



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0004227
(43) 공개일자 2020년01월13일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) H04L 12/24 (2006.01)
H04L 29/06 (2006.01) H04W 12/04 (2009.01)
H04W 12/06 (2009.01) H04W 36/00 (2009.01)
(52) CPC특허분류
H04L 9/0844 (2013.01)
H04L 41/083 (2013.01)
(21) 출원번호 10-2018-0096764
(22) 출원일자 2018년08월20일
심사청구일자 2018년08월20일
(30) 우선권주장
1020180077050 2018년07월03일 대한민국(KR)

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암
동5가)
(72) 발명자
김태윤
서울특별시 양천구 목동동로 130, 1404동 202호
(신정동, 목동신시가지14단지아파트)
민성기
서울 중랑구 상봉로 131, A동 3402호 (상봉동, 상
봉 듀오트리스 주상복합)
(뒷면에 계속)
(74) 대리인
윤귀상

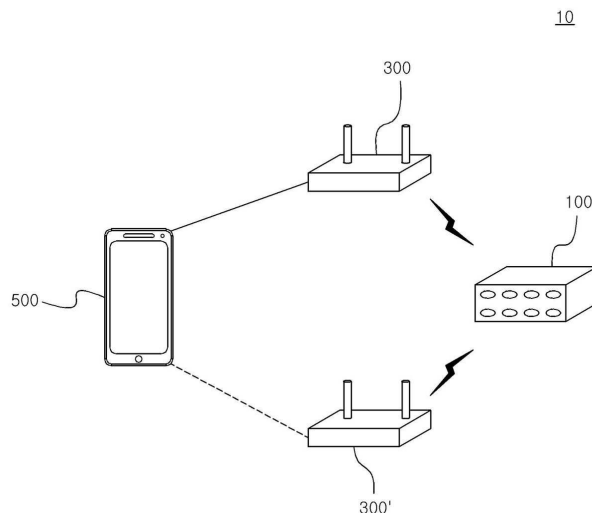
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 FT 프로토콜을 이용한 인증 방법 및 이를 수행하기 위한 장치

(57) 요약

FT 프로토콜을 이용한 인증 방법은, 제1 공유기와 로밍되어 있는 단말기가 제2 공유기와 로밍하기 위해 FT(Fast BSS Transition) 방식을 요구하는 요청메시지를 통신제어기로 송신하고, 통신제어기로부터 FT 방식을 수락하는 응답메시지를 수신한 단말기는 제1 세션키를 생성하고, 단말기는 제1 세션키를 이용하여 제1 마스터키를 생성한 뒤 1차단말키를 생성하고, 1차단말키를 생성한 단말기는 상기 통신제어기로부터 수신된 정보를 이용하여 2차단말키를 생성하고, 2차단말키를 생성한 단말기는 차후 로밍을 위해 통신제어기로 2차단말키 생성에 대한 인증값(MIC)을 송신할 수 있다. 이에 따라, 디바이스와 공유기 간의 통신 키를 주고받는 추가적인 통신 프로토콜이 불필요해지기 때문에 기존 FT프로토콜에 비해 구현을 간소화시킬 수 있다.

대표도 - 도1



(52) CPC특허분류

H04L 63/061 (2013.01)

H04L 69/24 (2013.01)

H04W 12/04 (2019.01)

H04W 12/06 (2019.01)

H04W 36/0016 (2013.01)

H04L 2209/80 (2013.01)

(72) 발명자

윤현기

서울특별시 송파구 바람드리길 10 (풍납동)

최주호

서울특별시 성동구 행당로 82, 116동 2004호(행당동, 행당 한진타운)

이 발명을 지원한 국가연구개발사업

과제고유번호 1711055347

부처명 과학기술정보통신부

연구관리전문기관 정보통신기술진흥센터

연구사업명 SW중심대학 지원사업 (SW전문인력양성사업 / 정보통신창의인재양성)

연구과제명 SW중심대학(고려대)

기 여 율 1/1

주관기관 고려대학교

연구기간 2015.10.01 ~ 2018.12.31

명세서

청구범위

청구항 1

제1 공유기와 로밍되어 있는 단말기가 제2 공유기와 로밍하기 위해 FT(Fast BSS Transition) 방식을 요구하는 요청메시지를 통신제어기로 송신하고,

상기 통신제어기로부터 FT 방식을 수락하는 응답메시지를 수신한 단말기는 제1 세션키를 생성하고,

상기 단말기는 상기 제1 세션키를 이용하여 제1 마스터키를 생성한 뒤 1차단말키를 생성하고,

상기 1차단말키를 생성한 단말기는 상기 통신제어기로부터 수신된 정보를 이용하여 2차단말키를 생성하고,

상기 2차단말키를 생성한 단말기는 차후 로밍을 위해 상기 통신제어기로 2차단말키 생성에 대한 인증값(MIC)을 송신하는, FT 프로토콜을 이용한 인증 방법.

청구항 2

제 1 항에 있어서,

상기 2차단말키를 생성하는 것은,

상기 통신제어기로부터 통신제어기에 대한 정보가 수신되면 1차단말키를 폐기하고,

상기 통신제어기로부터 제공받은 정보인 상기 통신제어기의 차기임의값(Next ANonce) 및 상기 단말기의 주소를 이용하여 생성하는, FT 프로토콜을 이용한 인증 방법.

청구항 3

제 1 항에 있어서,

상기 1차단말키를 생성하는 것은,

상기 통신제어기로부터 제공받은 정보인 상기 통신제어기의 임의값(ANonce) 및 상기 단말기의 주소를 이용하여 생성하는, FT 프로토콜을 이용한 인증 방법.

청구항 4

제 1 항에 있어서,

상기 제1 세션키는,

상기 응답메시지를 수신한 단말기가 인증과정을 수행하여 인증에 성공한 경우 생성되는, FT 프로토콜을 이용한 인증 방법.

청구항 5

제 1 항에 있어서,

상기 단말기는 제3 공유기와 로밍하기 위해 상기 통신제어기로 2차단말키 생성에 대한 신호를 송신하고,

상기 제3 공유기와 로밍된 단말기는 2차단말키를 폐기한 뒤 상기 통신제어기로부터 제공받은 정보를 이용하여 3차단말키를 생성하는, FT 프로토콜을 이용한 인증 방법.

청구항 6

제 1 항에 있어서,

상기 단말기는,

상기 통신제어부로부터 제공받은 정보를 이용하여 n차단말키를 생성하면, 상기 통신제어부로 인증값(MIC)을 송신하여 n차단말키가 생성된 것을 알려 저장할 수 있도록 하는, FT 프로토콜을 이용한 인증 방법.

청구항 7

적어도 하나의 단말기로부터 FT(Fast BSS Transition) 방식을 요구하는 요청메시지를 수신하면, 해당 단말기와 인증과정을 수행하는 인증수행부;

상기 인증수행부에서 인증에 성공한 단말기가 존재하면 제2 세션키를 생성하고, 상기 제2 세션키를 이용하여 제2 마스터키를 생성하는 마스터키 생성부;

상기 단말기로부터 수신한 정보를 이용하여 1차제어키를 생성하고, 임의값(ANonce)을 생성하여 상기 단말기로 송신하는 제어부; 및

상기 제어부에서 임의값을 송신한 상기 단말기로부터 2차단말키가 생성된 신호를 수신하면 차후 로밍을 위해 2차단말키 생성에 대한 신호를 저장하는 단말키 저장부;를 포함하는, FT 프로토콜을 이용한 인증 장치.

