(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2008년07월03일
(11) 등록번호 10-0843072
(24) 등록일자 2008년06월26일

(51) Int. Cl.
H04L 9/32 (2006.01)
(21) 출원번호 10-2005-0010069
(22) 출원일자 2005년02월03일
심사청구일자 2005년02월03일
(65) 공개번호 10-2006-0089008
(43) 공개일자 2006년08월08일
(56) 선행기술조사문헌
KR1020000038664 A
(뒷면에 계속)

(73) 특허권자
삼성전자주식회사
경기도 수원시 영통구 매탄동 416
(72) 발명자
이성민
서울 서초구 잠원동 신반포한신아파트 326동 1006호
오승재
서울 강남구 청담동 16-3
한세희
서울 송파구 풍납동 미성아파트 5-602
(74) 대리인
정상빈, 특허법인가산

전체 청구항 수 : 총 35 항 심사관 : 전영상

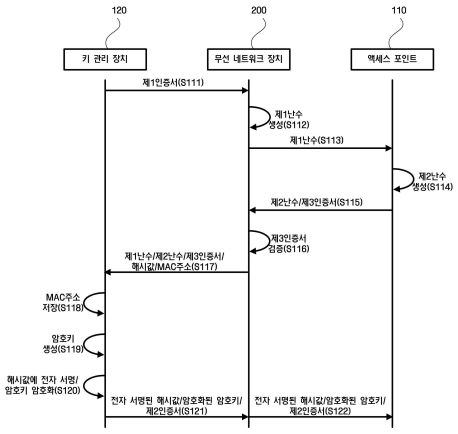
(54) 무선 네트워크 시스템 및 이를 이용한 통신 방법

(57) 요 약

본 발명은 무선 네트워크 시스템 및 이를 이용한 통신 방법에 관한 것으로서, 더욱 상세하게는 무선 네트워크에 한시적으로 접속하는 외부 네트워크 장치의 용이한 참여 및 탈퇴가 가능한 무선 네트워크 시스템 및 이를 이용한 통신 방법에 관한 것이다.

본 발명의 실시예에 따른 키 관리 장치는 무선 네트워크 장치로부터 암호화 정보를 수신하는 제한 통신부와, 상기 무선 네트워크 장치의 인증을 위한 인증 정보를 저장하는 저장부와, 상기 수신되는 암호화 정보를 통해 상기 무선 네트워크 장치가 참여하려는 무선 네트워크에서의 무선 통신을 위한 암호키를 생성하고, 상기 생성된 암호키를 상기 무선 네트워크 장치로 송신하는 키 생성부를 포함한다.

대표도 - 도6



(56) 선행기술조사문헌
KR1020010106325 A
KR1020040056485 A
WO2004017617 A1
공개특허공보 제2002-0051127호2002.06.28)*
*는 심사관에 의하여 인용된 문헌

특허청구의 범위

청구항 1

무선 네트워크 장치에서 생성된 제 1난수 및 무선 네트워크의 액세스 포인트에서 생성된 제 2난수를 포함하는 암호화 정보를 수신하는 제한 통신부와,

상기 무선 네트워크 장치의 인증을 위한 인증 정보를 저장하는 저장부와,

상기 수신된 암호화 정보 및 제 3난수를 통해 상기 무선 네트워크 장치가 참여하려는 무선 네트워크에서의 무선 통신을 위한 암호키를 생성하고, 상기 생성된 암호키를 상기 무선 네트워크 장치로 송신하는 키 생성부를 포함하는 키 관리 장치.

청구항 2

제 1 항에 있어서,

상기 제한 통신부는, 상기 무선 네트워크내의 무선 네트워크 장치들간의 통신 반경에 비하여 좁은 통신 반경을 가지는 키 관리 장치.

청구항 3

제 2 항에 있어서,

상기 제한 통신부는, 적외선 통신, 근거리 통신 및 블루투스 통신 중 적어도 하나를 사용하는 키 관리 장치.

청구항 4

제 3 항에 있어서,

상기 암호화 정보는, 상기 무선 네트워크 장치의 MAC 주소를 포함하는 키 관리 장치.

청구항 5

제 4 항에 있어서,

상기 인증 정보는, 상기 액세스 포인트로부터 발급된 인증서를 포함하는 키 관리 장치.

청구항 6

제 5 항에 있어서,

상기 키 생성부는, 상기 생성된 암호키를 상기 액세스 포인트의 인증서에 포함된 공개로 암호화하여 상기 무선 네트워크 장치로 송신하는 키 관리 장치.

청구항 7

암호키를 생성하는 키 관리 장치와 암호화 정보를 송수신하는 제한 통신부와,

소정 무선 네트워크의 액세스 포인트와 통신을 수행하는 무선 통신부와,

상기 키 관리 장치가 상기 암호화 정보에 포함된 제 1난수 및 상기 액세스 포인트로부터 수신한 제 2난수와 상기 키 관리 장치가 생성한 제 3난수를 통해 생성한 암호키를 수신하고, 상기 수신된 암호키를 통해 상기 액세스 포인트와 무선 통신을 수행하는 제어부를 포함하는 무선 네트워크 장치.

청구항 8

제 7 항에 있어서,

상기 암호화 정보는, 상기 무선 네트워크 장치의 MAC 주소를 포함하는 무선 네트워크 장치.

청구항 9

제 7 항에 있어서,

상기 수신되는 암호키는, 상기 액세스 포인트의 인증서에 포함된 공개키로 암호화되는 무선 네트워크 장치.

청구항 10

제 9 항에 있어서,

상기 암호키는, 상기 키 관리 장치의 비밀키로 전자 서명된 해쉬값과 함께 수신되는 무선 네트워크 장치.

청구항 11

제 10 항에 있어서,

상기 제한 통신부는, 상기 무선 네트워크내의 무선 네트워크 장치들간의 통신 반경에 비하여 좁은 통신 반경을 가지는 무선 네트워크 장치.

청구항 12

제 11 항에 있어서,

상기 제한 통신부는, 적외선 통신, 근거리 통신 및 블루투스 통신 중 적어도 하나를 사용하는 무선 네트워크 장치.

청구항 13

무선 네트워크에 참여하는 무선 네트워크 장치의 인증을 위한 암호화 정보를 발급하는 암호화 정보 관리부와,

상기 무선 네트워크 장치로부터 수신되는 제 1난수, 키 관리 장치로 송신되는 제 2난수 및 상기 키 관리 장치에서 생성된 제 3난수를 통해 생성된 암호키를 상기 무선 네트워크 장치로 전송하는 상기 키 관리 장치와 통신을 수행하는 제한 통신부와,

상기 무선 네트워크 장치와 통신을 수행하는 무선 통신부와,

상기 무선 네트워크 장치의 인증을 수행하고, 상기 인증된 무선 네트워크 장치와 상기 암호키를 사용하여 통신이 수행되도록 하는 제어부를 포함하는 액세스 포인트.

청구항 14

제 13 항에 있어서,

상기 암호화 정보는, 상기 무선 네트워크 장치 및 상기 키 관리 장치로 송신되는 인증서를 포함하는 액세스 포인트.

청구항 15

삭제

청구항 16

제 14 항에 있어서,

상기 제한 통신부는, 상기 키 관리 장치로부터 송신되는 상기 무선 네트워크 장치의 MAC 주소를 수신하는 액세스 포인트.

청구항 17

제 16 항에 있어서,

상기 제한 통신부는, 상기 무선 네트워크내의 무선 네트워크 장치들간의 통신 반경에 비하여 좁은 통신 반경을 가지는 액세스 포인트.

청구항 18

제 17 항에 있어서,

상기 제한 통신부는, 적외선 통신, 근거리 통신 및 블루투스 통신 중 적어도 하나를 사용하는 액세스 포인트.

청구항 19

무선 네트워크 장치에서 생성된 제 1난수 및 무선 네트워크의 액세스 포인트에서 생성된 제 2난수를 포함하는 암호화 정보를 수신하는 단계와,

상기 무선 네트워크 장치의 인증을 위한 인증 정보를 수신하는 단계와,

상기 수신되는 암호화 정보 및 제 3난수를 통해 상기 무선 네트워크 장치가 참여하려는 무선 네트워크에서의 무선 통신을 위한 암호키를 생성하고, 상기 생성된 암호키를 상기 무선 네트워크 장치로 송신하는 단계를 포함하는 키 관리 방법.

청구항 20

제 19 항에 있어서,

상기 암호화 정보를 수신하는 단계는, 상기 무선 네트워크내의 무선 네트워크 장치들간의 통신 반경에 비하여 좁은 통신 반경을 가지는 통신 수단을 통해 수신하는 단계를 포함하는 키 관리 방법.

청구항 21

제 20 항에 있어서,

상기 암호화 정보는, 적외선 통신, 근거리 통신 및 블루투스 통신 중 적어도 하나의 통신 수단을 통해 수신되는 키 관리 방법.

청구항 22

제 21 항에 있어서,

상기 암호화 정보는, 상기 무선 네트워크 장치의 MAC 주소를 포함하는 키 관리 방법.

청구항 23

제 22 항에 있어서,

상기 인증 정보는, 상기 액세스 포인트로부터 발급된 인증서를 포함하는 키 관리 방법.

청구항 24

제 23 항에 있어서,

상기 암호키를 생성하는 단계는, 상기 생성된 암호키를 상기 액세스 포인트의 인증서에 포함된 공개키로 암호화하여 상기 무선 네트워크 장치로 송신하는 단계를 포함하는 키 관리 방법.

