(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0043855
(43) 공개일자 2020년04월28일

(51) 국제특허분류(Int. Cl.)
G06F 21/44 (2013.01) *G06F 21/33* (2013.01)
G06F 21/62 (2013.01) *H04L 9/08* (2006.01)
H04L 9/32 (2006.01)
(52) CPC특허분류
G06F 21/44 (2013.01)
G06F 21/33 (2013.01)
(21) 출원번호 10-2018-0124740
(22) 출원일자 2018년10월18일
심사청구일자 없음
기술이전 희망 : 기술양도

전체 청구항 수 : 총 19 항

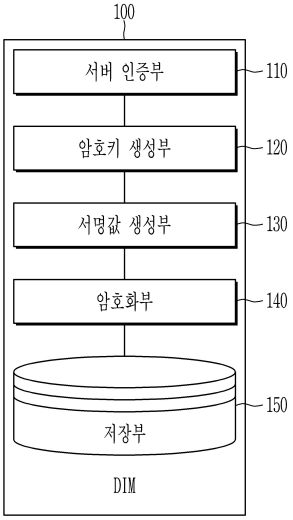
(71) 출원인
한국전자통신연구원
대전광역시 유성구 가정로 218 (가정동)
(72) 발명자
김건우
대전광역시 유성구 지족로 362, 302동 1703호(지족동, 반석마을3단지)
강유성
대전광역시 유성구 대덕대로 598, 803호 (도룡동, 더포엠2)
(뒷면에 계속)
(74) 대리인
팬코리아특허법인

(54) 발명의 명칭 **DIM을 이용한 드론 인증 방법 및 장치**

(57) 요 약

드론을 관리하는 서버로부터, 서버의 인증서를 포함하는 드론 인증 요구를 수신하는 단계, 공인 인증 기관의 공개키를 이용하여 서버의 인증서를 검증하는 단계, 그리고 서버의 인증서가 검증되면, 서버의 인증서로부터 추출된 공개키에 기반하여 생성되는 제1 비밀값에 기반하여, 서버와 드론 간의 통신을 위한 암호키를 생성하는 단계를 포함하는 드론 인증 방법과, 위 방법을 사용하여 인증을 수행하는 드론 식별 모듈, 및 무인 비행 장치가 제공된다.

대 표 도 - 도3



(52) CPC특허분류
G06F 21/62 (2013.01)
H04L 9/0825 (2013.01)
H04L 9/0869 (2013.01)
H04L 9/3263 (2013.01)
H04L 2209/80 (2013.01)

(72) 발명자
김주한
대전광역시 유성구 노은로 353, 305동 1803호 (하기동, 송림마을아파트3단지)
김익균
대전광역시 유성구 대덕대로 594, 904호 (도룡동, 타워코리아나)
진승헌
대전광역시 서구 청사서로 65, 109동 1005호 (월평동, 한아름아파트)

이 발명을 지원한 국가연구개발사업
과제고유번호 1711061026
부처명 과학기술정보통신부
연구관리전문기관 한국연구재단
연구사업명 무인이동체 미래선도핵심기술개발사업
연구과제명 저고도 무인비행장치 교통관리체계 보안기술 및 불법 행위 억제 기술 개발
기 여 율 1/1
주관기관 한국전자통신연구원
연구기간 2017.05.01~2021.12.31

명 세 서

청구범위

청구항 1

드론의 인증 방법으로서,

상기 드론을 관리하는 서버로부터, 상기 서버의 인증서를 포함하는 드론 인증 요구를 수신하는 단계,

공인 인증 기관의 공개키를 이용하여 상기 서버의 인증서를 검증하는 단계, 그리고

상기 서버의 인증서가 검증되면, 상기 서버의 인증서로부터 추출된 공개키에 기반하여 생성되는 제1 비밀값에 기반하여, 상기 서버와 상기 드론 간의 암호 통신을 위한 암호키를 생성하는 단계

를 포함하고,

상기 제1 비밀값은 상기 드론의 인증서로부터 추출된 상기 드론의 공개키에 기반하여 상기 서버에 의해 생성되는 제2 비밀값과 동일하고, 상기 암호키는 상기 제2 비밀값에 기반하여 상기 서버에 의해 생성되는 암호키와 동일한, 드론 인증 방법.

청구항 2

제1항에서,

상기 서버와의 암호 통신을 위한 상기 암호키를 생성하는 단계는,

제1 난수를 생성하는 단계, 그리고

상기 제1 비밀값, 상기 제1 난수, 및 상기 서버에 의해 생성된 제2 난수를 키 유도 함수의 변수로서 사용하여 상기 암호키를 생성하는 단계

를 포함하고,

상기 제2 난수는 상기 드론 인증 요구에 포함되는, 드론 인증 방법.

청구항 3

제2항에서,

상기 키 유도 함수는 해시 함수인, 드론 인증 방법.

청구항 4

제1항에서,

상기 드론의 개인키와 상기 서버의 공개키를 사용하여 상기 제1 비밀값을 생성하는 단계

를 더 포함하는 드론 인증 방법.

청구항 5

제4항에서,

상기 서버의 공개키는 상기 서버의 개인키와 타원 곡선 암호 알고리즘의 베이스 포인트의 곱이고, 상기 제1 비밀값은 상기 드론의 개인키와 상기 서버의 공개키의 곱인, 드론 인증 방법.

청구항 6

제1항에서,

제1 난수를 생성하는 단계,

상기 드론의 아이디 및 상기 드론에 연결된 드론 식별 모듈의 고유 식별 정보에 기반하여 상기 드론의 드론 식

별 정보를 생성하는 단계, 그리고

상기 제1 난수, 상기 드론 식별 정보, 및 상기 드론의 인증서를 상기 서버에게 전송하는 단계

를 더 포함하는 드론 인증 방법.

청구항 7

제1항에서,

상기 드론의 아이디와 상기 드론에 연결된 드론 식별 모듈의 고유 식별 정보를 바탕으로 상기 드론의 드론 식별 정보의 서명값을 생성하는 단계, 그리고

상기 드론의 아이디, 상기 고유 식별 정보, 및 상기 서명값을 주기적으로 상기 서버에게 송신하는 단계

를 더 포함하고,

상기 서명값은 상기 드론을 식별하기 위해서 상기 서버에 의해 사용되는, 드론 인증 방법.

청구항 8

제7항에서,

상기 드론의 아이디, 상기 고유 식별 정보, 및 상기 서명값을 주기적으로 상기 서버에게 송신하는 단계는,

상기 드론의 아이디, 상기 고유 식별 정보, 및 상기 서명값을 상기 암호키를 사용하여 암호화하는 단계

를 포함하는, 드론 인증 방법.

청구항 9

드론 식별 모듈로서,

프로세서, 메모리, 및 인터페이스 장치를 포함하고,

상기 프로세서는 상기 메모리에 저장된 프로그램을 실행하여,

드론으로부터, 상기 드론을 관리하는 서버의 인증서를 포함하는 드론 인증 요구와, 상기 드론의 아이디를 상기 인터페이스 장치를 통해 수신하는 단계,

공인 인증 기관의 공개키를 이용하여 상기 서버의 인증서를 검증하는 단계, 그리고

상기 서버의 인증서가 검증되면, 상기 서버의 인증서로부터 추출된 공개키에 기반하여 생성되는 제1 비밀값에 기반하여, 상기 서버와 상기 드론 간의 암호 통신을 위한 암호키를 생성하는 단계

를 수행하고,

상기 제1 비밀값은 상기 드론의 인증서로부터 추출된 공개키에 기반하여 상기 서버에 의해 생성되는 제2 비밀값과 동일하고, 상기 암호키는 상기 제2 비밀값으로부터 상기 서버에 의해 생성되는 암호키와 동일한, 드론 식별 모듈.