청구항 8

제 7 항에 있어서,

상기 제어부는,

AP 주소와 상기 단말기로부터 제공받은 상기 단말기의 임의값(SNonce)을 이용하여 1차제어키를 생성하는, FT 프로토콜을 이용한 인증 장치.

청구항 9

제 7 항에 있어서,

상기 단말키 저장부는,

공유기로 로밍하기 위한 단말기로부터 2차단말키 생성에 대한 정보를 수신하면 상기 단말기를 해당 공유기로 로밍할 수 있도록 하고, 상기 제어부로 상기 1차제어키를 폐기하고, 2차제어키를 생성하는 신호를 송신하는, FT 프로토콜을 이용한 인증 장치.

청구항 10

제 9 항에 있어서,

상기 제어부는,

상기 단말키 저장부로부터 제어키를 생성하라는 신호를 수신하면, n-2차제어키를 폐기한 뒤 n-1차제어키를 생성하여 상기 단말기로 송신하는, FT 프로토콜을 이용한 인증 장치.

발명의 설명

기술분야

- [0001] 본 발명은 FT 프로토콜을 이용한 인증 방법 및 이를 수행하기 위한 장치에 관한 것으로서, 더욱 상세하게는 단말기가 공유기에 로밍하는 시간을 감소시키기 위해 소프트웨어 정의 네트워킹(Software-Defined-Networking;SDN)을 활용하는 FT 프로토콜을 이용한 인증 방법 및 이를 수행하기 위한 장치에 관한 것이다.

배경기술

- [0003] 일반적으로 무선 LAN 환경에서는 이동 중에도 실시간 모바일 멀티미디어 서비스를 지속적으로 제공받기 위해 로밍(Roaming)이 이루어져야 한다.
- [0004] IEEE 802.11r 표준에서는 하나의 ESS(Extended Service Set)에 포함된 BSS(Basic Service Set) 간의 고속 전환(Fast Transition)에서 IEEE 802.1X 4-way handshake 인증(Authentication) 절차의 시간 지연을 축소시킬 수 있는 기술이 제안되고 있는 실정이다.
- [0005] 기존의 FT 프로토콜을 사용하여 로밍을 하면, 새로운 AP에 직접 통신하는 Over-the-Air 방식을 이용하거나, 이전 AP를 중간자로 이용하는 Over-the-DS 방식으로 다른 AP와 연결을 맺는다.
- [0006] Over-the-Air 방식과 Over-the-DS 방식은 모두 STA와 AP간에 네 번의 패킷 송신이 이루어지고, 추가로 AP간에 초기 인증과정을 통해 만들어진 PMK(통신하기 위한 키를 만들기 위한 Seed Key) 전송이 이루어져야 한다.
- [0007] 이때, 배터리로 운용되는 간단한 센서들은 패킷의 송수신 횟수에 따라 전력의 요구량이 달라지기 때문에, 패킷의 송수신 횟수가 많아질수록 불리하다는 문제점이 있다.

선행기술문헌

특허문헌

- [0009] (특허문헌 0001) 한국등록특허 제10-1680137호
(특허문헌 0002) 한국등록특허 제10-1852104호

발명의 내용

해결하려는 과제

- [0010] 본 발명의 일측면은 한 번의 인증과정을 성공한 단말기가 새로운 공유기로 로밍을 요청할 때, 인증과정을 다시 거치지 않아도 공유기로 로밍할 수 있는 FT 프로토콜을 이용한 인증 방법 및 이를 수행하기 위한 장치를 제공한다.
- [0011] 본 발명의 기술적 과제는 이상에서 언급한 기술적 과제로 제한되지 않으며, 언급되지 않은 또 다른 기술적 과제들은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

- [0013] 본 발명의 일 실시예에 따른 FT 프로토콜을 이용한 인증 방법은 제1 공유기와 로밍되어 있는 단말기가 제2 공유기와 로밍하기 위해 FT(Fast BSS Transition) 방식을 요구하는 요청메시지를 통신제어기로 송신하고, 상기 통신제어기로부터 FT 방식을 수락하는 응답메시지를 수신한 단말기는 제1 세션키를 생성하고, 상기 단말기는 상기 제1 세션키를 이용하여 제1 마스터키를 생성한 뒤 1차단말키를 생성하고, 상기 1차단말키를 생성한 단말기는 상기 통신제어기로부터 수신된 정보를 이용하여 2차단말키를 생성하고, 상기 2차단말키를 생성한 단말기는 차후 로밍을 위해 상기 통신제어기로 2차단말키 생성에 대한 인증값(MIC)을 송신한다.
- [0014] 상기 2차단말키를 생성하는 것은, 상기 통신제어기로부터 통신제어기에 대한 정보가 수신되면 1차단말키를 폐기

하고, 상기 통신제어기로부터 제공받은 정보인 상기 통신제어기의 차기임의값(Next ANonce) 및 상기 단말기의 주소를 이용하여 생성할 수 있다.

- [0015] 상기 1차단말키를 생성하는 것은, 상기 통신제어기로부터 제공받은 정보인 상기 통신제어기의 임의값(ANonce) 및 상기 단말기의 주소를 이용하여 생성할 수 있다.
- [0016] 상기 제1 세션키는, 상기 응답메시지를 수신한 단말기가 인증과정을 수행하여 인증에 성공한 경우 생성될 수 있다.
- [0017] 상기 단말기는 제3 공유기와 로밍하기 위해 상기 통신제어기로 2차단말키 생성에 대한 신호를 송신하고, 상기 제3 공유기와 로밍된 단말기는 2차단말키를 폐기한 뒤 상기 통신제어기로부터 제공받은 정보를 이용하여 3차단말키를 생성할 수 있다.
- [0018] 상기 단말기는, 상기 통신제어부로부터 제공받은 정보를 이용하여 n차단말키를 생성하면, 상기 통신제어부로 인증값(MIC)을 송신하여 n차단말키가 생성된 것을 알려 저장할 수 있도록 할 수 있다.
- [0019] 본 발명의 일 실시예에 따른 FT 프로토콜을 이용한 인증 장치는 적어도 하나의 단말기로부터 FT(Fast BSS Transition) 방식을 요구하는 요청메시지를 수신하면, 해당 단말기와 인증과정을 수행하는 인증수행부; 상기 인증수행부에서 인증에 성공한 단말기가 존재하면 제2 세션키를 생성하고, 상기 제2 세션키를 이용하여 제2 마스터키를 생성하는 마스터키 생성부; 상기 단말기로부터 수신한 정보를 이용하여 1차제어키를 생성하고, 임의값(ANonce)을 생성하여 상기 단말기로 송신하는 제어부; 및 상기 제어부에서 임의값을 송신한 상기 단말기로부터 2차단말키가 생성된 신호를 수신하면 차후 로밍을 위해 2차단말키 생성에 대한 신호를 저장하는 단말키 저장부;를 포함한다.
- [0020] 상기 제어부는, AP 주소와 상기 단말기로부터 제공받은 상기 단말기의 임의값(SNonce)을 이용하여 1차제어키를 생성할 수 있다.
- [0021] 상기 단말키 저장부는, 공유기로 로밍하기 위한 단말기로부터 2차단말키를 수신하면 저장한 2차단말키를 이용하여 상기 단말기를 해당 공유기로 로밍할 수 있도록 하고, 상기 제어부로 상기 1차제어키를 폐기하고, 2차제어키를 생성하는 신호를 송신할 수 있다.
- [0022] 상기 제어부는, 상기 단말키 저장부로부터 제어키를 생성하라는 신호를 수신하면, n-2차제어키를 폐기한 뒤 n-1차제어키를 생성하여 상기 단말기로 송신할 수 있다.

