(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2015년01월29일
(11) 등록번호 10-1487348
(24) 등록일자 2015년01월22일

(51) 국제특허분류(Int. Cl.)
H04W 12/06 (2009.01) *H04W 88/08* (2009.01)
G06K 17/00 (2006.01)
(21) 출원번호 10-2013-0059002
(22) 출원일자 2013년05월24일
심사청구일자 2013년05월24일
(65) 공개번호 10-2014-0137855
(43) 공개일자 2014년12월03일
(56) 선행기술조사문헌
KR1020120129249 A*
KR1020110013038 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
주식회사 스트릭스
경기도 의왕시 이미로 40, 디동112호(포일동, 인덕원아이티밸리)
(72) 발명자
이근용
경기 안양시 동안구 운곡로56번길 7, 2층 (비산동)
(74) 대리인
정승훈

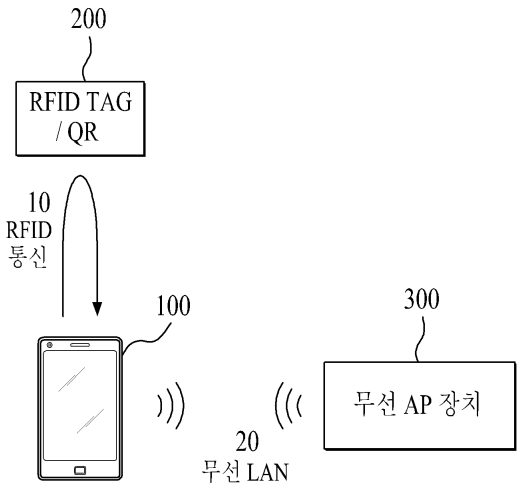
전체 청구항 수 : 총 3 항 심사관 : 이상윤

(54) 발명의 명칭 **무선 AP에서의 단말 인증 방법 및 이를 이용한 무선 AP**

(57) 요 약

무선통신 AP와 사용자 단말간의 접속 인증 방법이 제공된다. 사용자 단말의 인증 절차를 수행하는 무선통신 AP는 사용자 단말과 태깅 수단과의 태깅(tagging)을 통해 취득한 AP 식별정보 및 상기 사용자 단말의 MAC 주소를 상기 사용자 단말로부터 수신하는 무선 통신부 및 상기 AP 식별정보의 유효 여부에 기초하여 로그인 ID 및 패스워드를 생성하여 상기 사용자 단말로 반환하고, 상기 로그인 ID, 패스워드 및 상기 MAC 주소를 접속허용 목록에 설정하는 제어부를 포함하도록 구성되며, 상기 제어부는 상기 사용자 단말로부터 상기 로그인 ID 및 패스워드를 이용한 Wi-Fi 접속 요청에 응답하여 상기 사용자 단말의 Wi-Fi 연결을 승인한다.

대 표 도 - 도1



특허청구의 범위

청구항 1

사용자 단말의 인증 절차를 수행하는 무선통신 AP에 있어서,

사용자 단말이 태깅 수단과의 태깅(tagging)을 통해 취득한 AP 식별정보 및 상기 사용자 단말의 MAC 주소를 상기 사용자 단말로부터 수신하는 무선 통신부; 및

상기 사용자 단말로부터 수신된 상기 AP 식별정보의 유효 여부에 기초하여 상기 사용자 단말에 대응하는 로그인 ID 및 패스워드를 생성하여 상기 사용자 단말로 반환하고, 상기 로그인 ID, 패스워드 및 상기 사용자 단말의 MAC 주소를 접속허용 목록에 설정하는 제어부;를 포함하고,

상기 제어부는, 상기 사용자 단말의 상기 MAC 주소 및 상기 생성된 로그인 ID 중 적어도 하나 이상을 해시 처리한 결과를 기초로 상기 패스워드를 랜덤하게 생성하고, 상기 사용자 단말로부터 상기 로그인 ID 및 패스워드를 이용한 Wi-Fi 접속 요청에 응답하여 상기 사용자 단말의 Wi-Fi 연결을 승인하며, 상기 사용자 단말의 Wi-Fi 연결이 종료되면 상기 로그인 ID 및 상기 패스워드를 삭제하는 것을 특징으로 하는,

무선통신 AP.

청구항 2

삭제

청구항 3

삭제

청구항 4

제 1 항에 있어서,

상기 태깅 수단은 RFID 태그, NFC 태그, QR태그, 바코드 태그 중 어느 하나인 것인,

무선통신 AP.