청구항 10

제9항에서,

상기 프로세서는 상기 서버와 상기 드론 간의 암호 통신을 위한 상기 암호키를 생성하는 단계를 수행할 때,

제1 난수를 생성하는 단계, 그리고

상기 제1 비밀값, 상기 제1 난수, 및 상기 서버에 의해 생성된 제2 난수를 키 유도 함수의 변수로서 사용하여 상기 암호키를 생성하는 단계

를 수행하고,

상기 제2 난수는 상기 드론 인증 요구에 포함되는, 드론 식별 모듈.

청구항 11

제10항에서,

상기 키 유도 함수는 해시 함수인, 드론 식별 모듈.

청구항 12

제9항에서,

상기 프로세서는 상기 프로그램을 실행하여,

상기 드론의 개인키와 상기 서버의 공개키를 사용하여 상기 제1 비밀값을 생성하는 단계

를 더 수행하는, 드론 식별 모듈.

청구항 13

제12항에서,

상기 서버의 공개키는 상기 서버의 개인키와 타원 곡선 암호 알고리즘의 베이스 포인트의 곱이고, 상기 제1 비밀값은 상기 드론의 개인키와 상기 서버의 공개키의 곱인, 드론 식별 모듈.

청구항 14

제9항에서,

상기 프로세서는 상기 프로그램을 실행하여,

제1 난수를 생성하는 단계,

상기 드론의 아이디 및 상기 드론에 연결된 드론 식별 모듈의 고유 식별 정보에 기반하여 상기 드론의 드론 식별 정보를 생성하는 단계, 그리고

상기 제1 난수, 상기 드론 식별 정보, 및 상기 드론의 인증서를 상기 서버에게 전송하는 단계

를 더 수행하는, 드론 식별 모듈.

청구항 15

제9항에서,

상기 드론의 아이디와 상기 드론 식별 모듈에 미리 저장된 고유 식별 정보를 바탕으로 상기 드론의 드론 식별 정보의 서명값을 생성하는 단계, 그리고

상기 드론의 아이디, 상기 고유 식별 정보, 및 상기 서명값을 주기적으로 상기 서버에게 송신하는 단계

를 더 포함하고,

상기 서명값은 상기 드론을 식별하기 위해서 상기 서버에 의해 사용되는, 드론 식별 모듈.

청구항 16

제15항에서,

상기 프로세서는 상기 드론의 아이디, 상기 고유 식별 정보, 및 상기 서명값을 주기적으로 상기 서버에게 송신하는 단계를 수행할 때,

상기 드론의 아이디, 상기 고유 식별 정보, 및 상기 서명값을 상기 암호키를 사용하여 암호화하는 단계

를 수행하는, 드론 식별 모듈.

청구항 17

무인 비행 장치로서,

프로세서, 메모리, 상기 무인 비행 장치를 관리하는 서버와의 통신을 위한 무선 통신부, 및 식별 모듈과의 연결

을 위한 인터페이스 장치를 포함하고,

상기 프로세서는 상기 메모리에 저장된 프로그램을 실행하여,

상기 서버로부터 상기 무선 통신부를 통해 상기 서버의 인증서를 포함하는 인증 요구를 수신하고, 상기 인터페이스 장치를 통해 상기 인증 요구 및 상기 무인 비행 장치의 아이디를 상기 식별 모듈에게 전달하는 단계,

상기 식별 모듈에 의해 상기 서버의 인증서가 검증되면, 상기 서버에게 상기 무선 통신부를 통해 상기 무인 비행 장치의 인증서, 상기 무인 비행 장치의 식별 정보, 제1 난수를 송신하는 단계, 그리고

상기 서버에게 상기 무선 통신부를 통해, 상기 드론 식별 모듈에 의해 상기 서버의 인증서에 기반하여 생성된 암호키를 사용하여 암호화된 데이터를 송신하는 단계

를 수행하고,

상기 암호키는 상기 드론 인증서 및 상기 제1 난수에 기반하여 상기 서버에 의해 생성되는 암호키와 동일한, 무인 비행 장치.

청구항 18

제17항에서,

상기 암호키는 상기 식별 모듈에 의해 생성된 비밀값, 상기 제1 난수, 및 상기 인증 요구에 포함된 제2 난수의 곱이고, 상기 비밀값은 상기 서버의 인증서로부터 추출된 상기 서버의 공개키와 상기 무인 비행 장치의 개인키의 곱인, 무인 비행 장치.

청구항 19

제18항에서,

상기 프로세서는 상기 프로그램을 실행하여,

상기 무인 비행 장치의 아이디, 상기 식별 모듈의 고유 식별 정보, 및 상기 무인 비행 장치의 아이디 및 상기 고유 식별 정보를 바탕으로 생성된 상기 무인 비행 장치의 식별 정보의 서명값을 상기 서버에게 상기 무선 통신부를 통해 주기적으로 송신하는 단계

를 더 수행하는, 무인 비행 장치.

발명의 설명

기 술 분 야

[0001] 본 기재는 DIM을 이용하여 드론을 인증하는 방법 및 장치에 관한 것이다.

배 경 기 술

[0002] 최근 소형 무인비행장치(드론)이 다양한 분야에서 활용되고 있지만, 드론을 이용한 불법 행위도 증가하고 있다. 드론이 불법 행위에 악용되는 것을 방지하기 위해 드론의 비행 허가제가 시행되었지만, 허가되지 않은 드론의 비행 사례도 발생하고 있다. 따라서 드론의 비행 중에 허가여부를 판단하는 것이 필요하다. 또한, 군사용 드론과 같은 특수 목적 드론은 주기적으로 인증되어야 하고, 드론에서 전송되는 데이터가 암호화되어야 한다. 이를 위해 드론과 드론 관리 서버 사이의 상호 인증 기술 및 암호키 생성 기술이 요구된다. 그리고 드론에서 송신되는 식별 정보가 올바른 정보인지 검증될 필요가 있다.

[0003] 종래 인터넷에서 PC와 서버 사이의 SSL/TLS 핸드쉐이크 프로토콜과 같은 인증 및 키생성 프로토콜은, 교환되는 메시지의 종류가 많고, 통신 경로도 다양하며, 키 생성 과정이 다수의 단계로 나뉘어져 있어서 사물인터넷 장치로 분류되는 드론에는 적합하지 않다. 예를 들어, 인터넷 분야의 인증 프로토콜에서, 클라이언트는 서버에게 먼저 상호인증을 위한 시작 메시지를 송신하기 때문에, 각 통신 경로마다 하나의 메시지가 서버로 송신되는데, 이는 드론의 통신환경을 고려할 때 적합하지 않다. 또한, 인터넷 분야의 키 생성 프로토콜에서, 클라이언트는 암호키 생성을 위한 비밀값을 일방적으로 생성한 후 서버의 공개키로 암호화하여 서버에게 전달하지만, 드론과 드론 관리 서버가 각각 동일한 방식으로 비밀값을 유도하고 이로부터 암호키를 생성하는 방식이 드론 시스템에 더 적합하다. 또한, 종래 드론을 식별하기 위해 드론 기체에 저장되어 있는 드론 ID(즉, 비행체 ID)가 드론 식별

정보로서 사용되었지만, 이는 해킹에 취약하고, 식별 정보의 복제가 용이하다는 단점을 갖는다. 따라서 불법적으로 제작된 드론이 식별 정보의 해킹 및 복제를 통해 합법 드론으로 위장하여도 이를 식별하기 어렵다.

발명의 내용

해결하려는 과제

[0004] 한 실시예는 드론 식별 모듈을 이용한 드론 인증 방법을 제공한다.

[0005] 다른 실시예는 드론 인증을 수행하는 드론 식별 모듈을 제공한다.

[0006] 또 다른 실시예는 드론 식별 모듈을 이용하여 드론 관리 서버와의 인증을 수행하는 무인 비행 장치를 제공한다.

