘을 수행하여 상기 적어도 하나의 드론의 ID에 대한 개인키를 생성하고, 상기 개인키를 상기 적어도 하나의 드론으로 송신하는 개인키 추출부;

RIBS의 업데이트키 생성 알고리즘을 수행하여 현재 시간에 대한 업데이트키를 생성하고, 상기 업데이트키를 브로트캐스팅하는 업데이트키 생성부; 및

RIBS의 폐기 알고리즘을 수행하여 갱신된 폐기 리스트를 생성하는 폐기부를 포함하는,
드론 인증 시스템.

청구항 2

제1항에 있어서,

상기 공개키와 상기 서명키는 PKI(Public Key Infrastructure, 공개키 기반 구조)에서 사용되는 공개키 서명(Public Key Signature)의 공개키와 서명키이고,

상기 제1 인증서는 PKI 기반의 인증서이고,

상기 제2 인증서는 RIBS 기반의 인증서인,

드론 인증 시스템.

청구항 3

제1항에 있어서,

상기 적어도 하나의 드론은 상기 드론 관리 서버로부터 수신된 상기 개인키와 상기 드론 관리 서버에 의해 브로트캐스팅되는 상기 업데이트키를 입력으로 하는 RIBS의 서명키 생성 알고리즘을 수행하여 서명키를 생성하는,

드론 인증 시스템.

청구항 4

제3항에 있어서,

상기 적어도 하나의 드론은 제2 드론 관리 서버에 의해 운용되는 제3 드론과 제1 인증 동작을 수행하고,

상기 제1 인증 동작은

상기 적어도 하나의 드론이 상기 적어도 하나의 드론의 아이디, 상기 제3 드론의 아이디 및 임의의 제1 난수를 상기 제3 드론에게 송신하는 단계;

상기 적어도 하나의 드론이 임의의 제2 난수와 상기 제1 난수에 대한 제1 서명값을 상기 제3 드론으로부터 수신하는 단계;

상기 적어도 하나의 드론이 상기 제1 서명값을 검증하는 단계; 및

상기 적어도 하나의 드론이 상기 제2 난수에 대한 제2 서명값을 생성하고, 상기 제2 서명값을 상기 제3 드론으로 송신하는 단계를 포함하고,

상기 제1 서명값과 상기 제2 서명값은 RIBS의 서명 알고리즘을 통해 생성되고,

상기 적어도 하나의 드론은 RIBS의 검증 알고리즘을 수행하여 상기 제1 서명값을 검증하는, 드론 인증 시스템.

청구항 5

제4항에 있어서,

상기 적어도 하나의 드론은 상기 드론 관리 서버에 의해 운용되는 제2 드론과 제2 인증 동작을 수행하고,

상기 제2 인증 동작은

상기 적어도 하나의 드론이 상기 적어도 하나의 드론의 아이디, 상기 제2 드론의 아이디 및 임의의 제3 난수를 상기 제2 드론에게 송신하는 단계;

상기 제2 드론이 상기 제3 난수에 대한 제3 서명값을 생성하고, 상기 제3 서명값과 임의의 제4 난수를 상기 적어도 하나의 드론으로 송신하는 단계;

상기 적어도 하나의 드론이 상기 제3 서명값을 검증하는 단계;

상기 적어도 하나의 드론이 상기 제4 난수에 대한 제4 서명값을 생성하고, 상기 제4 서명값을 상기 제2 드론으로 송신하는 단계; 및

상기 제2 드론이 상기 제4 서명값을 검증하는 단계를 포함하고,

상기 제3 서명값과 상기 제4 서명값은 RIBS의 서명 알고리즘을 통해 생성되고,

상기 적어도 하나의 드론과 상기 제2 드론 각각은 RIBS의 검증 알고리즘을 수행하여 상기 제3 서명값과 상기 제4 서명값을 각각 검증하는,

드론 인증 시스템.

청구항 6

제5항에 있어서,

상기 적어도 하나의 드론은 사용자 단말과 제3 인증 동작을 수행하고,

상기 제3 인증 동작은

상기 적어도 하나의 드론이 상기 적어도 하나의 드론의 아이디, 상기 사용자 단말의 아이디 및 임의의 제5 난수를 상기 사용자 단말로 송신하는 단계;

상기 적어도 하나의 드론이 임의의 제6 난수와 상기 제5 난수에 대한 제5 서명값을 상기 사용자 단말로부터 수신하는 단계;

상기 적어도 하나의 드론이 상기 제5 서명값을 검증하는 단계; 및

상기 적어도 하나의 드론이 상기 제6 난수에 대한 제6 서명값을 생성하고, 상기 제6 서명값을 상기 사용자 단말

로 송신하는 단계를 포함하고,
 상기 제5 서명값과 상기 제6 서명값은 공개키 서명의 서명 알고리즘을 통해 생성되고,
 상기 적어도 하나의 드론은 공개키 서명의 검증 알고리즘을 통해 상기 제5 서명값을 검증하는,
 드론 인증 시스템.

청구항 7

공개키와 서명키 쌍을 생성하고, 상기 공개키를 포함하는 인증서 발급 요청 메시지를 인증 서버로 송신하고, 상기 인증서 발급 요청 메시지에 대응하는 제1 인증서를 상기 서버로부터 수신하는 제1 인증서 수신부;

폐기 가능한 ID 기반 서명(Revocable ID-based Signature, RIBS)의 설정 알고리즘을 수행하여 마스터키와 마스터 공개키 쌍을 생성하고, 상기 제1 인증서로부터 상기 마스터 공개키에 대응하는 제2 인증서를 생성하는 제2 인증서 생성부;

RIBS의 개인키 추출 알고리즘을 수행하여 적어도 하나의 드론의 ID에 대한 개인키를 생성하고, 상기 개인키를 상기 적어도 하나의 드론으로 송신하는 개인키 추출부;

RIBS의 업데이트키 생성 알고리즘을 수행하여 현재 시간에 대한 업데이트키를 생성하고, 상기 업데이트키를 브로트캐스팅하는 업데이트키 생성부; 및

RIBS의 폐기 알고리즘을 수행하여 갱신된 폐기 리스트를 생성하는 폐기부를 포함하는,
 드론 관리 서버.

청구항 8

제7항에 있어서,

상기 공개키와 상기 서명키는 PKI에서 사용되는 공개키 서명의 공개키와 서명키이고,

상기 제1 인증서는 PKI 기반의 인증서이고,

상기 제2 인증서는 RIBS 기반의 인증서이고,

상기 적어도 하나의 드론은 상기 드론 관리 서버로부터 수신된 상기 개인키와 상기 드론 관리 서버에 의해 브로트캐스팅되는 상기 업데이트키를 입력으로 하는 RIBS의 서명키 생성 알고리즘을 수행하여 서명키를 생성하는,

드론 관리 서버.

청구항 9

제7항에 있어서,

상기 제1 인증서는 상기 공개키를 상기 서버의 비밀키를 이용하여 서명한 서명값을 포함하고,

상기 제2 인증서는 상기 마스터 공개키를 상기 서명키를 이용하여 서명한 서명값을 포함하는,

드론 관리 서버.