청구항 5

삭제

청구항 6

삭제

청구항 7

삭제

청구항 8

무선통신 AP에서의 사용자 단말 인증 방법에 있어서,

사용자 단말이 태깅 수단과의 태깅(tagging)을 통해 취득한 AP 식별정보 및 상기 사용자 단말의 MAC 주소를 상기 사용자 단말로부터 수신하는 단계;

상기 AP 식별정보의 유효 여부를 판단하고, 유효하면 상기 사용자 단말에 대응하는 로그인 ID 및 패스워드를 생성하여 상기 사용자 단말로 반환하는 단계;

상기 로그인 ID, 패스워드 및 MAC 주소를 접속허용 목록에 설정하는 단계;

상기 사용자 단말로부터의 상기 로그인 ID 및 패스워드를 이용한 Wi-Fi 접속 요청에 응답하여 상기 사용자 단말의 Wi-Fi 연결을 승인하는 단계; 및

상기 사용자 단말의 Wi-Fi 연결이 종료되면 상기 사용자 단말에 대응하는 상기 로그인 ID 및 상기 패스워드를 삭제하는 단계;를 포함하고,

상기 패스워드는 상기 사용자 단말의 상기 MAC 주소 및 상기 생성된 로그인 ID 중 적어도 하나 이상을 해시 처리한 결과를 기초로 랜덤하게 생성된 것을 특징으로 하는,

무선통신 AP에서의 사용자 단말 인증 방법.

청구항 9

삭제

명 세 서

기 술 분 야

[0001] 본 발명은 무선 AP에서의 단말 인증 방법에 관한 것으로서, 보안성과 편리성을 강화한 인증 방법을 구비한 무선 AP에 관한 것이다.

배 경 기 술

[0002] 무선랜(Wireless LAN)은 두 대 이상의 장치가 무선으로 연결된 LAN을 말한다. 무선랜은 통신을 위해 케이블 대신 라디오 주파수를 물리 채널로 사용하며, 특히 노트북, 스마트폰, 태블릿 패드 등의 모바일 장치 사용자들의 증가로 인해 무선랜 환경은 기존의 유선랜 환경을 빠르게 교체하며 성장하고 있다.

[0003] 하지만, 무선랜은 라디오 주파수를 사용하므로 유선랜에 비해 통신 간섭이나 보안에 취약하다. 종래의 무선랜 시스템에서는 통신 단말의 접근 제어를 위하여 다양한 보안 방법을 사용하고 있다. 이러한 예로서, 허가받은 사용자 단말과 AP가 동일한 공유키(Public Key)를 보유하여, 사용자 단말로부터의 접속 요청시에 공유키를 사용하여 사용자 인증을 수행하는 방법이 있다. 또 다른 예로서, 허가받은 사용자 단말의 무선랜 카드의 MAC(Medium Access Control) 주소를 AP에 미리 입력시키고, 사용자 단말로부터 접속 요청이 있으면 해당 단말의 무선랜 카드의 MAC 주소를 저장된 MAC 주소와 비교하여 사용자 인증을 수행하는 방법 등이 있다.

[0004] 그러나, 상기의 방법은 악의적인 목적을 가지는 사용자가 무선통신 구간(On Air) 내에서 데이터를 수집하여 Key를 추출할 수 있다는 문제점이 있다. 또한, 무선랜 카드의 MAC 주소를 입력하여 사용자 인증을 수행하는 방법의 경우, 다수의 불특정 사용자가 존재하는 공중망 서비스 또는 사용자의 수가 많은 경우에는 관리가 거의 불가능하다는 문제점이 있다.

[0005] 따라서, 종래의 무선랜 보안 방법을 보안하면서 불특정 사용자에 대한 안정적인 보안 방법을 제공하는 것이 요구된다.

선행기술문헌

특허문헌

[0006] (특허문헌 0001) 한국공개특허 제2006-0027633호, "무선랜 기반 네트워크에서 무선랜 접속장치와 정보기기간의 접속 방법"

발명의 내용

해결하려는 과제

[0007] 상술한 종래 기술의 문제점을 해결하기 위해, 본 발명은 불특정 사용자 단말이 무선통신 AP에 접속하여 무선랜에 연결될 수 있도록 인증 절차를 제공한다.

[0008] 또한, 본 발명은 불특정 사용자 단말에 대한 무선랜 접속을 허용하면서도 외부의 비허가 접속시도를 차단할 수 있는 인증 방법을 제공한다.