과제의 해결 수단

[0007] 한 실시예에 따르면 드론의 인증 방법이 제공된다. 상기 드론 인증 방법은, 드론을 관리하는 서버로부터, 서버의 인증서를 포함하는 드론 인증 요구를 수신하는 단계,

[0008] 공인 인증 기관의 공개키를 이용하여 서버의 인증서를 검증하는 단계, 그리고 서버의 인증서가 검증되면, 서버의 인증서로부터 추출된 공개키에 기반하여 생성되는 제1 비밀값에 기반하여, 서버와 드론 간의 암호 통신을 위한 암호키를 생성하는 단계를 포함하고, 제1 비밀값은 드론의 인증서로부터 추출된 드론의 공개키에 기반하여 서버에 의해 생성되는 제2 비밀값과 동일하고, 암호키는 제2 비밀값에 기반하여 서버에 의해 생성되는 암호키와 동일하다.

[0009] 상기 드론 인증 방법에서 서버와의 암호 통신을 위한 암호키를 생성하는 단계는, 제1 난수를 생성하는 단계, 그리고 제1 비밀값, 제1 난수, 및 서버에 의해 생성된 제2 난수를 키 유도 함수의 변수로서 사용하여 암호키를 생성하는 단계를 포함하고, 제2 난수는 드론 인증 요구에 포함될 수 있다.

[0010] 상기 드론 인증 방법에서 키 유도 함수는 해시 함수일 수 있다.

[0011] 상기 드론 인증 방법은, 드론의 개인키와 서버의 공개키를 사용하여 제1 비밀값을 생성하는 단계를 더 포함할 수 있다.

[0012] 상기 드론 인증 방법에서 서버의 공개키는 서버의 개인키와 타원 곡선 암호 알고리즘의 베이스 포인트의 곱이고, 제1 비밀값은 드론의 개인키와 서버의 공개키의 곱일 수 있다.

[0013] 상기 드론 인증 방법은, 제1 난수를 생성하는 단계, 드론의 아이디 및 드론에 연결된 드론 식별 모듈의 고유 식별 정보에 기반하여 드론의 드론 식별 정보를 생성하는 단계, 그리고 제1 난수, 드론 식별 정보, 및 드론의 인증서를 서버에게 전송하는 단계를 더 포함할 수 있다.

[0014] 상기 드론 인증 방법은, 드론의 아이디와 드론에 연결된 드론 식별 모듈의 고유 식별 정보를 바탕으로 드론의 드론 식별 정보의 서명값을 생성하는 단계, 그리고 드론의 아이디, 고유 식별 정보, 및 서명값을 주기적으로 서버에게 송신하는 단계를 더 포함하고, 서명값은 드론을 식별하기 위해서 서버에 의해 사용될 수 있다.

[0015] 상기 드론 인증 방법에서 드론의 아이디, 고유 식별 정보, 및 서명값을 주기적으로 서버에게 송신하는 단계는, 드론의 아이디, 고유 식별 정보, 및 서명값을 암호키를 사용하여 암호화하는 단계를 포함할 수 있다.

[0016] 다른 실시예에 따르면 드론 식별 모듈이 제공된다. 상기 드론 식별 모듈은, 프로세서, 메모리, 및 인터페이스 장치를 포함하고, 프로세서는 메모리에 저장된 프로그램을 실행하여, 드론으로부터, 드론을 관리하는 서버의 인증서를 포함하는 드론 인증 요구와, 드론의 아이디를 인터페이스 장치를 통해 수신하는 단계, 공인 인증 기관의 공개키를 이용하여 서버의 인증서를 검증하는 단계, 그리고 서버의 인증서가 검증되면, 서버의 인증서로부터 추출된 공개키에 기반하여 생성되는 제1 비밀값에 기반하여, 서버와 드론 간의 암호 통신을 위한 암호키를 생성하는 단계를 수행하고, 제1 비밀값은 드론의 인증서로부터 추출된 공개키에 기반하여 서버에 의해 생성되는 제2 비밀값과 동일하고, 암호키는 제2 비밀값으로부터 서버에 의해 생성되는 암호키와 동일하다.

[0017] 상기 드론 식별 모듈에서 프로세서는 서버와 드론 간의 암호 통신을 위한 암호키를 생성하는 단계를 수행할 때, 제1 난수를 생성하는 단계, 그리고 제1 비밀값, 제1 난수, 및 서버에 의해 생성된 제2 난수를 키 유도 함수의 변수로서 사용하여 암호키를 생성하는 단계를 수행하고, 제2 난수는 드론 인증 요구에 포함될 수 있다.

[0018] 상기 드론 식별 모듈에서 키 유도 함수는 해시 함수일 수 있다.

[0019] 상기 드론 식별 모듈에서 프로세서는 프로그램을 실행하여, 드론의 개인키와 서버의 공개키를 사용하여 제1 비밀값을 생성하는 단계를 더 수행할 수 있다.

[0020] 상기 드론 식별 모듈에서 서버의 공개키는 서버의 개인키와 타원 곡선 암호 알고리즘의 베이스 포인트의 곱이고, 제1 비밀값은 드론의 개인키와 서버의 공개키의 곱일 수 있다.

[0021] 상기 드론 식별 모듈에서 프로세서는 프로그램을 실행하여, 제1 난수를 생성하는 단계, 드론의 아이디 및 드론에 연결된 드론 식별 모듈의 고유 식별 정보에 기반하여 드론의 드론 식별 정보를 생성하는 단계, 그리고 제1 난수, 드론 식별 정보, 및 드론의 인증서를 서버에게 전송하는 단계를 더 수행할 수 있다.

[0022] 상기 드론 식별 모듈에서 드론의 아이디와 드론 식별 모듈에 미리 저장된 고유 식별 정보를 바탕으로 드론의 드론 식별 정보의 서명값을 생성하는 단계, 그리고 드론의 아이디, 고유 식별 정보, 및 서명값을 주기적으로 서버에게 송신하는 단계를 더 포함하고, 서명값은 드론을 식별하기 위해서 서버에 의해 사용될 수 있다.

[0023] 상기 드론 식별 모듈에서 프로세서는 드론의 아이디, 고유 식별 정보, 및 서명값을 주기적으로 서버에게 송신하는 단계를 수행할 때, 드론의 아이디, 고유 식별 정보, 및 서명값을 암호키를 사용하여 암호화하는 단계를 수행할 수 있다.

[0024] 또 다른 실시예에 따르면, 무인 비행 장치가 제공된다. 상기 무인 비행 장치는, 프로세서, 메모리, 무인 비행 장치를 관리하는 서버와의 통신을 위한 무선 통신부, 및 식별 모듈과의 연결을 위한 인터페이스 장치를 포함하고, 프로세서는 메모리에 저장된 프로그램을 실행하여, 서버로부터 무선 통신부를 통해 서버의 인증서를 포함하는 인증 요구를 수신하고, 인터페이스 장치를 통해 인증 요구 및 무인 비행 장치의 아이디를 식별 모듈에게 전달하는 단계, 식별 모듈에 의해 서버의 인증서가 검증되면, 서버에게 무선 통신부를 통해 무인 비행 장치의 인증서, 무인 비행 장치의 식별 정보, 제1 난수를 송신하는 단계, 그리고 서버에게 무선 통신부를 통해, 드론 식별 모듈에 의해 서버의 인증서에 기반하여 생성된 암호키를 사용하여 암호화된 데이터를 송신하는 단계를 수행하고, 암호키는 드론 인증서 및 제1 난수에 기반하여 서버에 의해 생성되는 암호키와 동일하다.

[0025] 상기 무인 비행 장치에서, 암호키는 식별 모듈에 의해 생성된 비밀값, 제1 난수, 및 인증 요구에 포함된 제2 난수의 곱이고, 비밀값은 서버의 인증서로부터 추출된 서버의 공개키와 무인 비행 장치의 개인키의 곱일 수 있다.

