

(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2022년 6월 16일 (16.06.2022) **WIPO | PCT**



(10) 국제공개번호
WO 2022/124652 A1

- (51) 국제특허분류:
H04L 61/00 (2022.01) *H04L 9/32* (2006.01)
H04L 9/40 (2022.01) *H04W 4/80* (2018.01)
- (21) 국제출원번호: PCT/KR2021/017482
- (22) 국제출원일: 2021년 11월 25일 (25.11.2021)
- (25) 출원언어: 한국어
- (26) 공개언어: 한국어
- (30) 우선권정보:
10-2020-0172676 2020년 12월 10일 (10.12.2020) KR
- (71) 출원인: 엘지전자 주식회사 (**LG ELECTRONICS INC.**) [KR/KR]; 07336 서울시 영등포구 여의대로 128, Seoul (KR).
- (72) 발명자: 이병주 (**LEE, Byungjoo**); 06772 서울시 서초구 양재대로11길 19 LG전자 특허센터, Seoul (KR). 김정환 (**KIM, Jeonghwan**); 06772 서울시 서초구 양재대

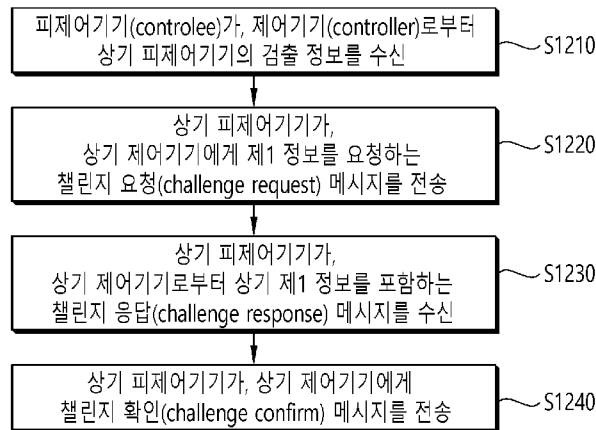
로11길 19 LG전자 특허센터, Seoul (KR). 조영준 (**JO, Youngjun**); 06772 서울시 서초구 양재대로11길 19 LG전자 특허센터, Seoul (KR). 조한규 (**CHO, Hangyu**); 06772 서울시 서초구 양재대로11길 19 LG전자 특허센터, Seoul (KR).

(74) 대리인: 인비전 특허법인 (**ENVISION PATENT & LAW FIRM**); 06193 서울시 강남구 테헤란로 70길 16, 8층, Seoul (KR).

(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC,

(54) Title: METHOD AND APPARATUS FOR SETTING REGISTRATION BETWEEN IOT CONTROLLER AND IOT CONTROLEE ON BASIS OF C2C CONNECTION IN WIRELESS LAN SYSTEM OF SMART HOME ENVIRONMENT

(54) 발명의 명칭: 스마트홈 환경의 무선랜 시스템에서 C2C 연결을 기반으로 IOT 제어기와 IOT 피제어기기 간 등록을 설정하는 방법 및 장치



S1210 ... Controlee receives detection information about controlee from controller

S1220 ... Controlee transmits, to controller, challenge request message for requesting controller of first information

S1230 ... Controlee receives, from controller, challenge response message including first information

S1240 ... Controlee transmits challenge confirm message to controller

(57) Abstract: Presented are a method and an apparatus for setting the registration between an IoT controller and an IoT controlee on the basis of a C2C connection in a wireless LAN system of a smart home environment. Particularly, the controlee receives detection information about the controlee from the controller. The controlee transmits a challenge request message for requesting the first information from the controller. The controlee receives a challenge response message including the first information from the controller. The controlee transmits a challenge confirm message to the controller.



WO 2022/124652 A1

SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT,
TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

- (84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역
내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE,
LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM,
ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유
럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI,
FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK,
MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI
(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML,
MR, NE, SN, TD, TG).

공개:

— 국제조사보고서와 함께 (조약 제21조(3))

(57) 요약서: 스마트홈 환경의 무선랜 시스템에서 C2C 연결을 기반으로 IoT 제어기기와 IoT 피제어기기 간 등록을 설정하는
방법 및 장치가 제안된다. 구체적으로, 피제어기기는 제어기기로부터 피제어기기의 검색 정보를 수신한다. 피제어기기는
제어기기에 제1 정보를 요청하는 챌린지 요청 메시지를 전송한다. 피제어기기는 제어기기로부터 제1 정보를 포함하는
챌린지 응답 메시지를 수신한다. 피제어기기는 제어기기에 챌린지 확인 메시지를 전송한다.

명세서

발명의 명칭: 스마트홈 환경의 무선랜 시스템에서 C2C 연결을 기반으로 IOT 제어기기와 IOT 피제어기기 간 등록을 설정하는 방법 및 장치

기술분야

- [1] 본 명세서는 스마트홈 환경의 무선랜 시스템에서 IoT 기기를 설정하는 방법에 관한 것으로, 보다 상세하게는, C2C 연결을 기반으로 IoT 제어기기와 IoT 피제어기기 간 등록을 설정하는 방법 및 장치에 관한 것이다.

배경기술

- [2] Amazon, Apple, Google 및 Zigbee Alliance는 오늘 스마트 홈 제품 간에 호환을 증대하고 근본적인 설계 원리에 보안을 탑재한 새롭고, 로열티 사용료가 없는 연결성 표준의 개발 및 도입 추진을 위한 새로운 공동 위원회(working group)를 발표했다. Zigbee Alliance의 이사회를 구성하는 이케아(IKEA), Legrand, 엔엑스피 반도체(NXP Semiconductors), Resideo, 삼성 스마트싱스(Samsung SmartThings), 슈나이더 일렉트릭(Schneider Electric), Signify(필립스 휴, Philips Hue), Silicon Labs, 솜피(Somfy), Wulian, ThinQ(LG Electronics) 등의 기업 역시 공동 위원회에 합류하여 공동의 목표를 향해 프로젝트에 기여할 예정이다.
- [3] Connected Home over IP(IP를 통한 커넥티드 홈) 프로젝트의 목표는 제조사의 개발을 간소화하고 소비자를 위해 호환성을 증대하는 것이다. 프로젝트는 스마트 홈 기기가 보안, 안정성을 보장하고 원활한 사용성을 보장해야 한다는 공통 신념을 근간으로 한다. 프로젝트는 인터넷 통신 규약(Internet Protocol, IP)을 기반으로 하여 스마트 홈 기기, 모바일 앱, 클라우드 서비스 간에 통신을 가능케 하고, 기기 인증을 위한 특정 IP 기반 네트워킹 기술 세트를 정의하고자 한다.
- [4] 산업 공동 위원회는 새로운 통합 연결성 규약의 개발 및 적용에 있어 오픈 소스 접근을 채택한다. 프로젝트는 시장에서 증명된 Amazon, Apple, Google, Zigbee Alliance 등의 스마트 홈 기술을 활용할 예정이다. 이러한 기술을 활용하기로 한 결정 덕분에 규약 개발 과정을 가속하고 제조사 및 소비자에 신속하게 혜택을 제공할 수 있을 것으로 예상된다.
- [5] 프로젝트는 기기 제조사를 위해 스마트 홈은 물론 Amazon의 Alexa, Apple의 Siri, Google의 Assistant와 같은 음성인식 서비스와 호환되는 기기 제작을 간편화하고자 한다. 예정된 규약은 기존 기술을 보완할 예정이며 공동 위원회 회원단은 기기 제조사에 기존 기술을 기반으로 혁신을 지속해서 추구하기를 권장한다.
- [6] Connected Home over IP(IP를 통한 커넥티드 홈) 프로젝트는 스마트 홈 업계의 기기 제조사, 실리콘 제공업체 및 개발자의 표준 개발 참여 및 기여를 장려하고 있다.

발명의 상세한 설명

기술적 과제

- [7] 본 명세서는 스마트홈 환경의 무선랜 시스템에서 C2C 연결을 기반으로 IoT 제어기기와 IoT 피제어기기 간 등록을 설정하는 방법 및 장치를 제안한다.

과제 해결 수단

- [8] 본 명세서의 일례는 C2C 연결을 기반으로 IoT 제어기기와 IoT 피제어기기 간 등록을 설정하는 방법을 제안한다.
- [9] 본 실시예는 스마트홈 환경에서 C2C(Cloud-to-Cloud) 연결을 통해 IoT 제어기기와 IoT 피제어기기 간 로컬(local)에서 등록을 설정하는 방법을 제안한다. 이를 위해 사용자는 상기 IoT 피제어기기가 물리적으로 자신에게 있음을 확인하는 소유 증명 절차를 수행하는데, 상기 소유 증명 절차에 따르면 상기 IoT 제어기기는 상기 IoT 피제어기기의 로컬 존재를 확인하여, BLE를 통해 검색되는 이웃집 기기나 로컬에 있지 않는 기기의 등록을 방지할 수 있다는 효과가 있다. 후술하는 제어기기는 상기 IoT 제어기기에 대응하고, 피제어기기는 상기 IoT 피제어기기에 대응할 수 있다.
- [10] 피제어기기(controlee)는 제어기기(controller)로부터 상기 피제어기기의 검출 정보를 수신한다.
- [11] 상기 피제어기기는 상기 제어기기에 제1 정보를 요청하는 챌린지 요청(challenge request) 메시지를 전송한다.
- [12] 상기 피제어기기는 상기 제어기기로부터 상기 제1 정보를 포함하는 챌린지 응답(challenge response) 메시지를 수신한다.
- [13] 상기 피제어기기는 상기 제어기기에 챌린지 확인(challenge confirm) 메시지를 전송한다.
- [14] 상기 피제어기기는 제1 계정을 기반으로 상기 제1 클라우드와 연결되고, 상기 제어기기는 제2 계정을 기반으로 제2 클라우드와 연결된다.
- [15] 상기 피제어기기의 검출 정보, 상기 챌린지 요청 메시지, 상기 챌린지 응답 메시지 및 상기 챌린지 확인 메시지는 상기 제1 및 제2 클라우드 간 연결을 기반으로 송수신된다. 즉, 상기 정보와 메시지는 상기 피제어기기와 상기 제어기기 간의 등록을 위해 C2C 연결(상기 피제어기기의 제1 클라우드와 상기 제어기기의 제2 클라우드 간 연결)을 통해 송수신될 수 있다.
- [16] 상기 제1 정보는 소유 증명(Proof of Possession) 값이다. 상기 챌린지 확인 메시지는 상기 제1 정보를 기반으로 상기 피제어기기와 상기 제어기기 간의 등록(commissioning)에 대한 검증 결과를 포함한다.