발명의 설명

기술 분야

[0001] 본 발명의 개념에 따른 실시 예는 드론 인증 시스템 및 드론 관리 서버에 관한 것으로, 특히 PKI(Public Key Infrastructuer, 공개키 기반 구조)와 폐기 가능한 ID 기반 전자 서명 기법을 이용하여, 드론의 인증용 키 관리 및 키 폐기를 효율적으로 수행할 수 있는 드론 인증 시스템 및 드론 관리 서버에 관한 것이다.

배경 기술

- [0003] 드론의 정의와 구분
- [0004] 국제민간항공기구(International Civil Aviation Organization, ICAO)는 드론을 '사람의 통제 하에 원격으로 조작되는 항공기'로 정의하고 이를 RPA(Remotely Piloted Aircraft)로 지칭한다. 드론은 사용 주체에 따라 군용과 민간(상업)용으로 구분되며, 국내에서는 무인 비행기의 중량에 따라 150kg 이상은 무인 항공기, 150kg 이하의 무인 비행 장치로 구분한다(항공법 제14조제6호). 본 명세서에서 지칭하는 드론은 상업용으로 사용되는 25kg 이하의 드론(무인 비행 장치)를 의미하지만, 본 발명의 권리범위가 반드시 이에 한정되는 것은 아니다.
- [0006] ID기반 암호 시스템(Identity-based Cryptography)
- [0007] ID 기반 암호 시스템은 사용자에게 관련된 임의의 문자열을 공개키로 사용하는 공개키 암호 시스템(Public Key Cryptography)이다. 기존의 공개키 암호 시스템은 임의의 난수를 공개키로 사용하므로 공개키의 소유자를 확인하기 위해 공개키 기반 구조(Public Key Infrastructure, PKI)를 사용하는데, 이를 관리하는데 많은 노력이 필요하다. 이러한 단점을 극복하기 위해 ID기반 암호 시스템이 제안되었으나, ID기반 암호 시스템 역시 마스터키와 사용자의 개인키를 관리하는 키 생성 기관(Private Key Generator, PKG)이 존재한다. 따라서, 일반적인 ID기반 암호 시스템은 PKG가 모든 사용자의 개인키를 생성하기 때문에 PKG를 유지하기 위한 많은 부담이 있다는 단점과 효율적인 사용자 폐기에 대한 문제가 있어 이에 대한 많은 연구가 진행되고 있는 실정이다.
- [0009] ID기반 서명(Identity-based Signature)
- [0010] 공개키 기반 전자 서명이라고도 불리는 공개키 서명(Public Key signature, PKS)은 서명키와 공개키로 구성되며 서명자만 알고 있는 서명키로 메시지에 대한 서명을 생성하고, 서명 검증자는 공개키를 이용하여 서명을 검증한다. ID기반 서명에서 사용자는 이메일(E-mail), 주소(address), IP(Internet Protocol) 주소, 전화 번호 등과 같은 자신의 ID에 대응되는 서명키를 PKG로부터 발급받고, 발급받은 서명키를 이용해 서명을 생성한다. 서명 검증자는 사용자의 ID를 검증키로 사용한다. PKI기반의 전자 서명과 달리 ID기반 서명은 공개키가 사용자의 ID이기 때문에 사용자의 공개키를 검증하기 위한 인증서가 따로 필요하지 않다는 장점을 가지고 있다.
- [0012] 폐기 가능한 ID기반 서명(Revocable Identity-based Signature, RIBS)
- [0013] ID기반 서명에서는 계약 기간이 만료되거나 개인키가 노출된 사용자에게 대한 효율적인 폐기 메커니즘을 제공해야 한다. 폐기 가능한 ID기반 서명 기법은 사용자가 등록 과정에서 PKG로부터 개인키를 발급받고, 이후 주기적으로 PKG가 폐기되지 않은 사용자들에 대한 업데이트키를 발급하여 폐기되지 않은 사용자들만 서명키를 생성할 수 있는 전자 서명 기법이다.
- [0015] 한편, 현재 기업이나 기관에서는 드론 택배 서비스, 드론을 활용한 물리 보안 등의 서비스를 제공하려는 움직임을 보이고 있다. 드론은 향후 다양한 산업 및 서비스 제공에 유용하게 사용될 것으로 예상되며, 드론의 수요 또한 급격히 늘어날 것으로 예상된다. 즉, 다양한 환경에서 운용되는 다수의 드론을 관리하는 기업이나 기관이 늘어날 것으로 예상된다. 드론을 안전하게 운용하는 방법 중 하나는 암호학적 인증 프로토콜을 사용하여 인증된 드론만이 정보 또는 공간에 접근할 수 있도록 사전에 인증하는 것이다. 기존 PKI 기반의 인증서를 드론에 발급하고, 이를 기반으로 인증하는 드론 인증 시스템의 경우, 상술된 환경에서 두 가지 문제점이 있을 수 있다. 첫째, 다수의 드론을 관리하는 관리자(기업이나 기관)가 CA(Certificate Authority)로부터 각각의 드론용 인증서를 발급받고 관리해야 하는 비효율성이다. 둘째, PKI기반의 키 폐기 방식인 CRL(Certificate Revocation List) 체크를 통한 키의 유효성 확인 과정은 인터넷에 항상 연결되어 있지 않은 드론에게는 적용할 수 없는 폐기 방식이다.
- [0017] 따라서, 본 명세서에서는 기존 인프라인 PKI에서 운용 가능한 효율적인 키 관리 및 폐기를 지원하는 인증 시스템

템을 제안한다. 본 명세서에서 제안하는 Hybrid PKI 기반 인증 시스템은 PKI와 폐기 가능한 ID 기반 시스템을 결합한 개념으로, CA, 드론 관리자, 드론 및 사용자로 구성되며, 계층적 구조를 갖는다. 1 계층에서는 CA로부터 드론 관리자 및 사용자가 기존의 PKI 기반 인증서를 발급받는 구조이다. 2 계층에서는 드론 관리자가 CA로부터 발급받은 인증서를 기반으로 폐기 가능한 ID 기반 서명 시스템을 설정하고, PKG 역할로서, 관리하는 드론에게 ID 기반 개인키 및 업데이트키를 발급하는 구조이다.

선행기술문헌

비특허문헌

- [0019] (비특허문헌 0001) J. H. S대 K. Emura, "Revocable Identity-Based Encryption Revisited: Security Model and Construction", PKC 2013. Volume 7778 of the series Lecture Notes in Computer science, pp 216-234, 2013.

발명의 내용

해결하려는 과제

- [0020] 본 발명이 이루고자 하는 기술적인 과제는 PKI 기반 기술과 폐기 가능한 ID 기반 전자 서명 기술을 결합하여, 기업이나 기관에서 운용하는 복수의 드론들 각각의 인증용 키 관리 및 키 폐기를 효율적으로 수행할 수 있는 드론 인증 시스템을 제공하는 것이다.

