



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2024-0027445
(43) 공개일자 2024년03월04일

(51) 국제특허분류(Int. Cl.)
H04L 9/40 (2022.01) H04L 9/08 (2006.01)
H04L 9/32 (2006.01)
(52) CPC특허분류
H04L 63/061 (2013.01)
H04L 63/0421 (2013.01)
(21) 출원번호 10-2022-0105656
(22) 출원일자 2022년08월23일
심사청구일자 2022년08월23일

(71) 출원인
국방과학연구소
대전광역시 유성구 북유성대로488번길 160 (수남동)
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
정익래
서울특별시 성북구 안암로 145
변진욱
경기도 평택시 서동대로 3825
(뒷면에 계속)
(74) 대리인
특허법인 광장리앤코

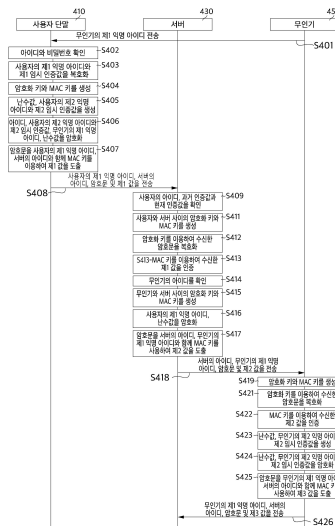
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 키 교환 프로토콜을 제공하는 전자 장치 및 이의 동작 방법

(57) 요약

키 교환 프로토콜을 제공하는 전자 장치의 동작 방법에 관한 것이다. 구체적으로, 동작 방법은 사용자 단말로부터 사용자의 ID, 상기 사용자의 ID에 대응하는 상기 사용자의 제1 익명 ID 및 상기 사용자의 제1 임시 인증값 중에서 적어도 하나를 획득하는 단계; 무인기로부터 상기 무인기의 ID, 상기 무인기의 ID에 대응하는 상기 무인기의 제1 익명 ID 및 상기 무인기의 제1 임시 인증값 중에서 적어도 하나를 획득하는 단계; 및 상기 사용자 단말의 키 교환 요청 또는 상기 무인기의 키 교환 요청에 대응하여 상기 사용자 단말로부터 획득된 정보를 포함하는 제1 정보와 상기 무인기로부터 획득된 정보를 포함하는 제2 정보에 기반하여 상기 무인기와 상기 사용자 단말 사이의 키 교환을 중계하는 단계를 포함할 수 있다.

대표도 - 도4a



(52) CPC특허분류

H04L 63/08 (2023.05)

H04L 9/0861 (2013.01)

H04L 9/3242 (2013.01)

H04L 2209/84 (2013.01)

(72) 발명자

정재열

서울특별시 성북구 안암로 145

최재현

서울특별시 성북구 안암로 145

명세서

청구범위

청구항 1

전자 장치의 동작 방법에 있어서,

사용자 단말로부터 사용자의 ID, 상기 사용자의 ID에 대응하는 상기 사용자의 제1 익명 ID 및 상기 사용자의 제1 임시 인증값 중에서 적어도 하나를 획득하는 단계;

무인기로부터 상기 무인기의 ID, 상기 무인기의 ID에 대응하는 상기 무인기의 제1 익명 ID 및 상기 무인기의 제1 임시 인증값 중에서 적어도 하나를 획득하는 단계; 및

상기 사용자 단말의 키 교환 요청 또는 상기 무인기의 키 교환 요청에 대응하여 상기 사용자 단말로부터 획득된 정보를 포함하는 제1 정보와 상기 무인기로부터 획득된 정보를 포함하는 제2 정보에 기반하여 상기 무인기와 상기 사용자 단말 사이의 키 교환을 중계하는 단계를 포함하는,

동작 방법.

청구항 2

제1항에 있어서,

상기 무인기의 키 교환 요청은,

상기 무인기에서 상기 사용자 단말로 상기 무인기의 제1 익명 ID를 전송하는 것에 대응하고,

상기 사용자 단말의 키 교환 요청은,

상기 사용자 단말에서 상기 무인기로 상기 사용자 단말의 제1 익명 ID를 전송하는 것에 대응하는,

동작 방법.

청구항 3

제2항에 있어서,

상기 사용자 단말의 키 교환 요청 또는 상기 무인기의 키 교환 요청에 대응하여 상기 무인기와 상기 사용자 단말 사이의 키 교환을 중계하는 단계는,

상기 제1 정보와 상기 제2 정보에 기반하여 상기 사용자 단말과 상기 무인기 사이 동일한 MAC(Message Authentication Code) 키와 세션 키를 공유하는 단계를 포함하는,

동작 방법.

청구항 4

제3항에 있어서,

상기 사용자의 제1 익명 ID 및 상기 사용자의 제1 임시 인증값은, 상기 사용자의 ID와 관계 없이 임의로 생성되는,

동작 방법.

청구항 5

제4항에 있어서,

상기 제1 정보는,

상기 사용자의 ID, 상기 사용자의 제1 익명 ID, 상기 사용자의 제1 임시 인증값, 상기 사용자의 제1 익명 ID와 다른 제2 익명 ID, 상기 사용자의 제1 임시 인증값과 다른 제2 임시 인증값 및 상기 사용자의 난수값 중에서 적

어도 하나를 포함하는,
동작 방법.

청구항 6

제1항에 있어서,
상기 무인기의 제1 익명 ID 및 상기 무인기의 제1 임시 인증값은, 상기 무인기의 ID와 관계 없이 임의로 생성되는,
동작 방법.

청구항 7

제6항에 있어서,
상기 제2 정보는,
상기 무인기의 ID, 상기 무인기의 제1 익명 ID, 상기 무인기의 제1 임시 인증값, 상기 무인기의 제1 익명 ID와 다른 제2 익명 ID, 상기 무인기의 제1 임시 인증값과 다른 제2 임시 인증값 및 상기 무인기의 난수값 중에서 적어도 하나를 포함하는,
동작 방법.

청구항 8

사용자 단말의 동작 방법에 있어서,
키 교환 요청하는 무인기로부터 상기 무인기의 ID에 대응하는 상기 무인기의 제1 익명 ID를 획득하는 단계;
사용자로부터 입력된 상기 사용자의 ID, 상기 사용자의 ID에 대응하는 상기 사용자의 제1 익명 ID 및 상기 사용자의 제1 임시 인증값 중에서 적어도 하나를 확인하는 단계;
상기 제1 임시 인증값을 이용하여 암호화 키와 제1 MAC(Message Authentication Code) 키를 생성하는 단계;
상기 사용자의 제1 익명 ID와 다른 제2 익명 ID 및 상기 사용자의 제1 임시 인증값과 다른 제2 임시 인증값을 생성하는 단계; 및
상기 사용자와 관련된 적어도 하나의 정보 및 상기 무인기와 관련된 적어도 하나의 정보에 기반하여 상기 사용자 단말과 상기 무인기 사이에서 공유되는 동일한 제2 MAC 키와 세션키를 생성하는 단계를 포함하는,
동작 방법.

청구항 9

무인기의 동작 방법에 있어서,
키 교환을 요청하는 사용자 단말로부터 상기 사용자 단말의 ID에 대응하는 상기 사용자 단말의 제1 익명 ID를 획득하는 단계;
상기 무인기의 ID, 상기 무인기의 ID에 대응하는 상기 무인기의 제1 익명 ID 및 상기 무인기의 제1 임시 인증값 중에서 적어도 하나를 확인하는 단계;
상기 제1 임시 인증값을 이용하여 암호화 키와 제1 MAC(Message Authentication Code) 키를 생성하는 단계;
상기 무인기의 제1 익명 ID와 다른 제2 익명 ID 및 상기 무인기의 제1 임시 인증값과 다른 제2 임시 인증값을 생성하는 단계; 및
상기 사용자 단말과 관련된 적어도 하나의 정보 및 상기 무인기와 관련된 적어도 하나의 정보에 기반하여 상기 사용자 단말과 상기 무인기 사이에서 공유되는 동일한 제2 MAC 키와 세션키를 생성하는 단계를 포함하는,
동작 방법.

청구항 10

통신 디바이스(communication device);

적어도 하나의 명령어(instruction)를 저장하는 메모리; 및

사용자 단말로부터 사용자의 ID, 상기 사용자의 ID에 대응하는 상기 사용자의 제1 익명 ID 및 상기 사용자의 제1 임시 인증값 중에서 적어도 하나를 획득하고, 무인기로부터 상기 무인기의 ID, 상기 무인기의 ID에 대응하는 상기 무인기의 제1 익명 ID 및 상기 무인기의 제1 임시 인증값 중에서 적어도 하나를 획득하고, 상기 사용자 단말의 키 교환 요청 또는 상기 무인기의 키 교환 요청에 대응하여 상기 사용자 단말로부터 획득된 정보를 포함하는 제1 정보와 상기 무인기로부터 획득된 정보를 포함하는 제2 정보에 기반하여 상기 무인기와 상기 사용자 단말 사이의 키 교환을 중계하는 제어부(controller)를 포함하는,

전자 장치.

발명의 설명

기술 분야

[0001] 본 명세서의 실시 예는 IoD(Internet of Drones) 환경에서 사용자와 무인기 사이의 전방향 연결 불가능성을 만족하면서 사용자뿐만 아니라 무인기가 먼저 키 교환 요청을 할 수 있는 프로토콜을 제공하는 전자 장치 및 이의 동작 방법에 관한 것이다.

배경 기술

[0002] 무인기(예: 드론, UAV)는 조종사가 직접 탑승하지 않고 GPS 장치 등을 이용하여 원격 조종 또는 자동 비행이 가능한 동력 비행체로서, 군사적 용도뿐만 아니라 영상 촬영, 택배 서비스, 농약 살포, 지능형 교통 관리, 3D 맵 정보 획득 등 다양한 분야에 걸쳐 사용 범위가 확장되고 있는 추세이다. 이러한 무인기는 사용자(관리자)의 단말과 양방향 통신 방식으로 연결되어 소정의 정보 또는 명령을 송수신할 수 있다.

[0003] IoD(Internet of Drones) 환경에서 키 교환 프로토콜은 사용자와 무인기가 서버를 통해서 상호 통신할 수 있는 키를 교환하는 것으로, 이 과정에서 사용자와 드론의 정보가 노출되면 프라이버시가 침해될 우려가 있다. 이에, 기존의 키 교환 프로토콜은 사용자의 아이디를 대체할 익명 아이디를 생성하여 사용자의 프라이버시를 보호하려고 하였다. 그러나, 익명 아이디를 사용하더라도 익명 아이디가 노출되면 익명 아이디가 사용된 시간, 장소 등을 통해서 실제 사용자를 추정할 수 있게 되는 등의 문제가 발생할 우려가 있었다.

[0004] 또한, 공중에 떠있는 무인기가 먼저 사건 사고를 발견하였을 때 관련된 정보를 먼저 사용자들에게 전달할 수 있어야 함에도 불구하고 기존에는 사용자만 먼저 요청할 수 있어서 무인기가 사건 사고를 발견하더라도 요청할 수 없는 문제가 있었다.