[0009] 본 발명의 목적들은 이상에서 언급한 목적들로 제한되지 않으며, 언급되지 않은 또 다른 목적들은 아래의 기재로부터 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0010] 상기 목적을 달성하기 위하여, 본 발명의 일 측면에 따른 사용자 단말의 인증 절차를 수행하는 무선통신 AP는, 사용자 단말과 태깅 수단과의 태깅(tagging)을 통해 취득한 AP 식별정보 및 상기 사용자 단말의 MAC 주소를 상기 사용자 단말로부터 수신하는 무선 통신부, 및 상기 AP 식별정보의 유효 여부에 기초하여 로그인 ID 및 패스워드를 생성하여 상기 사용자 단말로 반환하고, 상기 로그인 ID, 패스워드 및 상기 MAC 주소를 접속허용 목록에 설정하는 제어부를 포함하고, 상기 제어부는, 상기 사용자 단말로부터 상기 로그인 ID 및 패스워드를 이용한 Wi-Fi 접속 요청에 응답하여 상기 사용자 단말의 Wi-Fi 연결을 승인한다. 이를 통해, 상기 무선통신 AP는 무선랜 네트워크 접속에 대한 보안성을 강화하고 무선통신 AP에 대한 접속 권한을 용이하게 관리할 수 있다.

[0011] 여기서, 상기 무선통신 AP는 사용자 단말의 Wi-Fi 연결이 성공하면 로그인 ID 및 패스워드를 저장하는 저장부를 더 포함하고, 상기 제어부는 상기 사용자 단말의 Wi-Fi 연결이 종료되면 상기 저장부에 저장된 상기 로그인 ID 및 패스워드를 삭제할 수 있다. 이를 통해, 상기 무선통신 AP는 외부의 비허가 접속시도를 원천적으로 차단할 수 있다.

[0012] 여기서, 상기 제어부는 상기 사용자 단말로부터 수신된 MAC 주소 및 상기 생성된 로그인 ID 중 적어도 하나 이상을 해시 처리한 결과를 기초로 상기 패스워드를 생성할 수 있다. 이를 통해, 상기 무선통신 AP는 외부로부터의 패스워드 유추를 통한 불법적인 접근을 최소화할 수 있다.

[0013] 여기서, 상기 태깅 수단은 RFID 태그, NFC 태그, QR 태그 및 바코드 태그 중 어느 하나일 수 있다.

[0014] 또한, 본 발명의 다른 측면에 따른 무선통신 AP과의 Wi-Fi 접속 인증을 수행하는 사용자 단말은, 태깅 수단과의 태깅(tagging)을 통해 무선통신 AP에 대한 AP 식별정보를 취득하는 근거리 통신부, 사용자 단말의 MAC 주소 및 상기 취득한 AP 식별정보를 상기 무선통신 AP로 전송하고, 이에 응답하여 상기 무선통신 AP에서 생성된 로그인 ID 및 패스워드를 수신하는 무선 통신부, 및 상기 로그인 ID 및 패스워드를 이용하여 상기 무선통신 AP로 Wi-Fi 접속 요청을 전송하는 제어부;를 포함하며, 상기 로그인 ID 및 패스워드는 상기 무선통신 AP에서 수신한 상기 AP 식별정보의 유효 여부를 기초로 생성된다.

[0015] 여기서, 상기 사용자 단말은 상기 무선통신 AP와의 Wi-Fi 연결이 성공하면 상기 로그인 ID 및 패스워드를 저장하는 메모리부를 더 포함하고, 상기 제어부는 상기 Wi-Fi 연결이 종료되면 상기 메모리부에 저장된 로그인 ID 및 패스워드를 삭제할 수 있다.

[0016] 여기서, 상기 패스워드는 상기 사용자 단말의 MAC 주소 및 상기 무선통신 AP에서 생성된 로그인 ID 중 하나 이상을 해시 처리한 결과를 기초로 생성될 수 있다.

[0017] 또한, 본 발명의 다른 측면에 따른 무선통신 AP에서의 사용자 단말 인증 방법은, 사용자 단말과 태깅 수단과의 태깅(tagging)을 통해 취득한 AP 식별정보 및 상기 사용자 단말의 MAC 주소를 상기 사용자 단말로부터 수신하는 단계, 상기 AP 식별정보의 유효 여부를 판단하고, 로그인 ID 및 패스워드를 생성하여 상기 사용자 단말로 반환하는 단계, 상기 로그인 ID, 패스워드 및 MAC 주소를 접속허용 목록에 설정하는 단계, 및 상기 사용자 단말로부터의 상기 로그인 ID 및 패스워드를 이용한 Wi-Fi 접속 요청에 응답하여 상기 사용자 단말의 Wi-Fi 연결을 승인하는 단계를 포함한다.

[0018] 여기서, 상기 사용자 단말과의 Wi-Fi 연결이 종료되면 상기 로그인 ID 및 패스워드를 삭제하는 단계를 더 포함할 수 있다.

[0019] 상기 목적을 달성하기 위한 구체적인 사항들은 첨부된 도면과 함께 상세하게 후술된 실시예들을 참조하면 명확

해질 것이다.

[0020] 그러나 본 발명은 이하에서 개시되는 실시예들에 한정되는 것이 아니라, 서로 다른 다양한 형태로 구성될 수 있으며, 본 실시예들은 본 발명의 개시가 완전하도록 하고 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이다.