발명의 효과

- [0024] 상술한 본 발명의 일측면에 따르면, 센서기기가 많이 필요한 IoT 서비스 환경에서 도움이 될 수 있고, 배터리의 양과 프로세스 능력이 낮아 통신 부하에 민감한 센서기기에 활용될 수 있다.
- [0025] 또한, 음성 또는 영상 등을 이용하는 통신 지연시간에 민감한 무선 디바이스에 활용될 수 있고, AP 간의 통신 키를 주고받는 추가적인 통신 프로토콜이 불필요해지기 때문에 기존 FT 프로토콜에 비해 구현을 간소화시킬 수 있다.
- [0026] 본 발명에서 얻을 수 있는 효과는 이상에서 언급한 효과로 제한되지 않으며, 언급하지 않은 또 다른 효과들은 아래의 기재로부터 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

- [0028] 도 1은 본 발명의 FT 프로토콜을 이용한 인증 시스템의 개략적인 구성을 나타내는 도면이다.
- 도 2는 본 발명의 일 실시예에 따른 FT 프로토콜을 이용한 인증 장치를 도시한 블록도이다.
- 도 3은 본 발명의 일 실시예에 따른 FT 프로토콜을 이용한 인증 방법을 자세히 도시한 흐름도이다.
- 도 4는 본 발명의 다른 실시예에 따른 FT 프로토콜을 이용한 인증 방법을 도시한 흐름도이다.

도 5는 본 발명에 따른 FT 프로토콜을 이용한 인증 장치와 단말기 간의 인증과정에 대한 예를 나타낸 도면이다.

도 6은 본 발명에 따른 공유기에 로밍되어 있는 단말기가 다른 공유기로 로밍하는 경우에 대한 인증과정에 대한 예를 나타낸 도면이다.

발명을 실시하기 위한 구체적인 내용

- [0029] 후술하는 본 발명에 대한 상세한 설명은, 본 발명이 실시될 수 있는 특정 실시예를 예시로서 도시하는 첨부 도면을 참조한다. 이들 실시예는 당업자가 본 발명을 실시할 수 있기에 충분하도록 상세히 설명된다. 본 발명의 다양한 실시예는 서로 다르지만 상호 배타적일 필요는 없음이 이해되어야 한다. 예를 들어, 여기에 기재되어 있는 특정 형상, 구조 및 특성은 일 실시예와 관련하여 본 발명의 정신 및 범위를 벗어나지 않으면서 다른 실시예로 구현될 수 있다. 또한, 각각의 개시된 실시예 내의 개별 구성요소의 위치 또는 배치는 본 발명의 정신 및 범위를 벗어나지 않으면서 변경될 수 있음이 이해되어야 한다. 따라서, 후술하는 상세한 설명은 한정적인 의미로서 취하려는 것이 아니며, 본 발명의 범위는, 적절하게 설명된다면, 그 청구항들이 주장하는 것과 균등한 모든 범위와 더불어 첨부된 청구항에 의해서만 한정된다. 도면에서 유사한 참조부호는 여러 측면에 걸쳐서 동일하거나 유사한 기능을 지칭한다.
- [0030] 이하, 도면들을 참조하여 본 발명의 바람직한 실시예들을 보다 상세하게 설명하기로 한다.
- [0031] 본 발명은 기존 FT프로토콜에 비해 AP 간의 통신 키를 주고받는 추가적인 통신 프로토콜이 불필요해지기 때문에 구현을 간소화시킬 수 있는 FT 프로토콜을 이용한 인증 방법 및 이를 수행하기 위한 장치이다.
- [0032] 도 1은 본 발명의 FT 프로토콜을 이용한 인증 시스템(10)의 개략적인 구성이 도시된 도면이다.
- [0033] 본 발명의 실시예에 따른 FT 프로토콜을 이용한 인증 시스템(10)은 통신제어기(100), 다수 개의 공유기(300, 300') 및 단말기(500)를 포함할 수 있고, 통신제어기(100)는 다수 개의 공유기(300, 300')를 제어(Control)할 수 있다.
- [0034] 도 1에서는 본 발명의 일 실시예에 따라 설명하기 위해 제1 공유기(300) 및 제2 공유기(300')로 한정되었으나 이는 실시예에 따른 예시일 뿐, 실제 통신제어기(100)는 보다 많은 수의 공유기를 제어할 수 있다.
- [0035] 통신제어기(100)는 다수 개의 공유기(300)를 관리할 수 있으며, 인증에 성공하여 제1 공유기(300)와 로밍되어 있는 단말기(500)로부터 제2공유기(300')와 로밍하기 위한 인증과정을 요청하는 메시지가 수신되면, 재인증 과정을 거치지 않고 해당 단말기(500)를 제2공유기(300')와 로밍시킬 수 있다.
- [0036] 통신제어기(100)는 네트워크 내의 모든 통신수단을 관리할 수 있는 SDN Controller 등의 서버(server) 또는 엔진(engine) 형태일 수 있고, 디바이스(device), 기구(apparatus), 단말(terminal), 무선기기(wireless device) 등 다른 용어로 불릴 수 있다.
- [0037] 단말기(500)는 제1 공유기(300)에 로밍되어 있는 상태일 수 있고, 제2공유기(300')와 로밍을 위하여 통신제어기(100)로 로밍할 수 있는 인증과정을 요청하는 메시지를 송신할 수 있다.
- [0038] 또한, 단말기(500)는 장치로써 이동성을 갖거나 고정될 수 있다. 상기 단말기(500)는, 서버(server) 또는 엔진(engine) 형태일 수 있으며, 디바이스(device), 기구(apparatus), 단말(terminal), UE(user equipment), MS(mobile station), 무선기기(wireless device), 휴대기기(handheld device) 등 다른 용어로 불릴 수 있다.
- [0039] 단말기(500)는 운영체제(Operation System; OS), 즉 시스템을 기반으로 다양한 소프트웨어를 실행하거나 제작할 수 있다. 상기 운영체제는 소프트웨어가 장치의 하드웨어를 사용할 수 있도록 하기 위한 시스템 프로그램으로서, 안드로이드 OS, iOS, 윈도우 모바일 OS, 바다 OS, 심비안 OS, 블랙베리 OS 등 모바일 컴퓨터 운영체제 및 윈도우 계열, 리눅스 계열, 유닉스 계열, MAC, AIX, HP-UX 등 컴퓨터 운영체제를 모두 포함할 수 있다.
- [0040] 일 예로, 단말기(500)는 스마트폰, PDA, 노트북, 태블릿PC, 웨어러블 장치 등의 형태일 수 있다. 이하에서는, 설명의 편의를 위해 단말기(500)는 스마트폰으로 정의한다. 하지만, 상술한 바와 같이 단말기(500)의 형태는 스마트폰에만 국한되는 것은 아니다.
- [0041] 도 2는 본 발명의 일 실시예에 따른 FT 프로토콜을 이용한 인증 장치를 자세히 도시한 블록도이다.
- [0042] 본 발명의 일 실시예에 따른 FT 프로토콜을 이용한 인증 장치인 통신제어기(100)는 인증수행부(110), 마스터키

생성부(130), 제어부(150) 및 단말키 저장부(170)를 포함할 수 있다.