청구항 25

암호키를 생성하는 키 관리 장치로 제 1난수를 포함하는 암호화 정보를 송신하는 단계와,

상기 키 관리 장치가 상기 제 1난수와 무선 네트워크의 액세스 포인트로부터 수신하는 제 2난수 및 상기 키 관리 장치가 생성한 제 3난수를 통해 생성한 암호키를 수신하는 단계와,

상기 수신된 암호키를 통해 상기 무선 네트워크의 액세스 포인트와 무선 통신을 수행하는 단계를 포함하는 무선 네트워크 장치의 통신 방법.

청구항 26

제 25 항에 있어서,

상기 송신되는 암호화 정보는, 상기 무선 네트워크 장치의 MAC 주소를 포함하는 무선 네트워크 장치의 통신 방법.

청구항 27

제 26 항에 있어서,

상기 수신되는 암호키는, 상기 액세스 포인트의 인증서에 포함된 공개키에 의해 암호화되는 무선 네트워크 장치의 통신 방법.

청구항 28

제 27 항에 있어서,

상기 암호키는, 상기 키 관리 장치의 비밀키로 전자 서명된 해쉬값과 함께 수신되는 무선 네트워크 장치의 통신 방법.

청구항 29

제 28 항에 있어서,

상기 송신되는 암호화 정보 및 상기 수신되는 암호키는, 상기 무선 네트워크내의 무선 네트워크 장치들간의 통신 반경에 비하여 좁은 통신 반경을 가지는 무선 네트워크 장치의 통신 방법.

청구항 30

제 29 항에 있어서,

상기 송신되는 암호화 정보 및 상기 수신되는 암호키는, 적외선 통신, 근거리 통신 및 블루투스 통신 중 적어도 하나에 의해 송수신되는 무선 네트워크 장치의 통신 방법.

청구항 31

무선 네트워크에 참여하려는 무선 네트워크 장치로 제 2난수를 포함하는 암호화 정보를 송신하는 단계와,

상기 무선 네트워크 장치로부터 송신된 제 1난수 및 상기 제 2난수를 수신하는 키 관리 장치가 상기 제 1난수, 상기 제 2난수 및 상기 키 관리 장치가 생성한 제 3난수를 통해 생성한 암호키를 수신하는 단계와,

상기 무선 네트워크 장치의 인증을 수행하고, 상기 인증된 무선 네트워크 장치와 상기 암호키를 사용하여 통신을 수행하는 단계를 포함하는 액세스 포인트의 통신 방법.

청구항 32

제 31 항에 있어서,

상기 암호화 정보는, 상기 무선 네트워크 장치로 송신되는 인증서를 포함하는 액세스 포인트의 통신 방법.

청구항 33

삭제

청구항 34

제 31 항에 있어서,

상기 키 관리 장치로부터 상기 무선 네트워크 장치의 MAC 주소를 수신하는 단계를 더 포함하는 액세스 포인트의 통신 방법.

청구항 35

제 34 항에 있어서,

상기 MAC 주소를 수신하는 단계는, 상기 무선 네트워크내의 무선 네트워크 장치들간의 통신 반경에 비하여 좁은 통신 반경을 가지는 통신에 의해 수신되는 단계를 포함하는 액세스 포인트의 통신 방법.

청구항 36

제 35 항에 있어서,

상기 MAC 주소를 수신하는 단계는, 상기 MAC 주소가 적외선 통신, 근거리 통신 및 블루투스 통신 중 적어도 하나를 사용하여 수신되는 단계를 포함하는 액세스 포인트의 통신 방법.

청구항 37

제 36 항에 있어서,

상기 수신된 MAC 주소와 일치하는 무선 네트워크 장치를 상기 무선 네트워크로부터 접속 해제시키는 단계를 더 포함하는 액세스 포인트의 통신 방법.

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

<12> 본 발명은 무선 네트워크 시스템 및 이를 이용한 통신 방법에 관한 것으로서, 더욱 상세하게는 무선 네트워크에 한시적으로 접속하는 외부 네트워크 장치의 용이한 참여 및 탈퇴가 가능한 무선 네트워크 시스템 및 이를 이용한 통신 방법에 관한 것이다.

<13> 통신 및 네트워크 기술의 발달에 따라 최근의 네트워크 환경은 동축 케이블 또는 광 케이블과 같은 유선 매체를 이용하는 유선 네트워크 환경으로부터 다양한 주파수 대역의 무선 신호를 이용하는 무선 네트워크 환경으로 변해가고 있다.

<14> 무선 네트워크는 유선 네트워크와 달리 데이터 전송 경로가 물리적으로 고정되어 있지 않으므로 유선 네트워크에 비해 통신의 보안성이 취약하다. 따라서 보다 안전한 무선 통신을 수행하기 위한 노력으로, 대부분의 무선 통신 프로토콜은 전송되는 데이터 패킷에 대한 암호화를 지원한다. 예를 들어, 무선랜에서 사용되는 WPA-PSK(Wi-Fi Protected Access Pre-Shared Key) 방식이나 WEP(Wired Equivalent Privacy) 방식 등을 사용하여 보다 안전한 무선 통신을 수행하고 있다.

<15> 이 중, WEP 방식은 공기 중의 프레임에 상대적으로 최소한의 보호를 제공하기 위해 설계되었다. 따라서, WEP은 높은 수준의 보안이 필요한 경우를 대비하여 설계된 것이 아니므로, 802.11의 광범위한 구축을 방해하는 많은 보안 문제는 WEP 설계의 결함으로 발생한다.

<16> 따라서, 802.1x는 확장 인증 프로토콜(Extensible Authentication Protocol, 이하 EAP라 함)에 기반하고 있다. EAP는 RFC 2284에서 스펙이 공식적으로 확정되어 있다.

<17> 도 1은 종래의 기술에 따른 암호키 설정 과정이 도시된 도면이다. 이때, 도 1의 액세스 포인트(Access Point)는 스테이션(Station)과 인증 서버(Authentication Server)간의 메시지를 중계해주는 역할만을 수행하게 된다.

<18> 도시된 바와 같이, 최초 액세스 포인트(20)는 스테이션(10)에게 사용자를 식별하기 위해 요청/식별자 메시지를 전송한다(S11). 이후, 스테이션(10)은 사용자 식별자(예를 들어, MyID 등)를 포함한 응답/식별자 메시지를 인증 서버(30)로 전송한다(S12).

<19> 이후, 스테이션(10)과 인증 서버(30)는 악의적 사용자에 의한 메시지의 재사용을 막기 위해 각각 제 1난수와 제 2난수를 생성하고(S13, S14), 생성된 제 1난수와 제 2난수를 서로 교환하게 된다(S15, S16). 이때, 난수란 임의성을 가지는 숫자 또는 문자열을 의미한다.

<20> 또한, 인증 서버(30)는 공인 인증서를 발급하는 인증 기관(Certificate Authority)으로부터 발급된 인증서를 제 2난수와 함께 스테이션(10)으로 전송하게 된다.

<21> 스테이션(10)는 인증 서버(30)로부터 전송된 인증서를 인증 기관의 공개키를 통해 검증하고(S17), 소정 바이트(예를 들어, 48바이트)의 제 3난수를 생성한다(S18).

<22> 스테이션(10)은 제 1난수 및 전송된 제 2난수와 생성된 제 3난수를 통해 암호키를 생성하고(S19), 인증 서버(30)의 인증서에 포함된 인증 서버(30)의 공개키를 사용하여 생성된 암호키를 암호화한다(S20). 이후, 스테이션

(10)은 암호화된 암호키와 자신의 인증서를 인증 서버(30)로 전송한다(S21).

<23> 인증 서버(30)는 스테이션(10)의 인증서를 인증 기관의 공개키를 통해 복호화하여 검증한후 수신된 암호키를 자신의 비밀키로 복호화하여 자신의 암호키로 사용하게 된다(S22).

<24> 이후, 스테이션(10)과 인증 서버(30)는 암호키를 공유하게 되고, 공유하는 암호키와 제 1난수 및 제 2난수를 이용하여 최종적으로 사용할 암호키를 생성하고, 생성된 최종 암호키를 통해 서로 무선 통신을 수행하게 된다.

<25> 전술한 바와 같은 암호키 생성 과정을 통해 별도의 인증 기관으로부터 발급된 인증서를 보유하는 무선 네트워크 장치들간에는 안전한 무선 통신이 가능하게 된다.

<26> 이때, 새로운 무선 네트워크 장치가 해당 무선 네트워크에 한시적으로 참여하기 위해서는 무선 네트워크 장치는 인증 기관으로부터 한시적인 유효 기간을 가지는 인증서를 발급받아야 되며, 이러한 인증서를 가진 무선 네트워크 장치는 발급받은 인증서에 명시된 허가된 기간동안만 무선 네트워크에 참여할 수 있게 된다.

<27> 그러나, 인증 기관으로부터 인증서를 발급받는 과정은, 무선 네트워크 장치가 무선 네트워크에 참여하는 과정과는 별도로 이루어지게 된다. 다시 말해서, 무선 네트워크 장치는 인증 기관에 유선으로 연결된 시스템을 이용하여 인증 기관에 접속한 다음, 소정의 인증서 발급 절차를 거쳐 인증서를 발급받은 후 소정의 이동 저장 매체(예를 들어, 디스켓 및 스마트 카드 등)를 이용해 발급받은 인증서를 스테이션으로 옮겨와야 하는 과정을 거치게 된다.

<28> 이와 같이, 인증 기관으로부터 인증서를 발급받은 과정을 마친 후, 무선 네트워크 장치가 해당 무선 네트워크에 참여하는 과정이 이루어지게 된다. 따라서, 무선 네트워크 장치가 무선 네트워크로의 무단으로 참여하는 것을 방지하기 위하여, 인증 기관으로부터 인증서를 발급받는 과정을 모두 거쳐야 된다. 또한, 무선 네트워크 장치의 한시적인 무선 네트워크로의 참여가 빈번히 발생하는 상황이라면 매번 인증서의 발급 및 폐기 과정이 반복적으로 필요하기 때문에 무선 네트워크 관리자의 네트워크 관리는 더욱 어려워질수밖에 없다.