발명의 내용

해결하려는 과제

[0005] 본 명세서의 실시 예는 상술한 문제점을 해결하기 위하여 제안된 것으로 IoD(Internet of Drones) 환경에서 사용자와 무인기 사이의 전방향 연결 불가능성을 만족하면서 사용자뿐만 아니라 무인기가 먼저 키 교환 요청을 할 수 있는 프로토콜을 제공하는 기술에 관한 것이다. 본 실시 예가 이루고자 하는 기술적 과제는 상기된 바와 같은 기술적 과제들로 한정되지 않으며, 이하의 실시 예들로부터 또 다른 기술적 과제들이 유추될 수 있다.

과제의 해결 수단

[0006] 상술한 과제를 달성하기 위하여, 본 명세서의 일 실시 예에 따르는 전자 장치의 동작 방법은 사용자 단말로부터 사용자의 ID, 상기 사용자의 ID에 대응하는 상기 사용자의 제1 익명 ID 및 상기 사용자의 제1 임시 인증값 중에서 적어도 하나를 획득하는 단계; 무인기로부터 상기 무인기의 ID, 상기 무인기의 ID에 대응하는 상기 무인기의 제1 익명 ID 및 상기 무인기의 제1 임시 인증값 중에서 적어도 하나를 획득하는 단계; 및 상기 사용자 단말의 키 교환 요청 또는 상기 무인기의 키 교환 요청에 대응하여 상기 사용자 단말로부터 획득된 정보를 포함하는 제1 정보와 상기 무인기로부터 획득된 정보를 포함하는 제2 정보에 기반하여 상기 무인기와 상기 사용자 단말 사이의 키 교환을 중계하는 단계를 포함할 수 있다.

[0007] 실시 예에 따르면, 상기 무인기의 키 교환 요청은, 상기 무인기에서 상기 사용자 단말로 상기 무인기의 제1 익

명 ID를 전송하는 것에 대응하고, 상기 사용자 단말의 키 교환 요청은, 상기 사용자 단말에서 상기 무인기로 상기 사용자 단말의 제1 익명 ID를 전송하는 것에 대응할 수 있다.

[0008] 실시 예에 따르면, 상기 사용자 단말의 키 교환 요청 또는 상기 무인기의 키 교환 요청에 대응하여 상기 무인기와 상기 사용자 단말 사이의 키 교환을 중계하는 단계는, 상기 제1 정보와 상기 제2 정보에 기반하여 상기 사용자 단말과 상기 무인기 사이 동일한 MAC(Message Authentication Code) 키와 세션 키를 공유하는 단계를 포함할 수 있다.

[0009] 실시 예에 따르면, 상기 사용자의 제1 익명 ID 및 상기 사용자의 제1 임시 인증값은, 상기 사용자의 ID와 관계없이 임의로 생성될 수 있다.

[0010] 실시 예에 따르면, 상기 제1 정보는, 상기 사용자의 ID, 상기 사용자의 제1 익명 ID, 상기 사용자의 제1 임시 인증값, 상기 사용자의 제1 익명 ID와 다른 제2 익명 ID, 상기 사용자의 제1 임시 인증값과 다른 제2 임시 인증값 및 상기 사용자의 난수값 중에서 적어도 하나를 포함할 수 있다.

[0011] 실시 예에 따르면, 상기 무인기의 제1 익명 ID 및 상기 무인기의 제1 임시 인증값은, 상기 무인기의 ID와 관계없이 임의로 생성될 수 있다.

[0012] 실시 예에 따르면, 상기 제2 정보는, 상기 무인기의 ID, 상기 무인기의 제1 익명 ID, 상기 무인기의 제1 임시 인증값, 상기 무인기의 제1 익명 ID와 다른 제2 익명 ID, 상기 무인기의 제1 임시 인증값과 다른 제2 임시 인증값 및 상기 무인기의 난수값 중에서 적어도 하나를 포함할 수 있다.

[0013] 상술한 과제를 달성하기 위하여, 본 명세서의 일 실시 예에 따르는 사용자 단말의 동작 방법은, 키 교환 요청하는 무인기로부터 상기 무인기의 ID에 대응하는 상기 무인기의 제1 익명 ID를 획득하는 단계; 사용자로부터 입력된 상기 사용자의 ID, 상기 사용자의 ID에 대응하는 상기 사용자의 제1 익명 ID 및 상기 사용자의 제1 임시 인증값 중에서 적어도 하나를 확인하는 단계; 상기 제1 임시 인증값을 이용하여 암호화 키와 제1 MAC(Message Authentication Code) 키를 생성하는 단계; 상기 사용자의 제1 익명 ID와 다른 제2 익명 ID 및 상기 사용자의 제1 임시 인증값과 다른 제2 임시 인증값을 생성하는 단계; 및 상기 사용자와 관련된 적어도 하나의 정보 및 상기 무인기와 관련된 적어도 하나의 정보에 기반하여 상기 사용자 단말과 상기 무인기 사이에서 공유되는 동일한 제2 MAC 키와 세션키를 생성하는 단계를 포함할 수 있다.

[0014] 상술한 과제를 달성하기 위하여, 본 명세서의 일 실시 예에 따르는 무인기의 동작 방법은, 키 교환을 요청하는 사용자 단말로부터 상기 사용자 단말의 ID에 대응하는 상기 사용자 단말의 제1 익명 ID를 획득하는 단계; 상기 무인기의 ID, 상기 무인기의 ID에 대응하는 상기 무인기의 제1 익명 ID 및 상기 무인기의 제1 임시 인증값 중에서 적어도 하나를 확인하는 단계; 상기 제1 임시 인증값을 이용하여 암호화 키와 제1 MAC(Message Authentication Code) 키를 생성하는 단계; 상기 무인기의 제1 익명 ID와 다른 제2 익명 ID 및 상기 무인기의 제1 임시 인증값과 다른 제2 임시 인증값을 생성하는 단계; 및 상기 사용자 단말과 관련된 적어도 하나의 정보 및 상기 무인기와 관련된 적어도 하나의 정보에 기반하여 상기 사용자 단말과 상기 무인기 사이에서 공유되는 동일한 제2 MAC 키와 세션키를 생성하는 단계를 포함할 수 있다.

[0015] 상술한 과제를 달성하기 위하여, 본 명세서의 일 실시 예에 따르는 전자 장치는 통신 디바이스(communication device); 적어도 하나의 명령어(instruction)를 저장하는 메모리; 및 사용자 단말로부터 사용자의 ID, 상기 사용자의 ID에 대응하는 상기 사용자의 제1 익명 ID 및 상기 사용자의 제1 임시 인증값 중에서 적어도 하나를 획득하고, 무인기로부터 상기 무인기의 ID, 상기 무인기의 ID에 대응하는 상기 무인기의 제1 익명 ID 및 상기 무인기의 제1 임시 인증값 중에서 적어도 하나를 획득하고, 상기 사용자 단말의 키 교환 요청 또는 상기 무인기의 키 교환 요청에 대응하여 상기 사용자 단말로부터 획득된 정보를 포함하는 제1 정보와 상기 무인기로부터 획득된 정보를 포함하는 제2 정보에 기반하여 상기 무인기와 상기 사용자 단말 사이의 키 교환을 중계하는 제어부(controller)를 포함할 수 있다.

[0016] 기타 실시 예들의 구체적인 사항들은 상세한 설명 및 도면들에 포함되어 있다.

발명의 효과

[0017] 본 개시에 따르면, IoD 환경에서 키 교환 프로토콜을 수행할 때 사용자의 아이디뿐만 아니라 익명 아이디의 노출도 보호하는 강한 익명성을 보장할 수 있다. 또한, 무인기가 탈취되거나 사용자의 기기를 분실할 경우 사용자나 무인기의 비밀키가 노출되어도 과거의 익명 아이디들을 알 수 없어서 무인기와 사용자 간의 전방향 연결불가능성을 만족할 수 있다. 또한, 익명 아이디를 매번 생성할 경우 생성된 익명 아이디들 간의 관련성이 없어 무인

기와 사용자 간의 전방향 연결불가능성을 만족할 수 있다. 또한, 익명 아이디가 노출되더라도 익명 아이디가 사용된 시간, 장소 등을 통해서 실제 사용자를 추정할 수 없어 무인기와 사용자 간의 전방향 연결불가능성을 만족할 수 있다. 그리고, 사용자뿐만 아니라 드론도 먼저 키 교환 요청을 할 수 있어서 사건이나 사고 등의 발생에 빠르게 대처할 수 있다.

[0018] 실시 예의 효과들은 이상에서 언급한 효과들로 제한되지 않으며, 언급되지 않은 또 다른 효과들은 청구범위의 기재로부터 당해 기술 분야의 통상의 기술자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

[0019] 도 1은 일 실시 예에 따른 키 교환 프로토콜을 제공하는 시스템에 관한 블록도이다.

도 2는 일 실시 예에 따른 서버에 사용자를 등록하는 과정을 설명하기 위한 도면이다.

도 3은 일 실시 예에 따른 서버에 무인기를 등록하는 과정을 설명하기 위한 도면이다.

도 4A와 도 4B는 일 실시 예에 따른 무인기의 요청으로 인하여 사용자 단말과 무인기 사이의 키 교환 절차를 설명하기 위한 도면이다.

도 5A와 도 5B는 일 실시 예에 따른 사용자 단말에서의 요청으로 인하여 사용자 단말과 무인기 사이의 키 교환 절차를 설명하기 위한 도면이다.

도 6은 일 실시 예에 따른 전자 장치의 동작 방법을 설명하기 위한 흐름도이다.

도 7은 일 실시 예에 따른 사용자 단말의 동작 방법을 설명하기 위한 흐름도이다.

도 8은 일 실시 예에 따른 무인기의 동작 방법을 설명하기 위한 흐름도이다.

도 9는 일 실시 예에 따른 전자 장치의 블록도를 나타낸다.

발명을 실시하기 위한 구체적인 내용

[0020] 실시 예들에서 사용되는 용어는 본 개시에서의 기능을 고려하면서 가능한 현재 널리 사용되는 일반적인 용어들을 선택하였으나, 이는 당 분야에 종사하는 기술자의 의도 또는 관례, 새로운 기술의 출현 등에 따라 달라질 수 있다. 또한, 특정한 경우는 출원인이 임의로 선정한 용어도 있으며, 이 경우 해당되는 설명 부분에서 상세히 그 의미를 기재할 것이다. 따라서 본 개시에서 사용되는 용어는 단순한 용어의 명칭이 아닌, 그 용어가 가지는 의미와 본 개시의 전반에 걸친 내용을 토대로 정의되어야 한다.

[0021] 명세서 전체에서 어떤 부분이 어떤 구성요소를 “포함” 한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있음을 의미한다. 또한, 명세서에 기재된 “~부”, “~모듈” 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어 또는 소프트웨어로 구현되거나 하드웨어와 소프트웨어의 결합으로 구현될 수 있다.

[0022] 명세서 전체에서 기재된 “a, b, 및 c 중 적어도 하나”의 표현은, ‘a 단독’, ‘b 단독’, ‘c 단독’, ‘a 및 b’, ‘a 및 c’, ‘b 및 c’, 또는 ‘a,b,c 모두’를 포괄할 수 있다.

[0023] 아래에서는 첨부한 도면을 참고하여 본 개시의 실시 예에 대하여 본 개시가 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 개시는 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시 예에 한정되지 않는다.

[0024] 이하에서는 도면을 참조하여 본 개시의 실시 예들을 상세히 설명한다.

[0025] 도 1은 일 실시 예에 따른 키 교환 프로토콜을 제공하는 시스템에 관한 블록도이다.