- [0043] 통신제어기(100)는 다수 개의 공유기(300)를 제어하고, FT프로토콜을 이용하여 인증 과정을 수행하기 위한 소프트웨어(어플리케이션)가 설치되어 실행될 수 있다.
- [0044] 이에 따라, 인증수행부(110), 마스터키 생성부(130), 제어부(150) 및 단말키 저장부(170)는 FT프로토콜을 이용하여 인증 과정을 수행하기 위한 소프트웨어(어플리케이션)에 의해 제어될 수 있다.
- [0045] 인증수행부(110), 마스터키 생성부(130), 제어부(150) 및 단말키 저장부(170)의 구성은 통합 모듈로 형성되거나, 하나 이상의 모듈로 이루어질 수 있다. 그러나, 이와 반대로 각 구성은 별도의 모듈로 이루어질 수도 있다.
- [0046] 인증수행부(110)는 적어도 하나의 단말기(500)로부터 FT(Fast BSS Transition) 방식을 요구하는 요청메시지(MDE)가 수신되면, 응답메시지(MDE)를 해당 단말기(500)로 송신할 수 있다. 응답메시지(MDE)를 수신받은 해당 단말기(500)로부터 인증과정을 수행하기 위한 정보가 수신되면, 수신된 정보를 이용하여 인증과정을 수행할 수 있다.
- [0047] 마스터키 생성부(130)는 인증수행부(110)로부터 인증에 성공한 단말기가 존재하면 제2 세션키를 생성할 수 있다. 생성한 제2 세션키에 대한 정보를 이용하여 제2 마스터키를 생성할 수 있고, 제2 마스터키를 생성한 뒤 임의값(ANonce)을 생성하여 인증에 성공한 단말기(500)로 송신될 수 있다.
- [0048] 한편, 단말기(500)에서도 통신제어기(100)와의 인증에 성공한 뒤 제1 세션키를 생성할 수 있고, 생성한 제1 세션키에 대한 정보를 이용하여 제1 마스터키를 생성할 수 있다.
- [0049] 여기서 제2 세션키는 MSK(Master Session Key)를 의미할 수 있는데 인증이 완료된 후 단말기(500) 및 통신제어기(100) 간에 갖게 되는 임시 대칭 키로써 제2 마스터키를 생성하기 위한 일종의 키 생성 재료로 구분될 수 있다.
- [0050] 또한, 제2 마스터키는 PMK(Pair wire Master Key)를 의미할 수 있는데 n 차제어키(여기서, n 은 자연수)를 유도하기 위한 보조 키로 구분될 수 있고, 해당 단말기(500)와 통신제어기(100) 간의 상호 인증이 완료되었다는 의미를 내포할 수 있다.
- [0051] 제어부(150)는 단말기(500)로부터 1차단말키 생성에 대한 신호가 수신되면, 단말기(500)로부터 수신된 임의값(SNonce)을 이용하여 1차제어키를 생성할 수 있다. 1차제어키 생성을 인증하기 위해 1차제어키 생성에 대한 인증값(MIC)을 인증에 성공한 단말기(500)로 송신될 수 있다.
- [0052] 또한, 제어부(150)는 제2공유기(300')와 로밍되어 있는 단말기(500)로부터 $n-1$ 차단말키(여기서, n 은 자연수) 생성에 대한 인증값(MIC)이 수신되면, 이에 대응하여 $n-2$ 차제어키(여기서, n 은 자연수)를 폐기한 후 $n-1$ 차제어키(여기서, n 은 자연수)를 생성할 수 있다.
- [0053] 여기서, $n-1$ 차제어키(여기서, n 은 자연수)는 통신제어기(100)에서 생성한 제2 마스터키에 대한 정보, 단말기(500)의 임의값(SNonce) 및 통신제어기(100)의 AP 주소를 이용하여 생성될 수 있으며, 실제 무선구간 암호화를 수행하기 위한 키로써 PTK(Pairwise Transient Key)를 의미할 수 있다.
- [0054] 단말기(500)에서 통신제어기(100)로 임의값(SNonce)을 송신할 때 보안값(RSNE)을 함께 송신할 수 있는데, 이는 해당 기기와 결합된 모든 무선단말에 보내는 정보를 암호화하기 위한 값을 의미할 수 있다.
- [0055] $n-1$ 차제어키(여기서, n 은 자연수)는 $n-1$ 차단말키(여기서, n 은 자연수)를 생성한 단말기(500)로부터는 $n-1$ 차단말키를 생성했다는 것을 인증하는 신호인 인증값(MIC)이 수신된 뒤 생성될 수 있다.
- [0056] 여기서, 단말기(500)의 임의값(SNonce)은 단말기(500)에서 키(key)생성을 위해 생성하는 임의의 값을 의미할 수 있고, 단말기(500)가 $n-1$ 차단말키(여기서, n 은 자연수)를 생성하여 통신제어기(100)로 송신하는 인증값(MIC)은 단말기(500)가 생성한 $n-1$ 차단말키 생성을 인증할 수 있는 값을 의미할 수 있다.
- [0057] 단말키 저장부(170)는 제어부(150)에서 1차제어키 생성에 대한 신호를 단말기(500)로 송신할 수 있고, 1차제어키 생성에 대한 신호를 수신한 단말기(500)로부터 2차단말키 생성에 대한 인증값(MIC)이 수신되면, 단말기(500)로부터 수신된 2차단말키 생성에 대한 인증값(MIC)을 저장할 수 있다.
- [0058] 또한, 단말키 저장부(170)는 해당 단말기(500)로부터 수신된 2차단말키 생성에 대한 인증값(MIC)을 저장한 뒤 제1 공유기(300)에 로밍된 해당 단말기(500)를 제2공유기(300')로 로밍시킬 수 있다.