<29> 한국 공개 특허 2002-0051127는 인증서버 또는 사용자에 의해 인증, 암/복호화 기능을 요청받으면, 휴대폰과 스마트 카드간 고속 무선 모뎀칩을 통해 근거리 통신을 수행하여, 스마트 카드에서 처리된 인증 및 암/복호화 데이터를 무선으로 휴대폰으로 전송하는 방법을 개시하고 있으나, 이는 휴대폰과 스마트 카드내에 근거리 통신을 전담하는 고속 무선 모뎀칩을 내장하여 데이터 전송률에 있어서의 대량 데이터를 고속으로 송수신하여 신뢰성 있는 통신을 보장하는 것으로서, 무선 네트워크에 한시적으로 참여하는 네트워크 장치에 대한 인증이나 무단으로 참여하는 네트워크 장치를 방지하기 위해서는 역부족이었다.

발명이 이루고자 하는 기술적 과제

<30> 본 발명은 무선 네트워크에 외부의 네트워크 장치가 한시적으로 참여할 경우 무선 네트워크에 존재하는 장치를 통해 네트워크 장치에게 인증을 위한 정보가 제공되도록 하는 무선 네트워크 시스템 및 이를 이용한 통신 방법을 제공하는데 그 목적이 있다.

<31> 본 발명의 목적은 이상에서 언급한 목적들로 제한되지 않으며, 언급되지 않은 또 다른 목적들은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

발명의 구성 및 작용

<32> 상기 목적을 달성하기 위하여, 본 발명의 실시예에 따른 키 관리 장치는, 무선 네트워크 장치로부터 암호화 정보를 수신하는 제한 통신부와, 상기 무선 네트워크 장치의 인증을 위한 인증 정보를 저장하는 저장부와, 상기 수신되는 암호화 정보를 통해 상기 무선 네트워크 장치가 참여하려는 무선 네트워크에서의 무선 통신을 위한 암호키를 생성하고, 상기 생성된 암호키를 상기 무선 네트워크 장치로 송신하는 키 생성부를 포함한다.

<33> 또한, 상기 목적을 달성하기 위하여, 본 발명의 실시예에 따른 무선 네트워크 장치는, 암호키를 생성하는 키 관리 장치와 암호화 정보를 송수신하는 제한 통신부와, 소정 무선 네트워크의 액세스 포인트와 통신을 수행하는 무선 통신부와, 상기 키 관리 장치로부터 생성된 암호키를 수신하고, 상기 수신된 암호키를 통해 무선 네트워크의 액세스 포인트와 무선 통신을 수행하는 제어부를 포함한다.

<34> 또한, 상기 목적을 달성하기 위하여, 본 발명의 실시예에 따른 액세스 포인트는, 무선 네트워크에 참여하는 무선 네트워크 장치의 인증을 위한 암호화 정보를 발급하는 암호화 정보 관리부와, 상기 무선 네트워크 장치로 암호키를 전송하는 키 관리 장치와 통신을 수행하는 제한 통신부와, 무선 네트워크 장치와 통신을 수행하는 무선

통신부와, 상기 무선 네트워크 장치의 인증을 수행하고, 상기 인증된 무선 네트워크 장치와 상기 암호키를 사용하여 통신을 수행되도록 하는 제어부를 포함한다.

<35> 또한, 상기 목적을 달성하기 위하여, 본 발명의 실시예에 따른 키 관리 방법은, 무선 네트워크 장치로부터 암호화 정보를 수신하는 단계와, 상기 무선 네트워크 장치의 인증을 위한 인증 정보를 저장하는 단계와, 상기 수신되는 암호화 정보를 통해 상기 무선 네트워크 장치가 참여하려는 무선 네트워크에서의 무선 통신을 위한 암호키를 생성하고, 상기 생성된 암호키를 상기 무선 네트워크 장치로 송신하는 단계를 포함한다.

<36> 또한, 상기 목적을 달성하기 위하여, 본 발명의 실시예에 따른 무선 네트워크 장치의 통신 방법은, 암호키를 생성하는 키 관리 장치로 암호화 정보를 송신하는 단계와, 상기 키 관리 장치로부터 상기 암호키를 수신하는 단계와, 상기 수신된 암호키를 통해 무선 네트워크의 액세스 포인트와 무선 통신을 수행하는 단계를 포함한다.

<37> 또한, 상기 목적을 달성하기 위하여, 본 발명의 실시예에 따른 액세스 포인트의 통신 방법은, 무선 네트워크에 참여하는 무선 네트워크 장치로 암호화 정보를 송신하는 단계와, 상기 무선 네트워크 장치로부터 송신된 암호키를 수신하는 단계와, 상기 무선 네트워크 장치의 인증을 수행하고, 상기 인증된 무선 네트워크 장치와 상기 암호키를 사용하여 통신을 수행하는 단계를 포함한다.

<38> 기타 실시예들의 구체적인 사항들은 상세한 설명 및 도면들에 포함되어 있다.

<39> 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 그러나 본 발명은 이하에서 개시되는 실시예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있으며, 단지 본 실시예들은 본 발명의 개시가 완전하도록 하고, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다. 명세서 전체에 걸쳐 동일 참조 부호는 동일 구성 요소를 지칭한다.

<40> 이하, 첨부된 도면을 참조하여 본 발명의 바람직한 실시예를 상세히 설명하기로 한다.

<41> 도 2는 본 발명의 실시예에 따른 무선 네트워크 시스템이 도시된 도면이다.

<42> 도시된 바와 같이, 무선 네트워크(100)는 액세스 포인트(110), 키 관리 장치(120) 및 적어도 하나 이상의 스테이션들(130, 140)을 포함할 수 있다.

<43> 이하, 본 발명의 실시예에서 무선 네트워크(100)를 구성하는 스테이션들(130, 140)을 '무선 네트워크 장치'라고 통칭하기로 한다. 또한, 본 발명의 실시예에 따른 액세스 포인트(110) 및 스테이션들(130, 140)은 EAP 방식을 사용하여 통신의 보안을 유지할 수 있다.

<44> 또한, 본 발명을 설명하는데 있어서, 스테이션은 노트북, 셀룰러폰, 디지털 TV, 셋탑 박스 등 무선 네트워크에 접속하여 무선 매체를 통해 통신을 수행할 수 있는 무선 네트워크 장치를 의미한다. 액세스 포인트는 스테이션에 대해 무선 네트워크로의 접속을 제어할 수 있는 네트워크 접속 제어 장치를 의미한다. 이때, 본 발명의 실시예에서 있어서, 액세스 포인트 및 스테이션은 무선랜에 대한 IEEE 802.11 표준에서 정의 되는 액세스 포인트 및 스테이션의 개념으로 설명될 수 있다.

<45> 도 3은 본 발명의 실시예에 따른 키 관리 장치가 도시된 도면이다.

<46> 키 관리 장치(120)는 플래시 메모리 등과 같이 데이터를 읽고 쓰고 지울 수 있는 성질을 갖는 비휘발성 저장 장치를 포함하며, 필요에 따라 전술한 비휘발성 저장 매체를 포함하는 이동 가능한 장치로 이해될 수 있다. 예를 들어, 키 관리 장치(120)는 스마트 카드나 멀티미디어 카드와 같은 휴대용 저장 장치이거나 휴대폰 및 PDA 등과 같은 휴대용 통신 장치일 수도 있다.

<47> 이러한 키 관리 장치(120)는 무선 네트워크 장치와 암호화 정보를 송수신하는 제한 통신부(121)와, 외부 네트워크 장치(150)가 무선 네트워크(100)에 참여할 경우, 참여할 외부 네트워크 장치(150)의 인증을 위한 인증 정보를 저장하는 저장부(122)와, 송수신하는 암호화 정보를 통해 암호키를 생성하는 키 생성부(123)와, 외부 네트워크 장치(150)가 무선 네트워크(100)로 참여할 경우, 참여하는 외부 네트워크 장치(150)의 인증을 수행하고, 생성된 암호키를 외부 네트워크 장치(150)로 송신시키는 제어부(124)를 포함할 수 있다.

<48> 이때, 제한 통신부(121)는 무선 네트워크(100)에 포함된 무선 네트워크 장치들간의 통신 반경보다 좁은 통신 반경을 가지게 된다. 이는 키 관리 장치(120)와 무선 네트워크 장치간의 통신을 외부에서 감지하기 못하게 하기 위함이다. 예를 들어, 제한 통신부(121)는 적외선 통신, 근거리 통신 및 블루투스 통신 등이 사용될 수 있으나, 이에 한정되지 않는다.

<49> 키 관리 장치(120)가 무선 네트워크 장치와 송수신하는 암호화 정보로는, 무선 네트워크 장치에서 생성된 제 1난수와, 액세스 포인트(110)로부터 생성된 제 2난수와, 무선 네트워크 장치의 MAC 주소를 포함할 수 있다. 또한, 인증 정보로는 액세스 포인트(110)로부터 발급된 인증서 및 비밀키를 포함할 수 있다. 이때, 본 발명의 실시예에 따른 액세스 포인트(110)는 무선 네트워크 장치와의 통신을 수행하는 기능 이외에 무선 네트워크(100)에 참여하려는 무선 네트워크 장치를 인증하는 인증 서버의 기능과 본 발명의 실시예에서 사용되는 모든 인증서를 발급하는 인증 기관(Certificate Authority)의 기능을 함께 수행할 수 있다. 본 발명의 실시예에 따른 액세스 포인트(110)에 대한 상세한 설명은 후술하기로 한다.