[0026] 다양한 실시예에 따르면, 양방향 키 교환 프로토콜을 제공하는 IoD(internet of Drons) 환경의 시스템은, 사용자 단말(110)과 무인기(130) 간의 양방향 통신을 위한 키 교환 프로토콜을 지원하는 서버(120)를 포함할 수 있다.

[0027] 서버(120)는, 사용자 단말(110)과 무인기(130) 간의 키 교환 프로토콜과 관련된 각종 제어 기능을 수행할 수 있다. 키 교환 프로토콜은, 일반적으로 두 개체(예: 사용자 단말(110), 무인기(130))가 대칭키를 교환하고, 해당 키를 이용하여 메시지를 암호화하는 방식으로 통신 시 보안성을 갖도록 하는 것을 의미할 수 있다. 또한, IoD 환경에서의 키 교환 프로토콜은, 사용자 단말(110)과 무인기(130)가 서버(120)를 통해 상호 통신할 수 있는 키

를 교환하는 것을 의미할 수 있다.

- [0028] 다양한 실시예에서, 서버(120)는, 대칭키 암호화 시스템, 공개키 암호화 시스템, 해시 함수, 메시지 인증 코드(이하, Message Authentication Code, "MAC"), 생체정보를 이용한 퍼지 추출 중 적어도 하나의 기술을 이용할 수 있다. 예를 들면, 서버(120)는 기존의 해시 함수와 XOR 연산을 사용하는 대신 대칭키와 해쉬, MAC를 이용함으로써 사용자에게 강한 익명성 및 전방향 연결불가능성을 제공할 수 있다.
- [0029] 사용자 단말(120)은, 이동성을 가지며 소정의 통신 모듈을 포함하는 장치로서, 예를 들면, 휴대폰, 스마트폰, 휴대용 콘솔, 네비게이션, 랩탑 컴퓨터, 또는 태블릿 중 어느 하나에 해당할 수 있으며, 사용자 장비(UE), 모바일 스테이션, 단말, STA, 사용자 장치, 휴대용 전자 장치 등으로 지칭될 수 있다. 다른 실시예에서 사용자 단말(120)은 위치가 고정된 장치에 해당할 수도 있다.
- [0030] 사용자 단말(120)은 무인기(130)에 제어 명령을 전송하거나, 또는 무인기(130)로부터 소정의 정보(예: 영상 정보)를 수신하기 위한 장치일 수 있다. 제어 명령은, 예컨대 무인기(130)의 동작 또는 이동성을 제어하기 위한 정보에 해당할 수 있다.
- [0031] 무인기(130)는, 조종사가 탑승하지 않은 상태에서 지정된 기능을 수행할 수 있는 장치일 수 있으며, 이동성을 갖는 무인 비행체에 해당할 수 있다. 예컨대, 무인기(130)는 지정된 기능을 수행하기 위하여 방향을 변경하거나 고도를 변경하며 비행할 수 있다. 예를 들면, 무인기(130)는 통신 연결된 서버(120) 또는 사용자 단말(110)의 제어에 따라 비행하며 소정의 정보를 선택적으로 취합할 수 있으며, 또는 자율적으로 비행하며 영상 정보를 획득하고 관련 정보에 기반하여 위험 여부를 탐지하고 관련 정보를 인접 위치 내의 서버(110) 또는 사용자 단말(120)에 제공할 수도 있다.
- [0032] 이하, 사용자 단말(110), 서버(120) 및 무인기(130) 사이의 동작에 대해 자세히 기재한다.
- [0033] 도 2는 일 실시 예에 따른 서버에 사용자를 등록하는 과정을 설명하기 위한 도면이다.
- [0034] 도 2를 참조하면, 사용자 단말(210)은 사용자가 사용하는 기기로서 예를 들면 스마트폰일 수 있다. S201에서 사용자는 사용자 단말(210)에 아이디(U_i)와 비밀번호(pw_i)를 입력할 수 있고, S202에서 사용자 단말(210)은 익명 아이디(PU_i)와 임시 인증값(α_i)을 임의로 생성할 수 있다.
- [0035] S203에서 사용자 단말(210)은 생성된 익명 아이디와 임시 인증값을 아이디와 비밀번호를 해시한 값을 키로 사용하여 하기 수학적 식 1에 따라 암호화(v_i)하여 저장할 수 있다. 구체적으로, 기 설정된 해시 알고리즘(예컨대, SHA256, SHA512)을 이용하여 아이디(U_i)와 비밀번호(pw_i)를 연결한 값을 입력값으로 하여 해시(hash) 연산을 수행하고, 연산 결과를 예컨대 AES(Advanced Encryption Standard)와 ARIA(Academy Research Institute Agency)와 같은 대칭키 암호의 비밀값(키)를 생성하고, 이를 이용하여 익명 아이디(PU_i)와 임시 인증값(α_i)을 암호화할 수 있다. 본 명세서에 기재된 많은 수학적식에 포함된 E_H 와 관련하여 동일한 과정이 적용될 수 있다.
- [0036] [수학적 식 1]
- [0037]
$$v_i = E_{H(U_i || pw_i)}(PU_i || \alpha_i)$$
- [0038] S204에서 사용자 단말(210)은 아이디, 생성된 익명 아이디와 임시 인증값을 서버(230)로 전송할 수 있다. S205에서 서버(230)는 데이터베이스에 사용자의 아이디, 익명 아이디 및 임시 인증값을 저장할 수 있다. 이때, 서버(230)는 수신한 익명 아이디를 과거 익명 아이디와 현재 익명 아이디로 저장할 수 있고, 수신한 임시 인증값을 과거 인증값과 현재 인증값으로 저장할 수 있다. 예를 들면, 서버(230)는 수신한 익명 아이디 1을 과거 익명 아이디 1과 현재 익명 아이디 1로 저장할 수 있다. 이후, 서버(230)는 익명 아이디가 익명 아이디 2로 업데이트될 경우, 현재 익명 아이디를 익명 아이디 2로 갱신하고 과거 익명 아이디는 익명 아이디 1로 저장할 수 있다.
- [0039] 도 3은 일 실시 예에 따른 서버에 무인기를 등록하는 과정을 설명하기 위한 도면이다.
- [0040] 도 3을 참조하면, 무인기(310)는 예컨대, 드론과 같은 기기를 포함할 수 있다. S301에서 무인기(310)은 익명 아이디(PD_i)와 임시 인증값(β_i)을 임의로 생성할 수 있다. S302에서 무인기(310)은 무인기의 아이디(D_i), 익명

아이디 및 임시 인증값을 저장할 수 있다. S303에서 무인기(310)는 무인기의 아이디, 익명 아이디 및 임시 인증값을 서버(330)로 전송할 수 있다.

[0041] S304에서 서버(330)는 수신한 무인기의 아이디, 익명 아이디 및 임시 인증값을 데이터베이스에 저장할 수 있다. 이때, 서버(330)는 수신한 익명 아이디를 과거 익명 아이디와 현재 익명 아이디에 저장할 수 있고, 수신한 임시 인증값을 과거 인증값과 현재 인증값에 저장할 수 있다. 예를 들면, 서버(330)는 수신한 익명 아이디 1을 과거 익명 아이디 1과 현재 익명 아이디 1로 저장할 수 있다. 이후, 서버(330)는 익명 아이디가 익명 아이디 2로 업데이트될 경우, 현재 익명 아이디를 익명 아이디 2로 갱신하고 과거 익명 아이디는 익명 아이디 1로 저장할 수 있다.

[0042] 도 4A와 도 4B는 일 실시 예에 따른 무인기의 요청으로 인하여 사용자 단말과 무인기 사이의 키 교환 절차를 설명하기 위한 도면이다. 도 4A 및 도 4B에서, 서버(430)는 도 2 및 도 3에 따라 사용자 단말(410)과 무인기(450)에 대한 정보를 저장하여 등록할 수 있다.

[0043] S401에서 무인기(450)는 사용자 단말(410)로 무인기의 제1 익명 아이디(PD_i)를 전송할 수 있다.

[0044] S402에서 사용자 단말(410)는 사용자가 입력한 아이디(U_i)와 비밀번호(pw_i)를 확인할 수 있다. S403에서 사용자 단말(410)는 확인한 정보를 이용하여 사용자의 제1 익명 아이디와 제1 임시 인증값을 수학적 2에 기초하여 복호화(D_H)할 수 있다.

[0045] [수학적 2]

$$PU_i \parallel \alpha_i = D_{H(U_i \parallel pw_i)}(v_i)$$

[0046]

[0047] S404에서 사용자 단말(410)은 임시 인증값을 이용하여 하기 수학적 3에 기초하여 암호화 키(ek_i)를 생성하고, 하기 수학적 4에 기초하여 MAC 키(mk_i)를 생성할 수 있다. 구체적으로, 기 설정된 해시 알고리즘(예컨대, SHA256)을 이용하여 임시 인증값(α_i)과 0을 연결한 값을 입력값으로 하여 암호화 키(ek_i)를 생성할 수 있고, 또는 기 설정된 해시 알고리즘(예컨대, SHA256)을 이용하여 임시 인증값(α_i)과 1을 연결한 값을 입력값으로 하여 MAC 키(mk_i)를 생성할 수 있다. 본 명세서에 기재된 많은 수학적식에 포함된 ek_i 및 mk_i 와 관련하여 동일한 과정이 적용될 수 있다.

[0048] [수학적 3]

$$ek_i = H(\alpha_i \parallel 0)$$

[0049]

[0050] [수학적 4]

$$mk_i = H(\alpha_i \parallel 1)$$

[0051]

[0052] S405에서 사용자 단말(410)은 난수값(r_i), 제1 익명 아이디와 다른 새로운 제2 익명 아이디(PU'_i)와 제1 임시 인증값과 다른 새로운 제2 임시 인증값(α'_i)을 생성할 수 있다.

[0053] S406에서 사용자 단말(410)은 암호화 키를 이용하여 아이디, 새롭게 생성된 제2 익명 아이디, 새롭게 생성된 제2 임시 인증값, 무인기의 제1 익명 아이디 및 난수값을 하기 수학적 5에 기초하여 암호화할 수 있다. 구체적으로

로, 수학식 3을 통해 생성된 ek_i 를 비밀값(즉, 암호화 키이자 복호화 키)으로 이용하여 아이디, 새롭게 생성된 제2 익명 아이디, 새롭게 생성된 제2 임시 인증값, 무인기의 제1 익명 아이디 및 난수값을 대칭키 암호화할 수 있다. 본 명세서에 기재된 많은 수학식에 포함된 E_{ek_i} 와 관련하여 동일한 과정이 적용될 수 있다.

[수학식 5]

$$c_i = E_{ek_i}(U_i \parallel PU_i' \parallel \alpha_i' \parallel PD_j \parallel ru_i)$$

S407에서 사용자 단말(410)은 암호문(c_i)을 사용자의 제1 익명 아이디, 서버의 아이디와 함께 MAC 키(mk_i)를 이용하여 하기 수학식 6에 기초하여 연산하여 제1 값(τ_i)을 도출할 수 있다. 구체적으로, 암호문(c_i), 사용자의 제1 익명 아이디 및 서버의 아이디와 함께 수학식 4를 통해 생성된 MAC 키(mk_i)를 이용하여 인증값(τ_i)을 생성할 수 있다. 이후, MAC 키를 이용하여 인증값(τ_i)이 정당한 메시지인지 인증될 수 있다. 본 명세서에 기재된 많은 수학식에 포함된 MAC 키를 이용한 연산에 대하여 동일한 과정이 적용될 수 있다.