- [0060] 도 3은 본 발명의 일 실시예에 따른 FT 프로토콜을 이용한 인증 방법을 도시한 흐름도이다.
- [0061] 도 3을 참조하면, 본 발명의 일 실시예에 따른 제1 공유기(300)와 로밍되어 있는 단말기(500)로부터 FT(Fast BSS Transition) 방식으로 인증과정 수행할 것을 요구하는 요청메시지(MDE)가 수신되면(S2000), 응답메시지(MDE)를 해당 단말기(500)로 송신할 수 있다(S2050).
- [0062] 응답메시지(MDE)를 수신받은 해당 단말기(500)로부터 인증과정을 수행하기 위한 정보가 수신되면, 수신된 정보를 이용하여 인증과정을 수행한 뒤 제2 세션키를 생성할 수 있다(S2100).
- [0063] 여기서 제2 세션키는 MSK(Master Session Key)를 의미할 수 있는데 인증이 완료된 후 단말기(500) 및 통신제어기(100) 간에 갖게 되는 임시 대칭 키로써 제2 마스터키를 생성하기 위한 일종의 키 생성 재료로 구분될 수 있다.
- [0064] 생성된 제2 세션키에 대한 정보를 이용하여 제2 마스터키를 생성할 수 있다(S2300). 여기서, 제2 마스터키는 PMK(Pair wire Master Key)를 의미할 수 있는데 n차제어키(여기서, n은 자연수)를 유도하기 위한 보조 키로 구분될 수 있고, 해당 단말기(500)와 통신제어기(100) 간의 상호 인증이 완료되었다는 의미를 내포할 수 있다.
- [0065] 제2 마스터키를 생성한 뒤 임의값(ANonce)을 생성하여 단말기(500)로 송신할 수 있고(S2500), 임의값(ANonce)을 수신한 단말기(500)로부터 1차단말키 생성에 대한 인증값(MIC)이 수신되면(S2700), 1차제어키를 생성한 뒤 해당 단말기(500)로 1차제어키 생성에 대한 신호를 송신할 수 있다(S2750).
- [0066] 여기서, n-1차제어키(여기서, n은 자연수)는 통신제어기(100)에서 생성한 제2 마스터키에 대한 정보, 단말기(500)의 임의값(SNonce) 및 통신제어기(100)의 AP 주소를 이용하여 생성될 수 있으며, 실제 무선구간 암호화를 수행하기 위한 키로써 PTK(Pairwise Transient Key)를 의미할 수 있다.
- [0067] n-1차제어키(여기서, n은 자연수)는 n-1차단말키(여기서, n은 자연수)를 생성한 단말기(500)로부터는 n-1차단말키를 생성했다는 것을 인증하는 인증값(MIC)이 수신된 뒤 생성될 수 있다.
- [0068] 단말기(500)에서 통신제어기(100)로 임의값(SNonce)을 송신할 때 보안값(RSNE)을 함께 송신할 수 있는데, 이는 해당 기기와 결합된 모든 무선단말에 보내는 정보를 암호화하기 위한 값을 의미할 수 있다.
- [0069] 여기서, 단말기(500)의 임의값(SNonce)은 단말기(500)에서 키(key)생성을 위해 생성하는 임의의 값을 의미할 수 있고, 단말기(500)가 n-1차단말키(여기서, n은 자연수)를 생성한 뒤 통신제어기(100)로 송신하는 인증값(MIC)은 단말기(500)가 생성한 n-1차단말키 생성에 대한 것을 인증할 수 있는 값을 의미할 수 있다.
- [0070] 1차제어키를 생성한 뒤 해당 단말기(500)로부터 2차단말키 생성에 대한 인증값(MIC)이 수신되면(S2900), 수신된 인증값(MIC)을 저장할 수 있고(S2950), 수신된 인증값(MIC)을 저장한 뒤 해당 단말기(500)를 제2공유기(300')로 로밍시킬 수 있다.
- [0071] 도 4는 본 발명의 다른 실시예에 따른 FT 프로토콜을 이용한 인증 방법을 도시한 흐름도이다.
- [0072] 도 4를 참조하면, 본 발명의 다른 실시예에 따른 제1 공유기(300)와 로밍되어 있는 단말기(500)는 제2공유기(300')로 로밍하기 위해 FT방식으로 인증과정 수행할 것을 요구하는 요청메시지를 통신제어기(100)로 송신할 수 있고(S1000), FT 방식을 요구하는 메시지를 수신한 통신제어기(100)로부터 응답메시지가 수신되면(S1100), 제1 세션키를 생성할 수 있다(S1150).
- [0073] 여기서 제1 세션키는 MSK(Master Session Key)를 의미할 수 있는데 인증이 완료된 후 단말기(500) 및 통신제어기(100) 간에 갖게 되는 임시 대칭 키로써 제1 마스터키를 생성하기 위한 일종의 키 생성 재료로 구분될 수 있다.
- [0074] 단말기(500)는 제1 세션키에 대한 정보를 이용하여 제1 마스터키를 생성할 수 있다(S1300). 여기서, 제1 마스터키는 PMK(Pair wire Master Key)를 의미할 수 있는데 n차단말키(여기서, n은 자연수)를 유도하기 위한 보조 키로 구분될 수 있고, 해당 단말기(500)와 통신제어기(100) 간의 상호 인증이 완료되었다는 의미를 내포할 수 있다.
- [0075] 제2 마스터키를 생성한 뒤 임의값(ANonce)을 생성한 통신제어기(100)로부터 통신제어기(100)의 임의값(ANonce)이 수신될 수 있고(S1500), 수신된 임의값(ANonce)을 이용하여 단말기(500)는 1차단말키를 생성할 수 있다(S1550).

- [0076] 여기서, 단말기(500)가 생성하는 n-1차단말키(여기서, n은 자연수)는 실제 무선구간 암호화를 수행하기 위한 키를 의미할 수 있고, 통신제어기(100)로부터 임의값(ANonce)이 수신된 후 생성할 수 있다.
- [0077] 여기서, 통신제어기(100)가 생성하여 단말기(500)로 송신하는 임의값(ANonce)은 통신제어기(100)에서 키(key)를 생성하기 위한 정보가 포함되어 있는 임의의 값을 의미할 수 있다.
- [0078] 단말기(500)는 통신제어기(100)로부터 제공받은 정보를 이용하여 1차단말키를 생성한 후, 1차단말키 생성에 대한 신호인 인증값(MIC)을 통신제어기(100)로 송신할 수 있다(S1700).
- [0079] 1차단말키를 송신한 통신제어기(100)로부터 1차제어키 생성에 대한 인증값(MIC)이 수신되면(S1900) 단말기(500)는 생성한 1차단말키를 폐기한 뒤 2차단말키를 생성할 수 있고, 2차단말키 생성에 대한 인증값(MIC)을 통신제어기(100)로 송신할 수 있고(S1950), 제2공유기(300')에 로딩될 수 있다.
- [0080] 여기서, 단말기(500)의 2차단말키는 통신제어기(100)로부터 제공받은 통신제어기(100)의 차기임의값(Next ANonce) 및 단말기(500)의 주소를 이용하여 생성될 수 있다.
- [0081] 또한, 2차단말키는 1차제어키를 생성한 통신제어기(100)로부터는 1차제어키를 생성했다는 것을 인증하는 신호인 인증값(MIC)이 수신된 뒤 생성될 수 있다.
- [0082] 여기서, 통신제어기(100)의 임의값(ANonce)은 통신제어기(100)에서 키(key)를 생성하기 위한 정보가 포함되어 있는 임의의 값을 의미할 수 있고, 통신제어기(100)의 인증값(MIC)은 1차제어키 생성에 대한 것을 인증할 수 있는 신호를 의미할 수 있다.
- [0083] 또한, 통신제어기(100)의 차기임의값(Next ANonce)은 재인증을 위한 요청메시지를 송신하지 않고 로딩시킬 수 있는 임의의 값을 의미할 수 있으며, 통신제어기(100)에서 차기임의값(Next ANonce)을 송신할 때 보안값(RSNE)을 함께 송신할 수 있다.
- [0084] 통신제어기(100)에서 차기임의값(Next ANonce)을 송신할 때 함께 송신하는 보안값(RSNE)은 해당 기기와 결합된 모든 무선단말에 보내는 정보를 암호화하기 위한 값을 의미할 수 있다.
- [0086] 도 5는 본 발명에 따른 FT 프로토콜을 이용한 인증 장치와 단말기 간의 인증과정에 대한 예를 나타낸 도면이다.
- [0087] 도 5를 참조하면, STA는 본 발명의 단말기(500)를 의미할 수 있고, STA가 생성하는 MSK는 제1 세션키를 의미할 수 있고, PMK는 제1 마스터키를 의미할 수 있으며, PTK는 n차단말키(여기서, n은 자연수)를 의미할 수 있다.
- [0088] 또한, Controller는 본 발명의 통신제어기(100)를 의미할 수 있고, Controller가 생성하는 MSK는 제2 세션키를 의미할 수 있고, PMK는 제2 마스터키를 의미할 수 있으며, PTK는 n차제어키(여기서, n은 자연수)를 의미할 수 있다.
- [0089] 제1 공유기(300)와 로밍되어 있는 단말기(500, STA)가 제2공유기(300')와 로밍하기 위해 통신제어기(100, Controller)로 FT방식으로 인증과정 수행할 것을 요구하는 요청메시지(MDE)를 송신할 수 있다.
- [0090] 단말기(500)로부터 요청메시지(MDE)를 수신한 통신제어기(100)는 이에 응하는 응답메시지(MDE)를 송신할 수 있다. 이로부터 단말기(500)와 통신제어기(100) 간의 FT 방식을 이용하여 인증과정을 수행하는 것에 대한 협상이 이루어졌으므로 인증과정이 수행될 수 있다.
- [0091] 인증과정이 성공적으로 마치게 되면, 단말기(500)는 제1 세션키 및 제1 마스터키를 생성할 수 있고, 통신제어기(100)는 제2 세션키 및 제2 마스터키를 생성할 수 있다.
- [0092] 여기서, 단말기(500)와 통신제어기(100)에서 각각 생성되는 세션키는 MSK(Master Session Key)를 의미할 수 있는데 인증이 완료된 후 단말기(500) 및 통신제어기(100) 간에 갖게 되는 임시 대칭 키로써 마스터키를 생성하기 위한 일종의 키 생성 재료로 구분될 수 있다.
- [0093] 또한, 단말기(500)와 통신제어기(100)에서 각각 생성되는 마스터키는 PMK(Pair wire Master Key)를 의미할 수 있는데 n차제어키(여기서, n은 자연수)를 유도하기 위한 보조 키로 구분될 수 있고, 해당 단말기(500)와 통신제어기(100) 간의 상호 인증이 완료되었다는 의미를 내포할 수 있다.
- [0094] 단말기(500)와 통신제어기(100)에서 각각 세션키와 마스터키가 생성된 후, 통신제어기(100)는 단말기(500)로 통신제어기(100)의 임의값(ANonce)을 송신할 수 있다. 통신제어기(100)의 임의값(ANonce)을 수신한 단말기(500)는