[0026] 상기 무인 비행 장치에서 프로세서는 프로그램을 실행하여, 무인 비행 장치의 아이디, 식별 모듈의 고유 식별 정보, 및 무인 비행 장치의 아이디 및 고유 식별 정보를 바탕으로 생성된 무인 비행 장치의 식별 정보의 서명값을 서버에게 무선 통신부를 통해 주기적으로 송신하는 단계를 더 수행할 수 있다.

발명의 효과

[0027] 드론 및 드론 관리 서버는, 드론과 드론 관리 서버 사이의 명시적이고 일방적인 키 교환 없이 독립적으로 인증 및 식별을 수행할 수 있다.

도면의 간단한 설명

[0028] 도 1 및 도 2는 한 실시예에 따른 드론과 드론 관리 서버를 나타내는 블록도이다.

도 3은 한 실시예에 따른 DIM을 나타낸 블록도이다.

도 4는 한 실시예에 따른 드론 및 드론 관리 서버의 상호 인증 및 암호키 생성 방법을 나타낸 흐름도이다.

도 5는 한 실시예에 따른 드론 및 드론 관리 서버의 주기적 드론 식별 방법을 나타낸 흐름도이다.

도 6은 한 실시예에 따른 드론 및 드론 관리 서버의 드론 식별 정보의 암호화 방법을 나타낸 흐름도이다.

도 7은 다른 실시예에 따른 DIM을 나타낸 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0029] 아래에서는 첨부한 도면을 참고로 하여 본 기재의 실시예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 기재는 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 기재를 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

[0030] 도 1 및 도 2는 한 실시예에 따른 드론과 드론 관리 서버를 나타내는 블록도이다.

[0031] 도 1 및 2를 참조하면, 한 실시예에 따른 드론(200)과 드론 관리 서버(300)는 WiFi 등의 근거리 무선 통신(WLAN) 네트워크 또는 LTE 등의 무선 이동 통신 네트워크를 통해 연결된다. 본 기재에서 드론(200)은 무인 비행 장치의 예시이며, 설명의 간략함을 위해 아래에서 '드론'이라는 용어는 무인 비행 장치와 동일한 의미로 사용된다. 도 1에서 드론 식별 모듈(Drone Identity Module, DIM)(100)은 드론(200) 내에 포함된다. 도 1에서 DIM(100)은 드론(200)과 인터페이스 장치를 통해 연결된다. 예를 들어 DIM(100)은 USIM(Universal Subscriber Identification Module) 타입의 IC 카드 또는 SD 카드 등에 탑재되어, 드론(200)의 카드 슬롯 등의 인터페이스 장치를 통해 드론(200)과 연결될 수 있다. 도 2를 참조하면 DIM(100)은 보안 보드에 부착되어, 드론(200)과 UART(Universal asynchronous receiver/transmitter), 시리얼 통신, USB(Universal Serial Bus) 등의 인터페이스 규격으로 연결된다. 도 2의 보안 보드는 드론의 보안 기능을 담당하는 하드웨어 장치로서, DIM(100)과 연결될 수 있도록 카드 슬롯을 포함할 수 있다. 도 1 및 도 2에서 DIM(100)은 미리 결정된 폼팩터(form factor)를 갖는 하드웨어 장치일 수도 있고 또는 논리적 기능을 가진 소프트웨어 모듈일 수도 있으며, 이에 한정되지 않는다.

[0032] 도 1과 같이 DIM(100)이 드론과 직접 연결될 때, 드론(200)은 드론 관리 서버(300)로부터 상호 인증 및 암호키 생성을 위한 데이터를 수신하고 상호 인증 및 암호키 생성을 위한 데이터를 애플리케이션 프로토콜 데이터 유닛(application protocol data unit, APDU) 형태로 변환하여 DIM(100)에게 전달한다. 이후 DIM(100)은 상호 인증 및 암호키 생성에 관한 기능을 수행한다. 이후 DIM(100)으로부터 APDU 형태의 데이터를 수신한 드론(200)은 무선 통신 규격에 적합한 형태로 APDU 형태의 데이터를 변환하고 드론 관리 서버(300)에게 전달할 수 있다.

[0033] 도 2와 같이 DIM(100)이 보안 보드를 통해 드론(200)과 연결될 때, 드론 관리 서버(300)로부터 상호 인증 및 암호키 생성을 위한 데이터를 수신한 드론(200)은, 상호 인증 및 암호키 생성을 위한 데이터를 보안 보드와 드론(200) 간의 연결 인터페이스를 통해 보안 보드에게 전달하고, 보안 보드가 상호 인증 및 암호키 생성을 위한 데이터를 APDU 형태로 변환하여 DIM(100)에게 전달한다. 이후 보안 보드는 DIM(100)으로부터 수신된, APDU 형태의 데이터를 드론(200)을 거쳐 드론 관리 서버(300)에게 전달한다.

[0034] 한 실시예에 따르면, DIM(100)은 드론(200) 및 드론 관리 서버(300) 간의 상호 인증을 수행하고, 암호키를 생성하는 주체로서, DIM(100)의 고유 식별 번호, 드론의 인증서, 공인 인증 기관(Certificate Authority, CA)의 공개키를 저장한다. 도 2와 같이 DIM(100)과 드론(200) 간의 통신을 위해 보안 보드가 사용되면, 보안 보드는 상호 인증 및 암호키 생성을 위한 데이터를 APDU 데이터로 변환/역변환 할 수 있다. 또한 보안 보드는, 드론이 촬영한 영상과 같은 대용량 데이터를 고속으로 암호화할 수 있다.

[0035] 위에서는 USIM 유형의 DIM(100)으로의 데이터 전송을 위해 APDU 규격이 사용되었지만, DIM(100)이 USIM이 아닌 다른 하드웨어 유형이면 그에 적합한 데이터 규격이 DIM(100)으로의 데이터 전송을 위해 사용될 수 있다. 예를 들어, DIM(100)이 소프트웨어 모듈일 때, DIM(100)은 드론(200)과의 데이터 송수신을 위한 애플리케이션 프로그래밍 인터페이스(application programming interface, API)를 가질 수 있다.

[0036] 도 3은 한 실시예에 따른 DIM을 나타낸 블록도이다.

[0037] 도 3을 참조하면, 한 실시예에 따른 DIM(100)은 서버 인증부(110), 암호키 생성부(120), 서명값 생성부(130), 암호화부(140), 및 저장부(150)를 포함한다.

[0038] 서버 인증부(110)는 CA의 공개키를 이용하여 드론 관리 서버의 인증서를 검증할 수 있다.

[0039] 암호키 생성부(120)는 드론 관리 서버의 인증서가 검증되면, 드론 관리 서버의 인증서로부터 드론 관리 서버의 공개키를 추출하고, 추출된 공개키와 드론의 개인키를 바탕으로 비밀값을 계산한다. 이때, 드론 관리 서버도 드론 관리 서버의 개인키와, 드론의 인증서로부터 추출된 드론의 공개키를 바탕으로 비밀값을 계산하는데, 이때 암호키 생성부(120)에 의해 계산된 비밀값과 드론 관리 서버에 의해 계산된 비밀값은 서로 동일하다. 즉, DIM(100) 및 드론 관리 서버에 의해 각각 계산된 비밀값은 직접적인 교환 없이도 동일하게 계산될 수 있다. 그리고, 암호키 생성부(120)는 암호키 생성을 위해 난수를 생성할 수 있고, 비밀값, 드론 관리 서버로부터 수신된 난수, 암호키 생성부(120)에서 생성된 난수를 변수로 갖는 키 유도 함수를 사용하여 암호키를 생성한다. 이후 암호키는 드론과 드론 관리 서버 간의 데이터 교환 시 데이터의 암호화 및 복호화에 사용될 수 있다. 암호키 생성부(120)에 의해 생성된 암호키 또한, 드론 관리 서버에 의해 생성된 암호키와 동일하다.