발명의 효과

[0021] 전술한 본 발명의 과제 해결 수단 중 하나에 의하면, 무선랜 네트워크에서 무선통신 AP에서의 접속 인증을 위해 고정된 패스워드를 이용하거나 사용자 단말의 MAC 주소를 일일이 설정하지 않아도 되어 네트워크 접속 권한 관리가 용이한 효과가 있다.

도면의 간단한 설명

[0022] 도 1은 본 발명의 일 실시예에 따른 무선랜 시스템의 전체적인 개요도이다.

도 2는 본 발명의 일 실시예에 따른 사용자 단말의 세부 구성을 나타내는 블록도이다.

도 3은 본 발명의 일 실시예에 따른 무선통신 AP의 세부 구성을 나타내는 블록도이다.

도 4는 본 발명의 일 실시예에 따른 무선통신 AP에서 사용자 단말의 접속 인증을 수행하는 방법을 나타내는 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0023] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 이를 상세한 설명을 통해 상세히 설명하고자 한다. 그러나, 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다.

[0024] 본 발명을 설명함에 있어서, 관련된 공지 기술에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다. 또한, 본 명세서의 설명 과정에서 이용되는 숫자(예를 들어, 제1, 제2 등)는 하나의 구성요소를 다른 구성요소와 구분하기 위한 식별기호에 불과하다.

[0025] 또한, 본 명세서에서, 일 구성요소가 다른 구성요소와 "연결된다" 거나 "접속된다" 등으로 언급된 때에는, 상기 일 구성요소가 상기 다른 구성요소와 직접 연결되거나 또는 직접 접속될 수도 있지만, 특별히 반대되는 기재가 존재하지 않는 이상, 중간에 또 다른 구성요소를 매개하여 연결되거나 또는 접속될 수도 있다고 이해되어야 할 것이다.

[0026] 본 명세서에서, 무선통신 AP는 Wi-Fi 등의 무선 데이터 트래픽을 송수신하는 무선통신 허브 또는 기지국으로 기능하는 장치이며, 사용자 단말은 Wi-Fi 등의 무선 데이터 트래픽을 무선통신 AP 또는 다른 사용자 단말들 간에 송수신하는 장치로서, 예를 들어, 휴대폰, 스마트폰(smart phone), 노트북 컴퓨터(laptop computer), 디지털방송용 단말기, PDA(Personal Digital Assistants), PMP(Portable Multimedia Player), 내비게이션 등과 같이 이동 가능한 모바일 단말일 수 있으며, 또는 벽걸이 TV, 전자 액자, 냉장고 등과 같이 무선 통신 모듈을 내장하는 가전 제품일 수도 있다.

[0027] 이하, 첨부된 도면들을 참조하여 본 발명의 실시를 위한 구체적인 내용을 설명하도록 한다.

[0028] 도 1은 본 발명의 일 실시예에 따른 무선랜 시스템을 개략적으로 설명하기 위한 전체 개요도이다. 본 발명의 무선랜 시스템은 하나 이상의 사용자 단말(100)과 무선통신 AP(300) 간에 연결된 통신 채널을 이용하여 무선 통신(20)을 수행한다. 이때, 사용자 단말(100)은 무선 네트워크에 연결하기 위하여 무선통신 AP(300)에 AP 식별정보와 함께 Wi-Fi 연결 승인을 요청한다.

[0029] 사용자 단말(100)은 상기 AP 식별정보를 무선통신 AP(300)가 속한 무선 네트워크 영역 내의 임의의 장소에 배치된 RFID 태그(200)로부터 취득할 수 있으며, 이때, 상기 AP 식별정보는 무선통신 AP(300)의 고유 IP 주소 등일 수 있다.

[0030] 사용자 단말(100)은 내장된 RFID 수신부를 이용하여 RFID 통신(10)을 통해 RFID 태그(200)에 저장된 AP 식별정

보를 취득하고, 상기 AP 식별정보를 이용하여 무선통신 AP(300)에 접속한 후 자신의 MAC 주소와 함께 AP 식별정보를 전송한다. 무선통신 AP(300)는 수신된 AP 식별정보의 유효 여부를 판단하여, 해당 정보가 유효하다고 인정되면 해당 사용자 단말(100)이 무선통신 AP(300)에 접속하기 위한 로그인 ID 및 패스워드를 생성하고 이를 사용자 단말(100)에 제공한다. 또한, 상기 로그인 ID와 패스워드는 무선통신 AP(300)에서 사용자 단말(100)의 인증 절차에 사용된다.

[0031] 이를 통해, 사용자 단말(100)은 무선통신 AP(300)에 접속하기 위하여 별도의 비밀번호를 저장 관리하거나 자신의 MAC 주소를 미리 무선통신 AP(300)에 등록시킬 필요 없이, 임의의 장소에 배치된 RFID 태그에 사용자 단말(100)을 근접시키는 것 만으로 무선 네트워크에 연결될 수 있는 효과가 있다.