발명의 효과

- [17] 본 명세서에서 제안된 실시예에 따르면, 사용자는 상기 IoT 피제어기기가 물리적으로 자신에게 있음을 확인하는 소유 증명 절차를 수행하는데, 상기 소유 증명 절차에 따르면 상기 IoT 제어기기는 상기 IoT 피제어기기의 로컬 존재를

확인하여, BLE를 통해 검색되는 이웃집 기기나 로컬에 있지 않는 기기의 등록을 방지할 수 있다는 효과가 있다.

도면의 간단한 설명

- [18] 도 1은 본 명세서의 송신 장치 및/또는 수신 장치의 일례를 나타낸다.
- [19] 도 2는 무선랜(WLAN)의 구조를 나타낸 개념도이다.
- [20] 도 3은 일반적인 링크 셋업(link setup) 과정을 설명하는 도면이다.
- [21] 도 4는 Zigbee 장치 유형을 도시한다.
- [22] 도 5는 Zigbee 스택을 도시한다.
- [23] 도 6은 본 명세서의 송신 장치 및/또는 수신 장치의 변형된 일례를 나타낸다.
- [24] 도 7은 각각의 클라우드에 연결된 Controller와 Controlee의 연결 구조를 나타낸다.
- [25] 도 8은 Controlee의 초기화 및 검색 과정 절차를 나타낸다.
- [26] 도 9는 클라우드의 계정 생성 및 연동 과정을 나타낸다.
- [27] 도 10은 Proof of Possession 과정을 나타낸다.
- [28] 도 11은 Controlee 기기의 Wi-Fi 연결 및 등록 과정을 나타낸다.
- [29] 도 12는 본 실시예에 따른 C2C 연결을 기반으로 IoT 제어기기와 IoT 피제어기기 간 등록을 설정하는 절차를 도시한 흐름도이다.

발명의 실시를 위한 형태

- [30] 본 명세서에서 “A 또는 B(A or B)”는 “오직 A”, “오직 B” 또는 “A와 B 모두”를 의미할 수 있다. 달리 표현하면, 본 명세서에서 “A 또는 B(A or B)”는 “A 및/또는 B(A and/or B)”으로 해석될 수 있다. 예를 들어, 본 명세서에서 “A, B 또는 C(A, B or C)”는 “오직 A”, “오직 B”, “오직 C” 또는 “A, B 및 C의 임의의 모든 조합(any combination of A, B and C)”를 의미할 수 있다.
- [31] 본 명세서에서 사용되는 슬래쉬(/)나 쉼표(comma)는 “및/또는(and/or)”을 의미할 수 있다. 예를 들어, “A/B”는 “및/또는 B”를 의미할 수 있다. 이에 따라 “A/B”는 “오직 A”, “오직 B”, 또는 “A와 B 모두”를 의미할 수 있다. 예를 들어, “A, B, C”는 “A, B 또는 C”를 의미할 수 있다.
- [32] 본 명세서에서 “적어도 하나의 A 및 B(at least one of A and B)”는, “오직 A” “오직 B” 또는 “A와 B 모두”를 의미할 수 있다. 또한, 본 명세서에서 “적어도 하나의 A 또는 B(at least one of A or B)”나 “적어도 하나의 A 및/또는 B(at least one of A and/or B)”라는 표현은 “적어도 하나의 A 및 B(at least one of A and B)”와 동일하게 해석될 수 있다.
- [33] 또한, 본 명세서에서 “적어도 하나의 A, B 및 C(at least one of A, B and C)”는, “오직 A”, “오직 B”, “오직 C” 또는 “A, B 및 C의 임의의 모든 조합(any combination of A, B and C)”를 의미할 수 있다. 또한, “적어도 하나의 A, B 또는 C(at least one of A, B or C)”나 “적어도 하나의 A, B 및/또는 C(at least one of A, B and/or C)”는 “적어도 하나의 A, B 및 C(at least one of A, B and C)”를 의미할 수

있다.

- [34] 또한, 본 명세서에서 사용되는 괄호는 “예를 들어(for example)”를 의미할 수 있다. 구체적으로, “제어 정보(EHT-Signal)”로 표시된 경우, “제어 정보”의 일례로 “EHT-Signal”이 제안된 것일 수 있다. 달리 표현하면 본 명세서의 “제어 정보”는 “EHT-Signal”로 제한(limit)되지 않고, “EHT-Signal”이 “제어 정보”의 일례로 제안된 것일 수 있다. 또한, “제어 정보(즉, EHT-signal)”로 표시된 경우에도, “제어 정보”의 일례로 “EHT-Signal”가 제안된 것일 수 있다.
- [35] 본 명세서에서 하나의 도면 내에서 개별적으로 설명되는 기술적 특징은, 개별적으로 구현될 수도 있고, 동시에 구현될 수도 있다.
- [36] 본 명세서의 이하의 일례는 다양한 무선 통신시스템에 적용될 수 있다. 예를 들어, 본 명세서의 이하의 일례는 무선랜(wireless local area network, WLAN) 시스템에 적용될 수 있다. 예를 들어, 본 명세서는 IEEE 802.11a/g/n/ac의 규격이나, IEEE 802.11ax 규격에 적용될 수 있다. 또한 본 명세서는 새롭게 제안되는 EHT 규격 또는 IEEE 802.11be 규격에도 적용될 수 있다. 또한 본 명세서의 일례는 EHT 규격 또는 IEEE 802.11be를 개선(enhance)한 새로운 무선랜 규격에도 적용될 수 있다. 또한 본 명세서의 일례는 이동 통신 시스템에 적용될 수 있다. 예를 들어, 3GPP(3rd Generation Partnership Project) 규격에 기반하는 LTE(Long Term Evolution) 및 그 진화(evolution)에 기반하는 이동 통신 시스템에 적용될 수 있다. 또한, 본 명세서의 일례는 3GPP 규격에 기반하는 5G NR 규격의 통신 시스템에 적용될 수 있다.
- [37] 이하 본 명세서의 기술적 특징을 설명하기 위해 본 명세서가 적용될 수 있는 기술적 특징을 설명한다.
- [38] 도 1은 본 명세서의 송신 장치 및/또는 수신 장치의 일례를 나타낸다.
- [39] 도 1의 일례는 이하에서 설명되는 다양한 기술적 특징을 수행할 수 있다. 도 1은 적어도 하나의 STA(station)에 관련된다. 예를 들어, 본 명세서의 STA(110, 120)은 이동 단말(mobile terminal), 무선 기기(wireless device), 무선 송수신 유닛(Wireless Transmit/Receive Unit; WTRU), 사용자 장비(User Equipment; UE), 이동국(Mobile Station; MS), 이동 가입자 유닛(Mobile Subscriber Unit) 또는 단순히 유저(user) 등의 다양한 명칭으로도 불릴 수 있다. 본 명세서의 STA(110, 120)은 네트워크, 기지국(Base Station), Node-B, AP(Access Point), 리피터, 라우터, 릴레이 등의 다양한 명칭으로 불릴 수 있다. 본 명세서의 STA(110, 120)은 수신 장치, 송신 장치, 수신 STA, 송신 STA, 수신 Device, 송신 Device 등의 다양한 명칭으로 불릴 수 있다.
- [40] 예를 들어, STA(110, 120)은 AP(access Point) 역할을 수행하거나 non-AP 역할을 수행할 수 있다. 즉, 본 명세서의 STA(110, 120)은 AP 및/또는 non-AP의 기능을 수행할 수 있다. 본 명세서에서 AP는 AP STA으로도 표시될 수 있다.
- [41] 본 명세서의 STA(110, 120)은 IEEE 802.11 규격 이외의 다양한 통신 규격을 함께 지원할 수 있다. 예를 들어, 3GPP 규격에 따른 통신 규격(예를 들어, LTE,

- LTE-A, 5G NR 규격)등을 지원할 수 있다. 또한 본 명세서의 STA는 휴대 전화, 차량(vehicle), 개인용 컴퓨터 등의 다양한 장치로 구현될 수 있다. 또한, 본 명세서의 STA는 음성 통화, 영상 통화, 데이터 통신, 자율 주행(Self-Driving, Autonomous-Driving) 등의 다양한 통신 서비스를 위한 통신을 지원할 수 있다.
- [42] 본 명세서에서 STA(110, 120)은 IEEE 802.11 표준의 규정을 따르는 매체 접속 제어(media access control, MAC)와 무선 매체에 대한 물리 계층(Physical Layer) 인터페이스를 포함할 수 있다.
- [43] 도 1의 부도면 (a)를 기초로 STA(110, 120)을 설명하면 이하와 같다.
- [44] 제1 STA(110)은 프로세서(111), 메모리(112) 및 트랜시버(113)를 포함할 수 있다. 도시된 프로세서, 메모리 및 트랜시버는 각각 별도의 칩으로 구현되거나, 적어도 둘 이상의 블록/기능이 하나의 칩을 통해 구현될 수 있다.
- [45] 제1 STA의 트랜시버(113)는 신호의 송수신 동작을 수행한다. 구체적으로, IEEE 802.11 패킷(예를 들어, IEEE 802.11a/b/g/n/ac/ax/be 등)을 송수신할 수 있다.
- [46] 예를 들어, 제1 STA(110)은 AP의 의도된 동작을 수행할 수 있다. 예를 들어, AP의 프로세서(111)는 트랜시버(113)를 통해 신호를 수신하고, 수신 신호를 처리하고, 송신 신호를 생성하고, 신호 송신을 위한 제어를 수행할 수 있다. AP의 메모리(112)는 트랜시버(113)를 통해 수신된 신호(즉, 수신 신호)를 저장할 수 있고, 트랜시버를 통해 송신될 신호(즉, 송신 신호)를 저장할 수 있다.
- [47] 예를 들어, 제2 STA(120)은 Non-AP STA의 의도된 동작을 수행할 수 있다. 예를 들어, non-AP의 트랜시버(123)는 신호의 송수신 동작을 수행한다. 구체적으로, IEEE 802.11 패킷(예를 들어, IEEE 802.11a/b/g/n/ac/ax/be 등)을 송수신할 수 있다.
- [48] 예를 들어, Non-AP STA의 프로세서(121)는 트랜시버(123)를 통해 신호를 수신하고, 수신 신호를 처리하고, 송신 신호를 생성하고, 신호 송신을 위한 제어를 수행할 수 있다. Non-AP STA의 메모리(122)는 트랜시버(123)를 통해 수신된 신호(즉, 수신 신호)를 저장할 수 있고, 트랜시버를 통해 송신될 신호(즉, 송신 신호)를 저장할 수 있다.
- [49] 예를 들어, 이하의 명세서에서 AP로 표시된 장치의 동작은 제1 STA(110) 또는 제2 STA(120)에서 수행될 수 있다. 예를 들어 제1 STA(110)이 AP인 경우, AP로 표시된 장치의 동작은 제1 STA(110)의 프로세서(111)에 의해 제어되고, 제1 STA(110)의 프로세서(111)에 의해 제어되는 트랜시버(113)를 통해 관련된 신호가 송신되거나 수신될 수 있다. 또한, AP의 동작에 관련된 제어 정보나 AP의 송신/수신 신호는 제1 STA(110)의 메모리(112)에 저장될 수 있다. 또한, 제2 STA(110)이 AP인 경우, AP로 표시된 장치의 동작은 제2 STA(120)의 프로세서(121)에 의해 제어되고, 제2 STA(120)의 프로세서(121)에 의해 제어되는 트랜시버(123)를 통해 관련된 신호가 송신되거나 수신될 수 있다. 또한, AP의 동작에 관련된 제어 정보나 AP의 송신/수신 신호는 제2 STA(110)의 메모리(122)에 저장될 수 있다.
- [50] 예를 들어, 이하의 명세서에서 non-AP(또는 User-STA)로 표시된 장치의 동작은