과제의 해결 수단

- [0022] 본 발명의 실시 예에 따른 드론 인증 시스템은 드론 관리 서버와 적어도 하나의 드론을 포함하고, 상기 드론 관리 서버는 상기 드론 관리 서버의 공개키와 서명키 쌍을 생성하고, 상기 공개키를 포함하는 인증서 발급 요청 메시지를 인증 서버로 송신하고, 상기 인증서 발급 요청 메시지에 대응하는 제1 인증서를 상기 서버로부터 수신하는 제1 인증서 수신부, 폐기 가능한 ID 기반 서명(Revocable ID-based Signature, RIBS)의 설정 알고리즘을 수행하여 상기 드론 관리 서버의 마스터키와 마스터 공개키 쌍을 생성하고, 상기 제1 인증서로부터 상기 마스터 공개키에 대응하는 제2 인증서를 생성하는 제2 인증서 생성부, RIBS의 개인키 추출 알고리즘을 수행하여 상기 적어도 하나의 드론의 ID에 대한 개인키를 생성하고, 상기 개인키를 상기 적어도 하나의 드론으로 송신하는 개인키 추출부, RIBS의 업데이트키 생성 알고리즘을 수행하여 현재 시간에 대한 업데이트키를 생성하고, 상기 업데이트키를 브로트캐스팅하는 업데이트키 생성부, 및 RIBS의 폐기 알고리즘을 수행하여 갱신된 폐기 리스트를 생성하는 폐기부를 포함한다.

- [0023] 또한, 본 발명의 일 실시 예에 의한 드론 관리 서버는 공개키와 서명키 쌍을 생성하고, 상기 공개키를 포함하는 인증서 발급 요청 메시지를 인증 서버로 송신하고, 상기 인증서 발급 요청 메시지에 대응하는 제1 인증서를 상기 서버로부터 수신하는 제1 인증서 수신부, 폐기 가능한 ID 기반 서명(Revocable ID-based Signature, RIBS)의 설정 알고리즘을 수행하여 마스터키와 마스터 공개키 쌍을 생성하고, 상기 제1 인증서로부터 상기 마스터 공개키에 대응하는 제2 인증서를 생성하는 제2 인증서 생성부, RIBS의 개인키 추출 알고리즘을 수행하여 적어도 하나의 드론의 ID에 대한 개인키를 생성하고, 상기 개인키를 상기 적어도 하나의 드론으로 송신하는 개인키 추출부, RIBS의 업데이트키 생성 알고리즘을 수행하여 현재 시간에 대한 업데이트키를 생성하고, 상기 업데이트키를 브로트캐스팅하는 업데이트키 생성부, 및 RIBS의 폐기 알고리즘을 수행하여 갱신된 폐기 리스트를 생성하는 폐기부를 포함한다.

발명의 효과

- [0025] 본 발명의 실시 예에 따른 인증 방법에 의할 경우, 드론을 위한 효율적인 PKI 기반의 인증 시스템을 구축할 수 있으며, 드론 관리자가 관리하는 드론의 인증 및 서명용 키를 각각 CA로부터 발급받을 필요 없이 도메인 내에서

자체적으로 발급 및 폐기할 수 있는 효율적인 시스템을 구축할 수 있다.

- [0026] 또한, 인증서 CRL(Certificate Revocation List)을 매번 확인하는 키 폐기 방식이 아닌 ID 기반의 키 폐기 메커니즘을 사용하기 때문에 드론이 인터넷에 연결되어 있지 않은 상황에서도 인증 절차를 수행할 수 있다.

도면의 간단한 설명

- [0028] 본 발명의 상세한 설명에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 상세한 설명이 제공된다.
- 도 1은 본 발명의 일 실시 예에 의한 인증 시스템을 도시한다.
- 도 2는 도 1에 도시된 인증 시스템 상에서 수행되는 드론 인증 동작을 설명하기 위한 흐름도이다.
- 도 3은 도 1에 도시된 인증 시스템 상에서 발생할 수 있는 인증 동작을 설명하기 위한 예시 도면으로, 사용자가 A사의 드론을 이용한 택배 서비스를 제공받는 상황을 예시한다.
- 도 4는 본 발명의 일 실시 예에 의한 제1 인증 프로토콜을 설명하기 위한 흐름도이다.
- 도 5는 본 발명의 일 실시 예에 의한 제2 인증 프로토콜을 설명하기 위한 흐름도이다.
- 도 6은 도 1에 도시된 드론 관리 서버의 기능 블록도이다.

발명을 실시하기 위한 구체적인 내용

- [0029] 본 명세서에 개시되어 있는 본 발명의 개념에 따른 실시 예들에 대해서 특정한 구조적 또는 기능적 설명은 단지 본 발명의 개념에 따른 실시 예들을 설명하기 위한 목적으로 예시된 것으로서, 본 발명의 개념에 따른 실시 예들은 다양한 형태들로 실시될 수 있으며 본 명세서에 설명된 실시 예들에 한정되지 않는다.
- [0030] 본 발명의 개념에 따른 실시 예들은 다양한 변경들을 가할 수 있고 여러 가지 형태들을 가질 수 있으므로 실시 예들을 도면에 예시하고 본 명세서에서 상세하게 설명하고자 한다. 그러나, 이는 본 발명의 개념에 따른 실시 예들을 특정한 개시 형태들에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물, 또는 대체물을 포함한다.
- [0031] 제1 또는 제2 등의 용어는 다양한 구성 요소들을 설명하는데 사용될 수 있지만, 상기 구성 요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성 요소를 다른 구성 요소로부터 구별하는 목적으로만, 예컨대 본 발명의 개념에 따른 권리 범위로부터 벗어나지 않은 채, 제1 구성 요소는 제2 구성 요소로 명명될 수 있고 유사하게 제2 구성 요소는 제1 구성 요소로도 명명될 수 있다.
- [0032] 어떤 구성 요소가 다른 구성 요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성 요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성 요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성 요소가 다른 구성 요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는 중간에 다른 구성 요소가 존재하지 않는 것으로 이해되어야 할 것이다. 구성 요소들 간의 관계를 설명하는 다른 표현들, 즉 "~사이에"와 "바로 ~사이에" 또는 "~에 이웃하는"과 "~에 직접 이웃하는" 등도 마찬가지로 해석되어야 한다.
- [0033] 본 명세서에서 사용한 용어는 단지 특정한 실시 예를 설명하기 위해 사용된 것으로서, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "포함하다" 또는 "가지다" 등의 용어는 본 명세서에 기재된 특징, 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.
- [0034] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가진다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미를 갖는 것으로 해석되어야 하며, 본 명세서에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0036] 우선, 본 발명에서 이용하는 폐기 가능한 ID기반 서명(Revocable Identity-based Signature, RIBS)에 포함되는 7 개의 알고리즘에 대한 설명은 다음과 같다.

[0037] $_Setup(1^\lambda) \rightarrow msk, mpk, st, RL$

[0038] PKG(Public Key Generator)에서 Setup 알고리즘(설정 알고리즘)을 통해 RIBS 시스템 또는 RIBS 기법에서 사용되는 마스터키(msk), 마스터 공개키(mpk), 사용자 정보(st), 폐기 리스트(RL)를 생성한다.