[0032] 이하에서, 본 발명의 일 실시예에 따른 사용자 단말(100) 및 무선통신 AP(300)의 세부 구성을 상세히 설명하기로 한다.

[0033] 도 2는 본 발명의 일 실시예에 따른 사용자 단말(100)의 세부 구성을 나타내고 있다.

[0034] 도 2에 도시된 바와 같이, 사용자 단말(100)은 근거리 통신부(110), 메모리부(120), 제어부(130) 및 무선 통신부(140)를 포함한다.

[0035] 근거리 통신부(110)는 근거리 통신을 위한 하나 이상의 모듈을 포함한다. 근거리 통신부(110)는 RFID(Radio Frequency Identification) 수신부(112), NFC(Near Field Communication) 통신부(114) 이외에 이와 균등하거나 유사한 기능을 수행하는 블루투스(Bluetooth), 적외선 통신(IrDA, infrared Data Association), UWB(Ultra Wideband), ZigBee 등의 통신 모듈을 더 포함할 수 있다. 경우에 따라서, RFID 수신부(112)와 NFC 통신부(114)는 단일 모듈 상에서 구현될 수 있으며 본 명세서 상에서는 설명의 용이함을 위하여 별도의 구성 요소로 분리하여 설명하기로 한다.

[0036] RFID 수신부(112)는 임의의 장소에 위치한 RFID 태그(200)로부터 접속하고자 하는 무선통신 AP(300)에 대한 AP 식별정보를 취득한다.

[0037] 구체적으로, RFID 수신부(112)는 지정된 주파수 대역에 맞게 RF 캐리어 신호와 에너지를 RFID 태그(200)에 송신하고, RFID 태그(200)는 입력된 RF 캐리어 신호의 위상 또는 진폭 등을 변조하여 태그에 저장된 AP 식별정보를 RFID 수신부(112)로 되돌려준다. 되돌려 받은 변조 신호는 RFID 수신부(112)에서 복조되어 메모리부(120)에 저장된다.

[0038] 한편, 상기 무선통신 AP(300)에 대한 AP 식별정보는 RFID 태그(200)가 아닌 다른 태깅 수단, 예를 들면, QR 코드 태그, 바코드 태그, NFC 태그 또는 이와 유사한 기능을 수행하는 저장 태그 등으로부터 취득할 수도 있다. 이 경우, 사용자 단말(100)은 RFID 수신부(112) 대신 QR 코드 리더기(미도시) 또는 NFC 통신부(114) 등을 통해 상기 AP 식별정보를 취득할 수 있다.

[0039] 메모리부(120)에는 상기 RFID 수신부(112)에서 취득한 무선통신 AP(100)에 대한 AP 식별정보가 저장된다. 또한, 후술할 제어부(130)에서 생성된 로그인 ID, 패스워드 및 해당 사용자 단말(100)로부터 상기 로그인 ID 및 패스워드와 함께 전송된 MAC 주소가 연동되어 저장될 수 있다.

[0040] 또한, 메모리부(120)에는 사용자 단말(100) 상에서 구동되는 인증 앱(122)이 격납될 수 있다. 상기 인증 앱(122)은 메모리부(120) 상에서 구동되어 RFID 수신부(112)를 통한 AP 식별정보의 취득 및 취득한 AP 식별정보를 무선통신 AP(300)에 전송하고 이에 따른 로그인 ID 및 패스워드를 취득하여 무선통신 AP(300)에 Wi-Fi 연결 요청하는 일련의 과정을 처리할 수 있다.

[0041] 제어부(130)는 상기 인증 앱(122)의 실행을 제어하며, 사용자 단말(100)의 전반적인 동작 및 기능 수행을 제어한다.

[0042] 제어부(130)는 취득한 AP 식별정보를 이용하여 무선통신 AP(300)에 접속하여 상기 AP 식별정보 및 사용자 단말(100)의 MAC 주소를 제공하고 Wi-Fi 접속을 위한 인증 정보를 요청한다. 또한, 제어부(130)는 무선통신 AP(300)로부터 수신된 로그인 ID 및 패스워드를 이용하여 무선통신 AP(300)에 접속 요청을 전송할 수 있다.

[0043] 무선 통신부(140)는 무선통신 AP(300)와의 무선 통신을 수행하며, 통신 제어를 위한 베이스밴드 프로세서, 트랜시버, 전력 증폭부 및 안테나 등을 포함할 수 있다. 무선 통신부(140)는 취득한 AP 식별정보를 이용하여 무선통신 AP(300)에 접속하여 상기 AP 식별정보 및 자신의 MAC 주소를 전송한다. 또한, 무선 통신부(140)는 무선통신

AP(300)로부터 로그인 ID 및 패스워드를 수신하여 제어부(130)에 전달한다.