[수학식 6]

$$\tau_i = Mac_{mk_i}(PU_i \parallel S \parallel c_i)$$

S408에서 사용자 단말(410)은 사용자의 제1 익명 아이디, 서버의 아이디, 암호문 및 제1 값을 서버(430)로 전송할 수 있다.

S409에서 서버(430)는 사용자의 제1 익명 아이디를 이용하여 사용자의 아이디, 과거 인증값과 현재 인증값을 확인할 수 있다. S411에서, 서버(430)는 현재 인증값 또는 과거 인증값을 이용하여 사용자와 서버 사이의 암호화 키를 하기 수학식 7에 기초하여 생성하거나, MAC 키를 하기 수학식 8에 기초하여 생성할 수 있다. 수학식 3 및 수학식 4에 기재된 내용이 적용될 수 있다.

[수학식 7]

$$ek_i = H(\alpha_i \parallel 0)$$

[수학식 8]

$$mk_i = H(\alpha_i \parallel 1)$$

S412에서 서버(430)는 암호화 키로 수신한 암호문을 복호화할 수 있고, S413에서 서버(430)는 MAC 키를 이용하여 수신한 제1 값을 인증할 수 있다. S414에서 서버(430)는 제1 값이 인증될 경우, 복호화한 무인기의 익명 아이디를 이용하여 무인기의 아이디, 과거 인증값과 현재 인증값을 확인할 수 있다. S415에서 서버(430)는 확인한 과거 인증값 또는 현재 인증값을 이용하여 무인기와 서버 사이의 암호화 키를 수학식 9에 기초하여 생성하고, MAC 키를 수학식 10에 기초하여 생성할 수 있다. 수학식 3 및 수학식 4에 기재된 내용이 적용될 수 있다.

[수학식 9]

$$ek_j = H(\beta_j \parallel 0)$$

[0068] [수학식 10]

$$mk_j = H(\beta_j \parallel 1)$$

[0069]

[0070] S416에서 서버(430)는 생성한 암호화 키로 사용자의 제1 익명 아이디(PU_i)와 사용자가 생성한 난수값(ru_i)을 수학식 11에 기초하여 암호화 할 수 있다. 수학식 5에 기재된 내용이 적용될 수 있다.

[0071] [수학식 11]

$$c_j = E_{ek_j}(PU_i \parallel ru_i)$$

[0072]

[0073] S417에서 서버(430)는 암호문(c_j)을 서버의 아이디, 드론의 제1 익명 아이디와 함께 MAC 키를 사용하여 수학식 12에 기초하여 연산하여 제2 값을 도출할 수 있다. 수학식 6에 기재된 내용이 적용될 수 있다.

[0074] [수학식 12]

$$\tau_j = Mac_{mk_j}(S \parallel PD_j \parallel c_j)$$

[0075]

[0076] S418에서 서버(430)는 서버의 아이디(S), 드론의 제1 익명 아이디(PD_j), 암호문(c_j)과 제2 값(τ_j)을 무인기(450)으로 전송할 수 있다.

[0077] S419에서 무인기(450)는 무인기의 인증값을 이용하여 암호화 키를 수학식 13에 기초하여 생성하고, MAC 키를 수학식 14에 기초하여 생성할 수 있다. 수학식 3 및 수학식 4에 기재된 내용이 적용될 수 있다.

[0078] [수학식 13]

$$ek_j = H(\beta_j \parallel 0)$$

[0079]

[0080] [수학식 14]

$$mk_j = H(\beta_j \parallel 1)$$

[0081]

[0082] S421에서 무인기(450)는 생성한 암호화 키를 이용하여 서버(430)에서 수신한 암호문을 복호화할 수 있고, S422에서 무인기(450)는 MAC 키를 이용하여 수신한 제2 값을 인증할 수 있다. S423에서 무인기(450)는 난수값, 새로운 제2 익명 아이디와 새로운 제2 임시 인증값을 생성할 수 있다. S424에서 무인기(450)는 생성한 제2 익명 아이디(PD_j')와 제2 임시 인증값(β_j') 및 난수값(rd_j), 사용자 단말(410)에서 생성된 난수값(ru_i)을 수학식 15에 기초하여 암호화할 수 있다. 수학식 5에 기재된 내용이 적용될 수 있다.

[0083] [수학식 15]

$$d_j = E_{ek_j}(PD_j' \parallel \beta_j' \parallel ru_i \parallel rd_j)$$

[0084]

[0085] S425에서 무인기(450)는 생성된 암호문(d_j)을 드론의 제1 익명 아이디(PD_j), 서버의 아이디(S)와 함께 MAC 키를 사용하여 수학식 16에 기초하여 연산하여 제3 값을 도출할 수 있다. 수학식 6에 기재된 내용이 적용될 수 있다.

[0086] [수학식 16]

$$\epsilon_j = \text{Mac}_{mk_j}(PD_j \parallel S \parallel d_j)$$

[0087]

[0088] S426에서 무인기(450)는 드론의 제1 익명 아이디(PD_j), 서버의 아이디(S), 암호문(d_j) 및 제3 값(ϵ_j)을 서버(430)로 전송할 수 있다.

[0089] S427에서 서버(430)는 무인기의 암호화 키를 이용하여 수신한 암호문을 복호화할 수 있고, S428에서 서버(430)는 MAC 키를 이용하여 제3 값을 인증할 수 있다. S429에서 서버(430)는 사용자의 암호화 키(ek_i)를 이용하여 수학식 17에 기초하여 암호화할 수 있다. 수학식 5에 기재된 내용이 적용될 수 있다.

[0090] [수학식 17]

$$d_i = E_{ek_i}(PD_j \parallel ru_i \parallel rd_j)$$

[0091]

[0092] S431에서 서버(430)는 암호문(d_i)을 MAC 키를 사용하여 수학식 18에 기초하여 연산하여 제4 값(ϵ_j)을 도출할 수 있다. 수학식 6에 기재된 내용이 적용될 수 있다.

[0093] [수학식 18]

$$\epsilon_j = \text{Mac}_{mk_j}(S \parallel PU_i \parallel d_i)$$

[0094]

[0095] S432에서 서버(430)는 사용자의 아이디(U_i), 사용자의 과거 제1 익명 아이디(PU_i), 사용자의 현재 제2 익명 아이디(PU_i'), 사용자의 과거 제1 임시 인증값(α_i), 사용자의 현재 제2 임시 인증값(α_i') 등을 수학식 19와 같이 저장할 수 있다.

[0096] [수학식 19]

$$U_i, PU_i^o = PU_i, PU_i^n = PU_i', \alpha_i^o = \alpha_i, \alpha_i^n = \alpha_i'$$

[0097]

[0098] S433에서 서버(430)는 무인기의 아이디(D_j), 무인기의 과거 제1 익명 아이디(PD_j), 무인기의 현재 제2 익명 아이디(PD_j'), 무인기의 과거 제1 임시 인증값(β_j), 무인기의 현재 제2 임시 인증값(β_j') 등을 수학식 20과 같이 저장할 수 있다.

[0099] [수학식 20]

$$D_j, PD_j^o = PD_j, PD_j^n = PD_j', \beta_j^o = \beta_j, \beta_j^n = \beta_j'$$

[0100]

[0101] S434에서 서버(430)는 사용자 단말(410)로 서버의 아이디, 사용자의 제1 익명 아이디, 암호문과 제4 값을 전송할 수 있다.

[0102] S435에서 사용자 단말(410)은 사용자의 암호화 키를 이용하여 수신한 암호문을 복호화할 수 있고, S436에서 사용자 단말(410)은 MAC 키를 이용하여 수신한 제4 값을 인증할 수 있다.

[0103] S437에서 사용자 단말(410)은 사용자의 제1 익명 아이디(PU_i)와 난수값(ru_i), 무인기의 제1 익명 아이디

(PD_j)와 난수값(rd_j)을 이용하여 수학적식 21에 기초하여 MAC 키를 생성할 수 있고, 수학적식 22에 기초하여 세션키를 생성할 수 있다. 수학적식 3 및 수학적식 4에 기재된 내용이 적용될 수 있다.

[수학적식 21]

$$mk_{i,j} = H(PU_i \parallel PD_j \parallel ru_i \parallel rd_j \parallel 0)$$

[수학적식 22]

$$sk_{i,j} = H(PU_i \parallel PD_j \parallel ru_i \parallel rd_j \parallel 1)$$

S438에서 사용자 단말(410)은 사용자의 제1 익명 아이디(PU_i)와 드론의 제1 익명 아이디(PD_j)를 MAC 키를 사용하여 수학적식 23에 기초하여 연산하여 제5 값($\delta_{i,j}$)을 도출할 수 있다. 수학적식 6에 기재된 내용이 적용될 수 있다.

[수학적식 23]

$$\delta_{i,j} = Mac_{mk_{i,j}}(PU_i \parallel PD_j \parallel 0)$$

S439에서 사용자 단말(410)은 사용자의 제2 익명 아이디(PU'_i)와 제2 임시 인증값(α'_i)을 수학적식 24에 기초하여 암호화한 후 저장할 수 있다. 수학적식 1에 기재된 내용이 적용될 수 있다.

[수학적식 24]

$$v_i = E_{H(U_i \parallel pw_i)}(PU'_i \parallel \alpha'_i)$$

S441에서 사용자 단말(410)은 사용자의 제1 익명 아이디, 드론의 제1 익명 아이디 및 제5 값을 무인기(450)로 전송할 수 있다.

S442에서 무인기(450)는 익명 아이디들과 난수값들을 이용하여 MAC 키를 수학적식 25에 기초하여 생성하고, 세션키를 수학적식 26에 기초하여 생성할 수 있다. 이때, 수학적식 25과 수학적식 26에 기초하여 생성된 MAC 키와 세션키는 수학적식 21과 수학적식 22에 기초하여 생성된 MAC 키와 세션키와 동일할 수 있다. 따라서, 사용자 단말과 무인기는 동일한 MAC 키와 세션 키를 공유할 수 있다. 수학적식 3 및 수학적식 4에 기재된 내용이 적용될 수 있다.

[수학적식 25]

$$mk_{i,j} = H(PU_i \parallel PD_j \parallel ru_i \parallel rd_j \parallel 0)$$

[수학적식 26]

$$sk_{i,j} = H(PU_i \parallel PD_j \parallel ru_i \parallel rd_j \parallel 1)$$

S443에서 무인기(450)는 사용자 단말로부터 수신한 제5 값을 인증할 수 있다. 이후, 무인기(450)는 무인기의 아이디, 무인기의 현재 제2 익명 아이디(PD'_j) 및 현재 제2 임시 인증값(β'_j)을 저장할 수 있다.

무인기의 요청으로 인하여 키 교환 프로토콜은 전술한 도 2, 도 3 및 도 4A, 4B 단계를 통해 수행될 수 있다.

도 5A와 도 5B는 일 실시 예에 따른 사용자 단말에서의 요청으로 인하여 사용자 단말과 무인기 사이의 키 교환 절차를 설명하기 위한 도면이다. 도 5A 및 도 5B에서, 서버(530)는 도 2 및 도 3에 따라 사용자 단말(510)과 무인기(550)에 대한 정보를 저장하여 등록할 수 있다.