[0039] $_Extract(ID, msk, st, mpk) \rightarrow sk_{ID}$

[0040] PKG에서 Extract 알고리즘(서명키 추출 알고리즘 또는 개인키 추출 알고리즘)을 통해 사용자의 ID, 마스터키(msk), 사용자 정보(st) 및 마스터 공개키(mpk)를 입력으로 사용자의 ID에 대한 개인키(sk_{ID})를 생성한다.

[0041] $_Updatekeygen(T, RL, msk, st, mpk) \rightarrow uk_T$

[0042] PKG에서 Updatekeygen 알고리즘(업데이트키 생성 알고리즘)을 통해 시간 정보(T), 폐기 리스트(RL), 마스터키(msk), 사용자 정보(st) 및 마스터 비밀키(mpk)를 입력으로 T 시간에 대한 업데이트키(uk_T)를 생성한다.

[0043] $_Singkeygen(uk_T, sk_{ID}, mpk) \rightarrow sik_{ID, T}$

[0044] 사용자는 Singkeygen 알고리즘(서명키 생성 알고리즘)을 통해 업데이트키(uk_T), 개인키(sk_{ID}) 및 마스터 공개키(mpk)를 입력으로 T 시간에 대한 ID기반 서명키($sik_{ID, T}$)를 생성한다.

[0045] $_Sign(sik_{ID, T}, M) \rightarrow \sigma_{ID, T, M}$

[0046] 사용자는 Sign 알고리즘(서명 알고리즘)을 통해 서명키($sik_{ID, T}$)와 메시지(M)를 입력으로 서명($\sigma_{ID, T, M}$)을 생성한다.

[0047] $_Verify(\sigma_{ID, T, M}, M', T', ID', mpk) \rightarrow \{0, 1\}$

[0048] 검증자는 Verify 알고리즘(검증 알고리즘)을 통해 서명($\sigma_{ID, T, M}$), M', T', ID', mpk 를 입력으로 메시지, 시간, ID에 대해 서명이 올바르게 생성된 것인지 확인(검증)한다.

[0049] $_Revoke(ID, T, st, RL) \rightarrow RL'$

[0050] Revoke 알고리즘(폐기 알고리즘)의 경우, PKG에서 폐기할 ID, 폐기되는 시간(T), 사용자 정보(st) 및 폐기 리스트(RL)를 입력으로 업데이트된 폐기 리스트(RL')를 생성한다.

[0052] 이하, 본 명세서에 첨부된 도면들을 참조하여 본 발명의 실시 예들을 상세히 설명한다.

[0054] 도 1은 본 발명의 일 실시 예에 의한 인증 시스템을 도시하고, 도 2는 도 1에 도시된 인증 시스템 상에서 수행되는 드론 인증 동작을 설명하기 위한 흐름도이다.

- [0055] 도 1과 도 2를 참조하면, 드론 인증 시스템, PKI(Public Key Infrastructure, 공개키 기반 구조) 기반 인증 시스템, 하이브리드 PKI 기반 인증 시스템 등으로 명명될 수도 있는 인증 시스템(10)은 서버(100), 드론 관리 서버(300), 사용자 단말(500) 및 복수의 드론들을 포함한다. 또한, 인증 시스템(10)은 계층적 구조를 갖으며, 서버(100), 드론 관리 서버(300) 및 사용자 단말(500)을 포함하는 제1 계층에서는 PKI 기반 인증서가 발급되거나 폐기되며, 드론 관리 서버(300)와 상기 복수의 드론들을 포함하는 제2 계층에서는 드론 관리 서버(300)가 PKI 기반 인증서를 기반으로 폐기 가능한 ID 기반 서명 시스템을 설정하고 PKG 역할을 수행하여 관리하는 드론들에게 ID 기반 개인키 및 업데이트키를 발급하거나 ID 기반 개인키를 폐기한다.
- [0057] 인증 서버, 키 생성 서버, 키 생성 기관(PKG) 등으로 명명될 수도 있는 서버(100)는 신뢰할 수 있는 기관에 의해 운영되는 서버로서, PKI 기반 인증서를 발급하거나 폐기하는 등의 인증서 관리 동작을 수행할 수 있다.
- [0058] 구체적으로, 서버(100)는 드론 관리 서버(300) 또는 사용자 단말(500)로부터 PKI에서 사용되는 공개키 서명(Public Key Signature, PKS)의 공개키(pk)를 포함하는 인증서 발급 요청 메시지를 수신하고, 상기 인증서 발급 요청 메시지에 응답하여 PKI 기반 인증서($Cert_{by\ CA} = \{pk\}_{PKS-sign-CA}$)를 생성하고, 생성된 인증서($Cert_{by\ CA} = \{pk\}_{PKS-sign-CA}$)를 상기 인증서 발급 요청 메시지를 송신한 드론 관리 서버(300) 또는 사용자 단말(500)로 송신할 수 있다.
- [0060] 드론 인증 서버, 드론 관리자 등으로 명명될 수도 있는 드론 관리 서버(300)는 PKI에서 사용되는 공개키 서명(PKS)의 공개키(pk)와 서명키(sk) 쌍을 생성하고, 상기 공개키(pk)를 포함하는 인증서 발급 요청 메시지를 서버(100)로 송신함으로써, 상기 공개키(pk)에 대응하는 PKI 기반 인증서($Cert_{by\ CA} = \{pk\}_{PKS-sign-CA}$)를 서버(100)로부터 수신할 수 있다.
- [0061] 또한, 드론 관리 서버(300)는 드론의 서명키 발급을 위해 폐기 가능한 ID 기반 서명(Revocable ID-based Signature, RIBS)의 Setup 알고리즘(설정 알고리즘)을 수행하여 마스터키(msk)와 마스터 공개키(mpk) 쌍을 생성할 수 있다. 드론 관리 서버(300)는 생성된 마스터 공개키(mpk)에 대한 신뢰를 CA(Certificate Authority, 인증 기관) 또는 서버(100)로부터 발급받은 인증서, 즉 PKI 기반 인증서로 제공해야 한다. 즉, Trust-chain을 제공하기 위해, 드론 관리 서버(300)는 서버(100)로부터 발급받은 PKI 기반 인증서로부터 새로운 RIBS 인증서($Cert_{by\ DM} = \{mpk\}_{PKS-sign-DM}$)를 생성하고, 생성된 RIBS 인증서($Cert_{by\ DM} = \{mpk\}_{PKS-sign-DM}$)를 해당 드론에게 송신할 수 있다. 이때, 서버(100)로부터 수신된 PKI 기반 인증서($Cert_{by\ CA} = \{pk\}_{PKS-sign-CA}$) 역시 해당 드론에게 송신될 수도 있다. 여기서, PKI 기반 인증서에는 드론 관리 서버(300)의 공개키를 서버(100)의 비밀키(개인키 또는 서명키로 명명될 수도 있음)로 서명한 서명값이 포함되어 있는 반면에, RIBS 인증서에는 드론 관리 서버(300)의 마스터 공개키(mpk)를 드론 관리 서버(300)의 서명키(sk)로 서명한 서명값이 포함되어 있다.
- [0062] 또한, 드론 관리 서버(300)는 인증에 사용할 ID 기반 개인키를 드론에게 발급하여야 한다. 드론 관리 서버(300)는 RIBS의 Extract 알고리즘(개인키 추출 알고리즘)을 수행하여 드론의 ID에 대응하는 개인키(sk_{ID})를 생성하고, 생성된 개인키(sk_{ID})를 RIBS 인증서($Cert_{by\ DM}$)와 함께 드론에게 송신한다. 드론은 발급받은 개인키(sk_{ID})와 드론 관리 서버(300)가 브로드캐스팅하는 최신 업데이트키를 입력으로 하는 Signkeygen 알고리즘(서명키 생성 알고리즘)을 주기적으로 또는 비주기적으로 수행하여 현재 시간에 대한 서명키(sk_{ID}, T)를 생성할 수 있다.
- [0063] 드론 관리 서버(300)는 운용하는 드론에 대한 물리적인 도난과 부채널 공격을 통한 키 노출 등의 상황이 발생하는 경우에 드론의 인증용 키를 폐기하여 더 이상 유효하게 인증을 수행하지 못하도록 드론의 개인키를 폐기하여야 한다. 구체적으로, 드론 관리 서버(300)는 인증 기관(CA), 즉 서버(100)를 통하지 않고 자체적으로 RIBS의