[0040] 서명값 생성부(130)는 드론 관리 서버에서 드론을 식별하기 위해 검증하는, 드론 식별 정보의 서명값을 생성한

다. 서명값 생성부(130)는 드론의 아이디 및 DIM(100)의 고유 식별 번호를 바탕으로 드론 식별 정보를 생성하고, 전자 서명 알고리즘을 사용하여 드론 식별 정보의 서명값을 생성한다.

[0041] 암호화부(140)는 암호키 생성부(120)에 의해 생성된 암호키를 사용하여 드론과 드론 관리 서버 간에 송수신되는 데이터를 암호화한다.

[0042] 저장부(150)는 인증 기관의 개인키로 서명되는 드론의 인증서($Cert_d$), 드론의 개인키(d_d), 드론의 공개키(Q_d)를 저장한다. 또한, 저장부(150)는 DIM(100)의 고유 식별 정보를 저장하고 있고, 드론의 아이디를 저장할 수 있으며, 서버로부터 수신되는 서버의 인증서, 서버의 아이디, 및 서버에서 생성된 난수를 저장할 수 있다. 또한, 저장부(150)는 서버의 인증서에 기반하여 추출되는 서버의 공개키, 서버의 공개키에 기반하여 생성되는 비밀값, 및 암호키 생성부(120)에서 생성된 난수와 암호키를 저장할 수 있다.

[0043] 도 4는 한 실시예에 따른 드론 및 드론 관리 서버의 상호 인증 및 암호키 생성 방법을 나타낸 흐름도이다.

[0044] 드론(200)은 비행하기 전 또는 비행을 위한 이륙 직후 드론 관리 서버(300)에게 상호 인증 요구를 송신한다(S110). 이때, DIM(100)은 드론 인증서($Cert_d$), 드론 개인키(d_d), 및 드론 개인키에 기반하여 생성된 드론 공개키($Q_d(=d_dP)$, P는 타원 곡선 암호 알고리즘의 베이스 포인트이다)를 저장하고 있다. 드론 인증서 $Cert_d$는 CA 개인키로 서명되어 있다. 또한, 드론 관리 서버(300)도 서버 인증서($Cert_s$), 서버 개인키(d_s), 및 서버 개인키에 기반하여 생성된 서버 공개키($Q_s(=d_sP)$)를 저장하고 있다. 서버 인증서 $Cert_s$ 또한 CA 개인키로 서명되어 있다. 한 실시예에 따른 DIM(100) 및 드론 관리 서버(300)는 각각 공개키 암호 알고리즘의 타원 곡선 암호(Elliptic curve cryptograph, ECC)를 사용할 수 있고, 다른 암호 알고리즘을 사용할 수도 있으며, 이에 한정되지 않는다.

[0045] 드론 관리 서버(300)는 난수($rand_s$)를 생성하고, 생성된 난수($rand_s$)를 포함하는 드론 인증 요구 메시지를 드론(200)에게 전달한다. 이때 드론 인증 요구 메시지는 서버의 식별정보인 아이디(id_s), 인증서($Cert_s$)를 더 포함할 수 있다. 한 실시예에 따른 드론 관리 서버(300)는 한 개의 통신 경로를 통해 난수($rand_s$), 서버의 아이디(id_s), 및 서버의 인증서($Cert_s$)를 한 번에 드론(200)에게 전송할 수 있다. 이후 드론(200)은 드론 관리 서버(300)로부터 수신한 난수($rand_s$), 아이디(id_s), 및 인증서($Cert_s$)를 자신의 비행체 아이디(id_d)와 함께 DIM(100)에게 전달한다(S120). DIM(100)은 드론(200)으로부터 수신되는, 드론 관리 서버(300)의 아이디(id_s) 및 인증서($Cert_s$)를 이용하여 드론 관리 서버(300)를 검증한다(S130). DIM(100)은 CA의 공개키를 이용하여 인증서($Cert_s$)를 검증한다. 이때 인증서($Cert_s$)는 발급시 CA의 비밀키에 의해 전자 서명되어 있으므로 DIM(100)은 CA의 공개키를 이용하여 인증서($Cert_s$)의 서명값을 검증할 수 있다. DIM(100)은 서명 생성 및 검증을 위해 타원 곡선 디지털 서명 알고리즘(Elliptic Curve Digital Signature Algorithm, ECDSA)을 사용할 수 있고, 또는 RSA 알고리즘 등 다른 공개키 기반 서명 알고리즘을 사용할 수 있다.

[0046] DIM(100)이 서버의 아이디(id_s) 및 서버의 인증서($Cert_s$)를 이용하여 드론 관리 서버(300)의 인증에 성공하면, DIM(100)은 드론(200)의 비행체 아이디(id_d) 및 고유 식별 정보를 결합하여 드론 식별 정보를 생성한다. 그리고 DIM(100)은 난수($rand_d$) 및 인증서($Cert_d$)와 함께 생성된 드론 식별 정보를 드론(200)을 경유하여 드론 관리 서버(300)에게 전달한다(S140). 즉, 한 실시예에 따르면, 드론 식별 정보, 난수($rand_d$), 및 인증서($Cert_d$)는 1회의 통신 경로를 통해 드론(200)에서 드론 관리 서버(300)에게 한꺼번에 전송될 수 있다. 이때 드론 식별 정보의 생성에 사용되는 고유 식별 정보는 DIM(100)에 미리 저장되어 있다. DIM(100)은 해킹이 불가능하므로 고유 식별 정보는 제3자에게 탈취되지 않는다. 또한 불법 드론이 합법 드론의 비행체 아이디를 복사하여 사용하더라도 DIM의 고유 식별 정보가 없는 이상 불법 드론은 드론 관리 서버(300)에 의해 인증될 수 없다.

[0047] 드론(200)으로부터 드론 식별 정보, 난수($rand_d$), 인증서($Cert_d$)를 수신한 드론 관리 서버(300)는 CA의 공개키를 이용하여 인증서($Cert_d$)의 서명값을 검증한다(S150). 드론(200)의 인증서($Cert_d$)도 CA의 비밀키에 의해 전자 서명 되어 있기 때문이다. 드론 관리 서버(300)가 드론(200)의 인증서($Cert_d$)에 기반하여 드론(200)의 인증에 성공하면, 드론 관리 서버(300)는 인증 성공 메시지를 드론(200)을 통해 DIM(100)에게 전달한다(S160). 이후 드론(200) 및 드론 관리 서버(300)는 데이터 통신의 암호화/복호화에 사용될 암호키를 생성한다. 한 실시예에 따르면, 드론(200)의 DIM(100)은 드론 관리 서버(300)의 인증서($Cert_s$)로부터 공개키 Q_s를 추출하고 추출된 공개

키 Q_s에 기반하여 비밀값 z($z=d_dQ_s=d_dd_sP$)를 계산한다. 드론 관리 서버(300)도 드론(200)의 인증서(Certd)로부터 공개키 Q_d를 추출하고, 추출된 공개키 Q_d를 바탕으로 비밀값 z($z=d_sQ_d=d_sd_dP$)를 계산한다(S170).

[0048] 한 실시예에 따른 DIM(100)(또는 드론(200)) 및 드론 관리 서버(300)는 ECDH(Elliptic Curve Diffie Hellman) 알고리즘에 기반한 키 교환 방식을 사용할 수 있고, 디피-헬먼(Diffie-Hellman, DH) 키교환 알고리즘 등 이미 알려진 다른 방식의 키교환 알고리즘을 사용할 수 있으며, 이에 한정되지 않는다. 이후 DIM(100) 및 드론 관리 서버(300)는 각각 비밀값 z, 드론 관리 서버(300)가 드론(200)에게 보낸 난수($rand_s$), 및 드론(200)이 드론 관리 서버(300)에게 보낸 난수($rand_d$)를 키 유도 함수의 변수로서 사용하여 암호키 $ek=H(z, rand_s, rand_d)$를 생성한다. H는 SHA256 등의 해시 함수(hash function)이다. 한 실시예에 따른 DIM(100) 및 드론 관리 서버(300)는 암호키 생성을 위해 해쉬 함수 외에 다른 키 유도 함수를 사용할 수 있으며, 이에 한정되지 않는다.