통신제어기(100)의 임의값(ANonce)을 이용하여 1차단말기를 생성할 수 있다.

- [0095] 여기서, 통신제어기(100)의 임의값(ANonce)은 통신제어기(100)에서 키(key)생성을 위해 생성하기 위한 정보를 포함하는 임의의 값을 의미할 수 있다.
- [0096] 1차단말기를 생성한 단말기(500)는 단말기(500)의 임의값(SNonce)을 보안값(RSNE)과 함께 통신제어기(100)로 송신할 수 있고, 통신제어기(100)는 단말기(500)로부터 제공받은 임의값(SNonce) 및 통신제어기(100)의 AP 주소를 이용하여 1차제어기를 생성할 수 있다.
- [0097] 1차단말기를 생성한 단말기(500)는 1차단말기를 생성했다는 것에 대한 인증을 하기 위해 1차단말기 생성에 대한 신호인 인증값(MIC)을 통신제어기(100)로 송신할 수 있고, 통신제어기(100)는 1차단말기 생성에 대한 인증값(MIC)을 저장할 수 있다.
- [0098] 여기서, 단말기(500)의 임의값(SNonce)은 단말기(500)에서 키(key)생성을 위해 생성하는 임의의 값을 의미할 수 있고, 임의값(ANonce)과 함께 송신하는 보안값(RSNE)은 해당 기기와 결합된 모든 무선단말에 보내는 정보를 암호화하기 위한 값을 의미할 수 있다.
- [0099] 1차제어기를 생성한 통신제어기(100)는 단말기(500)의 2차단말기 생성을 위해 통신제어기(100)의 차기임의값(Next ANonce)과 함께 통신제어기(100)의 보안값(RNSE)을 단말기(500)로 송신할 수 있다.
- [0100] 한편, 통신제어기(100)는 1차제어기를 생성한 것을 인증하기 위한 1차제어기에 대한 인증값(MIC)을 단말기(500)로 송신할 수 있고, 단말기(500)는 1차제어기에 대한 인증값(MIC)을 저장할 수 있다.
- [0101] 단말기(500)는 통신제어기(100)로부터 차기임의값(Next ANonce)이 수신되면 1차단말기를 폐기한 뒤 제공받은 차기임의값(Next ANonce)과 단말기(500)의 주소를 이용하여 2차단말기를 생성할 수 있고, 2차단말기를 생성한 뒤 2차단말기 생성에 대한 신호인 인증값(MIC)을 통신제어기(100)로 송신할 수 있다.
- [0102] 여기서, 통신제어기(100)의 차기임의값(Next ANonce)은 재인증을 위한 요청메시지를 송신하지 않고 로딩시킬 수 있는 임의의 값을 의미할 수 있고, 차기임의값(Next ANonce)과 함께 송신하는 보안값(RSNE)은 해당 기기와 결합된 모든 무선단말에 보내는 정보를 암호화하기 위한 값을 의미할 수 있다.
- [0103] 또한, 단말기(500)로 송신하는 통신제어기(100)의 인증값(MIC)은 통신제어기(100)의 1차제어기 생성을 인증할 수 있는 신호를 의미할 수 있고, 통신제어기(100)로 송신하는 단말기(500)의 인증값(MIC)은 단말기(500)의 2차단말기 생성을 인증할 수 있는 신호를 의미할 수 있다.
- [0104] 단말기(500)로부터 2차단말기 생성에 대한 인증값(MIC)을 수신한 통신제어기(100)는 2차단말기 생성에 대한 인증값(MIC)을 저장한 후, 단말기(500)를 제2공유기(300')로 로밍시켜줄 수 있다.
- [0105] 도 6은 본 발명에 따른 공유기에 로밍되어 있는 단말기가 다른 공유기로 로밍하는 경우에 대한 인증과정에 대한 예를 나타낸 도면이다.
- [0106] 도 6을 참조하여, 제2공유기(300')와 로밍하기 위해 통신제어기(100)와 인증과정을 수행한 단말기(500)가 제3공유기(300'')로 로밍하는 경우에 대한 인증과정에 대한 예를 설명하기로 한다.
- [0107] 제2공유기(300')와 로밍되어 있는 단말기(500)가 제3공유기(300'')와 로밍하기 위하여 제2공유기(300')와 로밍하기 위하여 생성한 2차단말기 생성에 대한 신호인 인증값(MIC)을 통신제어기(100)로 송신할 수 있다.
- [0108] 한편, 단말기(500)에서 키(key)생성을 위해 생성하는 임의의 값인 단말기(500)의 임의값(SNonce)과 보안값(RSNE)을 통신제어기(100)로 송신할 수 있다.
- [0109] 단말기(500)의 2차단말기 생성에 대한 인증값(MIC)을 수신한 통신제어기(100)는 1차제어기를 폐기한 뒤 2차제어기를 생성할 수 있고, 수신한 인증값(MIC)은 저장할 수 있다.
- [0110] 2차제어기를 생성한 통신제어기(100)는 단말기(500)로 통신제어기(100)의 2차제어기 생성에 대한 신호인 인증값(MIC)과 함께 통신제어기(100)의 차기임의값(Next ANonce)과 보안값(RNSE)을 송신할 수 있다.
- [0111] 통신제어기(100)로부터 2차제어기 생성에 대한 신호인 인증값(MIC)을 수신한 단말기(500)는 2차제어기 생성에 대한 인증값(MIC)을 저장할 수 있다.
- [0112] 여기서, 통신제어기(100)의 차기임의값(Next ANonce)은 재인증을 위한 요청메시지를 송신하지 않고 로딩시킬 수 있는 임의의 값을 의미할 수 있고, 차기임의값(Next ANonce)과 함께 송신되는 보안값(RSNE)은 AP와 결합된 모든

무선단말에 보내는 정보를 암호화하기 위한 값을 의미할 수 있다.