폐기 방식을 사용하여 드론의 키를 폐기할 수 있다. 즉, 드론 관리 서버(300)는 주기적으로 또는 비주기적으로 새롭게 폐기할 드론의 ID와 폐기 시간 및 관리하고 있는 폐기 리스트(RL)를 입력으로 하는 RIBS의 Revoke 알고리즘(폐기 알고리즘)을 수행하여 새로운(갱신된 또는 업데이트된) 폐기 리스트(RL')를 생성할 수 있다. 또한, 드론 관리 서버(300)는 RIBS의 업데이트키 생성 알고리즘(Updatekeygen 알고리즘)을 수행하여 현재 시간 T에 대한 업데이트키(uk_T)를 생성하고, 생성된 업데이트키(uk_T)를 브로드캐스팅할 수 있다.

[0065] 도 1에는 단일의 드론 관리 서버(300)만이 도시되어 있으나, 본 발명의 권리범위가 이에 제한되는 것은 아니며, 실시 예에 따라 인증 시스템(10)은 n(n은 2 이상의 자연수) 개의 드론 관리 서버들을 포함할 수 있다. 상기 복수의 드론 관리 서버들 각각은 관리 대상 드론들 각각의 제어, 키 관리, 인증서 발급, 키 폐기 등의 동작을 수행할 수 있다.

[0067] 상기 복수의 드론들은 각각이 복수의 드론들을 포함하는 복수의 드론 그룹들을 포함할 수 있다. 예컨대 제1 드론 그룹은 드론 관리 서버(300) 또는 드론 관리 서버(300)를 실질적으로 운영하는 사람 또는 회사가 운영하는 드론들의 그룹을 의미할 수 있으며, 제2 드론 그룹은 도시되지 않은 제2 드론 관리 서버 또는 상기 제2 드론 관리 서버를 실질적으로 운영하는 사람 또는 회사가 운영하는 드론들의 그룹을 의미할 수 있다.

[0069] 사용자 단말(500)은 PKI에서 사용되는 공개키 기반 전자 서명 또는 공개키 서명(PKS)의 공개키(pk)와 서명키(sk) 쌍을 생성하고, 상기 공개키(pk)를 포함하는 인증서 발급 요청 메시지를 서버(100)로 송신함으로써, 상기 공개키(pk)에 대응하는 PKI 기반 인증서($Cert_{by\ CA} = \{pk\}_{PKS-sign-CA}$)를 서버(100)로부터 수신할 수 있다.

[0070] 도 1에는 단일의 사용자 단말(500)만이 도시되어 있으나, 본 발명의 권리범위가 이에 제한되는 것은 아니며, 실시 예에 따라 인증 시스템(10)은 m(m은 2 이상의 자연수) 개의 사용자 단말들을 포함할 수 있다. 또한, 사용자 단말(500)은 드론을 이용한 서비스를 제공받는 임의의 사용자의 단말을 의미할 수 있다.

[0071] 사용자 단말(500)은 PC(personal computer), 태블릿 PC, 노트북(notebook), 넷-북(net-book), e-리더(e-reader), PDA(personal digital assistant), PMP(portable multimedia player), MP3 플레이어, 또는 MP4 플레이어와 같은 데이터 처리 장치로 구현되거나, 모바일폰(mobile phone), 스마트폰(smart phone) 등과 같은 핸드헬드 장치(handheld device)로 구현될 수 있다.

[0073] 도 3은 도 1에 도시된 인증 시스템 상에서 발생할 수 있는 인증 동작을 설명하기 위한 예시 도면으로, 사용자가 A사의 드론을 이용한 택배 서비스를 제공받는 상황을 예시한다.

[0074] 드론을 이용한 택배 서비스를 제공하는 A사의 제1 드론이 물품을 신고 이동하는 도중에 B사의 제3 드론과 근접하여 비행하는 상황이 발생할 수 있다. 이 경우, 상기 제1 드론과 상기 제3 드론 상호 간에 통신 등을 위한 인증 동작이 수행될 수 있다. 이때 수행되는 인증 동작을 제1 인증(authentication₁)이라 할 수 있다.

[0075] 서로 다른 회사(또는 드론 관리자) 소속의 드론(상기 제1 드론과 상기 제3 드론) 간, 즉 서로 다른 그룹에 속하는 드론들 간의 인증(제1 인증)은 서버(100)로부터 발급받은 드론 관리 서버의 PKI 인증서 검증과 RIBS 인증서 검증을 통해 각 상대방 드론 관리 서버의 마스터 공개키(mpk)를 확인한다. 구체적으로, 서버(100)의 공개키를 이용하여 PKI 인증서가 검증되고, 드론 관리 서버의 공개키를 이용하여 RIBS 인증서가 검증될 수 있다. 검증을 완료한 후에는 RIBS의 서명 알고리즘($sign$)과 검증 알고리즘($verify$)을 이용한 제1 인증 프로토콜을 진행할 수 있다. 상기 제1 인증 프로토콜은 도 4를 통해 상세하게 설명하기로 한다.

[0077] 상기 제1 드론이 물품을 신고 이동하는 도중에 같은 회사, 즉 A사의 다른 드론인 제2 드론과 물품 이동 등을 위한 통신 등을 수행할 필요가 있으며, 이 경우 역시 인증 동작이 수행될 수 있다. 이때 수행되는 인증 동작을 제

2 인증(authentication₂)이라 할 수 있다.