제 STA(110) 또는 제2 STA(120)에서 수행될 수 있다. 예를 들어 제2 STA(120)이 non-AP인 경우, non-AP로 표시된 장치의 동작은 제2 STA(120)의 프로세서(121)에 의해 제어되고, 제2 STA(120)의 프로세서(121)에 의해 제어되는 트랜시버(123)를 통해 관련된 신호가 송신되거나 수신될 수 있다. 또한, non-AP의 동작에 관련된 제어 정보나 AP의 송신/수신 신호는 제2 STA(120)의 메모리(122)에 저장될 수 있다. 예를 들어 제1 STA(110)이 non-AP인 경우, non-AP로 표시된 장치의 동작은 제1 STA(110)의 프로세서(111)에 의해 제어되고, 제1 STA(110)의 프로세서(111)에 의해 제어되는 트랜시버(113)를 통해 관련된 신호가 송신되거나 수신될 수 있다. 또한, non-AP의 동작에 관련된 제어 정보나 AP의 송신/수신 신호는 제1 STA(110)의 메모리(112)에 저장될 수 있다.

- [51] 이하의 명세서에서 (송신/수신) STA, 제1 STA, 제2 STA, STA1, STA2, AP, 제1 AP, 제2 AP, AP1, AP2, (송신/수신) Terminal, (송신/수신) device, (송신/수신) apparatus, 네트워크 등으로 불리는 장치는 도 1의 STA(110, 120)을 의미할 수 있다. 예를 들어, 구체적인 도면 부호 없이 (송신/수신) STA, 제1 STA, 제2 STA, STA1, STA2, AP, 제1 AP, 제2 AP, AP1, AP2, (송신/수신) Terminal, (송신/수신) device, (송신/수신) apparatus, 네트워크 등으로 표시된 장치도 도 1의 STA(110, 120)을 의미할 수 있다. 예를 들어, 이하의 일례에서 다양한 STA이 신호(예를 들어, PPDU)를 송수신하는 동작은 도 1의 트랜시버(113, 123)에서 수행되는 것일 수 있다. 또한, 이하의 일례에서 다양한 STA이 송수신 신호를 생성하거나 송수신 신호를 위해 사전에 데이터 처리나 연산을 수행하는 동작은 도 1의 프로세서(111, 121)에서 수행되는 것일 수 있다. 예를 들어, 송수신 신호를 생성하거나 송수신 신호를 위해 사전에 데이터 처리나 연산을 수행하는 동작의 일례는, 1) PPDU 내에 포함되는 서브 필드(SIG, STF, LTF, Data) 필드의 비트 정보를 결정/획득/구성/연산/디코딩/인코딩하는 동작, 2) PPDU 내에 포함되는 서브 필드(SIG, STF, LTF, Data) 필드를 위해 사용되는 시간 자원이나 주파수 자원(예를 들어, 서브캐리어 자원) 등을 결정/구성/획득하는 동작, 3) PPDU 내에 포함되는 서브 필드(SIG, STF, LTF, Data) 필드를 위해 사용되는 특정한 시퀀스(예를 들어, 파일럿 시퀀스, STF/LTF 시퀀스, SIG에 적용되는 엑스트라 시퀀스) 등을 결정/구성/획득하는 동작, 4) STA에 대해 적용되는 전력 제어 동작 및/또는 파워 세이빙 동작, 5) ACK 신호의 결정/획득/구성/연산/디코딩/인코딩 등에 관련된 동작을 포함할 수 있다. 또한, 이하의 일례에서 다양한 STA이 송수신 신호의 결정/획득/구성/연산/디코딩/인코딩을 위해 사용하는 다양한 정보(예를 들어, 필드/서브필드/제어필드/파라미터/파워 등에 관련된 정보)는 도 1의 메모리(112, 122)에 저장될 수 있다.

- [52] 상술한 도 1의 부도면 (a)의 장치/STA는 도 1의 부도면 (b)와 같이 변형될 수 있다. 이하 도 1의 부도면 (b)을 기초로, 본 명세서의 STA(110, 120)을 설명한다.

- [53] 예를 들어, 도 1의 부도면 (b)에 도시된 트랜시버(113, 123)는 상술한 도 1의 부도면 (a)에 도시된 트랜시버와 동일한 기능을 수행할 수 있다. 예를 들어, 도

1의 부도면 (b)에 도시된 프로세싱 칩(114, 124)은 프로세서(111, 121) 및 메모리(112, 122)를 포함할 수 있다. 도 1의 부도면 (b)에 도시된 프로세서(111, 121) 및 메모리(112, 122)는 상술한 도 1의 부도면 (a)에 도시된 프로세서(111, 121) 및 메모리(112, 122)와 동일한 기능을 수행할 수 있다.

- [54] 이하에서 설명되는, 이동 단말(mobile terminal), 무선 기기(wireless device), 무선 송수신 유닛(Wireless Transmit/Receive Unit; WTRU), 사용자 장비(User Equipment; UE), 이동국(Mobile Station; MS), 이동 가입자 유닛(Mobile Subscriber Unit), 유저(user), 유저 STA, 네트워크, 기지국(Base Station), Node-B, AP(Access Point), 리피터, 라우터, 릴레이, 수신 장치, 송신 장치, 수신 STA, 송신 STA, 수신 Device, 송신 Device, 수신 Apparatus, 및/또는 송신 Apparatus는, 도 1의 부도면 (a)/(b)에 도시된 STA(110, 120)을 의미하거나, 도 1의 부도면 (b)에 도시된 프로세싱 칩(114, 124)을 의미할 수 있다. 즉, 본 명세서의 기술적 특징은, 도 1의 부도면 (a)/(b)에 도시된 STA(110, 120)에 수행될 수도 있고, 도 1의 부도면 (b)에 도시된 프로세싱 칩(114, 124)에서만 수행될 수도 있다. 예를 들어, 송신 STA가 제어 신호를 송신하는 기술적 특징은, 도 1의 부도면 (a)/(b)에 도시된 프로세서(111, 121)에서 생성된 제어 신호가 도 1의 부도면 (a)/(b)에 도시된 트랜시버(113, 123)을 통해 송신되는 기술적 특징으로 이해될 수 있다. 또는, 송신 STA가 제어 신호를 송신하는 기술적 특징은, 도 1의 부도면 (b)에 도시된 프로세싱 칩(114, 124)에서 트랜시버(113, 123)로 전달될 제어 신호가 생성되는 기술적 특징으로 이해될 수 있다.
- [55] 예를 들어, 수신 STA가 제어 신호를 수신하는 기술적 특징은, 도 1의 부도면 (a)에 도시된 트랜시버(113, 123)에 의해 제어 신호가 수신되는 기술적 특징으로 이해될 수 있다. 또는, 수신 STA가 제어 신호를 수신하는 기술적 특징은, 도 1의 부도면 (a)에 도시된 트랜시버(113, 123)에 수신된 제어 신호가 도 1의 부도면 (a)에 도시된 프로세서(111, 121)에 의해 획득되는 기술적 특징으로 이해될 수 있다. 또는, 수신 STA가 제어 신호를 수신하는 기술적 특징은, 도 1의 부도면 (b)에 도시된 트랜시버(113, 123)에 수신된 제어 신호가 도 1의 부도면 (b)에 도시된 프로세싱 칩(114, 124)에 의해 획득되는 기술적 특징으로 이해될 수 있다.
- [56] 도 1의 부도면 (b)을 참조하면, 메모리(112, 122) 내에 소프트웨어 코드(115, 125)가 포함될 수 있다. 소프트웨어 코드(115, 125)는 프로세서(111, 121)의 동작을 제어하는 instruction이 포함될 수 있다. 소프트웨어 코드(115, 125)는 다양한 프로그래밍 언어로 포함될 수 있다.
- [57] 도 1에 도시된 프로세서(111, 121) 또는 프로세싱 칩(114, 124)은 ASIC(application-specific integrated circuit), 다른 칩셋, 논리 회로 및/또는 데이터 처리 장치를 포함할 수 있다. 프로세서는 AP(application processor)일 수 있다. 예를 들어, 도 1에 도시된 프로세서(111, 121) 또는 프로세싱 칩(114, 124)은 DSP(digital signal processor), CPU(central processing unit), GPU(graphics processing unit), 모뎀(Modem; modulator and demodulator) 중 적어도 하나를 포함할 수 있다.

예를 들어, 도 1에 도시된 프로세서(111, 121) 또는 프로세싱 칩(114, 124)은 Qualcomm®에 의해 제조된 SNAPDRAGON™ 시리즈 프로세서, Samsung®에 의해 제조된 EXYNOS™ 시리즈 프로세서, Apple®에 의해 제조된 A 시리즈 프로세서, MediaTek®에 의해 제조된 HELIO™ 시리즈 프로세서, INTEL®에 의해 제조된 ATOM™ 시리즈 프로세서 또는 이를 개선(enhance)한 프로세서일 수 있다.

[58] 본 명세서에서 상향링크는 non-AP STA로부터 AP STA으로의 통신을 위한 링크를 의미할 수 있고 상향링크를 통해 상향링크 PPDU/패킷/신호 등이 송신될 수 있다. 또한, 본 명세서에서 하향링크는 AP STA로부터 non-AP STA으로의 통신을 위한 링크를 의미할 수 있고 하향링크를 통해 하향링크 PPDU/패킷/신호 등이 송신될 수 있다.

[59] 도 2는 무선랜(WLAN)의 구조를 나타낸 개념도이다.

[60] 도 2의 상단은 IEEE(institute of electrical and electronic engineers) 802.11의 인프라스트럭처 BSS(basic service set)의 구조를 나타낸다.

[61] 도 2의 상단을 참조하면, 무선랜 시스템은 하나 또는 그 이상의 인프라스트럭처 BSS(200, 205)(이하, BSS)를 포함할 수 있다. BSS(200, 205)는 성공적으로 동기화를 이루어서 서로 통신할 수 있는 AP(access point, 225) 및 STA1(Station, 200-1)과 같은 AP와 STA의 집합으로서, 특정 영역을 가리키는 개념은 아니다. BSS(205)는 하나의 AP(230)에 하나 이상의 결합 가능한 STA(205-1, 205-2)를 포함할 수도 있다.