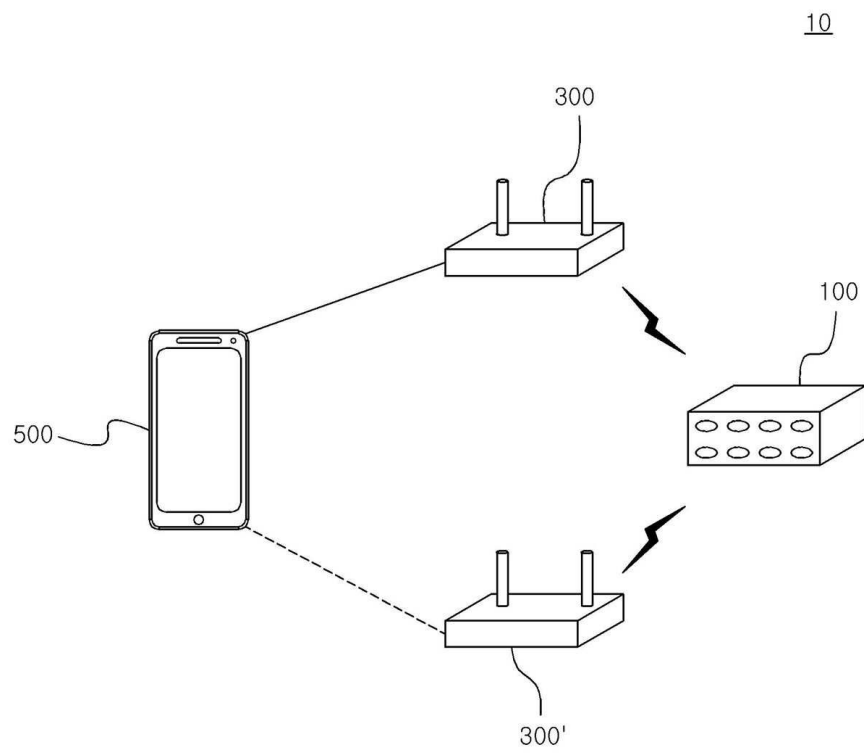
- [0113] 단말기(500)가 n차단말키(여기서, n은 자연수)를 생성하여 통신제어기(100)로 송신하는 인증값(MIC)은 단말기(500)가 n차단말키를 생성한 것에 대해 인증할 수 있는 값을 의미할 수 있다.
- [0114] 단말기(500)는 통신제어기(100)로부터 차기임의값(Next ANonce)이 수신되면 2차단말키를 폐기한 뒤 제공받은 차기임의값(Next ANonce)을 이용하여 3차단말키를 생성할 수 있고, 3차단말키를 생성한 후 3차단말키 생성에 대한 신호인 인증값(MIC)을 통신제어기(100)로 송신할 수 있다.
- [0115] 단말기(500)로부터 3차단말키 생성에 대한 인증값(MIC)을 수신한 통신제어기(100)는 3차단말키에 대한 인증값(MIC)을 저장한 후, 단말기(500)를 제3공유기(300')로 로밍시켜줄 수 있다.
- [0116] 여기서, 통신제어기(100)가 생성하는 n차제어키(여기서, n은 자연수) 및 단말기(500)가 생성하는 n차단말키(여기서, n은 자연수)는 각각 생성되기 위한 정보(SNonce, ANonce)가 수신되면, n-1차제어키 및 n-1차단말키를 폐기한 뒤 n차제어키 및 n차단말키를 생성할 수 있다.
- [0117] 전술한 바와 같이, 본 발명의 FT 프로토콜을 이용한 인증 장치인 통신제어기(100)는 음성 또는 영상 등을 이용하는 통신 지연시간에 민감한 무선 디바이스에 활용될 수 있고, 디바이스와 공유기 간의 통신 키를 주고받는 추가적인 통신 프로토콜이 불필요해지기 때문에 기존 FT프로토콜에 비해 구현을 간소화시킬 수 있다.
- [0118] 이와 같은, FT 프로토콜을 이용한 인증 방법은 어플리케이션으로 구현되거나 다양한 컴퓨터 구성요소를 통하여 수행될 수 있는 프로그램 명령어의 형태로 구현되어 컴퓨터 판독 가능한 기록 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능한 기록 매체는 프로그램 명령어, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다.
- [0119] 상기 컴퓨터 판독 가능한 기록 매체에 기록되는 프로그램 명령어는 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 분야의 당업자에게 공지되어 사용 가능한 것일 수도 있다.
- [0120] 컴퓨터 판독 가능한 기록 매체의 예에는, 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM, DVD 와 같은 광기록 매체, 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 ROM, RAM, 플래시 메모리 등과 같은 프로그램 명령어를 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다.
- [0121] 프로그램 명령어의 예에는, 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드도 포함된다. 상기 하드웨어 장치는 본 발명에 따른 처리를 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.
- [0122] 이상에서는 실시예들을 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 특허 청구범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

부호의 설명

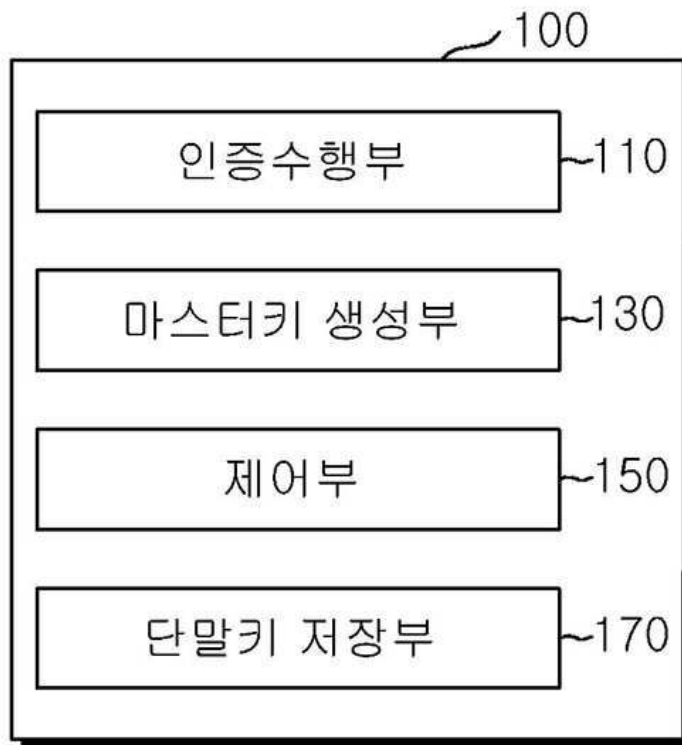
- [0124] 10: FT 프로토콜을 이용한 인증 시스템
- 100: 통신제어기
- 110: 인증수행부
- 130: 마스터키 생성부
- 150: 제어부
- 170: 단말키 저장부
- 300: 공유기
- 500: 단말기