도 5A 및 도 5B를 참조하면, 도 4A 및 도 4B에서 무인기 - 사용자 단말 - 서버 - 무인기- 서버 - 사용자 단말 -

무인기 순으로 진행되는 것과 달리, 사용자 단말 - 무인기 - 서버 - 사용자 단말 - 서버 - 무인기 - 사용자 단말 순으로 진행될 수 있다. 도 4A 및 도 4B와 기재된 단어와 도 5A 및 도 5B에 기재된 단어는 동일한 의미를 포함할 수 있다.

[0124] 도 4A 및 도 4B의 수학적식에 기재된 내용이 도 5A 및 도 5B의 수학적식 연산 과정에서도 적용될 수 있다.

[0125] S501에서 사용자 단말(510)은 사용자의 아이디와 비밀번호를 이용하여 익명 아이디와 인증값을 복호화하고 암호화 키와 MAC 키를 생성할 수 있다. S502에서 사용자 단말(510)은 무인기(550)로 사용자의 제1 익명 아이디를 전송할 수 있다.

[0126] S503에서 무인기(550)는 제1 임시 인증값(β_j)을 이용하여 암호화 키를 수학적식 27에 기초하여 생성하고, MAC 키를 수학적식 28에 기초하여 생성할 수 있다.

[0127] [수학적식 27]

$$ek_j = H(\beta_j \parallel 0)$$

[0128] [수학적식 28]

$$mk_j = H(\beta_j \parallel 1)$$

[0131] S504에서 무인기(550)는 난수값(rd_j), 새로운 제2 익명 아이디(PD_j') 및 제2 임시 인증값(β_j')을 생성할 수 있다. S505에서 무인기(550)는 무인기의 아이디(D_j), 제2 익명 아이디(PD_j'), 제2 임시 인증값(β_j'), 사용자의 제1 익명 아이디(PU_i) 및 난수값(rd_j)을 수학적식 29에 기초하여 암호화할 수 있다.

[0132] [수학적식 29]

$$c_j = E_{ek_j}(D_j \parallel PD_j' \parallel \beta_j' \parallel PU_i \parallel rd_j)$$

[0134] S506에서 무인기(550)는 암호문(c_j)을 무인기의 제1 익명 아이디(PD_j), 서버의 아이디(S)와 함께 MAC 키(mk_j)를 이용하여 수학적식 30에 기초하여 연산하여 제1 값(τ_j)을 도출할 수 있다.

[0135] [수학적식 30]

$$\tau_j = Mac_{mk_j}(PD_j \parallel S \parallel c_j)$$

[0137] S507에서 무인기(550)는 무인기의 제1 익명 아이디(PD_j), 서버의 아이디(S), 암호문(c_j) 및 제1 값(τ_j)을 서버(530)로 전송할 수 있다.

[0138] S508에서 서버(530)는 무인기의 기존 제1 익명 아이디를 이용하여 무인기의 아이디, 과거 제1 임시 인증값과 현재 제2 임시 인증값을 확인할 수 있다.

[0139] S509에서 서버(530)는 과거 제1 임시 인증값 또는 현재 제2 임시 인증값을 이용하여 무인기와 서버 사이의 암호화 키와 MAC 키를 생성할 수 있다. S511에서 서버(530)는 생성된 암호화 키를 이용하여 수신한 암호문(c_j)을 복호화할 수 있다. S512에서 서버(530)는 생성된 MAC 키를 이용하여 수신한 제1 값(τ_j)을 인증할 수 있다.

[0140] S513에서 서버(530)는 인증될 경우, 복호화한 사용자의 제1 익명 아이디(PU_i)를 이용하여 사용자의 아이디

(U_i), 과거 제1 임시 인증값(PU_i)과 현재 제2 임시 인증값(PU'_i)을 확인할 수 있다.

[0141] S514에서 서버(530)는 제1 임시 인증값(PU_i)과 제2 임시 인증값(PU'_i)을 이용하여 사용자와 서버 사이의 암호화 키와 MAC 키를 생성할 수 있다.

[0142] S515에서 서버(530)는 생성한 암호화 키를 이용하여 무인기의 제1 익명 아이디(PD_j)와 무인기가 생성한 난수값(rd_j)을 수학적 식 31에 기초하여 암호화할 수 있다.

[0143] [수학적 식 31]

$$c_i = E_{ek_i}(PD_j || rd_j)$$

[0145] S516에서 서버(530)는 암호문(c_i)을 서버의 아이디(S), 사용자의 제1 익명 아이디(PU_i)와 함께 MAC 키(mk_i)를 사용하여 수학적 식 32에 기초하여 연산하여 제2 값(τ_i)을 도출할 수 있다.

[0146] [수학적 식 32]

$$\tau_i = Mac_{mk_i}(S || PU_i || c_i)$$

[0148] S517에서 서버(530)는 서버의 아이디(S), 사용자의 제1 익명 아이디(PU_i), 암호문(c_i) 및 제2 값(τ_i)을 사용자 단말(510)으로 전송할 수 있다.

[0149] S518에서 사용자 단말(510)은 암호화 키를 이용하여 수신한 암호문(c_i)을 복호화할 수 있다. S519에서 사용자 단말(510)은 MAC 키를 이용하여 수신한 제2 값(τ_i)을 인증할 수 있다. S521에서 사용자 단말(510)은 난수값(ru_i), 사용자의 제2 익명 아이디(PU'_i)와 제2 임시 인증값(α'_i)을 생성할 수 있다.

[0150] S522에서 사용자 단말(510)은 난수값(ru_i , rd_j), 사용자의 제2 익명 아이디(PU'_i)와 제2 임시 인증값(α'_i)을 수학적 식 33에 기초하여 암호화할 수 있다.

[0151] [수학적 식 33]

$$d_i = E_{ek_i}(PU'_i || \alpha'_i || ru_i || rd_j)$$

[0153] S523에서 사용자 단말(510)은 암호문(d_i)을 사용자의 제1 익명 아이디(PU_i), 서버의 아이디(S)와 함께 MAC 키(mk_i)를 사용하여 수학적 식 34에 기초하여 연산하여 제3 값(ϵ_i)을 도출할 수 있다.

[0154] [수학적 식 34]

$$\epsilon_i = Mac_{mk_i}(PU_i || S || d_i)$$

[0156] S524에서 사용자 단말(510)은 사용자의 제1 익명 아이디(PU_i), 서버의 아이디(S), 암호문(d_i) 및 제3 값(ϵ_i)을 서버(530)로 전송할 수 있다.

[0157] S525에서 서버(530)는 사용자의 암호화 키를 이용하여 수신한 암호문을 복호화할 수 있고, S526에서 서버(530)는 MAC 키를 이용하여 수신한 제3 값을 인증할 수 있다.

[0158] S527에서 서버(530)는 무인기의 암호화 키를 이용하여 사용자의 제1 익명 아이디(PU_i) 및 난수값들(ru_i , rd_j)을 수학적 식 35에 기초하여 암호화할 수 있다.

[0159] [수학적 식 35]

$$d_j = E_{ek_j}(PU_i || ru_i || rd_j)$$

[0160]

[0161] S528에서 서버(530)는 서버의 아이디, 무인기의 제1 익명 아이디 등을 암호문(d_j)을 MAC 키를 이용하여 수학적 식 36에 기초하여 연산하여 제4 값(ϵ_j)을 도출할 수 있다.

[0162] [수학적 식 36]

$$\epsilon_j = Mac_{mk_j}(S || PD_j || d_j)$$

[0163]

[0164] S529에서 서버(530)는 사용자의 아이디(U_i), 사용자의 과거 제1 익명 아이디(PU_i), 사용자의 현재 제2 익명 아이디(PU'_i), 사용자의 과거 제1 임시 인증값(α_i), 사용자의 현재 제2 임시 인증값(α'_i)을 수학적 식 37과 같이 저장할 수 있다. 또한, 서버(530)는 무인기의 아이디(D_j), 무인기의 과거 제1 익명 아이디(PD_j), 무인기의 현재 제2 익명 아이디(PD'_j), 무인기의 과거 제1 임시 인증값(β_j), 무인기의 현재 제2 임시 인증값(β'_j)을 수학적 식 37과 같이 저장할 수 있다.

[0165] [수학적 식 37]

$$\begin{aligned} & \text{Store}(U_i, PU_i^o = PU_i, PU_i^n = PU'_i, \\ & \quad \alpha_i^o = \alpha_i, \alpha_i^n = \alpha'_i) \\ & \text{and}(D_j, PD_j^o = PD_j, PD_j^n = PD'_j, \\ & \quad \beta_j^o = \beta_j, \beta_j^n = \beta'_j) \end{aligned}$$

[0166]

[0167] S531에서 서버(530)는 무인기의 제1 익명 아이디(PD_j), 서버의 아이디(S), 암호문(d_j) 및 제4 값(ϵ_j)을 무인기(550)로 전송할 수 있다.

[0168] S532에서 무인기(550)는 무인기의 암호화 키를 이용하여 수신한 암호문을 복호화할 수 있다. S533에서 무인기(550)는 MAC 키를 이용하여 수신한 제4 값을 인증할 수 있다.

[0169] S534에서 무인기(550)는 무인기의 제1 익명 아이디(PD_j)와 난수값(rd_j), 사용자의 제1 익명 아이디(PU_i)와 난수값(ru_i)을 이용하여 수학적 식 38에 기초하여 MAC 키를 생성하고, 수학적 식 39에 기초하여 세션 키를 생성할 수 있다.

[0170] [수학적 식 38]

$$mk_{i,j} = H(PU_i || PD_j || ru_i || rd_j || 0)$$

[0171]

[0172] [수학적 식 39]

$$sk_{i,j} = H(PU_i || PD_j || ru_i || rd_j || 1)$$

[0173]

[0174] S535에서 무인기(550)는 사용자의 제1 익명 아이디(PU_i)와 무인기의 제1 익명 아이디(PD_j)를 MAC 키를 이용

하여 수학적식 40에 기초하여 연산하여 제5 값($\delta_{i,j}$)을 도출할 수 있다.

[수학적식 40]

$$\delta_{i,j} = \text{Mac}_{mk_{i,j}}(PU_i || PD_j || 0)$$

무인기(550)는 무인기의 아이디(D_j), 무인기의 제2 익명 아이디(PD'_j), 제2 임시 인증값(β'_j)을 저장할 수 있다. S536에서 무인기(550)는 사용자의 제1 익명 아이디(PU_i)와 무인기의 제1 익명 아이디(PD_j) 및 제5 값($\delta_{i,j}$)을 사용자 단말(510)로 전송할 수 있다.

S537에서 사용자 단말(510)은 무인기의 제1 익명 아이디, 사용자의 제1 익명 아이디, 난수값들을 이용하여 수학적식 41에 기초하여 MAC 키를 생성하고, 수학적식 42에 기초하여 세션 키를 생성할 수 있다. 이때, 수학적식 41과 수학적식 42에 기초하여 생성된 MAC 키와 세션키는 수학적식 38과 수학적식 39에 기초하여 생성된 MAC 키와 세션키와 동일할 수 있다. 따라서, 사용자 단말과 무인기는 동일한 MAC 키와 세션 키를 공유할 수 있다.

[수학적식 41]

$$mk_{i,j} = H(PU_i || PD_j || ru_i || rd_j || 0)$$

[수학적식 42]

$$sk_{i,j} = H(PU_i || PD_j || ru_i || rd_j || 1)$$

S538에서 사용자 단말(510)은 MAC 키를 사용하여 제5 값을 인증할 수 있고, 이후 사용자의 제2 익명 아이디와 제2 임시 인증값을 수학적식 43에 기초하여 암호화하여 저장할 수 있다.