[0044] 경우에 따라서, 무선통신 AP(300)에 MAC 주소를 전송하기 위하여 무선 통신부(140) 대신 NFC 통신부(114)를 이용할 수도 있다. 이 경우, 사용자 단말(100)의 NFC 통신부(114)는 RF 필드를 생성하고 이를 통해 무선통신 AP(300)의 NFC 통신모듈(미도시)로 MAC 주소 및 AP 식별정보를 전송한다. 무선통신 AP(300)의 NFC 통신모듈은 RF 필드를 생성하고 이를 통해 사용자 단말(100)의 NFC 통신부(114)로 로그인 ID 및 패스워드를 전송한다.

[0045] 도 3은 본 발명의 일 실시예에 따른 무선통신 AP의 세부 구성을 나타내고 있다.

[0046] 도 3에 도시된 바와 같이, 무선통신 AP(300)는 제어부(310), LAN 포트(320), 무선 통신부(330) 및 저장부(340)를 포함한다.

[0047] 제어부(310)는 사용자 단말(100)로부터 수신된 AP 식별정보의 유효성을 판단하고, 상기 정보가 유효한 값이면 해당 사용자 단말(100)에게 제공할 로그인 ID 및 패스워드를 생성한다. 생성된 로그인 ID 및 패스워드는 후술할 무선 통신부(330) 또는 NFC 통신 모듈(미도시)을 이용하여 해당 사용자 단말(100)로 반환된다. 이때, 상기 패스워드는 사용자 단말(100)과 연관된 정보들을 이용하여 랜덤하게 생성될 수 있다, 예를 들어, 제어부(310)는 사용자 단말(100)의 MAC 주소 또는 로그인 ID 를 이용하여 해시 처리한 결과 데이터를 기초로 패스워드를 생성할 수 있다.

[0048] 또한, 제어부(310)는 사용자 단말(100)로부터 상기 AP 식별정보와 함께 수신된 MAC 주소를 생성된 로그인 ID 및 패스워드와 함께 저장부(340)에 저장하고, Wi-Fi 통신 설정정보 중 접속허용 목록에 상기 MAC 주소 등을 설정한다.

[0049] 이후, 해당 사용자 단말(100)로부터 상기 보내준 로그인 ID 및 패스워드를 이용한 접속 요청이 수신된 경우에, 제어부(310)는 해당 사용자 단말(100)의 MAC 주소가 접속허용 목록에 포함되었는지 여부를 확인한 후, 사용자 단말(100)의 Wi-Fi 연결을 승인한다.

[0050] LAN 포트(320)는 유선 LAN 인터페이스로서, 유선으로 무선통신 AP(300)에 접속하고자 하는 사용자 단말과의 통신 채널로서 기능한다. 이때, 사용자 단말과 무선통신 AP(300)간의 연결을 위해 RJ-45 케이블 등이 사용될 수 있다.

[0051] 무선 통신부(330)는 사용자 단말(100)과의 무선통신을 수행하며, 무선 통신을 위한 베이스밴드 프로세서, 트랜시버, 전력 증폭부, 안테나 등을 포함한다. 무선 통신부(330)는 사용자 단말(100)로부터 AP 식별정보 및 MAC 주소를 수신하고 사용자 단말(100)로 생성된 로그인 ID 및 패스워드를 전송한다.

[0052] 저장부(340)는 사용자 단말(100)로부터 수신된 MAC 정보 및 생성된 로그인 ID, 패스워드 등의 인증정보를 저장하고 관리한다. 또한, 저장부(340)는 사용자 단말(100)과의 Wi-Fi 연결이 종료되면 해당 사용자 단말(100)에 할당되었던 로그인 ID 및 패스워드를 삭제한다. 이 때, 접속허용 목록에 등록되었던 로그인 ID 및 패스워드 등의 접속 정보도 함께 삭제될 수 있다.

[0053] 이상에서 설명한 무선통신 AP 및 사용자 단말 간의 접속 인증 과정을 설명하기로 한다.

[0054] 도 4는 본 발명의 일 실시예에 따른 무선통신 AP에서 사용자 단말의 접속 인증을 수행하는 방법을 나타내는 흐름도이다.

[0055] 도 4에 도시된 바와 같이, 우선, 사용자 단말(100)에서 Wi-Fi 접속 인증을 수행하기 위한 인증 앱(122)이 구동된 후에(S100), 상기 인증 앱(122)을 통해 인접한 장소에 위치하는 RFID 태그 또는 QR 코드 태그(200)에 태깅(tagging)하여 무선통신 AP(300)의 AP 식별정보를 취득한다(S102).