도면

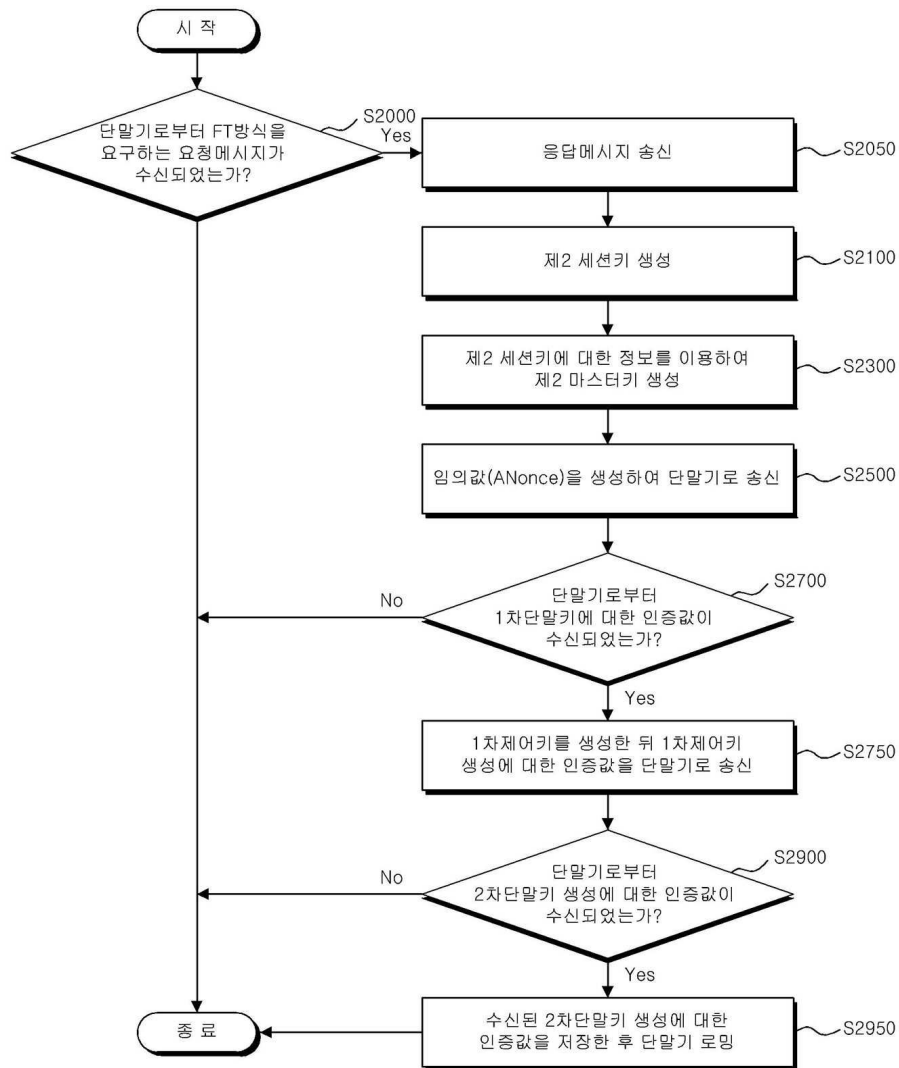
도면1



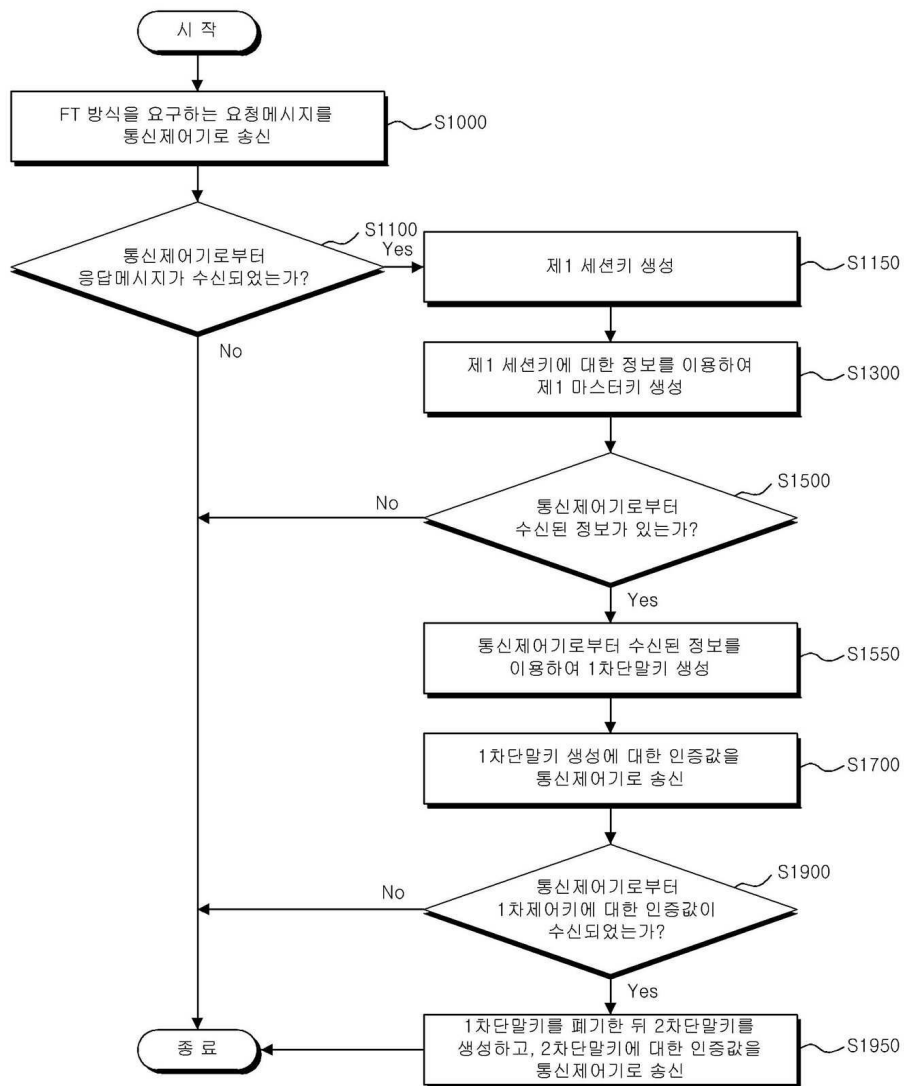
도면2



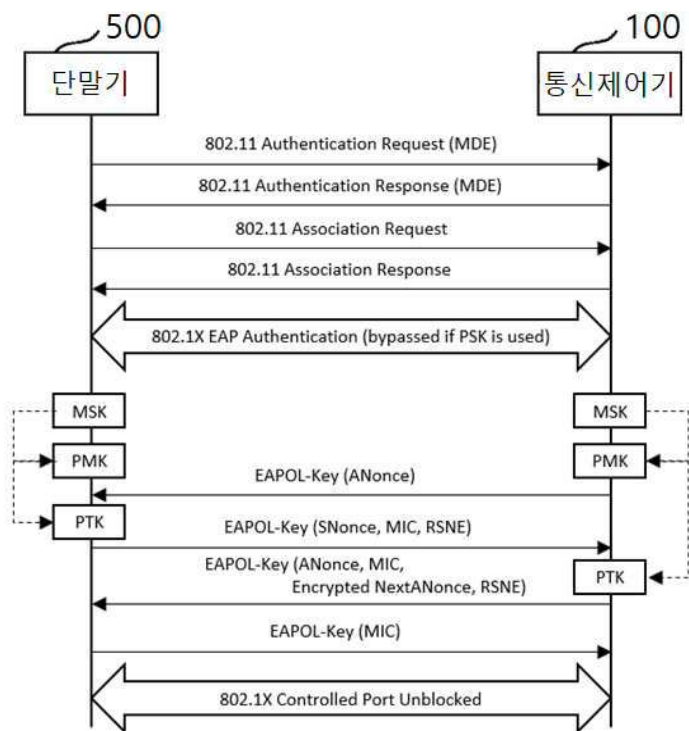
도면3



도면4



도면5



도면6