[수학적식 43]

$$v_i = E_{H(U_i || pw_i)}(PU'_i || \alpha'_i)$$

사용자의 요청으로 인하여 키 교환 프로토콜은 전술한 도 2, 도 3 및 도 5A, 5B 단계를 통해 수행될 수 있다.

도 6은 일 실시 예에 따른 전자 장치의 동작 방법을 설명하기 위한 흐름도이다. 참고로, 전자 장치는 앞서 전술한 서버에 포함되는 기기일 수 있으며, 앞서 전술한 내용이 도 6에도 적용될 수 있다.

도 6을 참조하면, 도 2에 기재된 사용자를 서버에 등록하는 과정을 통해 S610에서 전자 장치는 사용자 단말로부터 사용자의 ID, 사용자의 ID에 대응하는 사용자의 제1 익명 아이디 및 사용자의 제1 임시 인증값 중에서 적어도 하나를 획득할 수 있다.

도 3에 기재된 무인기를 서버에 등록하는 과정을 통해 S620에서 전자 장치는 무인기로부터 무인기의 ID, 무인기의 ID에 대응하는 무인기의 제1 익명 ID 및 무인기의 제1 임시 인증값 중에서 적어도 하나를 획득할 수 있다.

도 4A, 4B 및 도 5A, 5B에 기재된 바와 같이 전자 장치는 사용자 단말과 무인기 사이 키 교환 절차를 중계할 수 있다.

S630에서 전자 장치는 사용자 단말의 키 교환 요청 또는 상기 무인기의 키 교환 요청에 대응하여 사용자 단말로부터 획득된 정보를 포함하는 제1 정보와 무인기로부터 획득된 정보를 포함하는 제2 정보에 기반하여 무인기와 사용자 단말 사이의 키 교환을 중계할 수 있다.

이때, 무인기의 키 교환 요청은, 도 4A 및 도 4B에 기재된 바와 같이 무인기에서 사용자 단말로 무인기의 제1 익명 ID를 전송하는 것에 대응할 수 있다. 또한, 사용자 단말의 키 교환 요청은, 도 5A 및 도 5B에 기재된 바와 같이 사용자 단말에서 무인기로 사용자 단말의 제1 익명 ID를 전송하는 것에 대응할 수 있다.

또한, 무인기와 사용자 단말 사이 키 교환으로 인하여, 사용자 단말과 무인기는 동일한 MAC 키와 세션키를 공유할 수 있다.

- [0194] 이때, 사용자의 제1 익명 ID 및 제1 임시 인증값은 사용자의 ID와 관계 없이 임의로 생성되고, 무인기의 제1 익명 ID 및 제1 임시 인증값도 무인기의 ID와 관계 없이 임의로 생성될 수 있다.
- [0195] 또한, 제1 정보는 사용자의 ID, 사용자의 제1 익명 ID, 사용자의 제1 임시 인증값, 사용자의 제1 익명 ID와 다른 제2 익명 ID, 사용자의 제1 임시 인증값과 다른 제2 임시 인증값 및 사용자의 난수값 중에서 적어도 하나를 포함할 수 있다.
- [0196] 또한, 제2 정보는 무인기의 ID, 무인기의 제1 익명 ID, 무인기의 제1 임시 인증값, 무인기의 제1 익명 ID와 다른 제2 익명 ID, 무인기의 제1 임시 인증값과 다른 제2 임시 인증값 및 무인기의 난수값 중에서 적어도 하나를 포함할 수 있다.
- [0197] 도 7은 일 실시 예에 따른 사용자 단말의 동작 방법을 설명하기 위한 흐름도이다. 도 4A 및 도 4B에 기재된 내용이 도 7에 적용될 수 있으며, 자세한 내용은 전술한 기재를 참조한다.
- [0198] 도 7을 참조하면, S710에서 사용자 단말은 키 교환 요청하는 무인기로부터 무인기의 ID에 대응하는 무인기의 제1 익명 ID를 획득할 수 있다. S720에서 사용자 단말은 사용자로부터 입력된 사용자의 ID, 사용자의 ID에 대응하는 사용자의 제1 익명 ID 및 사용자의 제1 임시 인증값 중에서 적어도 하나를 확인할 수 있다. S730에서 사용자 단말은 제1 임시 인증값을 이용하여 암호화 키와 제1 MAC(Message Authentication Code) 키를 생성할 수 있다. S740에서 사용자 단말은 사용자의 제1 익명 ID와 다른 제2 익명 ID 및 사용자의 제1 임시 인증값과 다른 제2 임시 인증값을 생성할 수 있다. S750에서 사용자 단말은 사용자와 관련된 적어도 하나의 정보 및 무인기와 관련된 적어도 하나의 정보에 기반하여 사용자 단말과 무인기 사이에서 공유되는 동일한 제2 MAC 키와 세션키를 생성할 수 있다.
- [0199] 도 8은 일 실시 예에 따른 무인기의 동작 방법을 설명하기 위한 흐름도이다. 도 5A 및 도 5B에 기재된 내용이 도 8에 적용될 수 있으며, 자세한 내용은 전술한 기재를 참조한다.
- [0200] 도 8을 참조하면, S810에서 무인기는 키 교환을 요청하는 사용자 단말로부터 사용자 단말의 ID에 대응하는 사용자 단말의 제1 익명 ID를 획득할 수 있다. S820에서 무인기는 무인기의 ID, 무인기의 ID에 대응하는 무인기의 제1 익명 ID 및 무인기의 제1 임시 인증값 중에서 적어도 하나를 확인할 수 있다. S830에서 무인기는 제1 임시 인증값을 이용하여 암호화 키와 제1 MAC(Message Authentication Code) 키를 생성할 수 있다. S840에서 무인기는 무인기의 제1 익명 ID와 다른 제2 익명 ID 및 무인기의 제1 임시 인증값과 다른 제2 임시 인증값을 생성할 수 있다. S850에서 무인기는 사용자 단말과 관련된 적어도 하나의 정보 및 무인기와 관련된 적어도 하나의 정보에 기반하여 사용자 단말과 무인기 사이에서 공유되는 동일한 제2 MAC 키와 세션키를 생성할 수 있다.
- [0201] 도 9는 일 실시 예에 따른 전자 장치의 블록도를 나타낸다.
- [0202] 전자 장치(900)는 일 실시 예에 따라, 통신 디바이스(910), 메모리(920) 및 제어부(930)를 포함할 수 있다. 도 9에 도시된 전자 장치(900)는 본 실시 예와 관련된 구성요소들만이 도시되어 있다. 따라서, 도 9에 도시된 구성요소들 외에 다른 범용적인 구성요소들이 더 포함될 수 있음을 본 실시 예와 관련된 기술분야에서 통상의 지식을 가진 자라면 이해할 수 있다. 전자 장치(900)는 전술한 내용이 적용될 수 있는 바, 중복되는 내용에 대해서는 설명을 생략한다.
- [0203] 통신 디바이스(910)는 유무선 통신을 수행할 수 있는 기기이고, 메모리(920)는 적어도 하나의 명령어(instruction)를 저장하는 기기일 수 있다. 제어부(930)는 전자 장치(900)의 전반의 동작을 제어하고 데이터 및 신호를 처리할 수 있다. 제어부(930)는 적어도 하나의 하드웨어 유닛으로 구성될 수 있다. 또한, 제어부(930)는 메모리(920)에 저장된 프로그램 코드를 실행하여 생성되는 하나 이상의 소프트웨어 모듈에 의해 동작할 수 있다. 제어부(930)는 메모리(920)에 저장된 프로그램 코드를 실행하여 전자 장치(900)의 전반의 동작을 제어하고 데이터 및 신호를 처리할 수 있다.
- [0204] 제어부(930)는 사용자 단말로부터 사용자의 ID, 상기 사용자의 ID에 대응하는 상기 사용자의 제1 익명 ID 및 상기 사용자의 제1 임시 인증값 중에서 적어도 하나를 획득하고, 무인기로부터 상기 무인기의 ID, 상기 무인기의 ID에 대응하는 상기 무인기의 제1 익명 ID 및 상기 무인기의 제1 임시 인증값 중에서 적어도 하나를 획득하고, 상기 사용자 단말의 키 교환 요청 또는 상기 무인기의 키 교환 요청에 대응하여 상기 사용자 단말과 관련된 정보와 상기 무인기와 관련된 정보에 기반하여 상기 무인기와 상기 사용자 단말 사이의 키 교환을 중계할 수 있다.
- [0205] 전술한 전자 장치 또는 단말은, 프로세서, 프로그램 데이터를 저장하고 실행하는 메모리, 디스크 드라이브와 같

은 영구 저장부(permanent storage), 외부 장치와 통신하는 통신 포트, 사용자 인터페이스 장치 등을 포함할 수 있다. 이 외에도 다른 범용적인 구성요소들이 더 포함될 수 있음을 본 실시 예와 관련된 기술분야에서 통상의 지식을 가진 자라면 이해할 수 있다. 프로세서는 공초점 반사 기기의 설계 방법의 전반의 동작을 제어하고 데이터 및 신호를 처리할 수 있다. 프로세서는 적어도 하나의 하드웨어 유닛으로 구성될 수 있다. 또한, 프로세서는 메모리에 저장된 프로그램 코드를 실행하여 생성되는 하나 이상의 소프트웨어 모듈에 의해 동작할 수 있다. 프로세서는 메모리에 저장된 프로그램 코드를 실행하여 공초점 반사 기기의 설계 방법의 전반의 동작을 제어하고 데이터 및 신호를 처리할 수 있다. 소프트웨어 모듈 또는 알고리즘으로 구현되는 방법들은 상기 프로세서상에서 실행 가능한 컴퓨터가 읽을 수 있는 코드들 또는 프로그램 명령들로서 컴퓨터가 읽을 수 있는 기록 매체 상에 저장될 수 있다. 여기서 컴퓨터가 읽을 수 있는 기록 매체로 마그네틱 저장 매체(예컨대, ROM(read-only memory), RAM(random-access memory), 플로피 디스크, 하드 디스크 등) 및 광학적 판독 매체(예컨대, 시디롬(CD-ROM), 디브이디(DVD: Digital Versatile Disc)) 등이 있다. 컴퓨터가 읽을 수 있는 기록 매체는 네트워크로 연결된 컴퓨터 시스템들에 분산되어, 분산 방식으로 컴퓨터가 판독 가능한 코드가 저장되고 실행될 수 있다. 매체는 컴퓨터에 의해 판독가능하며, 메모리에 저장되고, 프로세서에서 실행될 수 있다.