[0056] 이후, 사용자 단말(100)은 취득한 AP 식별정보를 이용하여 해당 무선 네트워크를 구성하는 무선통신 AP(300)에 접속한 후 상기 AP 식별정보 및 자신의 MAC 주소를 무선통신 AP(300)에 전송한다(S104).

[0057] 사용자 단말(100)로부터 AP 식별정보를 수신한 무선통신 AP(300)는 해당 AP 식별정보의 유효성 여부를 체크한 후(S106), 유효한 정보라고 판단되면 해당 사용자 단말(100)에게 제공할 로그인 ID 및 대응되는 패스워드를 생성한다(S108). 만일, 상기 수신된 AP 식별정보가 유효하지 않은 정보인 경우, 무선통신 AP(300)는 사용자 단말

(100)로 접속불가 메시지를 반환한다(S110).

[0058] 이후, 무선통신 AP(300)는 생성된 로그인 ID와 패스워드를 해당 사용자 단말(100)의 MAC 주소와 연동시켜 Wi-Fi 설정의 접속허용 목록에 추가하고(S112), 로그인 ID 및 패스워드를 사용자 단말(100)로 반환한다(S114).

[0059] 사용자 단말(100)은 수신된 로그인 ID 및 패스워드를 이용하여 무선통신 AP(300)로의 Wi-Fi 접속을 시도한다(S116, S118). 만일 로그인 ID가 잘못 입력되거나 유효 기간이 경과하는 등 유효하지 않은 경우에는 접속 불가 안내 메시지를 인증 앱을 통해 사용자에게 표시한다(S120).

[0060] 사용자 단말(100)로부터 Wi-Fi 접속 인증 요청을 받은 무선통신 AP(300)는 수신된 로그인 ID 및 패스워드의 유효성을 체크하고, 해당 로그인 ID에 매칭되어 저장된 MAC 주소가 상기 사용자 단말(100)의 MAC 주소와 일치하는 경우 Wi-Fi 연결을 승인한다(S122, S123).

[0061] 이후, 사용자 단말(100)과 무선통신 AP(300) 간의 Wi-Fi 연결이 종료되면(S124, S125), 사용자 단말(100) 및 무선통신 AP(300) 각각에 저장된 상기 로그인 ID 및 패스워드 등의 접속 정보가 자동으로 삭제된다(S126, S127).

[0062] 이와 같은 구성의 무선통신 인증 방법에 의하면, 무선통신 AP에서 다수의 사용자 단말들의 MAC 주소 목록을 일일이 관리하거나 또는 사용자 단말이 무선 통신 AP에의 로그인 ID 및 패스워드를 미리 취득하거나 저장할 필요 없이 불특정 다수의 사용자 단말에 보안성이 강화되고 관리가 용이한 무선통신 인증을 제공할 수 있는 효과가 발생한다.

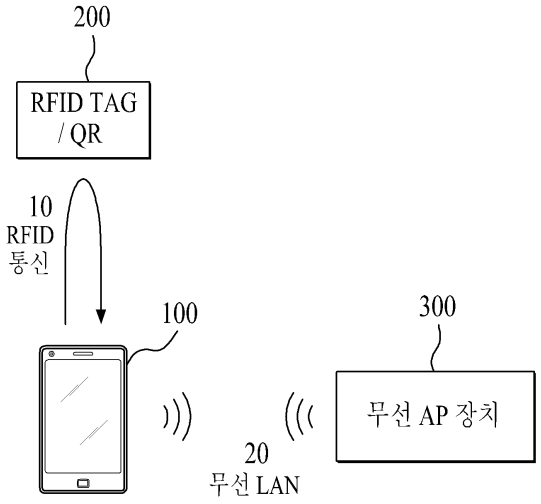
[0063] 이상의 설명은 본 발명의 기술 사상을 예시적으로 설명한 것에 불과한 것으로서, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자라면 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 다양한 수정 및 변형이 가능할 것이다.

[0064] 따라서, 본 발명에 개시된 실시 예들은 본 발명의 기술 사상을 한정하기 위한 것이 아니라 설명하기 위한 것이고, 이러한 실시 예에 의하여 본 발명의 기술 사상의 범위가 한정되는 것은 아니다.

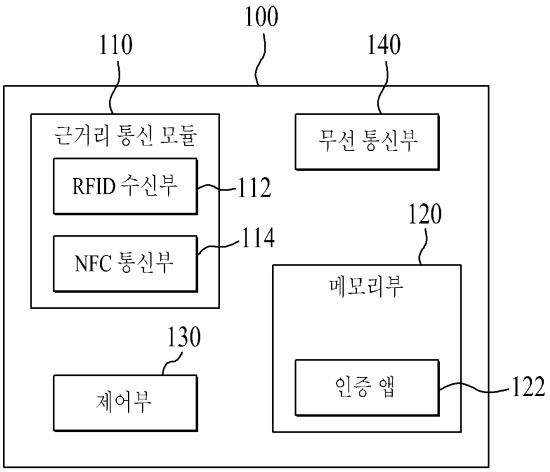
[0065] 본 발명의 보호 범위는 아래의 청구범위에 의하여 해석되어야 하며, 그와 동등한 범위 내에 있는 모든 기술 사상은 본 발명의 권리범위에 포함되는 것으로 해석되어야 할 것이다.