<50> 또한, 저장부(122)에 저장된 인증서는 인증 기관으로서 액세스 포인트(110)가 발급한 루트(root) 인증서(이하, 제 1인증서라함) 및 키 관리 장치(120)의 인증서(이하, 제 2인증서라함)를 포함할 수 있다. 이때, 제 1인증서는 인증 기관으로서의 액세스 포인트(110)가 발급한 인증서로서 액세스 포인트(110)에서 발급된 모든 인증서를 검증할 수 있는 공개키를 포함할 수 있다.

<51> 따라서, 키 관리 장치(120)는 제 1인증서를 저장하고 있기 때문에 전술한 공개키를 알 수 있으며, 액세스 포인트(110)에서 발급된 모든 인증서를 검증할 수 있다.

<52> 또한, 저장부(122)는 무선 네트워크 장치의 MAC 주소를 저장하게 되는데, 이는 MAC 주소를 통해 무선 네트워크(100)로부터 탈퇴하는 무선 네트워크 장치를 확인하고, 접속을 해제할 수 있기 때문이다.

<53> 한편, 키 생성부(123)는 수신된 제 1난수 및 제 2난수와 더불어 소정의 제 3난수를 생성하여 암호키를 생성하고, 제어부(124)는 생성된 암호키를 액세스 포인트(110)로부터 수신한 액세스 포인트(110)의 인증서(이하, 제 3인증서라 함)에 포함된 공개키를 사용하여 암호화하고, 암호화된 암호키를 제한 통신부(121)를 통해 무선 네트워크 장치로 송신하게 된다. 이때, 암호화된 암호키와 함께 그때까지 송수신한 모든 메시지를 모아 연결한 메시지의 해쉬 값에 저장부(122)에 저장되어 있는 비밀키를 사용하여 전자 서명한 값을 무선 네트워크 장치로 송신하게 된다.

<54> 암호화되어 송신되는 암호키와 전자 서명된 해쉬 값은 이후 무선 네트워크 장치와 액세스 포인트(110)간 통신에 사용할 키를 생성하는 데 사용되거나 액세스 포인트(110)가 무선 네트워크 장치를 인증하는 데 사용될 수 있다.

<55> 도 4는 본 발명의 실시예에 따른 무선 네트워크 장치가 도시된 도면이다. 이때, 도시된 무선 네트워크 장치는 전술한 도 2의 스테이션(130, 140) 및 외부 네트워크 장치(150)로 이해될 수 있으며, 각 스테이션의 구성은 동일하게 사용될 수 있다.

<56> 도시된 바와 같이, 본 발명의 실시예에 따른 무선 네트워크 장치(200)는 전술한 키 관리 장치(120)와 암호화 정보를 송수신하는 제한 통신부(210)와, 액세스 포인트(110)와의 무선 통신을 위한 무선 통신부(220)와, 키 관리 장치(120)로부터 송신된 암호키와 전자 서명된 해시값을 저장하는 저장부(230)와, 저장된 암호키를 통해 액세스 포인트(110)와의 인증 과정을 수행하는 제어부(240)를 포함할 수 있다. 또한, 저장부(230)는 키 관리 장치(120)로부터 송신된 제 1인증서를 저장하게 된다. 이때, 저장된 제 1인증서는 인증 기관으로서의 액세스 포인트(110)로부터 발급된 루트 인증서로서, 무선 네트워크 장치(200)는 제 1인증서에 포함된 공개키를 통해 액세스 포인트(110)로부터 발급된 모든 인증서를 검증할 수 있다.

<57> 한편, 제어부(240)는 소정의 제 1난수를 생성하여 액세스 포인트(110)로 송신하고, 액세스 포인트(110)로부터 생성된 제 2난수 및 제 3인증서를 수신하게 된다. 이때, 제어부(240)는 제 1인증서에 포함된 공개키를 사용하여 수신된 액세스 포인트(110)의 제 3인증서를 검증할 수 있다.

<58> 이후, 제어부(240)는 제한 통신부(210)를 사용하여 제 1난수 및 제 2난수, 제 3인증서, 그때까지 액세스 포인트와 송수신한 메시지를 모아 연결시킨 메시지의 해시값을 키 관리 장치(120)로 송신하게 되고, 송신 결과 수신하게 되는 암호키와 전자 서명된 해쉬값을 통해 액세스 포인트(110)와 인증 과정을 수행할 수 있다. 이때 키 관리 장치(120)로부터 수신되는 암호키는 전술한 키 관리 장치(120)의 저장부(122)에 저장된 제 3인증서에 포함된 공개키를 통해 암호화되어 수신된다. 또한, 암호키와 더불어 키 관리 장치의 비밀키로 전자 서명된 해쉬값을 수신할 수 있다. 이와 같이 암호화된 암호키 및 서명된 해쉬값은 액세스 포인트(110)와 무선 네트워크 장치와의 인증에 사용될 수 있다. 다시 말해서, 제어부(240)는 암호화된 암호키 및 서명된 해쉬값을 키 관리 장치(120)의 제 2인증서와 함께 액세스 포인트(110)로 송신하게 된다. 따라서, 액세스 포인트(110)는 수신된 키 관리 장치(120)의 인증서를 검증하여 키 관리 장치(120)의 공개키를 확인하고, 검증된 공개키를 사용하여 무선 네트워크 장치로부터 수신한 전자 서명된 해쉬값을 검증하여 무선 네트워크 장치(200)의 무선 네트워크(100)에 참여 여부를 결정한 다음, 자신의 비밀키를 사용하여 암호화된 암호키 복호화하여 이후 무선 네트워크 장치와 액세스 포

인트 간의 통신에 사용할 키를 생성하는데 사용할 수 있다.

<59> 도 5는 본 발명의 실시예에 따른 액세스 포인트가 도시된 도면이다.

<60> 도시된 바와 같이, 본 발명의 실시예에 따른 액세스 포인트(110)는 무선 네트워크 장치(200)와의 통신을 위한 무선 통신부(111)와, 키 관리 장치(120)와의 통신을 위한 제한 통신부(112)와, 암호화 정보를 생성하는 암호화 정보 관리부(113)와, 사용자가 액세스 포인트(110)의 제어 명령을 입력할 수 있는 사용자 인터페이스부(114)와, 인증 정보를 저장하는 저장부(115)와, 무선 네트워크(100)의 무선 네트워크 장치들에 대한 인증을 수행하는 제어부(116)를 포함할 수 있다.

<61> 이때, 무선 통신부(111)는 무선 네트워크 장치(200)로부터 생성된 제 1난수를 수신하고, 액세스 포인트(110)에서 생성된 제 2난수와 제 3인증서를 송신하기 위해 사용될 수 있다. 이때, 송신되는 제 3인증서는 액세스 포인트(110)로서의 인증서로서, 본 발명의 실시예에 따른 액세스 포인트(110)가 인증 기관의 역할을 수행하기 위한 인증 기관의 제 1인증서와는 다르게 이해될 수 있다.

<62> 제한 통신부(112)는 전술한 적외선 통신, 근거리 통신 및 블루투스 통신 등을 사용하여 키 관리 장치(120)의 통신을 외부에서 감지할 수 없게 한다.

<63> 암호화 정보 관리부(113)는 전술한 제 1인증서, 제 2인증서 및 제 3인증서와 비밀키를 생성할 수 있다. 또한, 전술한 키 관리 장치(120)로 발급되는 인증 정보의 생성 및 폐기를 수행한다.

<64> 제어부(116)는 키 관리 장치(120)로부터 생성된 암호키와 서명된 해쉬값을 무선 통신부(111)를 통해 수신하여 무선 네트워크 장치의 인증을 수행하게 된다. 구체적으로, 수신되는 암호키는 액세스 포인트(110)의 공개키로 암호화되어 있으며, 키 관리 장치(120)의 비밀키로 전자 서명된 해쉬값과 함께 수신될 수 있다. 이때, 제어부(116)는 키 관리 장치(120)의 인증서를 함께 수신하게 된다.

<65> 따라서, 제어부(116)는 인증 기관의 인증서를 가지고 있기 때문에 자신이 발급한 모든 인증서를 검증할 수 있는 공개키를 보유하고 있으므로, 수신된 키 관리 장치(120)의 인증서를 통해 키 관리 장치(120)의 공개키를 검증하고, 자신의 비밀키를 이용해 암호화된 암호키를 복호화 하며 전자 서명된 해쉬값을 검증하여 무선 네트워크 장치의 인증을 수행하게 된다.

<66> 한편, 제한 통신부(112)는 키 관리 장치(120)와의 통신을 통해 무선 네트워크 장치(200)가 해당 무선 네트워크에서 탈퇴한 경우, 해당 무선 네트워크 장치의 MAC 주소를 수신하고, 제어부(116)는 수신된 MAC 주소와 일치하는 네트워크 장치를 무선 네트워크(100)로부터 접속 해제시키게 된다.

<67> 상기와 같은 키 관리 장치(120), 무선 네트워크 장치(200) 및 액세스 인트(110) 간의 암호키 생성 과정을 살펴보면 다음과 같다.

<68> 도 6은 본 발명의 실시예에 따른 암호키 생성 과정을 개략적으로 도시하고 있다. 이때, 본 발명의 실시예에서, 키 관리 장치(120)는 액세스 포인트(110)가 인증 기관으로서 발급한 제 1인증서 및 자신의 인증서인 제 2인증서와 비밀키를 가지고 있고, 액세스 포인트(110)는 인증 기관으로서의 인증서인 제 1인증서 및 자신의 인증서인 제 3인증서와 비밀키를 가지고 있는 경우를 예를 들어 설명하기로 한다.