[0049] 한 실시예에 따른 암호키 생성 방법에서 비밀값 z는 드론(200)에서 생성되어 드론 관리 서버(300)에게 전달되지 않는다. 즉, 한 실시예에 따르면, DIM(100)과 드론 관리 서버(300)는 각각 서로의 인증에 성공한 후 동일한 방식으로 동일한 비밀값 z를 생성하고 비밀값 z로부터 암호키를 유도한다. DIM(100) 및 드론 관리 서버(300)가 암호키를 유도할 때 적용하는 키 유도 함수가 동일하므로, 둘은 동일한 암호키를 비밀값의 교환 또는 전달 없이 생성할 수 있다.

[0050] 도 5는 한 실시예에 따른 드론 및 드론 관리 서버의 주기적 드론 식별 방법을 나타낸 흐름도이다.

[0051] 도 4에 따른 DIM(100)(또는 드론(200))과 드론 관리 서버(300) 간의 상호 인증이 완료된 후, 드론(200)의 비행 중에 드론 관리 서버(300)에게 드론 식별 정보를 주기적으로 전송하고, 드론 관리 서버(300)는 주기적으로 전송되는 드론 식별 정보를 바탕으로 드론(200)을 식별한다.

[0052] 도 5를 참조하면, 드론(200)이 DIM(100)에게 비행체 아이디를 전달하면(S210), DIM(100)은 비행체 아이디를 DIM(100)에 미리 저장되어 있는 고유 식별 정보와 결합하여 드론 식별 정보에 관한 서명값 "Sig(비행체ID‖고유식별정보)"을 생성한다(S220). 예를 들어, 한 실시예에 따른 DIM(100)은 ECDSA와 같은 전자 서명 알고리즘을 사용하여 서명값 "Sig(비행체ID‖고유식별정보)"를 생성할 수 있다. 이후 DIM(100)은 드론(200)을 거쳐 드론 관리 서버(300)에게 "비행체ID‖고유식별정보‖Sig(비행체ID‖고유식별정보)"를 전송한다(S230). 드론 관리 서버(300)는 드론 인증서($Cert_d$)의 드론 공개키(Q_d)를 이용하여 서명값 Sig(비행체ID‖고유식별정보)를 검증한다(S240). 이때 도 4에 따라 드론 관리 서버(300)가 드론 상호 인증에 실패하였거나 또는 유효한 드론 인증서를 가지고 있지 않다면, 드론 관리 서버(300)는 드론(200)의 주기적 식별 절차에도 실패하게 된다.

[0053] 한 실시예에 따른 DIM(100) 및 드론 관리 서버(300)는 드론 식별 정보의 서명값의 생성 및 검증에 ECDSA를 사용하였지만, 다른 공개키 기반 서명 알고리즘도 사용할 수 있고, 이에 한정되지 않는다.

[0054] 도 6은 한 실시예에 따른 드론 및 드론 관리 서버의 드론 식별 정보의 암호화 방법을 나타낸 흐름도이다.

[0055] 도 6을 참조하면, 드론(200) 및 드론 관리 서버(300)는 드론 식별 인증 절차를 암호화할 수 있다. 이때, DIM(100)은 도 4에 도시된 상호 인증 절차에서 생성된 암호키 ek를 사용하여 드론 식별 정보 및 드론 식별 정보의 서명값을 암호화할 수 있다. 이때 암호화 알고리즘은 AES(Advanced Encryption Standard) 등의 대칭키 기반 암호화 알고리즘을 포함한다. 도 6에서 드론(200)으로부터 비행체 ID를 수신(S310)한 DIM(100)은 서명값 "Sig(비행체ID‖고유식별정보)"를 생성하고, 암호키 ek를 사용하여 "비행체ID‖고유식별정보"와 "Sig(비행체ID‖고유식별정보)"를 암호화한다(S320). DIM(100)으로부터 드론(200)을 거쳐 암호화된 메시지(E_ek[비행체ID‖고유식별정보‖Sig(비행체ID‖고유식별정보)])를 수신(S330)한 드론 관리 서버(300)는 상호 인증 절차에서 생성된 암호키를 사용하여 암호화된 메시지를 복호하고 서명값을 검증함으로써 드론(200)을 식별한다(S340). 따라서, 드론(200)이 드론 관리 서버(300)에게 전송하는 드론 식별 정보와 드론 식별 정보의 검증값은 드론(200)과 드론 관리 서버(300) 간의 통신 상에서 보호될 수 있다. 즉, 드론 관리 서버(300)만이 드론 식별 정보 및 검증값을 복호하여 드론 식별 정보가 올바른지 여부를 검증할 수 있다.

[0056] 위에서 설명한 바와 같이 한 실시예에 따른 드론과 드론 관리 서버 간의 상호 인증 절차에 따르면, USIM과 같은 형태로 드론에 부착되거나 또는 다양한 방법으로 드론과 긴밀히 유선 연결될 수 있는 DIM을 사용하여 암호키 또는 암호키 생성을 위한 비밀값의 명시적인 전송 없이 드론과 드론 관리 서버 간의 상호 인증이 수행될 수 있다. DIM은 고유 식별 정보와, 드론의 개인키, 드론의 인증서 등을 미리 저장하고 있으며, 드론과 드론 관리 서버 간의 상호 인증, 드론 식별, 암호 연산의 수행 능력을 갖춘 기능적 모듈이다. DIM은 USIM 카드, 마이크로 SD 카드, eSIM 등 다양한 유형의 하드웨어 형상일 수 있고 또는 소프트웨어로서 구현된 논리적인 기능 모듈일 수

있으며, 그러한 하드웨어 및 소프트웨어의 결합일 수 있다. 해킹 불가능한 DIM을 이용함으로써, 무허가 드론 또는 불법 드론은 드론 관리 서버와의 상호 인증에 성공할 수 없고, 드론 관리 서버는 쉽게 무허가 드론 및 불법 드론을 식별할 수 있다.

[0057] 도 7은 다른 실시예에 따른 DIM을 나타낸 블록도이다.

[0058] 한 실시예에 따른 DIM은, 컴퓨터 시스템, 예를 들어 컴퓨터 판독 가능 매체로 구현될 수 있다. 도 7을 참조하면, 컴퓨터 시스템(700)은, 버스(770)를 통해 통신하는 프로세서(710), 메모리(730), 사용자 인터페이스 입력 장치(750), 사용자 인터페이스 출력 장치(760), 및 저장 장치(740) 중 적어도 하나를 포함할 수 있다. 컴퓨터 시스템(700)은 또한 네트워크에 결합된 통신 장치(720)를 포함할 수 있다. 프로세서(710)는 중앙 처리 장치(central processing unit, CPU)이거나, 또는 메모리(730) 또는 저장 장치(740)에 저장된 명령을 실행하는 반도체 장치일 수 있다. 메모리(730) 및 저장 장치(740)는 다양한 형태의 휘발성 또는 비휘발성 저장 매체를 포함할 수 있다. 예를 들어, 메모리는 ROM(read only memory) 및 RAM(random access memory)를 포함할 수 있다. 본 기재의 실시예에서 메모리는 프로세서의 내부 또는 외부에 위치할 수 있고, 메모리는 이미 알려진 다양한 수단을 통해 프로세서와 연결될 수 있다. 메모리는 다양한 형태의 휘발성 또는 비휘발성 저장 매체이며, 예를 들어, 메모리는 읽기 전용 메모리(read-only memory, ROM) 또는 랜덤 액세스 메모리(random access memory, RAM)를 포함할 수 있다. 통신 장치(720)는 유선 신호 또는 무선 신호를 송신 또는 수신할 수 있다.