[0078] 동일한 회사(또는 드론 관리 서버) 소속의 드론들(상기 제1 드론과 상기 제2 드론) 간, 즉 동일한 그룹에 속하는 드론들 간의 인증(제2 인증) 시에는 동일한 드론 관리 서버의 마스터 공개키(mpk)를 신뢰하고 있으므로, 서버(100)로부터 발급받은 드론 관리 서버의 인증서 및 RIBS 인증서를 통한 마스터 공개키 검증 절차가 생략되고, RIBS의 서명 알고리즘($sign$)과 검증 알고리즘($verify$)을 이용한 제1 인증 프로토콜을 진행할 수 있다. 상기 제1 인증 프로토콜은 도 4를 통해 상세하게 설명하기로 한다.

[0080] 물품을 배달하는 제1 드론 또는 제2 드론이 미리 정해진 배달 장소에 도착하였을 경우, 사용자의 진위 여부를 판단하기 위하여 드론과 사용자 단말(500) 사이의 인증 동작이 수행되어야 한다. 이때 수행되는 인증 동작을 제3 인증(authentication₃)이라 할 수 있다. 이하에서, 제3 인증에서 인증의 일방 당사자인 상기 제1 드론 또는 상기 제2 드론을 간략하게 드론이라 명명하기로 한다.

[0081] 상기 드론은 드론 관리 서버(300)로부터 발급받은 RIBS 기반 서명키($sk_{ID,T}$)를 사용하고, 사용자 단말(500)은 PKI 기반의 서명키(sk)를 사용하여 상대방을 인증할 수 있다. 사용자 단말(500)은 상기 드론을 관리하는 드론 관리 서버(300)의 PKI 인증서와 RIBS 인증서 검증을 통해 상기 드론이 속한 드론 관리 서버의 마스터 공개키(mpk)를 확인하고, 상기 드론은 사용자 단말(500)의 인증서 검증을 통해 사용자 단말(500)의 공개키(pk)를 확인할 수 있다. 상기 드론과 사용자 단말(500) 각각이 상대방의 인증서 검증을 완료한 후 PKI의 공개키 서명과 RIBS를 이용한 제2 인증 프로토콜을 진행할 수 있다. 상기 제2 인증 프로토콜은 도 5를 통해 상세하게 설명하기로 한다.

[0083] 도 4는 본 발명의 일 실시 예에 의한 제1 인증 프로토콜을 설명하기 위한 흐름도이다.

[0084] 서로 다른 드론 관리 서버 소속인 드론 A(drone_A)와 드론 B(drone_B)가 상호 인증할 때, 드론 A(drone_A)는 드론 A(drone_A)의 아이디(dID_A), 드론 B(drone_B)의 아이디(dID_B) 및 임의의 제1 난수(R₁)를 드론 B(drone_B)에게 송신한다(S110).

[0085] 드론 B(drone_B)는 드론 A(drone_A)로부터 수신한 제1 난수(R₁)를 RIBS 서명키($sk_{dID_B,T}$)로 서명한 서명값($\{R_1\}_{RIBS-sign-drone_B}$)을 생성하고, 생성된 서명값($\{R_1\}_{RIBS-sign-drone_B}$)과 임의의 제2 난수(R₂)를 드론 A(drone_A)로 송신한다(S120). 즉, 드론 B(drone_B)는 RIBS 서명 알고리즘(Sign 알고리즘)을 수행하여 제1 난수(R₁)에 대한 서명값($\{R_1\}_{RIBS-sign-drone_B}$)을 생성하고, 생성된 서명값($\{R_1\}_{RIBS-sign-drone_B}$)과 제2 난수(R₂)를 드론 A(drone_A)로 송신할 수 있다.

[0086] 드론 A(drone_A)는 RIBS 검증 알고리즘(Verify 알고리즘)을 이용하여 드론 B(drone_B)로부터 수신한 서명값($\{R_1\}_{RIBS-sign-drone_B}$)을 검증한다(S130). 이때, 검증에 실패한 경우 프로토콜 진행(인증 동작)이 중단될 수 있다.

[0087] 드론 A(drone_A)가 드론 B(drone_B)의 서명값($\{R_1\}_{RIBS-sign-drone_B}$) 검증을 완료한 경우, 드론 A(drone_A)는 드론 B(drone_B)로부터 수신된 제2 난수(R₂)를 RIBS 서명키($sk_{dID_A,T}$)로 서명한 서명값

($\{R_2\}_{RIBS-sign-drone_A}$)을 생성하고, 생성된 서명값($\{R_2\}_{RIBS-sign-drone_A}$)을 드론 B($drone_B$)로 송신한다(S140). 즉, 드론 A($drone_A$)는 RIBS 서명 알고리즘(Sign 알고리즘)을 수행하여 제2 난수(R_2)에 대한 서명값($\{R_2\}_{RIBS-sign-drone_A}$)을 생성하고, 생성된 서명값($\{R_2\}_{RIBS-sign-drone_A}$)을 드론 B($drone_B$)로 송신할 수 있다.

[0088] 서명값($\{R_2\}_{RIBS-sign-drone_A}$)을 수신한 드론 B($drone_B$)는 RIBS 검증 알고리즘을 이용하여 드론 A($drone_A$)로부터 수신한 서명값($\{R_2\}_{RIBS-sign-drone_A}$)을 검증한다(S150).

[0089] 상술한 과정을 통해 드론 A($drone_A$)와 드론 B($drone_B$) 각각은 상대방을 인증할 수 있다.

[0091] 도 5는 본 발명의 일 실시 예에 의한 제2 인증 프로토콜을 설명하기 위한 흐름도이다.

[0092] 드론(drone)과 사용자 단말(user)이 상호 인증할 때, 드론(drone)은 드론(drone)의 아이디(dID), 사용자 단말(user)의 아이디 또는 사용자 단말(user)의 사용자의 아이디(uID) 및 제1 난수(R_1)를 사용자 단말(user)에게 송신한다(S210).

[0093] 사용자 단말(user)은 드론(drone)으로부터 수신한 제1 난수(R_1)를 PKI 기반의 서명키(sk_{user})로 서명한 서명값($\{R_1\}_{PKS-sign-user}$)을 생성하고, 생성된 서명값($\{R_1\}_{PKS-sign-user}$)과 임의의 제2 난수(R_2)를 드론(drone)에게 송신한다(S220). 즉, 사용자 단말(user)은 공개키 서명(PKS)의 서명 알고리즘(Sign 알고리즘)을 수행하여 제1 난수(R_1)에 대한 서명값($\{R_1\}_{PKS-sign-user}$)을 생성하고, 생성된 서명값($\{R_1\}_{PKS-sign-user}$)을 드론(drone)에게 송신할 수 있다.

[0094] 드론(drone)은 PKI 검증 알고리즘(Verify 알고리즘)을 이용하여 사용자 단말(user)로부터 수신한 서명값($\{R_1\}_{PKS-sign-user}$)을 검증한다(S230). 이때, 검증에 실패한 경우 프로토콜 진행(인증 동작)이 중단될 수 있다.