<69> 도시된 바와 같이, 먼저 키 관리 장치(120)가 무선 네트워크 장치(200)로 제 1인증서를 송신한다(S111). 본 발명의 실시예에 따른 액세스 포인트(110)가 인증 기관의 역할(예를 들어, 인증서 발급 및 폐기 등)과 무선 네트워크 장치(120)와의 인증을 수행하는 인증 서버의 역할을 수행하며, 제 1인증서는 인증 기관으로서의 루트 인증서로 이해될 수 있다. 따라서, 무선 네트워크 장치(200)는 제 1인증서를 수신하게 됨에 따라 액세스 포인트(110)에서 발급된 모든 인증서를 검증할 수 있는 공개키를 보유할 수 있게 된다.

<70> 이후, 무선 네트워크 장치(112)는 제 1난수를 생성하고, 생성된 제 1난수를 액세스 포인트(110)로 송신한다(S113). 이때, 제 1난수를 수신한 액세스 포인트(110)는 제 2난수를 생성하여(S114), 생성된 제 2난수와 인증서버로서의 인증서인 제 3인증서를 무선 네트워크 장치(200)로 송신한다(S115).

<71> 이때, 무선 네트워크 장치(200)는 제 1인증서에 포함된 공개키를 통해 수신된 제 3인증서를 검증하게 된다(S116). 제 3인증서에 대한 검증이 완료되면, 무선 네트워크 장치(200)는 제 1난수, 제 2난수, 제 3인증서, 그때까지 액세스 포인트(110)와 송수신한 메시지를 모아 연결시킨 메시지의 해시값 및 자신의 MAC 주소를 키 관리 장치(120)로 송신한다.(S117). 이때, 송신되는 제 1난수 및 제 2난수는 키 관리 장치(120)에서 암호키를 생성하기 위해 사용되며, 제 3인증서는 생성된 암호키를 암호화하기 위해 사용되며, 해시값은 액세스 포인트(110)와의

인증을 위해 사용되며, MAC 주소는 무선 네트워크 장치(200)가 무선 네트워크(100)에서 탈퇴할 경우, 탈퇴 처리를 위해 사용된다.

<72> 키 관리 장치(120)는 수신된 MAC 주소를 저장하고(S118), 수신된 제 1난수 및 제 2난수와 소정의 제 3난수를 통해 암호키를 생성한다(S119).

<73> 또한, 키 관리 장치(120)는 무선 네트워크 장치로(200)부터 수신한 해시값에 저장부(122)에 저장된 키 관리 장치(120)의 비밀키로 전자 서명을 하고, 제 1난수, 제 2난수를 이용해 생성된 암호키를 제 3인증서에 포함된 액세스 포인트(110)의 공개키를 통해 암호화한다(S120). 이후, 전자 서명된 해시값과 암호화된 암호키를 자신의 인증서인 제 2인증서와 함께 무선 네트워크 장치(200)로 송신한다(S121). 이때, 함께 송신하는 제 2인증서는 전술한 초기에 무선 네트워크 장치(200)에게 제 1인증서를 송신하는 단계(S111)에서 함께 송신할 수도 있다.

<74> 이후, 무선 네트워크 장치(200)는 전자 서명된 해시값과 암호화된 암호키 및 제 2인증서를 액세스 포인트(110)로 전송하고(S122), 액세스 포인트(110)는 인증 기관으로서의 인증서인 제 1인증서에 포함된 공개키를 통해 제 2인증서를 검증하고, 자신의 비밀키를 이용해 암호화된 암호키를 복호화 하고, 수신한 제 2인증서에 포함된 공개키를 통해 전자 서명된 해시값을 검증하게 된다.

<75> 이때, 전자 서명된 해쉬값이 검증되면, 무선 네트워크 장치(200)의 무선 네트워크(100)에 대한 참여를 허용하고 복호화하여 얻은 암호키를 사용해 이후 통신에 사용될 키를 생성할 수 있으며, 그렇지 않은 경우 무선 네트워크(100)에 대한 참여를 거부하게 된다.

<76> 이와 같이, 본 발명의 실시예에 따른 무선 네트워크 장치(200)는 액세스 포인트(110)와의 인증을 위한 비밀키를 키 관리 장치(120)가 별도로 가지고 있기 때문에 무선 네트워크 장치(200)가 무선 네트워크(100)로부터 탈퇴하고나서 키 관리 장치(120)가 없을 경우에는, 인증을 위한 비밀키가 없기 때문에 무선 네트워크(100)에 재참여를 하지 못하게 된다. 다시 말해서, 키 관리 장치(120)가 있는 경우에만 무선 네트워크(100)에 참여가 가능한 것이다. 또한, 무선 네트워크 장치(200)에게 키 관리 장치(120)의 비밀키를 노출 시키지 않고 키 관리 장치(120) 내부에서만 비밀키를 사용하여 인증 정보를 생성하여 무선 네트워크 장치에게 제공하기 때문에 무선 네트워크 장치(200)가 한시적으로 무선 네트워크(100)에 참여하거나, 참여 및 탈퇴가 빈번히 발생할 경우 참여 및 탈퇴가 발생할 때마다 매번 인증 기관으로부터 공개키 쌍을 발급받을 필요가 없어져 네트워크 관리자의 네트워크 관리가 보다 용이하게 된다. 이러한 점을 이용해 무선 네트워크 관리자는 고정된 키 관리 장치(120)의 대여 및 수거를 통해 무선 네트워크 장치(200)가 무선 네트워크(100)에 한시적으로만 참여할 수 있도록 제어할 수 있다.

<77> 또한, 본 발명의 실시예에서 제 1내지 제 3인증서의 유효 기간은 기존에 인증 기관에서 인증서의 유효 기간을 연단위로 설정한 것에 비하여 날짜 및 시간 단위 등 다양한 단위로 설정할 수 있다. 또한, 본 발명의 실시예에 따른 엑세스 포인트(110)는 무선 네트워크 장치(200)가 전술한 적외선 통신, 근거리 통신 및 블루투스 통신 등의 통신 방식을 지원하지 않는 경우 기존과 같이 무선 네트워크 장치(200)에 직접 인증서 등을 발급하게 되는데, 이때 무선 네트워크 장치(200)가 무선 네트워크(100)에 가입한 후 탈퇴할 경우 발급된 인증서 등을 폐기하는 기능도 함께 수행할 수 있다.

<78> 도 7은 본 발명의 실시예에 따른 무선 네트워크 장치의 탈퇴 과정이 도시된 도면이다.

<79> 도시된 바와 같이, 무선 네트워크(100)에 참여한 무선 네트워크 장치(200)가 탈퇴할 경우, 네트워크 관리자는 키 관리 장치(120)를 액세스 포인트(110)에 접근시키게 되고, 키 관리 장치(120)는 액세스 포인트(110)로 탈퇴할 무선 네트워크 장치(200)의 MAC 주소를 송신하게 된다(S211).

<80> 해당 무선 네트워크 장치의 MAC 주소를 수신한 액세스 포인트(110)는 수신된 MAC 주소와 동일한 MAC 주소를 가지는 무선 네트워크 장치의 접속을 해제시키게 된다(S212).

<81> 이때, 키 관리 장치(120)와 액세스 포인트(110)는 서로 제한 통신부(121, 112)를 통해 MAC 주소를 전송하게 되어, 외부에서 전송되는 MAC 주소가 감지되는 것을 방지하게 된다.

<82> 한편, 다른 실시예로, 키 관리 장치(120)에서 암호키를 생성하지 않고, 무선 네트워크 장치(200)에서 암호키를 생성할 수도 있다. 다시 말해서, 키 관리 장치(120)가 무선 네트워크 장치(200)와 액세스 포인트(110)간의 인증 과정에만 관여하고, 이후 암호키를 생성하는 과정을 전술한 도 1과 같이 무선 네트워크 장치(200)와 액세스 포인트(110)간에 수행되도록 하는 것이다.

<83> 도 8은 본 발명의 실시예에 따른 키 관리 장치를 이용한 인증 과정이 도시된 도면이다. 또한, 도 8은 전술한 도 7과 같이, 키 관리 장치(120)는 인증 기관으로서 액세스 포인트(110)가 발급한 제 1인증서 및 자신의 인증서인

제 2인증서와 비밀키를 가지고 있고, 액세스 포인트(110)는 인증 기관으로서의 제 1인증서 및 자신의 인증서인 제 3인증서와 비밀키를 가지고 있는 경우를 예를 들어 설명하기로 한다.

<84> 도시된 바와 같이, 먼저, 키 관리 장치(120)가 제 1인증서를 무선 네트워크 장치(200)로 송신한다(S311). 따라서, 무선 네트워크 장치(200)는 제 1인증서를 수신하게 됨에 따라 액세스 포인트(110)에서 발급된 모든 인증서를 검증할 수 있는 공개키를 보유할 수 있게 된다.

<85> 이후, 무선 네트워크 장치(200)은 제 1난수를 생성하여 액세스 포인트에 전송한다(S312). 무선 네트워크 장치(200)으로부터 제 1난수를 수신한 액세스 포인트(110)는 제 2난수를 생성하여(S313), 생성된 제 2난수와 자신의 인증서인 제 3인증서를 무선 네트워크 장치(200)로 송신한다(S314). 이때, 무선 네트워크 장치(200)는 제 3인증서를 검증한 다음 검증에 성공한 경우(S315), 액세스 포인트(110)에서 생성된 제 2난수, 현재까지 송수신한 메시지를 연결한 메시지의 해시값 및 자신의 MAC 주소를 키 관리 장치(120)로 송신한다(S316).

<86> 키 관리 장치(120)는 송신된 MAC 주소를 저장하고(S317), 무선 네트워크 장치(200)로부터 수신한 해시값에 자신의 비밀키로 전자 서명한다(S318).