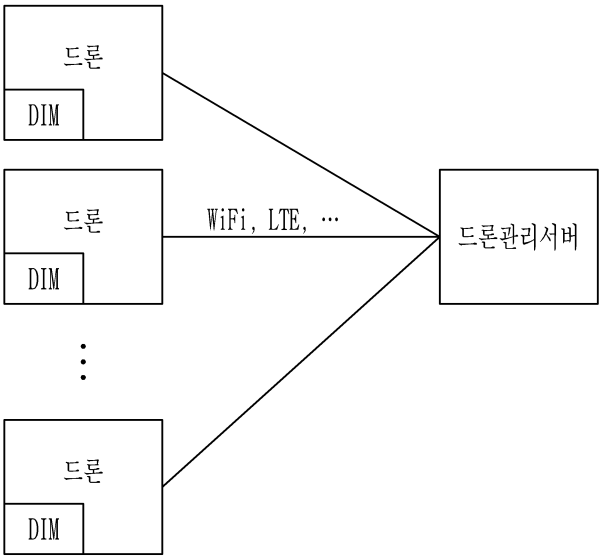
[0059] 따라서, 본 발명의 실시예는 컴퓨터에 구현된 방법으로서 구현되거나, 컴퓨터 실행 가능 명령이 저장된 비일시적 컴퓨터 판독 가능 매체로서 구현될 수 있다. 한 실시예에서, 프로세서에 의해 실행될 때, 컴퓨터 판독 가능 명령은 본 기재의 적어도 하나의 양상에 따른 방법을 수행할 수 있다.

[0060] 한편, 본 발명의 실시예는 지금까지 설명한 장치 및/또는 방법을 통해서만 구현되는 것은 아니며, 본 발명의 실시예의 구성에 대응하는 기능을 실현하는 프로그램 또는 그 프로그램이 기록된 기록 매체를 통해 구현될 수도 있으며, 이러한 구현은 상술한 실시예의 기재로부터 본 발명이 속하는 기술 분야의 통상의 기술자라면 쉽게 구현할 수 있는 것이다. 구체적으로, 본 발명의 실시예에 따른 방법(예, 네트워크 관리 방법, 데이터 전송 방법, 전송 스케줄 생성 방법 등)은 다양한 컴퓨터 수단을 통해 수행될 수 있는 프로그램 명령 형태로 구현되어, 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 컴퓨터 판독 가능 매체에 기록되는 프로그램 명령은, 본 발명의 실시예를 위해 특별히 설계되어 구성된 것이거나, 컴퓨터 소프트웨어 분야의 통상의 기술자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체는 프로그램 명령을 저장하고 수행하도록 구성된 하드웨어 장치를 포함할 수 있다. 예를 들어, 컴퓨터 판독 가능 기록 매체는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광 기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 롬(ROM), 램(RAM), 플래시 메모리 등일 수 있다. 프로그램 명령은 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라, 인터프리터 등을 통해 컴퓨터에 의해 실행될 수 있는 고급 언어 코드를 포함할 수 있다.

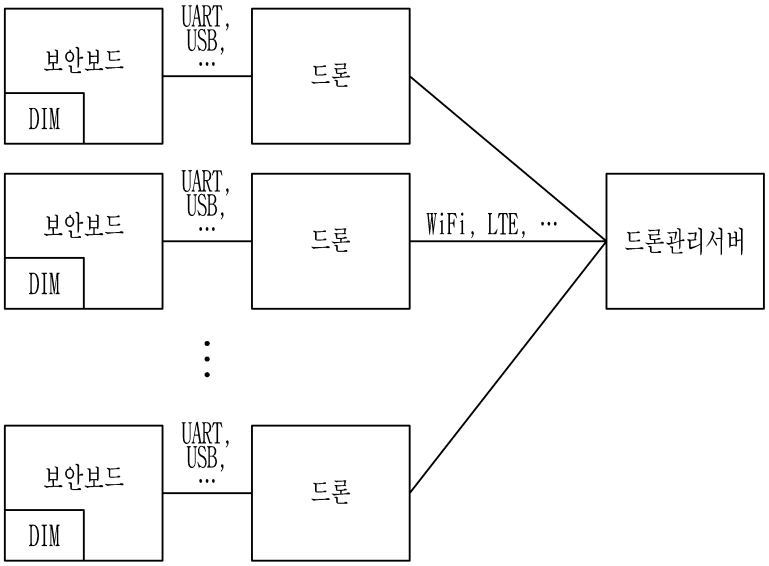
[0061] 이상에서 본 발명의 실시예에 대하여 상세하게 설명하였지만 본 발명의 권리범위는 이에 한정되는 것은 아니고 다음의 청구범위에서 정의하고 있는 본 발명의 기본 개념을 이용한 당업자의 여러 변형 및 개량 형태 또한 본 발명의 권리범위에 속하는 것이다.