[62] BSS는 적어도 하나의 STA, 분산 서비스(distribution Service)를 제공하는 AP(225, 230) 및 다수의 AP를 연결시키는 분산 시스템(distribution System, DS, 210)을 포함할 수 있다.

[63] 분산 시스템(210)은 여러 BSS(200, 205)를 연결하여 확장된 서비스 셋인 ESS(extended service set, 240)를 구현할 수 있다. ESS(240)는 하나 또는 여러 개의 AP가 분산 시스템(210)을 통해 연결되어 이루어진 하나의 네트워크를 지시하는 용어로 사용될 수 있다. 하나의 ESS(240)에 포함되는 AP는 동일한 SSID(service set identification)를 가질 수 있다.

[64] 포털(portal, 220)은 무선랜 네트워크(IEEE 802.11)와 다른 네트워크(예를 들어, 802.X)와의 연결을 수행하는 브리지 역할을 수행할 수 있다.

[65] 도 2의 상단과 같은 BSS에서는 AP(225, 230) 사이의 네트워크 및 AP(225, 230)와 STA(200-1, 205-1, 205-2) 사이의 네트워크가 구현될 수 있다. 하지만, AP(225, 230)가 없이 STA 사이에서도 네트워크를 설정하여 통신을 수행하는 것도 가능할 수 있다. AP(225, 230)가 없이 STA 사이에서도 네트워크를 설정하여 통신을 수행하는 네트워크를 애드-혹 네트워크(Ad-Hoc network) 또는 독립 BSS(independent basic service set, IBSS)라고 정의한다.

[66] 도 2의 하단은 IBSS를 나타낸 개념도이다.

[67] 도 2의 하단을 참조하면, IBSS는 애드-혹 모드로 동작하는 BSS이다. IBSS는

AP를 포함하지 않기 때문에 중앙에서 관리 기능을 수행하는 개체(centralized management entity)가 없다. 즉, IBSS에서 STA(250-1, 250-2, 250-3, 255-4, 255-5)들은 분산된 방식(distributed manner)으로 관리된다. IBSS에서는 모든 STA(250-1, 250-2, 250-3, 255-4, 255-5)이 이동 STA으로 이루어질 수 있으며, 분산 시스템으로의 접속이 허용되지 않아서 자기 완비적 네트워크(self-contained network)를 이룬다.

[68] 도 3은 일반적인 링크 셋업(link setup) 과정을 설명하는 도면이다.

[69] 도시된 S310 단계에서 STA은 네트워크 발견 동작을 수행할 수 있다. 네트워크 발견 동작은 STA의 스캐닝(scanning) 동작을 포함할 수 있다. 즉, STA이 네트워크에 액세스하기 위해서는 참여 가능한 네트워크를 찾아야 한다. STA은 무선 네트워크에 참여하기 전에 호환 가능한 네트워크를 식별하여야 하는데, 특정 영역에 존재하는 네트워크 식별과정을 스캐닝이라고 한다. 스캐닝 방식에는 능동적 스캐닝(active scanning)과 수동적 스캐닝(passive scanning)이 있다.

[70] 도 3에서는 예시적으로 능동적 스캐닝 과정을 포함하는 네트워크 발견 동작을 도시한다. 능동적 스캐닝에서 스캐닝을 수행하는 STA은 채널들을 옮기면서 주변에 어떤 AP가 존재하는지 탐색하기 위해 프로브 요청 프레임(probe request frame)을 전송하고 이에 대한 응답을 기다린다. 응답자(responder)는 프로브 요청 프레임을 전송한 STA에게 프로브 요청 프레임에 대한 응답으로 프로브 응답 프레임(probe response frame)을 전송한다. 여기에서, 응답자는 스캐닝되고 있는 채널의 BSS에서 마지막으로 비콘 프레임(beacon frame)을 전송한 STA일 수 있다. BSS에서는 AP가 비콘 프레임을 전송하므로 AP가 응답자가 되며, IBSS에서는 IBSS 내의 STA들이 돌아가면서 비콘 프레임을 전송하므로 응답자가 일정하지 않다. 예를 들어, 1번 채널에서 프로브 요청 프레임을 전송하고 1번 채널에서 프로브 응답 프레임을 수신한 STA은, 수신한 프로브 응답 프레임에 포함된 BSS 관련 정보를 저장하고 다음 채널(예를 들어, 2번 채널)로 이동하여 동일한 방법으로 스캐닝(즉, 2번 채널 상에서 프로브 요청/응답 송수신)을 수행할 수 있다.

[71] 도 3의 일례에는 표시되지 않았지만, 스캐닝 동작은 수동적 스캐닝 방식으로 수행될 수도 있다. 수동적 스캐닝을 기초로 스캐닝을 수행하는 STA은 채널들을 옮기면서 비콘 프레임을 기다릴 수 있다. 비콘 프레임은 IEEE 802.11에서 관리 프레임(management frame) 중 하나로서, 무선 네트워크의 존재를 알리고, 스캐닝을 수행하는 STA으로 하여금 무선 네트워크를 찾아서, 무선 네트워크에 참여할 수 있도록 주기적으로 전송된다. BSS에서 AP가 비콘 프레임을 주기적으로 전송하는 역할을 수행하고, IBSS에서는 IBSS 내의 STA들이 돌아가면서 비콘 프레임을 전송한다. 스캐닝을 수행하는 STA은 비콘 프레임을 수신하면 비콘 프레임에 포함된 BSS에 대한 정보를 저장하고 다른 채널로 이동하면서 각 채널에서 비콘 프레임 정보를 기록한다. 비콘 프레임을 수신한

STA은, 수신한 비콘 프레임에 포함된 BSS 관련 정보를 저장하고 다음 채널로 이동하여 동일한 방법으로 다음 채널에서 스캐닝을 수행할 수 있다.

- [72] 네트워크를 발견한 STA은, 단계 S320를 통해 인증 과정을 수행할 수 있다. 이러한 인증 과정은 후술하는 단계 S340의 보안 셋업 동작과 명확하게 구분하기 위해서 첫 번째 인증(first authentication) 과정이라고 칭할 수 있다. S320의 인증 과정은, STA이 인증 요청 프레임(authentication request frame)을 AP에게 전송하고, 이에 응답하여 AP가 인증 응답 프레임(authentication response frame)을 STA에게 전송하는 과정을 포함할 수 있다. 인증 요청/응답에 사용되는 인증 프레임(authentication frame)은 관리 프레임에 해당한다.
- [73] 인증 프레임은 인증 알고리즘 번호(authentication algorithm number), 인증 트랜잭션 시퀀스 번호(authentication transaction sequence number), 상태 코드(status code), 검문 텍스트(challenge text), RSN(Robust Security Network), 유한 순환 그룹(Finite Cyclic Group) 등에 대한 정보를 포함할 수 있다.
- [74] STA은 인증 요청 프레임을 AP에게 전송할 수 있다. AP는 수신된 인증 요청 프레임에 포함된 정보에 기초하여, 해당 STA에 대한 인증을 허용할지 여부를 결정할 수 있다. AP는 인증 처리의 결과를 인증 응답 프레임을 통하여 STA에게 제공할 수 있다.
- [75] 성공적으로 인증된 STA은 단계 S330을 기초로 연결 과정을 수행할 수 있다. 연결 과정은 STA이 연결 요청 프레임(association request frame)을 AP에게 전송하고, 이에 응답하여 AP가 연결 응답 프레임(association response frame)을 STA에게 전송하는 과정을 포함한다. 예를 들어, 연결 요청 프레임은 다양한 능력(capability)에 관련된 정보, 비콘 청취 간격(listen interval), SSID(service set identifier), 지원 레이트(supported rates), 지원 채널(supported channels), RSN, 이동성 도메인, 지원 오퍼레이팅 클래스(supported operating classes), TIM 방송 요청(Traffic Indication Map Broadcast request), 상호동작(interworking) 서비스 능력 등에 대한 정보를 포함할 수 있다. 예를 들어, 연결 응답 프레임은 다양한 능력에 관련된 정보, 상태 코드, AID(Association ID), 지원 레이트, EDCA(Enhanced Distributed Channel Access) 파라미터 세트, RCPI(Received Channel Power Indicator), RSNI(Received Signal to Noise Indicator), 이동성 도메인, 타임아웃 간격(연관 컴백 시간(association comeback time)), 중첩(overlapping) BSS 스캔 파라미터, TIM 방송 응답, QoS 맵 등의 정보를 포함할 수 있다.
- [76] 이후 S340 단계에서, STA은 보안 셋업 과정을 수행할 수 있다. 단계 S340의 보안 셋업 과정은, 예를 들어, EAPOL(Extensible Authentication Protocol over LAN) 프레임을 통한 4-웨이(way) 핸드셰이킹을 통해서, 프라이빗 키 셋업(private key setup)을 하는 과정을 포함할 수 있다.

[77] **1. Zigbee 및 CHIP(Connected Home over IP)**

[78] <Zigbee의 필요성>

[79] 현재 음성, PC LANs, 비디오 등의 데이터에 대한 표준은 마련되어 있지만,

센서나 컨트롤 디바이스 등의 특별한 필요를 충족시킬 만한 무선 네트워크 표준은 없었다. 센서 및 컨트롤 디바이스들은 높은 주파수 대역폭을 필요로 하지 않지만, 배터리의 장기간 사용과 디바이스들의 넓은 배열을 위해서, 짧은 대기시간 및 낮은 에너지 소비를 필요로 한다.

[80] 오늘날 높은 데이터율을 필요로 하지 않으면서 적은 비용과 적은 소비 전력으로 동작할 수 있는 다양한 무선통신 시스템이 생산되고 있다.

[81] 이렇게 생산되는 제품들은 표준 없이 제작되고 있고, 결국 이러한 과거의 제품들은 각 제품들과의 호환성 문제를 일으키고, 더불어 새로운 기술들과의 호환성에도 문제가 생긴다.

[82] <Zigbee 소개>

[83] 지그비는 IEEE 802.15.4-2003을 기반으로 한 작고, 저전력의 디지털 라디오를 사용하는 하이레벨 통신 프로토콜이다. IEEE 802.15.4-2003는 단거리 라디오 주파수를 사용하는 램프, 전자계량기, 소비자용 전자제품과 같은 근거리 개인 무선통신망의 기준이다. 지그비는 낮은 데이터율, 적은 배터리 소모, 네트워크의 안전성을 요구하는 RF(Radio Frequency) 어플리케이션에 주로 사용된다.

[84] <Zigbee 특징>

[85] 1) 저전력 소모, 간단한 구현

[86] 2) 한번의 배터리 충전으로 수 개월, 또는 수년간 사용 가능

[87] 3) 활성 모드(수신, 송신), 슬립 모드를 가짐.