<87> 이후, 키 관리 장치(120)는 전자 서명된 해시값과 자신의 인증서인 제 2인증서를 무선 네트워크 장치(200)로 송신한다(S319).

<88> 이후, 전자 서명된 해시값과 제 2인증서를 수신한 무선 네트워크 장치(200)는 제 3난수를 생성하고(S320), 자신이 생성했던 제 1난수와 액세스 포인트로(110)부터 수신한 제 2난수를 이용해 암호키를 생성하고(S321), 생성된 암호키를 액세스 포인트(110)의 공개키로 암호화한다(S322)

<89> 이후, 무선 네트워크 장치(200)은 키 관리 장치(120)로부터 수신한 전자 서명된 해시값과 제 2인증서 및 무선 네트워크 장치(200)에서 액세스 포인트(110)의 공개키로 암호화한 암호키를 액세스 포인트(110)로 송신한다(S323). 이때, 액세스 포인트(110)는 제 1인증서를 보유하고 있기 때문에 제 2인증서를 검증하여 키 관리 장치(120)의 인증서를 검증하고, 자신의 비밀키를 통해 암호화된 암호키를 복호화하여 암호키를 얻을 수 있으며, 전자 서명된 해시값을 검증함으로써 무선 네트워크 장치(200)에 대해 인증한다(S324).

<90> 이상과 같이 본 발명에 따른 무선 네트워크 시스템 및 이를 이용한 통신 방법을 예시된 도면을 참조로 하여 설명하였으나, 본 명세서에 개시된 실시예와 도면에 의해 본 발명은 한정되지 않으며 그 발명의 기술사상 범위내에서 당업자에 의해 다양한 변형이 이루어질 수 있음은 물론이다.

발명의 효과

<91> 상기한 바와 같은 본 발명의 무선 네트워크 시스템 및 이를 이용한 통신 방법은에 따르면 다음과 같은 효과가 하나 혹은 그 이상 있다.

<92> 첫째, 외부 네트워크 장치가 무선 네트워크에 한시적으로 참여하는 경우, 해당 무선 네트워크에 존재하는 키 관리 장치가 외부 네트워크 장치에 임시로 사용할 수 있는 암호키를 생성하여 기존의 무선 네트워크에 영향을 주지 않으며 네트워크 설정을 변경할 수 있는 장점이 있다.

<93> 둘째, 외부 네트워크 장치에게 제공되는 암호키를 생성하기 위한 비밀키가 키 관리 장치에만 저장되기 때문에 외부 네트워크 장치의 무단 접근을 방지할 수 있는 장점도 있다.

<94> 셋째, 키 관리 장치와 외부 네트워크 장치간에는 무선 네트워크내의 무선 네트워크 장치들간의 통신 반경보다 좁은 통신 반경을 사용하는 통신 수단을 사용하여 암호키 전송시 보안을 유지할 수 있는 장점도 있다.

도면의 간단한 설명

<1> 도 1은 종래의 기술에 따른 암호키 생성 과정이 도시된 도면.

<2> 도 2는 본 발명의 실시예에 따른 무선 네트워크가 도시된 도면.

<3> 도 3은 본 발명의 실시예에 따른 키 관리 장치가 도시된 도면.

<4> 도 4는 본 발명의 실시예에 따른 무선 네트워크 장치가 도시된 도면.

<5> 도 5는 본 발명의 실시예에 따른 액세스 포인트가 도시된 도면.

<6> 도 6은 본 발명의 실시예에 따른 암호키 생성 과정이 도시된 도면.

<7> 도 7은 본 발명의 실시예에 따른 무선 네트워크 장치의 탈퇴 과정이 도시된 도면.

<8> 도 8은 본 발명의 실시예에 따른 무선 네트워크 장치의 인증 과정이 도시된 도면.