[0095] 드론(drone)이 사용자 단말(user)의 서명값($\{R_1\}_{PKS-sign-user}$) 검증을 완료한 경우, 드론(drone)은 사용자 단말(user)로부터 수신된 제2 난수(R_2)를 RIBS 서명키($sk_{dID, T}$)로 서명한 서명값($\{R_2\}_{RIBS-sign-drone}$)을 생성하고, 생성된 서명값($\{R_2\}_{RIBS-sign-drone}$)을 사용자 단말(user)로 송신한다(S240). 즉, 드론(drone)은 RIBS의 서명 알고리즘(Sing 알고리즘)을 수행하여 제2 난수(R_2)에 대한 서명값($\{R_2\}_{RIBS-sign-drone}$)을 생성하고, 생성된 서명값($\{R_2\}_{RIBS-sign-drone}$)을 사용자 단말(user)로 송신할 수 있다.

[0096] 서명값($\{R_2\}_{RIBS-sign-drone}$)을 수신한 사용자 단말(700)은 PKS 검증 알고리즘(Verify 알고리즘)을 이용하여 드론(drone)으로부터 수신한 서명값($\{R_2\}_{RIBS-sign-drone}$)을 검증한다(S250).

- [0097] 상술한 과정을 통해 드론(drone)과 사용자 단말(user) 각각은 상대방을 인증할 수 있다.
- [0099] 도 6은 도 1에 도시된 드론 관리 서버의 기능 블록도이다.
- [0100] 드론 관리 서버(300)는 제1 인증서 수신부(310), 제2 인증서 생성부(330), 개인키 추출부(350), 업데이트키 생성부(370) 및 폐기부(390)를 포함한다.
- [0101] 제1 인증서 수신부(310)는 PKI에서 사용되는 공개키 서명(PKS)의 공개키(pk)와 서명키(sk) 쌍을 생성하고, 상기 공개키(pk)를 포함하는 인증서 발급 요청 메시지를 서버(100)로 송신하고, 상기 인증서 발급 요청 메시지에 대응하는 PKI 기반 인증서($Cert_{byCA} = \{pk\}_{PKS-sign-CA}$)를 서버(100)로부터 수신할 수 있다. 실시 예에 따라 PKI 기반 인증서($Cert_{byCA} = \{pk\}_{PKS-sign-CA}$)는 제1 인증서 수신부(310)에 의해 운용되는 드론으로 송신될 수도 있다.
- [0103] 제2 인증서 생성부(330)는 RIBS의 설정 알고리즘(Setup 알고리즘)을 수행하여 마스크(msk)와 마스터 공개키(mpk) 쌍을 생성한다. 또한, 제2 인증서 생성부(330)는 서버(100)로부터 수신된 PKI 기반 인증서($Cert_{byCA} = \{pk\}_{PKS-sign-CA}$)로부터 새로운 RIBS 인증서($Cert_{byDM} = \{mpk\}_{PKS-sign-DM}$)를 생성할 수 있다. 생성된 RIBS 인증서($Cert_{byDM} = \{mpk\}_{PKS-sign-DM}$)는 제2 인증서 생성부(330)에 의해 운용되는 드론으로 송신될 수 있다.
- [0105] 개인키 추출부(350)는 인증에 사용될 ID 기반 개인키를 드론에게 발급한다. 구체적으로 개인키 추출부(350)는 RIBS의 개인키 추출 알고리즘(Extract 알고리즘)을 수행하여 드론의 ID에 대응하는 개인키(sk_{ID})를 생성하고, 생성된 개인키(sk_{ID})를 상기 드론으로 송신할 수 있다. 실시 예에 따라, RIBS 인증서, 개인키 및 PKI 기반 인증서 중 적어도 하나는 제1 인증서 수신부(310), 제2 인증서 생성부(330) 및 개인키 추출부(350) 중 어느 하나에 의해 상기 드론에게 송신될 수도 있다. 또한, 개인키(sk_{ID}) 생성에 필요한 상기 드론의 ID는 상기 드론에 의해 개인키 추출부(350)으로 송신될 수 있다.
- [0107] 업데이트키 생성부(370)는 RIBS의 업데이트키 생성 알고리즘(Updatekeygen 알고리즘)을 수행하여 현재 시간 T에 대한 업데이트키(uk_T)를 생성하고, 생성된 업데이트키(uk_T)를 브로드캐스팅할 수 있다.
- [0109] 폐기부(390)는 주기적으로 또는 비주기적으로 폐기해야 할 ID와 폐기 시간 및 폐기 리스트를 입력으로 하는 RIBS의 폐기 알고리즘(Revoke 알고리즘)을 수행하여 새로운(갱신된 또는 업데이트된) 폐기 리스트(RL')을 생성할 수 있다.
- [0111] 본 발명은 도면에 도시된 실시 예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시 예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