[88] 4) 디바이스, 설치, 유지 등 모두 상대적으로 낮은 비용으로 가능

[89] 5) 안전성(보안성)

[90] 6) 신뢰성

[91] 7) 유연성

[92] 8) 매우 작은 프로토콜 스택

[93] 9) 상호 호환가능 및 어느 곳에서나 사용 가능

[94] 10) 네트워크당 높은 노트 밀집(지그비의 IEEE 802.15.4 사용은 네트워크에서 많은 디바이스를 다루는 것을 가능케 함. 이러한 특징으로 방대한 센서 배열과 네트워크의 통제가 가능)

[95] 11) 간단한 프로토콜, 국제적으로 구현(지그비 프로토콜 스택 코드의 크기는 블루투스나 802.11의 사이즈에 비해 4분의 1 정도에 불과하다.)

[96] <Zigbee의 사용분야>

[97] Zigbee는 현재, 산업용 제어, 임베디드 센서, 의학자료 수집, 화재 및 도난, 빌딩 자동화, 홈 오토메이션 등의 분야에 사용되고 있다.

[98] 1) 스마트 에너지

[99] 스마트 에너지는 유틸리티/에너지 서비스 제공자에게, 에너지를 관리할 수 있는 안전하고 사용이 편한 가정 무선 네트워크를 제공한다. 스마트 에너지는 유틸리티/에너지 서비스 제공자 혹은 그들의 고객들에게 온도조절장치 또는 다른 연계된 장치들을 직접 통제할 수 있도록 해준다.

- [100] 2) 홈 엔터테인먼트와 제어
- [101] 스마트 전원, 발전된 온도조절 시스템, 안전성 과 보안성, 영화와 음악
- [102] 3) 홈 인식 시스템
- [103] 수온 센서, 전원센서, 에너지 모니터링, 화재 및 도난 감시, 스마트 장치들과
접속 센서
- [104] 4) 모바일 서비스
- [105] 모바일 결제, 모바일 모니터링 및 통제, 모바일 보안과 접속 통제, 모바일
헬스케어 및 원격 지원
- [106] 5) 상업 빌딩
- [107] 에너지 모니터링, 공기조화설비, 조명, 출입 통제
- [108] 6) 산업용 공장
- [109] 프로세스 통제, 자재관리, 환경관리, 에너지 관리, 산업 디바이스 제어, M2M
통신
- [110] <Zigbee 장치 유형>
- [111] 도 4는 Zigbee 장치 유형을 도시한다.
- [112] Zigbee 장치에는 도 4와 같이 3가지 종류가 있다
- [113] 1) 지그비 코디네이터(Zigbee Coordinator)
- [114] 가장 중요한 디바이스로 네트워크를 형성하고 다른 네트워크들과 연결시킨다.
각각의 네트워크에는 단 한 개의 코디네이터가 있다. 지그비 코디네이터는
네트워크에 관한 정보를 저장할 수 있고, trust center 또는 보안 키를 위한
저장소로서의 역할도 수행한다.
- [115] 2) 지그비 라우터(Zigbee Router)
- [116] 라우터는 애플리케이션 기능뿐만 아니라, 다른 디바이스로부터의 데이터를
전달할 수 있는 라이터로서의 기능도 할 수 있다.
- [117] 3) 지그비 엔드 디바이스(Zigbee End Device)
- [118] 지그비 엔드 디바이스는 부모 노드와 통신할 수 있는 기능을 포함한다. 이러한
관계는 노드가 오랜 시간을 대기할 수 있도록 하여 배터리 수명을 더욱 길게
연장할 수 있다.
- [119] <Zigbee 스택>
- [120] 도 5는 Zigbee 스택을 도시한다.
- [121] Zigbee는 다른 많은 프로토콜 스택보다 간단하며, Zigbee 스택 코드의 크기는
다른 프로토콜에 비해 작다. MAC과 PHY는 IEEE 802.15.4 표준에 의해서
정의된다. 네트워크와 애플리케이션 레이어들은 장비 디자이너에 의해
제공되는 actual application과 Zigbee Alliance에 의해서 정의된다.
- [122] 802.15.4는 가벼운 무선 네트워크를 위한 간단한 패킷 데이터 프로토콜이다.
802.15.4는 배터리 수명이 중요한 애플리케이션을 모니터링하고 제어하기
위해서 만들어졌다. 802.15.4는 지그비의 뛰어난 배터리 수명의 근원이 된다.
- [123] 802.15.4는 IEEE long/short addressing 둘다 적용 가능하다. Short addressing은

- 네트워크 ID가 임시로 정해지는 네트워크 관리에 사용된다. 이것은 적은 비용이 들도록 하지만 여전히 65,000여개의 네트워크 노드를 사용 가능케 한다.
- [124] 또한, 802.15.4는 신뢰성 있는 데이터 전송과 비콘 관리가 가능하다.
- [125] 네트워크 레이어는 MAC 레이어(Layer)의 적절한 운영을 보장하고, 애플리케이션 레이어에 인터페이스를 제공한다. 네트워크 레이어는 스타, 트리, 매쉬 토폴로지를 지원한다. 네트워크 레이어는 네트워크가 시작되고, 결합하고, 소멸되고, 검색되는 곳이다.
- [126] 네트워크 레이어는 라우팅과 보안을 담당한다.
- [127] 애플리케이션 프레임워크는, 애플리케이션 객체가 데이터를 주고 받을 수 있는 실행 환경이다. 애플리케이션 객체는 Zigbee 장치의 생산자에 의해서 정해진다. Zigbee에 의해 정의된 바에 의하면, 애플리케이션 객체는 애플리케이션 레이어의 최상단에 위치하고, 디바이스 제조자에 의해 결정된다. 애플리케이션 객체는 실질적으로 애플리케이션을 구축한다; 이것은 전구, 조명 스위치, LED, I/O 라인 등등이 될 수 있다.
- [128] 요즘 출시되는 가전제품을 살펴보면 '스마트'라는 수식어가 거의 필수로 붙고 있다. 스마트 TV, 스마트 냉장고, 스마트 에어컨, 스마트 세탁기 등 '스마트'를 적용하지 않은 제품군을 찾아보기 어려울 정도다. 이런 스마트 제품군은 유무선 네트워크를 탑재, 서로 긴밀히 통신하며 연동하는 IoT(Internet On Things, 사물인터넷) 기술을 기반으로 다양한 편의 기능을 구현한다. 여기에 온습도 센서나 도어센서, 모션센서, IP카메라 등 IoT 기술을 품은 다양한 센서까지 결합한다면 한층 정밀하고 다양한 자동화 기능을 쓸 수 있다.
- [129] 이런 다수의 스마트 제품들을 모아 하나의 집에 적용하면 '스마트홈'이 탄생한다. 이런 집에 거주한다면 사용자가 바깥 일을 마치고 귀가할 즈음이 되면 자동으로 전등이나 에어컨이 켜지고, 그날 날씨에 따라 적절한 음악이 자동으로 재생되는 등의 다양한 자동화, 혹은 원격 기능을 이용할 수 있다. 그 외에 유사한 개념으로는 '스마트 빌딩'이나 '스마트 팩토리(공장)' 등이 있다.
- [130] 다만 스마트 제품이 우후죽순처럼 쏟아지고 다양한 규격의 제품이 난립하게 되면서 생긴 부작용도 있다. 바로 호환성 문제다. IoT 기술은 각 기기간의 통신과 연동이 핵심인데 각 기기가 각기 다른 IoT 플랫폼을 이용하고 있어 서로 연동이 되지 않는다면 활용성이 크게 저하된다.
- [131] 이를테면 스피커는 '애플 홈팟' 플랫폼 기반의 제품인데 TV는 '삼성 스마트싱스' 플랫폼에만 호환된다면 음성명령을 통해 TV를 켜거나 채널을 전환하는 기능을 이용하지 못할 수도 있다. 물론 최근에는 하나의 제품이 2가지 이상의 IoT 플랫폼을 동시에 지원하기도 한다. 아니면 아예 모든 제품을 동일 플랫폼 기반의 것으로만 구매해서 스마트 환경을 꾸미는 방법도 있다. 하지만 그렇다고 해도 제품을 구매할 때마다 호환성을 면밀히 따져야 한다는 건 불편한 일이다.
- [132] 하지만 앞으로는 이런 걱정을 하지 않아도 될 것 같다. IoT 관련 주요 업체들이

모여 플랫폼 종속 없이 모든 기기가 호환성을 갖출 수 있는 표준 규격을 발표했기 때문이다. 지난 5월, CSA(Connectivity Standards Alliance) 표준 연합은 '매터(Matter)'라는 IoT 표준 규약(프로토콜)을 선보였다. 과거 프로젝트 칩(Project CHIP ; Connected Home over IP)으로 알려졌던 이번 매터(Matter) 표준은 아마존과 구글, 시그니파이(필립스 휴), 스마트씽스(SmartThings) 및 여타 스마트홈 시장의 주요 업체들로부터 지지를 받고 있다.

- [133] 매터 표준 제정에 참여하거나 협력을 발표한 기업은 삼성전자, 구글, 아마존, 애플, 투야, 화웨이, 슈나이더 일렉트릭 등 수십여개사에 이르는데 이들은 하나같이 IoT 시장에서 높은 점유율을 갖춘 글로벌 기업들이다. 매터 표준이 널리 퍼진다면 이제는 제조사나 플랫폼을 따질 필요없이 모든 스마트 기기들이 원활하게 연동될 것이다.
- [134] 매터는 와이파이, 이더넷(Ethernet), 쓰레드(Thread)와 같은 기존 네트워크 기술에서 실행될 수 있는 IP 기반 프로토콜이다. 연맹 측은 매터 장치가 블루투스 로우 에너지(BLE)를 사용해 쉽게 설정될 수 있다고 밝혔다. 스마트홈 기기 스스로의 정체와 가능 작업을 서로에게 알릴 수 있기 때문에 사용자가 복잡한 구성 작업을 할 필요가 없다는 설명이다.
- [135] 특히 '다중 관리자'(multi-admin)이라는 매터의 기능은 애플 홈킷이나 아마존 알렉사와 같은 다양한 생태계의 제품이 최종 사용자의 복잡한 작업없이 함께 동작할 수 있도록 해준다. 다중 관리자는 또 제어 계층을 설정해 다양한 가족 구성원이 다양한 제어 수준으로 가정의 스마트 제품에 연결하도록 돕는다.
- [136] 도 6은 본 명세서의 송신 장치 및/또는 수신 장치의 변형된 일례를 나타낸다.
- [137] 도 1의 부도면 (a)/(b)의 각 장치/STA는 도 6와 같이 변형될 수 있다. 도 6의 트랜시버(630)는 도 1의 트랜시버(113, 123)와 동일할 수 있다. 도 6의 트랜시버(630)는 수신기(receiver) 및 송신기(transmitter)를 포함할 수 있다.
- [138] 도 6의 프로세서(610)는 도 1의 프로세서(111, 121)와 동일할 수 있다. 또는, 도 6의 프로세서(610)는 도 1의 프로세싱 칩(114, 124)과 동일할 수 있다.
- [139] 도 6의 메모리(150)는 도 1의 메모리(112, 122)와 동일할 수 있다. 또는, 도 6의 메모리(150)는 도 1의 메모리(112, 122)와는 상이한 별도의 외부 메모리일 수 있다.
- [140] 도 6을 참조하면, 전력 관리 모듈(611)은 프로세서(610) 및/또는 트랜시버(630)에 대한 전력을 관리한다. 배터리(612)는 전력 관리 모듈(611)에 전력을 공급한다. 디스플레이(613)는 프로세서(610)에 의해 처리된 결과를 출력한다. 키패드(614)는 프로세서(610)에 의해 사용될 입력을 수신한다. 키패드(614)는 디스플레이(613) 상에 표시될 수 있다. SIM 카드(615)는 휴대 전화 및 컴퓨터와 같은 휴대 전화 장치에서 가입자를 식별하고 인증하는 데에 사용되는 IMSI(international mobile subscriber identity) 및 그와 관련된 키를 안전하게 저장하기 위하여 사용되는 집적 회로일 수 있다.
- [141] 도 6을 참조하면, 스피커(640)는 프로세서(610)에 의해 처리된 소리 관련

결과를 출력할 수 있다. 마이크(641)는 프로세서(610)에 의해 사용될 소리 관련 입력을 수신할 수 있다.