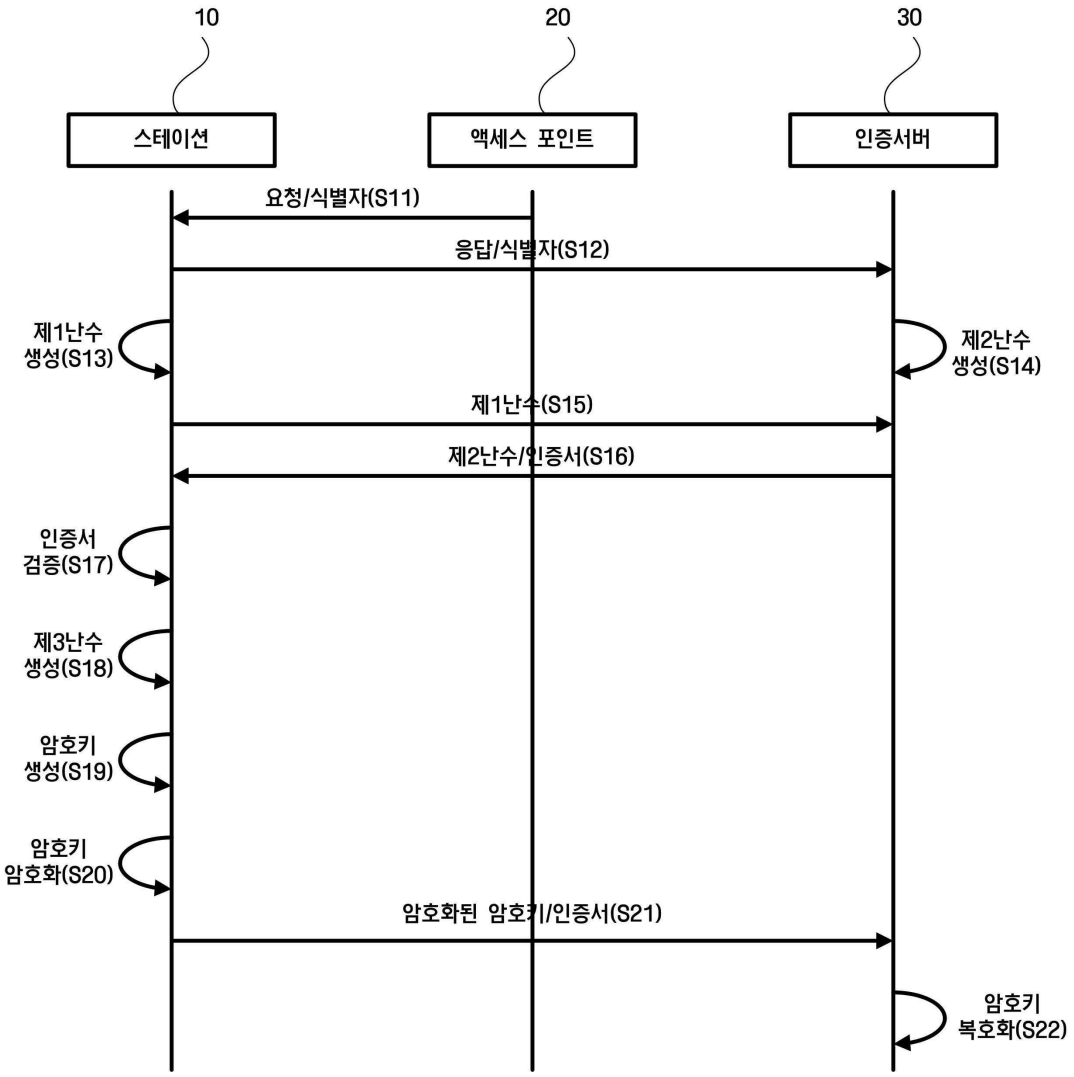
<9> <도면의 주요 부분에 관한 부호의 설명>

<10> 121: 제한 통신부 122: 저장부

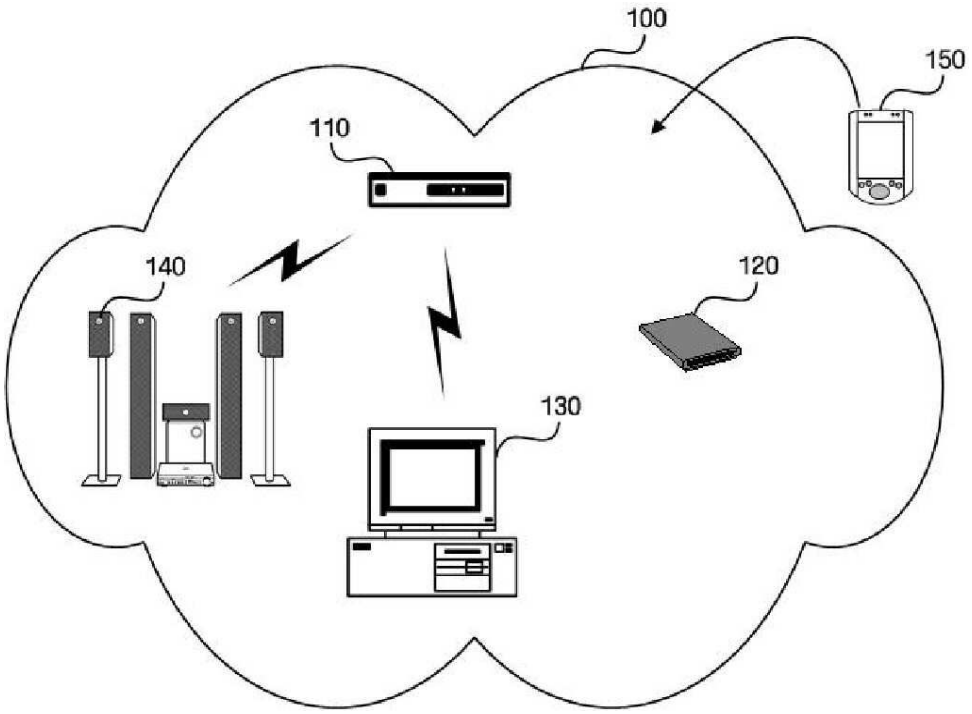
<11> 123: 키생성부 124: 제어부

도면

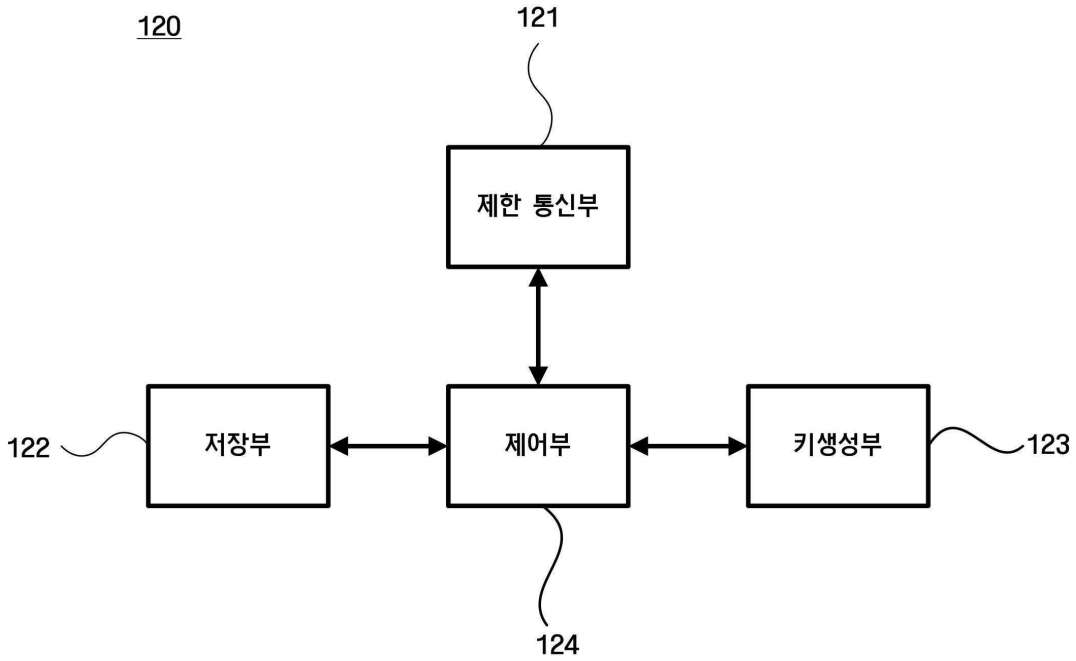
도면1



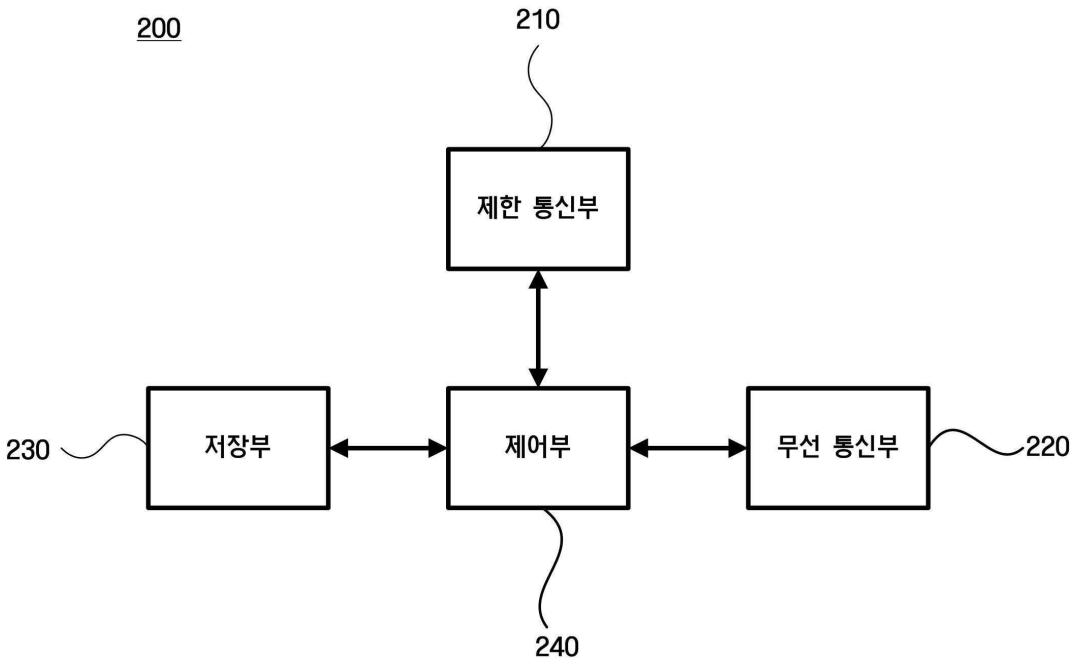
도면2



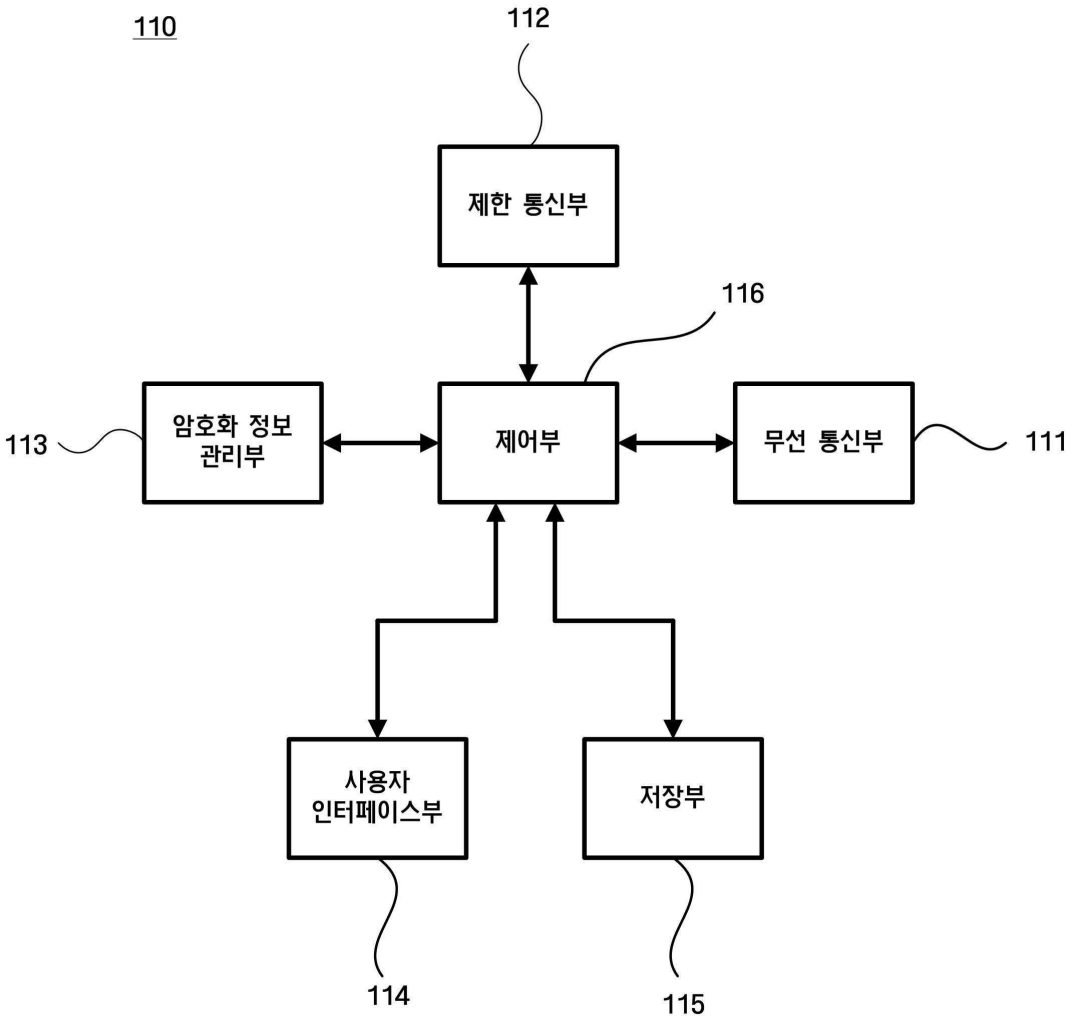
도면3



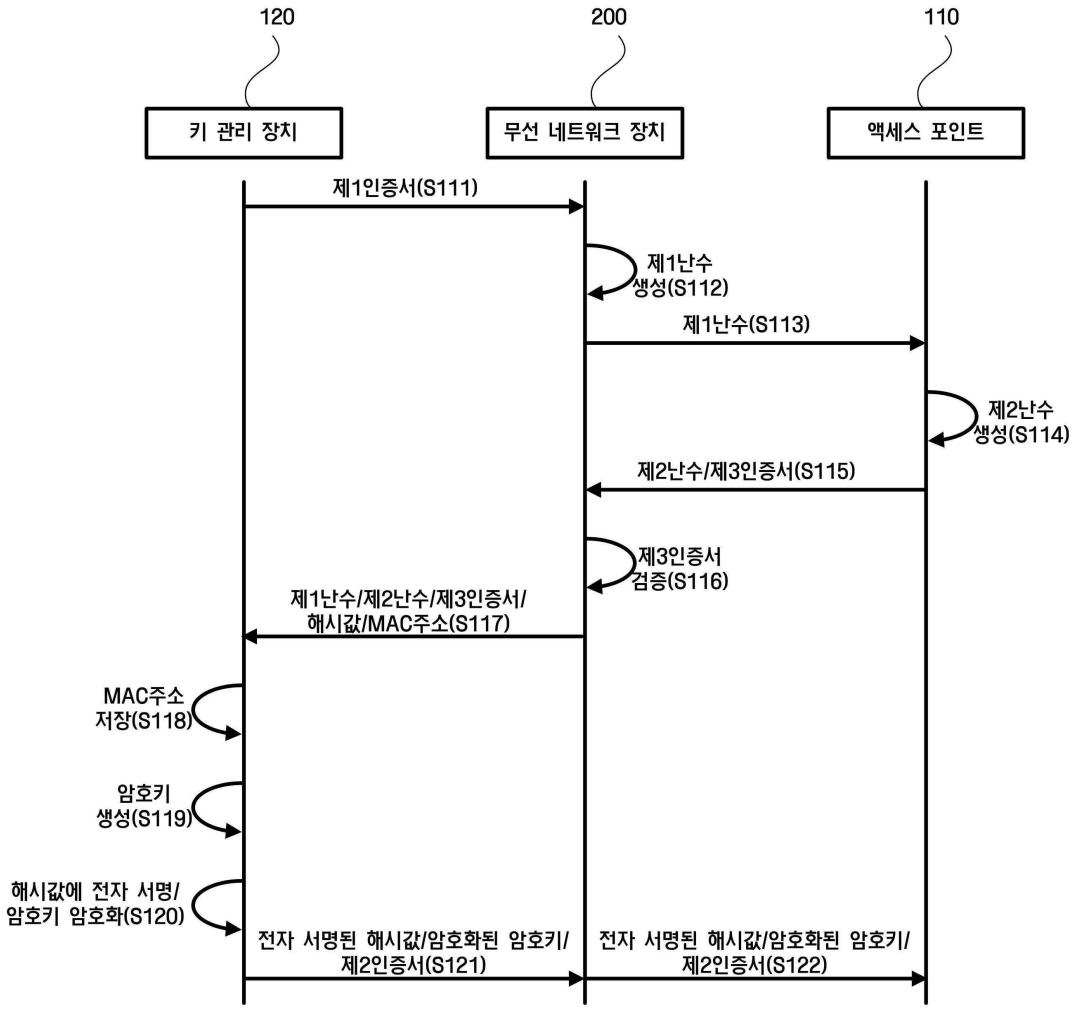
도면4



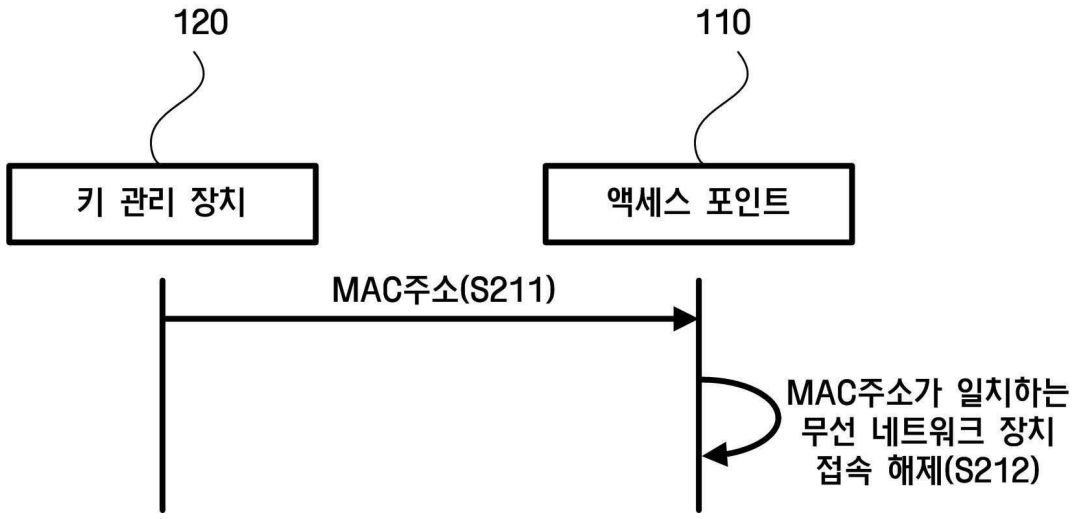
도면5


110
112
제한 통신부
116
113
암호화 정보 관리부
제어부
무선 통신부
111
사용자 인터페이스부
저장부
114
115

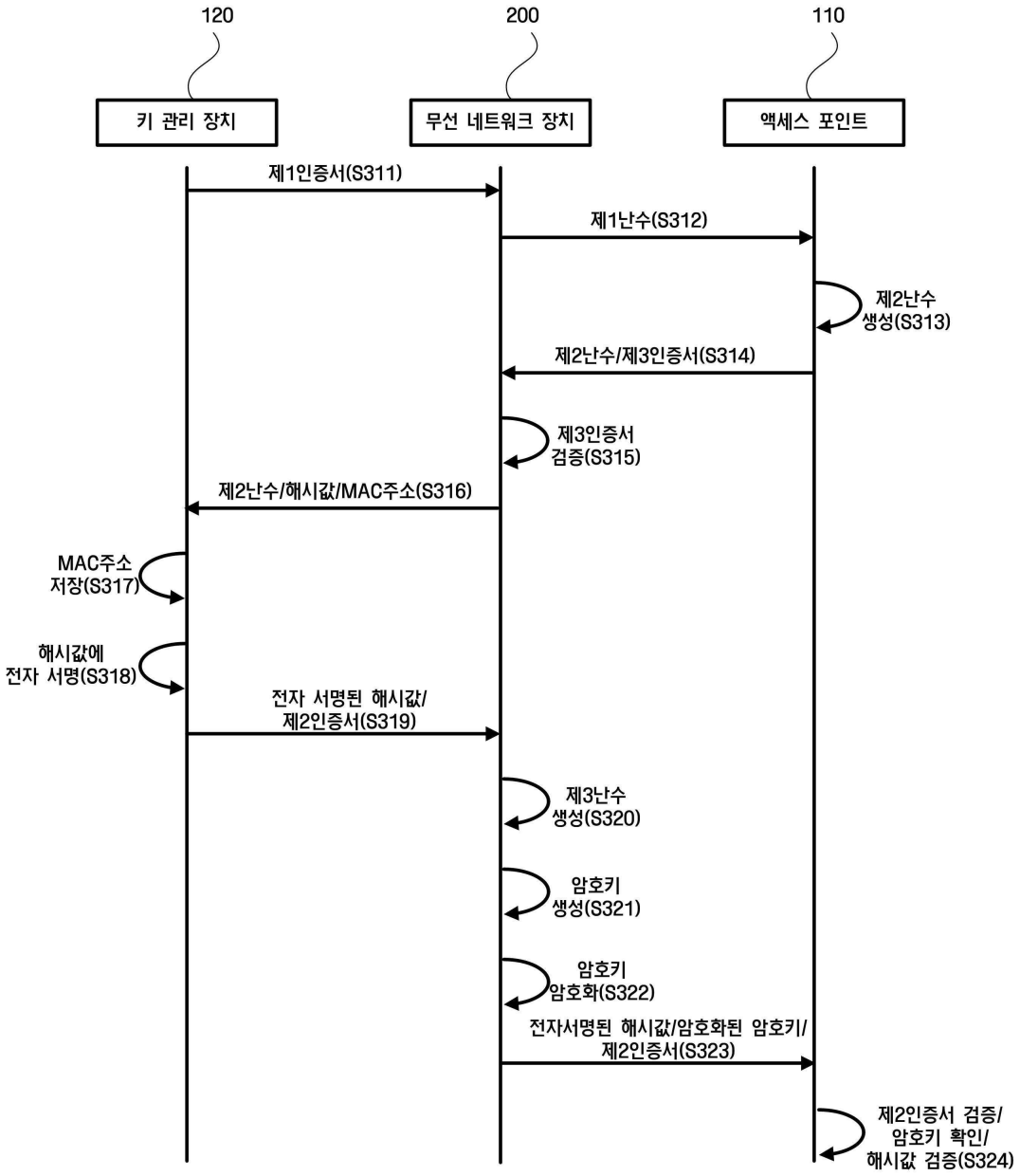
도면6


120
200
110
키 관리 장치
무선 네트워크 장치
액세스 포인트
제1인증서(S111)
제1난수 생성(S112)