도면

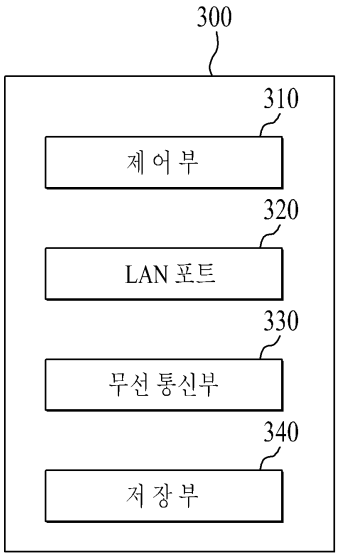
도면1



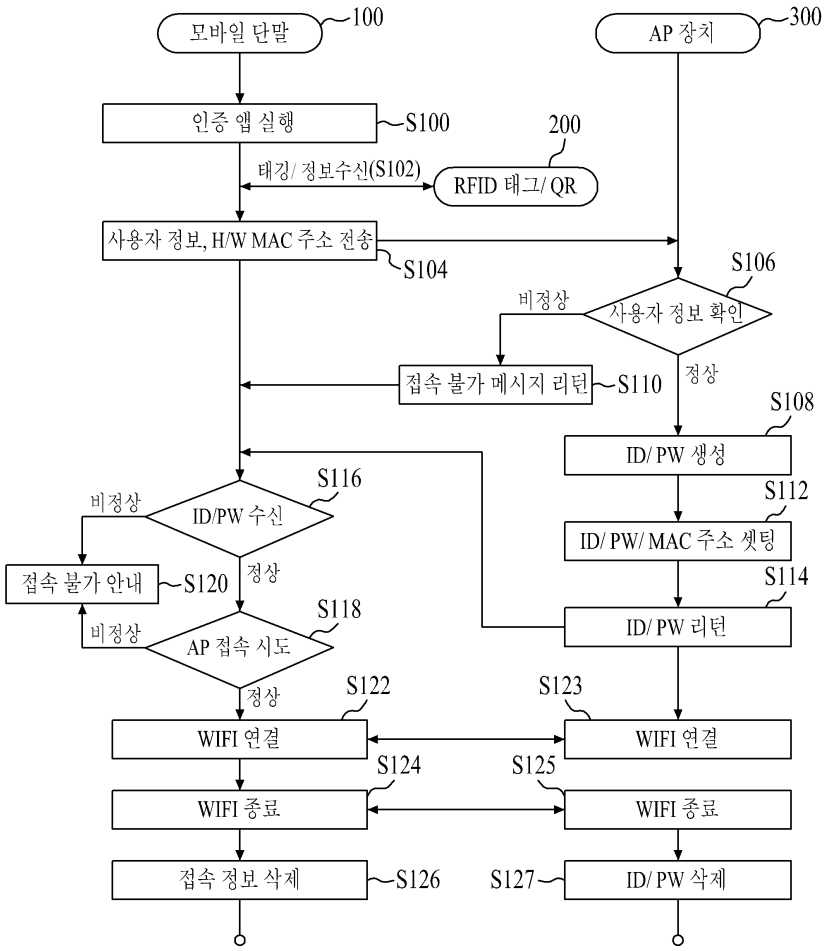
도면2


100
110
140
근거리 통신 모듈
RFID 수신부
112
NFC 통신부
114
무선 통신부
120
메모리부
인증 앱
122
130
제어부

도면3


300
310
제 어 부
320
LAN 포트
330
무선 통신부
340
저 장 부

도면4


모바일 단말
100
AP 장치
300
인증 앱 실행
S100
200
태깅/ 정보수신(S102)
RFID 태그/ QR
사용자 정보, H/W MAC 주소 전송
S104
S106
비정상
사용자 정보 확인
정상
접속 불가 메시지 리턴
S110
S108
ID/ PW 생성
S116
비정상
ID/PW 수신
S112
ID/ PW/ MAC 주소 셋팅
접속 불가 안내
S120
정상
S114
ID/ PW 리턴
S118
비정상
AP 접속 시도
정상
S122
S123
WIFI 연결
WIFI 연결
S124
S125
WIFI 종료
WIFI 종료
접속 정보 삭제
S126
S127
ID/ PW 삭제