[142] **2. 본 명세서에 적용 가능한 실시예**

[143] 본 명세서는 CHIP(Connected Home over IP) 기기의 등록(Commissioning)을 위해서 CHIP Controlee 기기가 필요한 정보를 생성하는 방법과 해당 정보를 CHIP Controller에서 획득하는 방법에 대한 내용이다. 특히 CHIP Controller가 정보 생성을 위한 값을 Cloud로 전달하여 Controlee의 Cloud와 Controller의 Cloud 간 확인 과정을 통해 연결에 필요한 값을 Controller에게 전달하여 두 기기 간 Local에서 기기 등록을 가능하게 하는 방법에 대해서 설명한다.

[144] 종래 CHIP 표준 기술은 Controlee 기기에 부착된 QR(Quick Response) 코드 혹은 숫자 코드(Manual Pairing Code)를 Controller 기기에서 카메라로 스캔하거나 직접 입력하는 방법으로 기기의 소유권 등록(Commissioning)을 수행한다. 이 경우 QR 코드 내에는 기기의 구분을 위해 사용되는 Device Discriminator 값(16bits)과 Setup PIN(Postal Index Number) Code 값(27bits)이 encoding되어 들어가게 된다. 이를 스마트폰과 같이 카메라를 가지고 있는 기기가 QR scan을 통해서 읽음으로써 Controller가 값을 가져올 수 있게 된다. 혹은 QR 외에 숫자 코드(11자리 숫자 혹은 21자리 숫자)를 Controlee에서 보여주고 Controller의 입력장치를 통해서 해당 코드를 입력하여 해당 값을 통해서 기기 등록을 수행하게 된다.

[145] 앞서 설명한 QR 코드나 PIN 코드를 입력하기 위해서는 Controller 기기에 QR을 스캔하기 위한 카메라 기기나 숫자를 입력하기 위한 키패드가 존재해야 한다. 또한 숫자 코드의 경우 정보의 길이가 길어 11자리 혹은 21자리 숫자를 사용자가 직접 입력해야 하여 사용자 경험상 좋지 못하거나 입력 시 오류가 발생할 수 있다. 또한 Controlee 기기의 종류에 따라서 QR Code의 값이나 숫자 코드를 변경하지 못하는 경우가 있어서 기기 등록의 보안상의 위협이 존재하게 된다.

[146] 본 명세서에서는 Controlee가 QR이나 숫자 코드에 포함되는 기기 등록에 필요한 값을 생성하기 위한 값(seed value)을 Controller가 획득하여 Controlee 제조사의 Cloud에 전달하여 기기 등록에 필요한 Setup PIN Code를 획득하는 방법에 대해서 설명한다. 기기의 실제로 존재 여부를 확인하기 위한 Proof of possession을 위해서 기존보다 짧은 숫자 코드를 사용함으로써 QR이나 긴 숫자의 입력 없이, Camera가 없는 기기나 음성으로 해당 기기의 등록을 실행할 수 있는 방법을 설명한다.

[147] **2.1. 기술 적용을 위한 환경**

[148] 도 7은 각각의 클라우드에 연결된 Controller와 Controlee의 연결 구조를 나타낸다.

[149] 본 명세서에서 제안하는 환경은 도 7과 같이 제조사 A의 Controlee와 제조사 B의 Controller가 초기 기기 등록을 하는 환경이다. 본 실시예에서는 제조사 A와 제조사 B를 다른 제조사인 경우를 예시하고 있으나 이에 한정하지 않고

Controlee와 Controller가 같은 제조사인 경우에도 동일하게 적용 가능하다.

[150] Controller B는 계정을 기반으로 Cloud B에 연결된 상태이며, Controlee A는 Cloud A에 연결 이전 상태이다. 즉 Controlee A의 경우 신규 제품의 실시예로 아직 인터넷 혹은 Wi-Fi 연결이 되지 않은 상태이다. Cloud B에 연결된 Controller B의 계정은 Cloud A의 계정과 계정 연동(Account Linking)이 있을 수도 있으며, 없을 수도 있는 상태이다.

[151] 2.2. Controlee의 초기화 과정 및 검색

[152] 도 8은 Controlee의 초기화 및 검색 과정 절차를 나타낸다.

[153] 도 8은 사용자가 Controlee A 기기의 전원을 인가하는 경우에 대한 절차의 순서도를 도시한다.

[154] 사용자는 Cloud B 연결을 위한 계정을 통해서 Controller B가 Cloud B에 login하게 한다. 사용자는 신규 Controlee인 Controlee A에 전원을 입력한다. 이를 통해 Controlee A는 초기화 과정을 수행하게 된다. Controlee A의 CHIP Stack은 초기화 과정에서 기기 등록에 필요한 값들을 생성하게 된다. 생성되는 값은 아래와 같다.

[155] - Device Discriminator: 12bit 숫자 값으로 네트워크상에서 Device(Controlee)을 검색하기 위한 식별자

[156] - Rotating ID : 18byte 값으로 2Byte 카운터 값과 16byte의 제조사가 정의한 기기의 고유 식별자

[157] - Setup PIN Code: 27bit 숫자 값으로 이후 CHIP Secure Session을 맺기 위해 사용되는 값

[158] - Proof of Possession Value: 숫자 PIN code (ex 4자리 숫자)로 사용자의 실제 기기가 있음 확인하는 용도로 사용

[159] Controlee가 기기 등록에 필요한 값을 생성하는 실시예는 아래와 같다.

[160] 1) Controlee는 Random Number Generator를 통해서 4자리 숫자인 Device Discriminator 값을 생성한다. 혹은 CHIP 규격에서 정의하는 Rotating ID (18byte)를 생성한다.

[161] 2) Controlee는 Controlee의 Unique한 값(ex, BLE MAC address, Wi-Fi MAC address등)을 추출한다.

[162] 3) Controlee는 Hash 함수(ex SHA256)의 input값으로 앞에서 생성한 Device Discriminator(혹은 Rotating ID) 값과 BLE MAC address를 concatenate한 값을 입력한다.

[163] 4) Controlee는 Hash 함수의 출력값(ex 256bit)을 생성한다.

[164] 4)-A. Controlee는 Hash 함수의 출력값의 상위 27bit를 Setup PIN Code 값으로 사용하기 위해서 내부에 저장한다.

[165] 4)-B. Controlee는 Hash 함수의 출력값의 하위 bit (12bit or 32bit)를 숫자 형태로 Proof of Possession Value로 내부에 저장한다.

[166] Controlee는 해당 값을 기반으로 BLE(Bluetooth Low Energy) Advertisement을

준비하게 된다. BLE Advertisement Packet은 CHIP 표준에서 정의한 Packet의 형태를 그대로 사용하며, Packet 내 포함되는 Device Discriminator(혹은 Rotating ID)는 앞에서 생성한 값을 포함하게 된다.

[167] Controller B는 해당하는 BLE Advertisement packet을 수신하고, 주위 Controlee 기기가 있음을 알게 된다. 이때 해당 Advertisement의 송신자인 Controlee의 MAC address을 함께 확인할 수 있다. Controller B는 해당 CHIP 기기에 대한 식별자(Device Discriminator(혹은 Rotating ID)와 BLE MAC Address를 포함하여) Cloud B에게 Controlee A를 찾았음을 알리게 된다.

[168] 만약 Controlee A가 화면이 있는 기기인 경우에 Proof of Possession 값(ex 4자리 숫자)을 화면에 보여주고 다른 기기에서 해당 숫자를 입력하여 Proof of possession 과정을 수행하게 된다.

[169] 2.3. Controller 클라우드에서 Controlee 클라우드의 계정 생성 과정

[170] 도 9는 클라우드의 계정 생성 및 연동 과정을 나타낸다.

[171] 도 9는 Controller 클라우드(Cloud B)에서 기기 검색의 결과를 Controller B에게 알리고 Controlee 클라우드(Cloud A)와 연동하는 과정을 보여준다. 본 실시예에서는 Controller B가 App(Application)으로 표현되었으나, Controller B는 스마트폰의 앱에 한정하지 않고, 인공지능 스피커, 태블릿, 월패드, TV, 로봇 등의 기기에 해당할 수 있다.

[172] Controller 클라우드인 Cloud B는 Controller B에게 Controlee A을 찾았다는 알림을 보내게 된다. 이 알림을 받은 사용자는 Controller B를 조작하여 Controlee A의 클라우드와 연동할 것인지 사용자의 확인을 받게 된다. 예를 들어, Controller B의 앱에서는 Controlee A을 찾았으니 Controlee A를 Wi-Fi 연결하기 위해서 Cloud A의 계정이 필요하다는 안내와 필요시 계정을 만들겠냐는 확인 과정을 사용자와 진행하게 된다. 사용자가 이에 대해서 동의하면 Cloud B는 Cloud A와 연동을 시작한다.

[173] 이때 Cloud B는 Cloud A의 임시 계정을 생성할 수 있으며, 해당 임시 계정을 통해서 Cloud A-Cloud B간 통신을 진행할 수 있다. 또한 사용자가 Cloud A의 계정을 이미 가지고 있다면 Controller B의 입력창에 해당 계정 정보를 입력하여 기존의 소유하고 있는 Cloud A의 계정과 Cloud B의 계정을 연동(Account Linking)할 수 있다.