[0206]

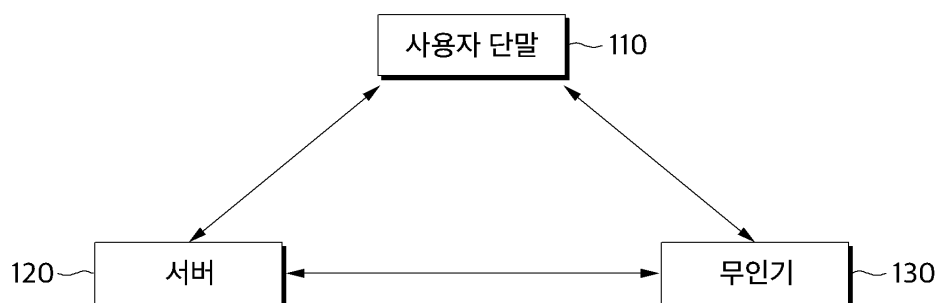
본 실시 예는 기능적인 블록 구성들 및 다양한 처리 단계들로 나타내어질 수 있다. 이러한 기능 블록들은 특정 기능들을 실행하는 다양한 개수의 하드웨어 또는/및 소프트웨어 구성들로 구현될 수 있다. 예를 들어, 실시 예는 하나 이상의 마이크로프로세서들의 제어 또는 다른 제어 장치들에 의해서 다양한 기능들을 실행할 수 있는, 메모리, 프로세싱, 로직(logic), 룩 업 테이블(look-up table) 등과 같은 직접 회로 구성들을 채용할 수 있다. 구성 요소들이 소프트웨어 프로그래밍 또는 소프트웨어 요소들로 실행될 수 있는 것과 유사하게, 본 실시 예는 데이터 구조, 프로세스들, 루틴들 또는 다른 프로그래밍 구성들의 조합으로 구현되는 다양한 알고리즘을 포함하여, C, C++, 자바(Java), 어셈블러(assembler) 등과 같은 프로그래밍 또는 스크립팅 언어로 구현될 수 있다. 기능적인 측면들은 하나 이상의 프로세서들에서 실행되는 알고리즘으로 구현될 수 있다. 또한, 본 실시 예는 전자적인 환경 설정, 신호 처리, 및/또는 데이터 처리 등을 위하여 종래 기술을 채용할 수 있다. “매커니즘”, “요소”, “수단”, “구성”과 같은 용어는 넓게 사용될 수 있으며, 기계적이고 물리적인 구성들로서 한정되는 것은 아니다. 상기 용어는 프로세서 등과 연계하여 소프트웨어의 일련의 처리들(routines)의 의미를 포함할 수 있다.

[0207]

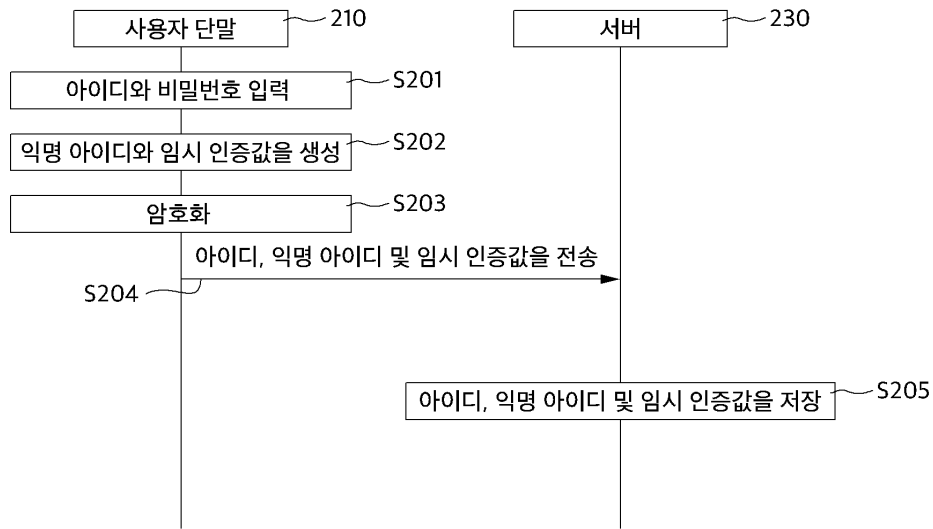
전술한 실시예들은 일 예시일 뿐 후술하는 청구항들의 범위 내에서 다른 실시예들이 구현될 수 있다.