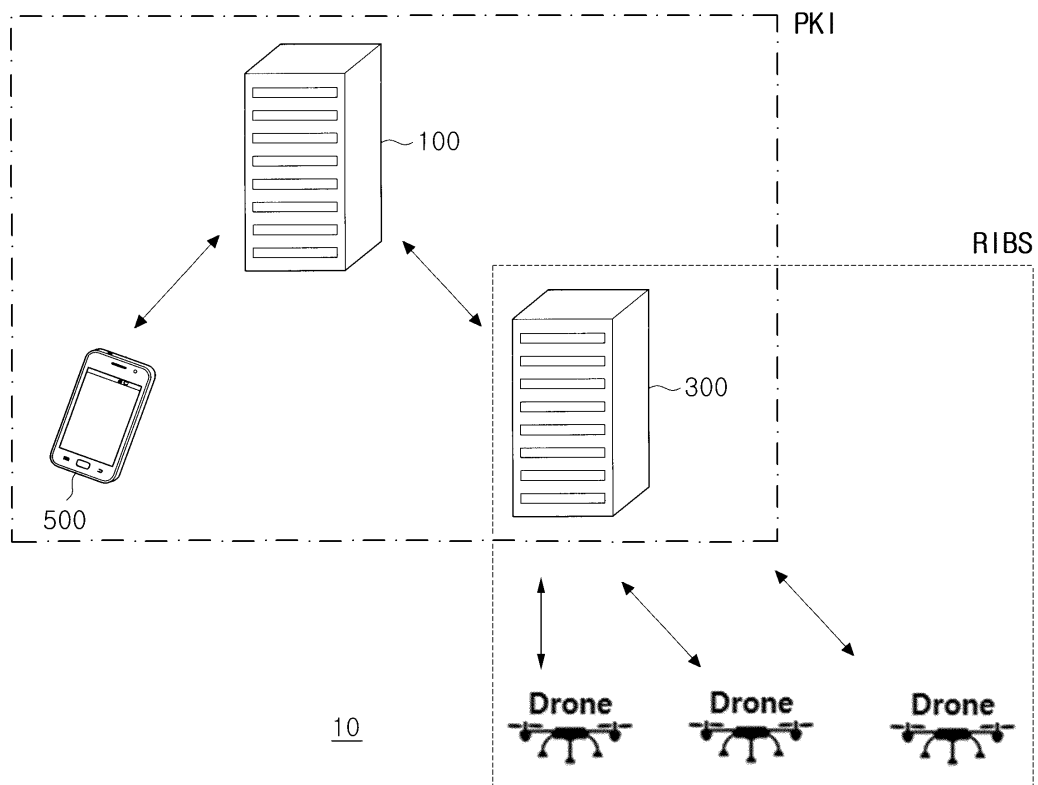
부호의 설명

- [0113] 10 : 인증 시스템

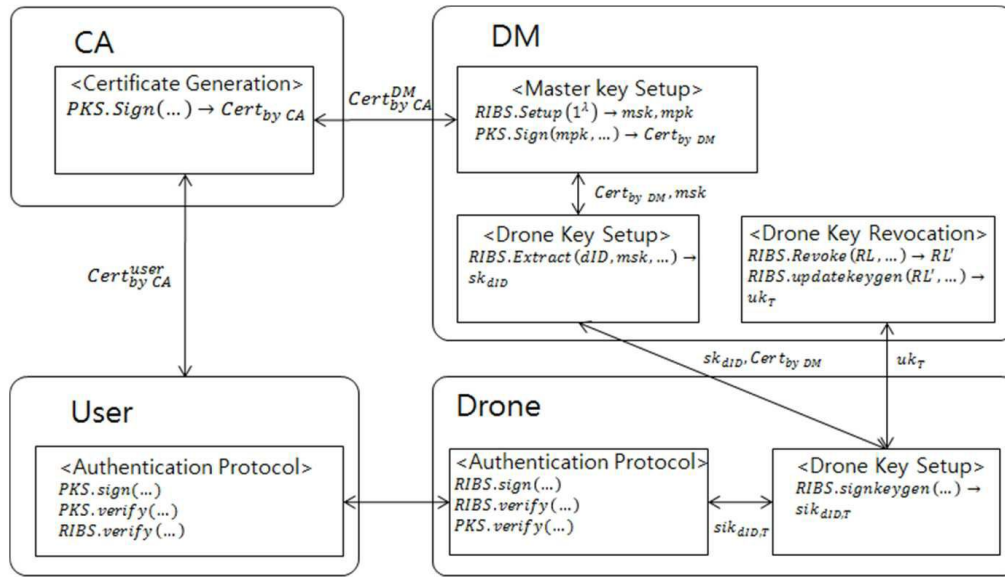
- 100 : 서버
- 300 : 드론 관리 서버
- 310 : 제1 인증서 수신부
- 330 : 제2 인증서 생성부
- 350 : 개인키 추출부
- 370 : 업데이트키 생성부
- 390 : 폐기부
- 500 : 사용자 단말

도면

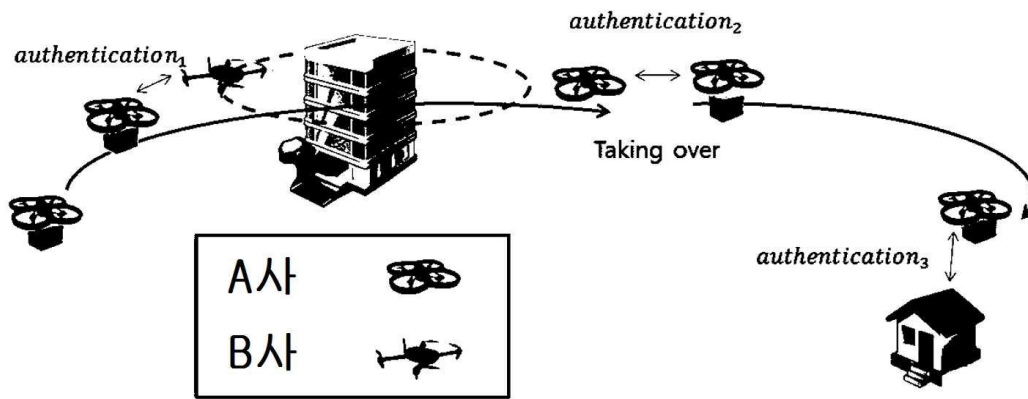
도면1



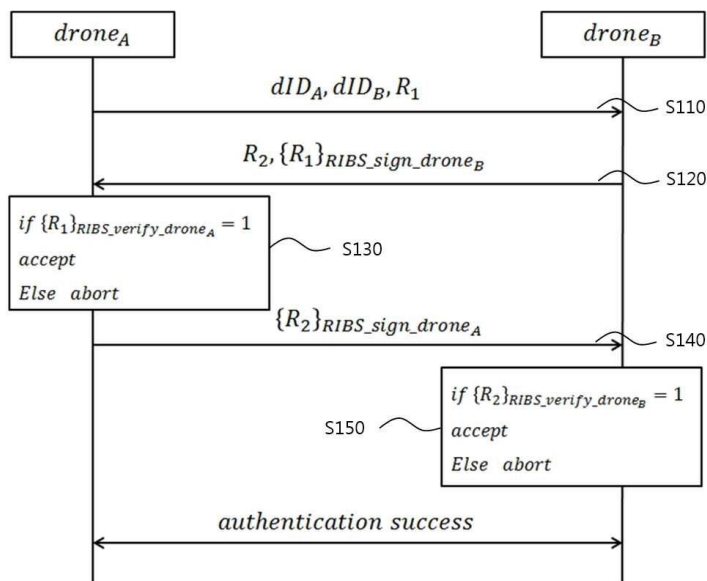
도면2



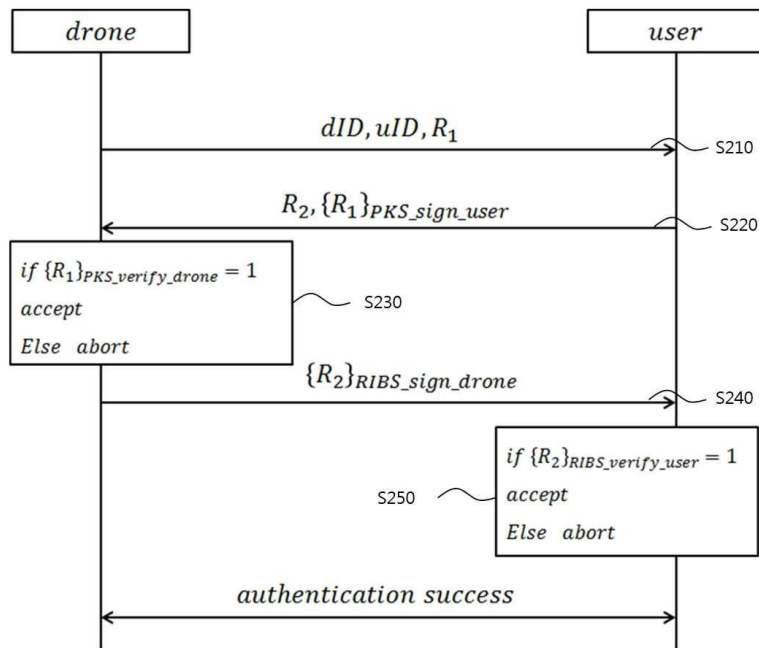
도면3



도면4



도면5



도면6