[174] 2.4. Proof of Possession 과정

[175] Proof of Possession은 기기를 네트워크에 연결하고 등록하기 이전에 해당 기기가 물리적으로(physically) 사용자에게 있음을 확인하는 과정이다. 이 증명 과정을 통해서 기기의 local 존재를 확인하여 BLE을 통해서 검색되는 이웃집 기기나 로컬에 있지 않은 기기의 등록을 방지하는 기능하게 된다. 일반적으로 동일한 제조사의 기기와 해당 제조사의 App 간에는 해당 과정을 물리적인 버튼, 화면에 보이는 PIN code을 입력하거나, NFC tagging과 같이 locality 검사를 통해서 진행하게 된다.

- [176] 도 10은 Proof of Possession 과정을 나타낸다.
- [177] 본 명세서에서는 도 10과 같이 클라우드 간 Challenge 요청과 응답 과정을 통해서 짧은 숫자(ex. 4자리 숫자)의 입력을 통해서 locality check을 수행한다. 실시예에서는 Controlee A는 Display에 2.2. 절에서 생성한 Proof of Possession 값을 보여주게 된다.
- [178] Controller B는 앞서 2.2. 절과 2.3. 절에서와 같이 기기를 주변에서 찾았음을 Cloud B에게 알리게 되며, 2.3. 절에서 연동한 Cloud 간 통신을 통해서 Cloud B는 Cloud A에게 기기 등록을 위해서 기기를 찾았음을 알리게 된다. 이때 기기의 식별을 위한 Device Discriminator 혹은 Rotating ID의 값과 Controlee A의 BLE MAC Address를 함께 알려주게 된다.
- [179] 이를 받은 Cloud A는 Challenge Request를 C2C(Cloud-to-Cloud) 연결을 통해서 Cloud B에게 요청하게 된다.
- [180] 이때 Cloud A는 앞선 2.2. 절에서 Controlee가 Setup PIN Code를 생성한 것과 동일한 알고리즘에 따라서 아래 순서로 값을 생성하게 된다.
- [181] Cloud A가 값을 생성하는 실시예는 아래와 같다.
- [182] 1) Cloud A는 Device Discriminator 혹은 Rotating ID와 BLE MAC Address를 Cloud B로부터 수신한다.
- [183] 2) Cloud A는 Hash 함수(ex SHA256)의 input값으로 앞에서 생성한 Device Discriminator값 혹은 Rotating ID와 BLE MAC address를 concatenate한 값을 입력한다.
- [184] 3) Hash 함수의 출력값 (ex 256bit)
- [185] 3)-A. Cloud A는 Hash 함수의 출력값의 상위 27bit를 Setup PIN Code 값으로 사용하기 위해서 내부에 저장한다.
- [186] 3)-B. Cloud A는 하위 bit (12bit or 32bit)를 숫자 형태로 Proof of Possession Value로 내부에 저장한다.
- [187] 이렇게 생성된 Hash 함수의 출력값인 Setup PIN Code와 Proof of Possession Value는 이전 Controlee A가 생성한 값과 완벽히 동일한 값이 된다. Cloud A는 내부적으로 이 값을 저장하게 되며, 이후 Cloud B로부터 수신하는 Challenge Response의 검증(Validation)에 사용한다.
- [188] Cloud B는 Controller B를 통해서 Controlee A에 출력되고 있는 Proof of Possession 값을 Controller B에게 입력하도록 가이드하게 된다. 이때 Controller B가 사용자 입력장치 키패드가 있는 경우 해당 숫자를 입력하게 되며, 인공지능 스피커나 로봇과 같이 음성 인식이 되는 기기의 경우 사용자가 Controlee A가 보여주는 숫자를 읽음으로써 입력하게 된다. 해당 입력을 받은 Controller B는 숫자 값을 본인의 Cloud B에게 전달하게 되며, 사용자로부터 입력 받은 숫자를 포함한 Challenge Response 메시지를 Cloud B에서 Cloud A로 송신하게 된다.
- [189] Cloud A는 수신한 Challenge Response 메시지에 포함된 Proof of Possession 값을 직전에 본인이 생성한 Proof of Possession 값과 비교하게 된다. 만약 수신 값과

Cloud A의 계산 값이 동일하다면 Cloud A는 해당 기기의 실제 사용자로부터 받은 것으로 인지하고, Controlee A를 등록하기 위한 Setup PIN Code를 Cloud B에게 Challenge Confirm 메시지로 송신하게 된다. 만약 해당 값이 다르다면, Cloud A는 Reason code에 fail을 통해서 실패했음을 Cloud B에게 알리게 된다.

- [190] 본 실시예에서는 단순화를 위해서 SHA256을 통해 생성하는 알고리즘을 사용하나, 실제 Controlee A와 Cloud A는 복잡한 방법으로 값을 생성할 수 있으며, 해당 알고리즘은 같은 제조사인 Vendor A 내에서 공유되기에 외부에서 Device Discriminator 혹은 Rotating ID와 MAC address을 통해서 유추할 수 없게 된다.
- [191] 2.5. Controller B가 수신한 Setup Code를 통해 기기 등록 과정
- [192] 도 11은 Controlee 기기의 Wi-Fi 연결 및 등록 과정을 나타낸다.
- [193] 도 11은 2.4절에서 Proof of Possession 과정을 통해서 획득한 Setup PIN code를 통해서 Controller B가 Controlee A를 기기 등록(Commissioning)하는 과정에 대해서 설명한다.
- [194] Controller B는 Cloud B를 통해서 Setup PIN Code를 받게 된다. 기존 CHIP 표준에서는 해당 Setup PIN Code는 앞 장에서 설명한 것과 같이 Controller B가 Controlee A의 QR 코드 스캔을 통해서 획득하거나, 사용자가 Controlee에 적혀있는 11자리 혹은 22자리 숫자를 Controlee에 직접 입력하여 획득할 수 있었다.
- [195] 이후 Controller B는 Controlee A와 CHIP 표준과 동일하게 BLE Rendezvous 과정을 통해서 BLE Connection을 수행하게 되고, 해당 BLE 연결을 통해서 Controller B가 연결된 AP(Access Point)의 정보인 Wi-Fi Credential 정보를 Controlee A에게 전달하게 된다.
- [196] 또한 Controller B는 이전 2.3에서 설명한 것과 같이 Cloud A의 계정 정보를 Controller B로부터 수신할 수 있게 된다. 이 정보를 통해서 Controlee A는 Cloud URL 정보 및 계정 정보 혹은 Access Token을 통해서 제조사의 앱이 아니더라도 Cloud A에 login할 수 있게 된다.
- [197] Wi-Fi Credential 정보를 획득한 Controlee A는 해당 정보를 바탕으로 Controller B가 접속한 동일한 AP에 접속할 수 있게 된다. 이 후 보안 세션을 연결할 때 Controlee A는 최초 자신이 생성한 Setup PIN Code 값을 사용하고, Controller B는 본인의 Cloud B로부터 수신한 Setup PIN code 값을 사용하게 된다. 이 두 값은 완벽하게 동일한 값이므로 둘 사이에 CHIP 표준에 따른 SPAKE2+ 알고리즘에 따라서 보안 세션을 연결할 수 있게 된다.
- [198] 보안 세션 연결 후에는 CHIP 표준에서 정의한 기기 인증(Device Attestation) 과정을 통해서 기기의 인증 및 인증서 등록을 통해서 CHIP Commissioning 과정을 완료할 수 있게 된다.
- [199] 이하에서는, 도 1 내지 도 11을 참조하여, 상술한 실시예를 설명한다.
- [200] 도 12는 본 실시예에 따른 C2C 연결을 기반으로 IoT 제어기기와 IoT

피제어기기 간 등록을 설정하는 절차를 도시한 흐름도이다.

- [201] 본 실시예는 스마트홈 환경에서 C2C(Cloud-to-Cloud) 연결을 통해 IoT 제어기기와 IoT 피제어기기 간 로컬(local)에서 등록을 설정하는 방법을 제안한다. 이를 위해 사용자는 상기 IoT 피제어기기가 물리적으로 자신에게 있음을 확인하는 소유 증명 절차를 수행하는데, 상기 소유 증명 절차에 따르면 상기 IoT 제어기기는 상기 IoT 피제어기기의 로컬 존재를 확인하여, BLE를 통해 검색되는 이웃집 기기나 로컬에 있지 않는 기기의 등록을 방지할 수 있다는 효과가 있다. 후술하는 제어기기는 상기 IoT 제어기기에 대응하고, 피제어기기는 상기 IoT 피제어기기에 대응할 수 있다.
- [202] S1210 단계에서, 피제어기기(controlee)는 제어기기(controller)로부터 상기 피제어기기의 검출 정보를 수신한다.
- [203] S1220 단계에서, 상기 피제어기기는 상기 제어기기에 제1 정보를 요청하는 챌린지 요청(challenge request) 메시지를 전송한다.
- [204] S1230 단계에서, 상기 피제어기기는 상기 제어기기로부터 상기 제1 정보를 포함하는 챌린지 응답(challenge response) 메시지를 수신한다.
- [205] S1240 단계에서, 상기 피제어기기는 상기 제어기기에 챌린지 확인(challenge confirm) 메시지를 전송한다.
- [206] 상기 피제어기기는 제1 계정을 기반으로 상기 제1 클라우드와 연결되고, 상기 제어기기는 제2 계정을 기반으로 제2 클라우드와 연결된다.
- [207] 상기 피제어기기의 검출 정보, 상기 챌린지 요청 메시지, 상기 챌린지 응답 메시지 및 상기 챌린지 확인 메시지는 상기 제1 및 제2 클라우드 간 연결을 기반으로 송수신된다. 즉, 상기 정보와 메시지는 상기 피제어기기와 상기 제어기기 간의 등록을 위해 C2C 연결(상기 피제어기기의 제1 클라우드와 상기 제어기기의 제2 클라우드 간 연결)을 통해 송수신될 수 있다.
- [208] 상기 제1 정보는 소유 증명(Proof of Possession) 값이다. 상기 챌린지 확인 메시지는 상기 제1 정보를 기반으로 상기 피제어기기와 상기 제어기기 간의 등록(commissioning)에 대한 검증 결과를 포함한다.
- [209] 즉, 상기 피제어기기(또는 상기 제1 클라우드)는 상기 제어기기(또는 상기 제2 클라우드)에게 상기 소유 증명 값(숫자 4자리)을 요청할 수 있다. 이때, 상기 제2 클라우드는 사용자에게 상기 소유 증명 값을 입력하거나 말하라고 요청할 수 있고, 상기 사용자는 상기 피제어기기 또는 상기 피제어기기의 App(Application)에 상기 소유 증명 값을 입력하거나 말할 수 있다. 상기 제어기기는 상기 사용자로부터 입력 받은 소유 증명 값을 상기 제2 클라우드에게 전달할 수 있고, 상기 제2 클라우드는 상기 사용자로부터 입력 받은 소유 증명 값을 상기 챌린지 응답 메시지에 포함시켜 상기 제1 클라우드에게 전달할 수 있다.
- [210] 상기 피제어기기의 검출 정보는 제2 및 제3 정보를 포함할 수 있다. 상기 제2 정보는 상기 피제어기기의 식별을 위한 기기 판별자(device discriminator 혹은

Rotating ID) 값이고, 상기 제3 정보는 상기 피제어기기의 BLE(Bluetooth Low Energy) MAC 주소 값일 수 있다.