도면

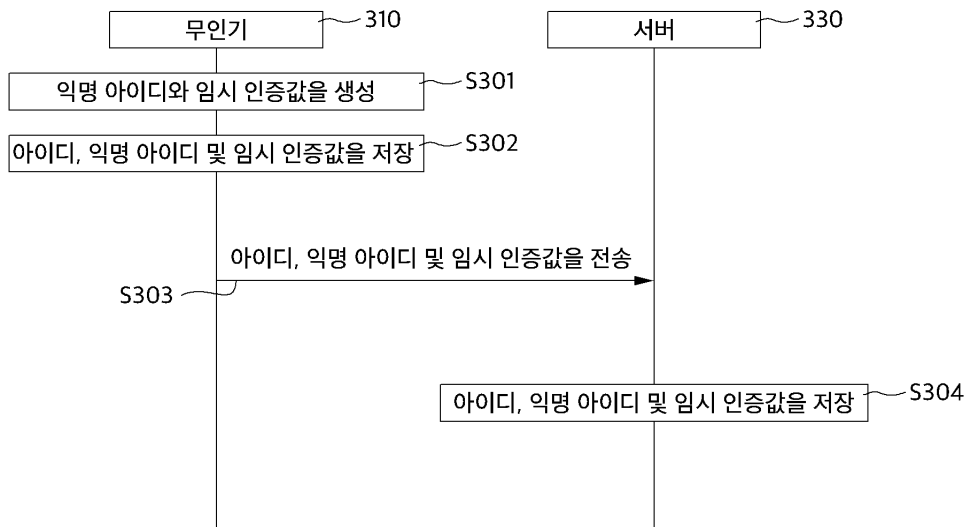
도면1



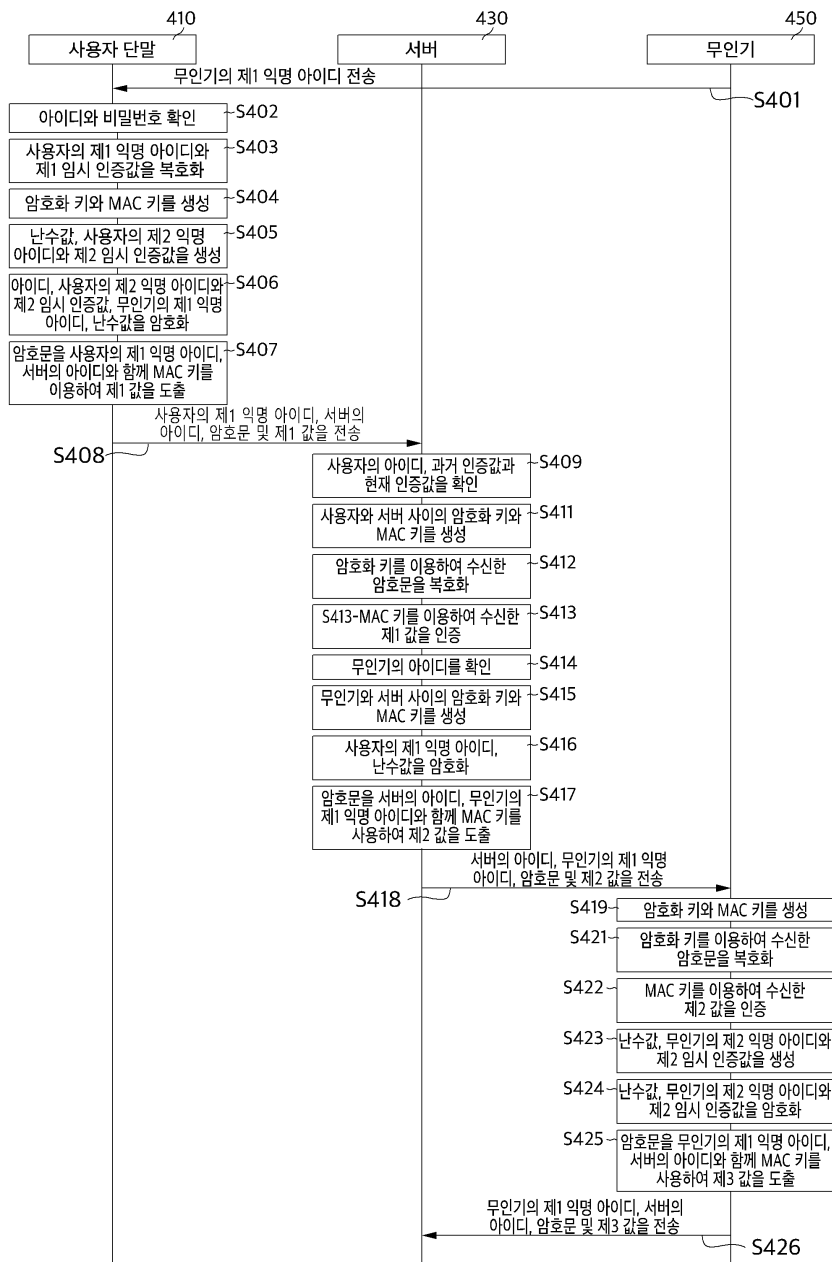
도면2



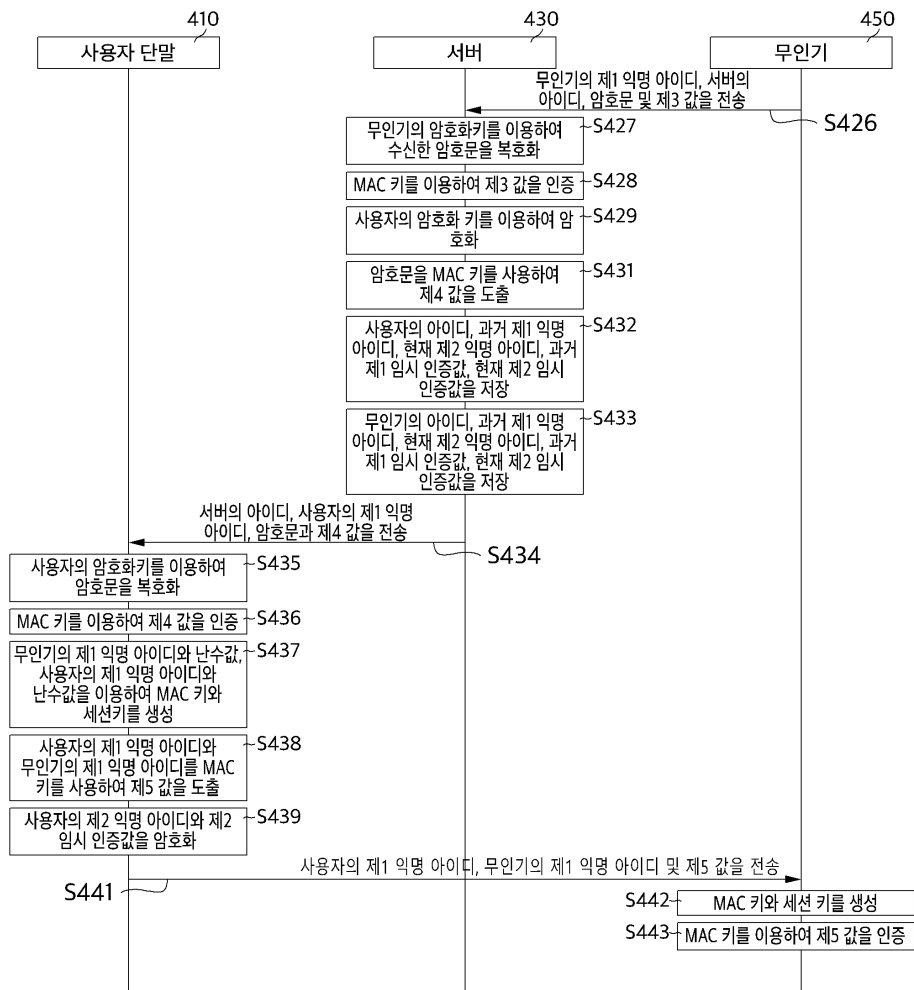
도면3



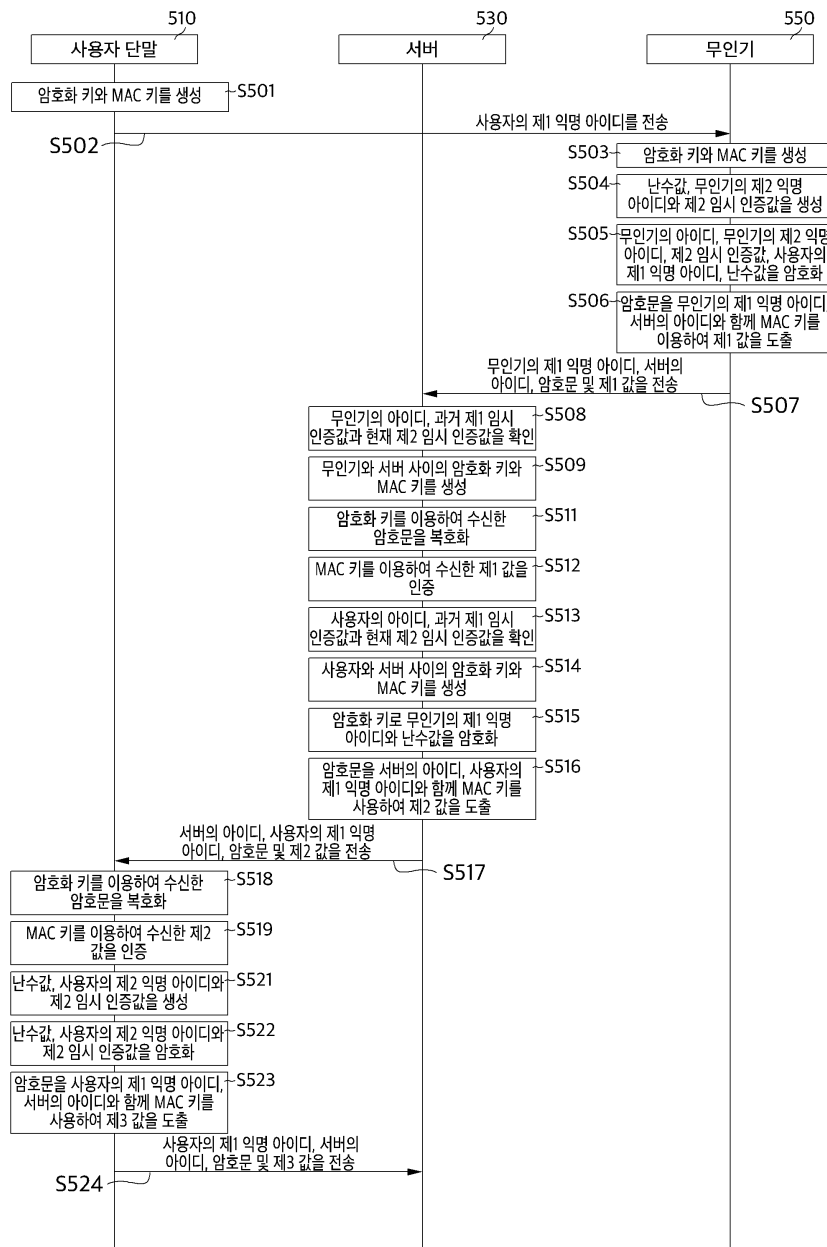
도면4a



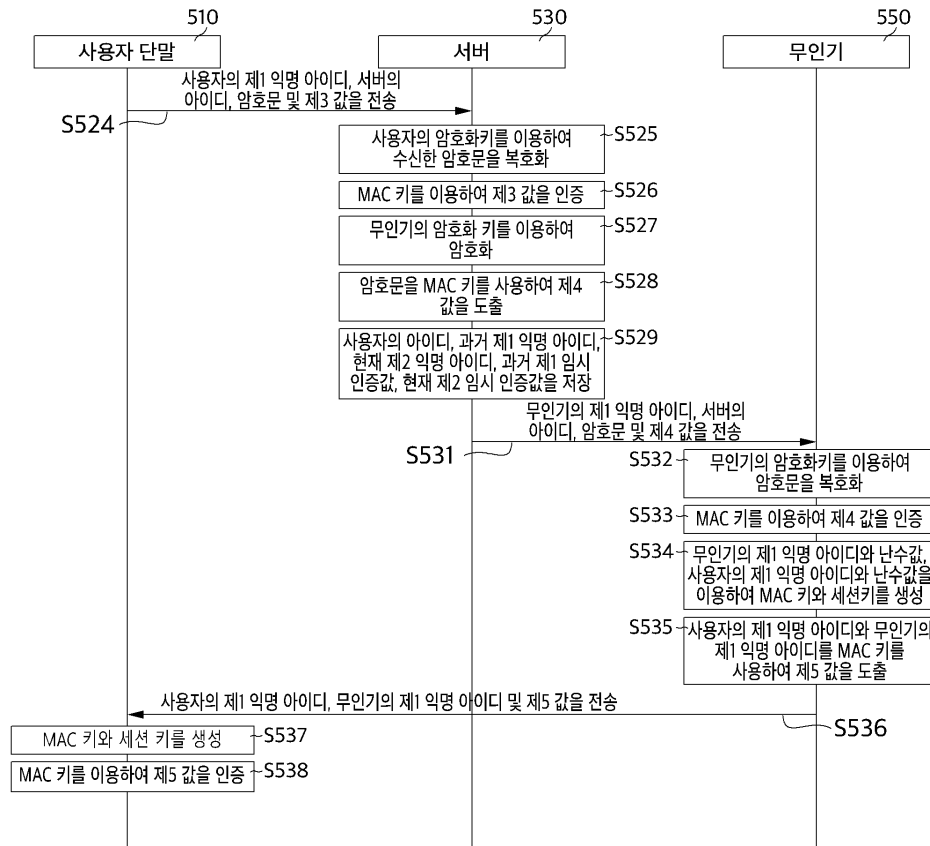
도면4b



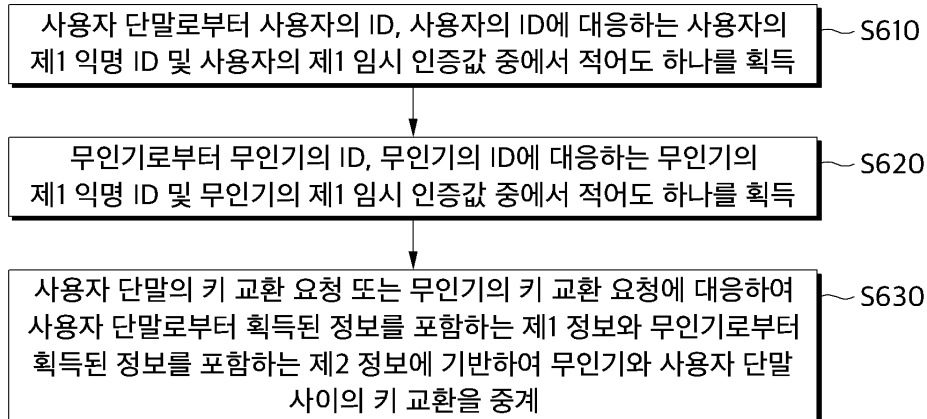
도면5a



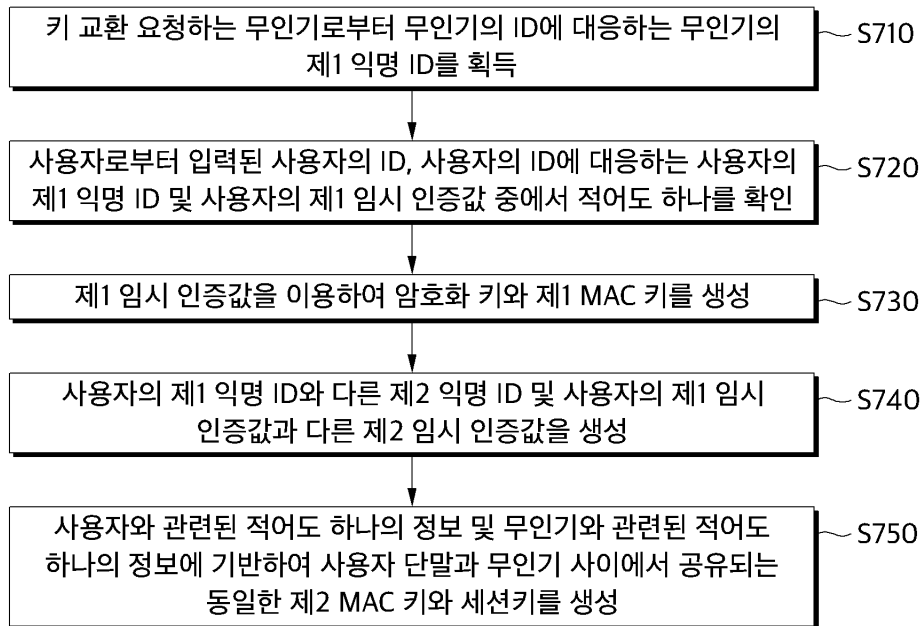
도면5b



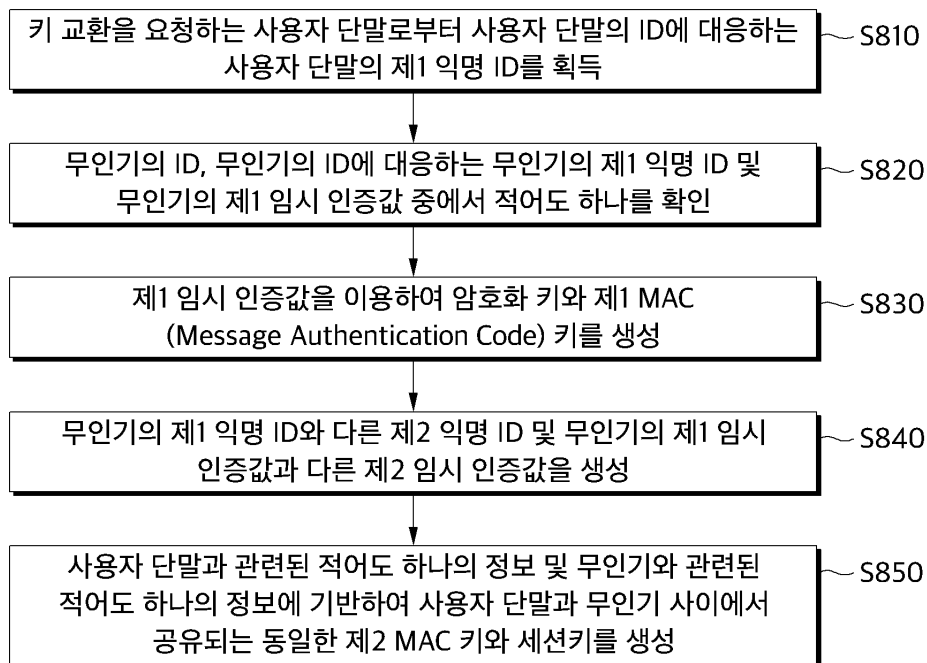
도면6



도면7



도면8



도면9