도면

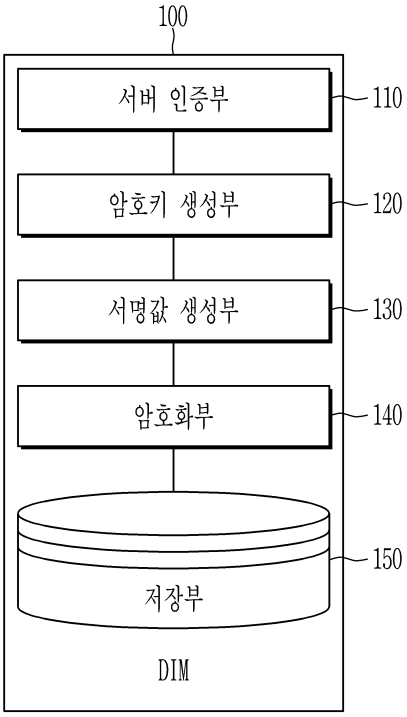
도면1


드론
DIM
드론
DIM
WiFi, LTE, …
드론관리서버
드론
DIM

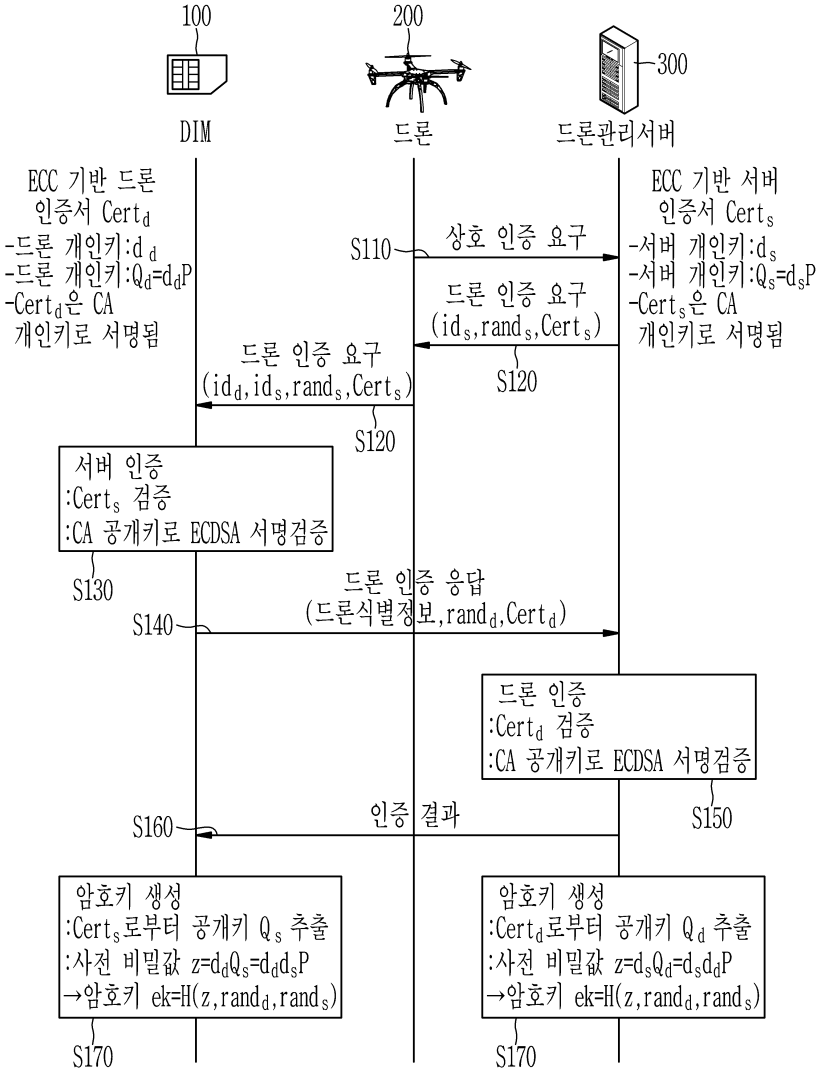
도면2


보안보드
DIM
UART,
USB,
…
드론
보안보드
DIM
UART,
USB,
…
드론
WiFi, LTE, …
드론관리서버
보안보드
DIM
UART,
USB,
…
드론

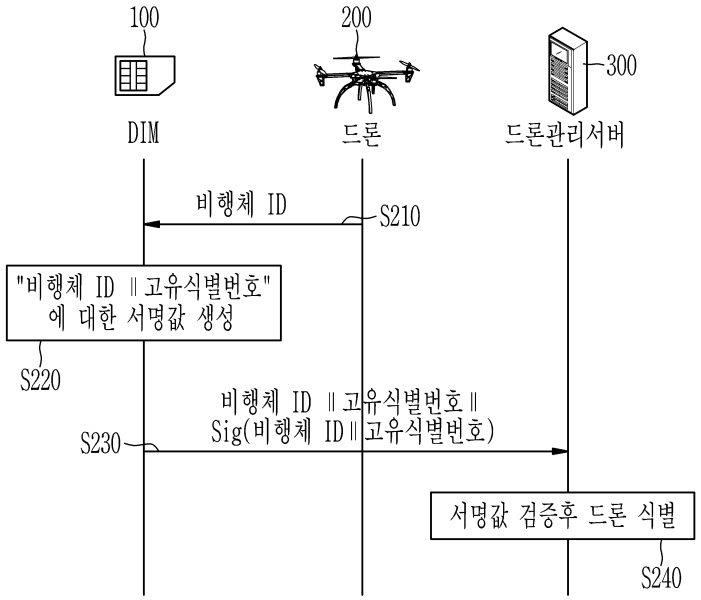
도면3



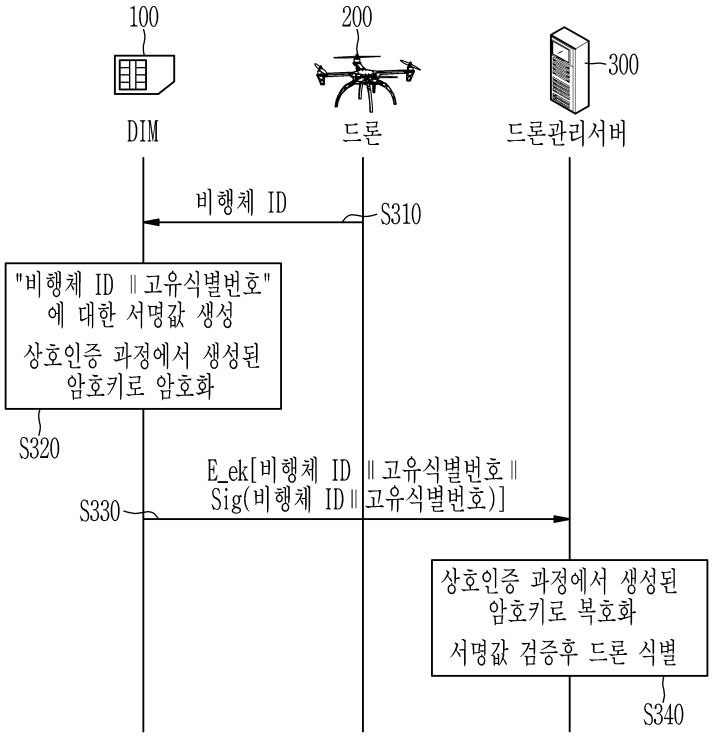
도면4


100
200
300
DIM
드론
드론관리서버
ECC 기반 드론 인증서 Certd
-드론 개인키:dd
-드론 개인키:Qd=ddP
-Certd은 CA 개인키로 서명됨
ECC 기반 서버 인증서 Certs
-서버 개인키:ds
-서버 개인키:Qs=dsP
-Certs은 CA 개인키로 서명됨
S110
상호 인증 요구
드론 인증 요구 (ids,rands,Certs)
S120
드론 인증 요구 (idd,ids,rands,Certs)
S120
서버 인증
:Certs 검증
:CA 공개키로 ECDSA 서명검증
S130
드론 인증 응답 (드론식별정보,randd,Certd)
S140
드론 인증
:Certd 검증
:CA 공개키로 ECDSA 서명검증
S150
인증 결과
S160
암호키 생성
:Certs로부터 공개키 Qs 추출
:사전 비밀값 z=dQs=ddsP
→암호키 ek=H(z,randd,rands)
S170
암호키 생성
:Certd로부터 공개키 Qd 추출
:사전 비밀값 z=dsQd=dsddP
→암호키 ek=H(z,randd,rands)
S170

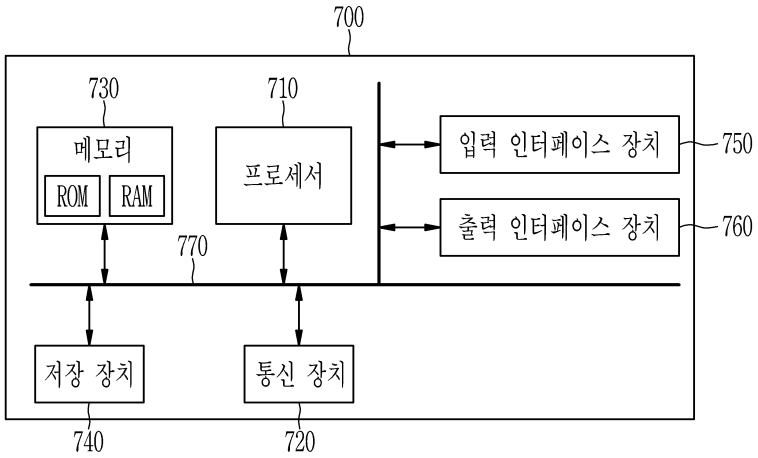
도면5


100
200
300
DIM
드론
드론관리서버
비행체 ID
S210
"비행체 ID ‖ 고유식별번호"
에 대한 서명값 생성
S220
비행체 ID ‖ 고유식별번호 ‖
Sig(비행체 ID ‖ 고유식별번호)
S230
서명값 검증후 드론 식별
S240

도면6


100
200
300
DIM
드론
드론관리서버
비행체 ID
S310
"비행체 ID ‖ 고유식별번호"
에 대한 서명값 생성
상호인증 과정에서 생성된
암호키로 암호화
S320
E_ek[비행체 ID ‖ 고유식별번호 ‖
Sig(비행체 ID ‖ 고유식별번호)]
S330
상호인증 과정에서 생성된
암호키로 복호화
서명값 검증후 드론 식별
S340

도면7


700
730
710
메모리
ROM
RAM
프로세서
입력 인터페이스 장치
750
출력 인터페이스 장치
760
770
저장 장치
통신 장치
740
720