제1난수(S113)
제2난수 생성(S114)
제2난수/제3인증서(S115)
제3인증서 검증(S116)
제1난수/제2난수/제3인증서/ 해시값/MAC주소(S117)
MAC주소 저장(S118)
암호키 생성(S119)
해시값에 전자 서명/ 암호키 암호화(S120)
전자 서명된 해시값/암호화된 암호키/ 제2인증서(S121)
전자 서명된 해시값/암호화된 암호키/ 제2인증서(S122)

도면7


120
110
키 관리 장치
액세스 포인트
MAC주소(S211)
MAC주소가 일치하는 무선 네트워크 장치 접속 해제(S212)

도면8


120
200
110
키 관리 장치
무선 네트워크 장치
액세스 포인트
제1인증서(S311)
제1난수(S312)
제2난수
생성(S313)
제2난수/제3인증서(S314)
제3인증서
검증(S315)
제2난수/해시값/MAC주소(S316)
MAC주소
저장(S317)
해시값에
전자 서명(S318)
전자 서명된 해시값/
제2인증서(S319)
제3난수
생성(S320)
암호키
생성(S321)
암호키
암호화(S322)
전자서명된 해시값/암호화된 암호키/
제2인증서(S323)
제2인증서 검증/
암호키 확인/
해시값 검증(S324)