- [211] 상기 피제어기기는 상기 제1 클라우드를 통해 제4 및 제5 정보를 생성할 수 있다(또는, 상기 제1 클라우드가 상기 제4 및 제5 정보를 생성할 수 있다). 상기 제4 정보는 설정(Setup) PIN(Personal Identification Number) 코드 값이고, 상기 제5 정보는 상기 제1 클라우드에 의해 계산된 기기 판별자 값일 수 있다.
- [212] 상기 제5 정보가 상기 제1 정보와 동일하면, 상기 피제어기기와 상기 제어기기 간의 등록에 대한 검증 결과는 상기 제4 정보를 포함할 수 있다. 즉, 검증 성공의 결과로 상기 피제어기기(또는 상기 제1 클라우드)는 상기 제어기기(또는 상기 제2 클라우드)에게 상기 설정 PIN 코드 값을 전달할 수 있다.
- [213] 상기 제5 정보가 상기 제1 정보와 다르다면, 상기 피제어기기와 상기 제어기기 간의 등록에 대한 검증 결과는 검증 실패에 대한 이유 코드(reason code)를 포함할 수 있다. 즉, 상기 피제어기기(또는 상기 제1 클라우드)는 상기 제어기기(또는 상기 제2 클라우드)에게 상기 이유 코드로 검증 실패를 알릴 수 있다.
- [214] 상기 피제어기기는 상기 제2, 상기 제4 및 제5 정보를 기반으로 상기 제어기기와 BLE 연결을 수행할 수 있다. 상기 피제어기기는 상기 제어기기로부터 상기 BLE 연결을 통해 상기 제어기기와 연결된 AP(Access Point)의 Wi-Fi 크리덴셜(credential) 정보를 수신할 수 있다. 상기 피제어기기는 상기 Wi-Fi 크리덴셜 정보를 기반으로 상기 AP와 연결을 수행할 수 있다. 상기 피제어기기는 상기 제4 정보를 기반으로 상기 제어기기와 보안 세션을 설정할 수 있다. 상기 피제어기기는 상기 피제어기기의 인증(attestation)을 기반으로 상기 피제어기기와 상기 제어기기 간의 등록을 완료할 수 있다.
- [215] 상기 사용자가 상기 피제어기기의 전원을 인가하여 초기화 및 검색 과정을 수행하는 절차는 다음과 같다.
- [216] (사용자로부터 전원이 인가되면) 상기 피제어기기는 상기 제어기기와의 등록을 위해 상기 소유 증명 값, 상기 기기 판별자 값 및 상기 설정 PIN 코드 값을 생성할 수 있다. 상기 기기 판별자 값은 임의 숫자 생성기(Random Number Generator)에 의해 4자리 숫자로 생성될 수 있다. 상기 설정 PIN 코드 값은 해쉬(Hash) 함수의 출력 값 중 상위 27비트의 숫자로 생성될 수 있다. 상기 소유 증명 값은 상기 해쉬 함수의 출력 값 중 하위 12비트 또는 13비트의 숫자로 생성될 수 있다. 상기 해쉬 함수의 입력 값은 상기 기기 판별자 값과 상기 BLE MAC 주소 값이 연결된(concatenate) 값일 수 있다.
- [217] 상기 피제어기기는 상기 제어기기에 상기 기기 판별자 값을 포함한 BLE 광고(BLE advertisement) 메시지를 전송할 수 있다. 상기 피제어기기는 상기 BLE 광고 메시지를 기반으로 상기 제어기기와 BLE 연결을 수행할 수 있다. 상기 피제어기기의 검출 정보는 상기 BLE 연결을 기반으로 상기 제어기기에 의해 획득될 수 있다. 즉, 상기 제어기기는 상기 BLE 연결을 통해 상기 피제어기기를 검색할 수 있으나, 상기 피제어기기가 물리적으로 로컬에 있지 않더라도 검색될

수 있다는 단점이 있다. 상술한 바와 같이, C2C 연결을 통한 소유 증명 절차에 따르면, 상기 제어기기는 상기 피제어기기의 로컬 존재를 확인하여, BLE를 통해 검색되는 이웃집 기기나 로컬에 있지 않는 기기의 등록을 방지할 수 있다는 효과가 있다.

[218] 또한, 상기 제어기기의 제2 클라우드에서 상기 피제어기기의 제1 클라우드의 계정을 생성할 수도 있다. 상기 피제어기기는 상기 제어기기로부터 상기 제1 및 제2 클라우드 간 연결을 기반으로 상기 제1 계정에 대한 정보를 수신할 수 있다. 상기 제1 계정은 상기 제2 클라우드에 의해 생성된 임시 계정일 수 있다. 상기 제1 및 제2 계정은 서로 연동될 수 있다. 이로써, 클라우드 간 통신이 구축될 수 있다.

[219] **3. 장치 구성**

[220] 상술한 본 명세서의 기술적 특징은 다양한 장치 및 방법에 적용될 수 있다. 예를 들어, 상술한 본 명세서의 기술적 특징은 도 1 및/또는 도 6의 장치를 통해 수행/지원될 수 있다. 예를 들어, 상술한 본 명세서의 기술적 특징은, 도 1 및/또는 도 6의 일부에만 적용될 수 있다. 예를 들어, 상술한 본 명세서의 기술적 특징은, 도 1의 프로세싱 칩(114, 124)을 기초로 구현되거나, 도 1의 프로세서(111, 121)와 메모리(112, 122)를 기초로 구현되거나, 도 6의 프로세서(610)와 메모리(620)를 기초로 구현될 수 있다. 예를 들어, 본 명세서의 장치는, 스마트홈 환경의 무선랜 시스템에서 동작하는 장치이고, 상기 장치는 메모리 및 상기 메모리와 동작 가능하게 결합된 프로세서를 포함하되, 상기 프로세서는, 제어기기(controller)로부터 상기 피제어기기의 검출 정보를 수신하고; 상기 제어기기에 제1 정보를 요청하는 챌린지 요청(challenge request) 메시지를 전송하고; 상기 제어기기로부터 상기 제1 정보를 포함하는 챌린지 응답(challenge response) 메시지를 수신하고; 및 상기 제어기기에 챌린지 확인(challenge confirm) 메시지를 전송한다.

[221] 본 명세서의 기술적 특징은 CRM(computer readable medium)을 기초로 구현될 수 있다. 예를 들어, 본 명세서에 의해 제안되는 CRM은 적어도 하나의 프로세서(processor)에 의해 실행됨을 기초로 하는 명령어(instruction)를 포함하는 적어도 하나의 컴퓨터로 읽을 수 있는 기록매체(computer readable medium)이다.

[222] 상기 CRM은, 제어기기(controller)로부터 상기 피제어기기의 검출 정보를 수신하는 단계; 상기 제어기기에 제1 정보를 요청하는 챌린지 요청(challenge request) 메시지를 전송하는 단계; 상기 제어기기로부터 상기 제1 정보를 포함하는 챌린지 응답(challenge response) 메시지를 수신하는 단계; 및 상기 제어기기에 챌린지 확인(challenge confirm) 메시지를 전송하는 단계를 포함하는 동작(operations)을 수행하는 명령어(instructions)를 저장할 수 있다. 본 명세서의 CRM 내에 저장되는 명령어는 적어도 하나의 프로세서에 의해 실행(execute)될 수 있다. 본 명세서의 CRM에 관련된 적어도 하나의 프로세서는 도 1의 프로세서(111, 121) 또는 프로세싱 칩(114, 124)이거나, 도 6의

프로세서(610)일 수 있다. 한편, 본 명세서의 CRM은 도 1의 메모리(112, 122)이거나 도 6의 메모리(620)이거나, 별도의 외부 메모리/저장매체/디스크 등일 수 있다.

- [223] 상술한 본 명세서의 기술적 특징은 다양한 응용예(application)나 비즈니스 모델에 적용 가능하다. 예를 들어, 인공 지능(Artificial Intelligence: AI)을 지원하는 장치에서의 무선 통신을 위해 상술한 기술적 특징이 적용될 수 있다.
- [224] 인공 지능은 인공적인 지능 또는 이를 만들 수 있는 방법론을 연구하는 분야를 의미하며, 머신 러닝(기계 학습, Machine Learning)은 인공 지능 분야에서 다루는 다양한 문제를 정의하고 그것을 해결하는 방법론을 연구하는 분야를 의미한다. 머신 러닝은 어떠한 작업에 대하여 꾸준한 경험을 통해 그 작업에 대한 성능을 높이는 알고리즘으로 정의하기도 한다.
- [225] 인공 신경망(Artificial Neural Network; ANN)은 머신 러닝에서 사용되는 모델로써, 시냅스의 결합으로 네트워크를 형성한 인공 뉴런(노드)들로 구성되는, 문제 해결 능력을 가지는 모델 전반을 의미할 수 있다. 인공 신경망은 다른 레이어의 뉴런들 사이의 연결 패턴, 모델 파라미터를 갱신하는 학습 과정, 출력값을 생성하는 활성화 함수(Activation Function)에 의해 정의될 수 있다.
- [226] 인공 신경망은 입력층(Input Layer), 출력층(Output Layer), 그리고 선택적으로 하나 이상의 은닉층(Hidden Layer)를 포함할 수 있다. 각 층은 하나 이상의 뉴런을 포함하고, 인공 신경망은 뉴런과 뉴런을 연결하는 시냅스를 포함할 수 있다. 인공 신경망에서 각 뉴런은 시냅스를 통해 입력되는 입력 신호들, 가중치, 편향에 대한 활성화 함수의 함숫값을 출력할 수 있다.
- [227] 모델 파라미터는 학습을 통해 결정되는 파라미터를 의미하며, 시냅스 연결의 가중치와 뉴런의 편향 등이 포함된다. 그리고, 하이퍼파라미터는 머신 러닝 알고리즘에서 학습 전에 설정되어야 하는 파라미터를 의미하며, 학습률(Learning Rate), 반복 횟수, 미니 배치 크기, 초기화 함수 등이 포함된다.
- [228] 인공 신경망의 학습의 목적은 손실 함수를 최소화하는 모델 파라미터를 결정하는 것으로 볼 수 있다. 손실 함수는 인공 신경망의 학습 과정에서 최적의 모델 파라미터를 결정하기 위한 지표로 이용될 수 있다.
- [229] 머신 러닝은 학습 방식에 따라 지도 학습(Supervised Learning), 비지도 학습(Unsupervised Learning), 강화 학습(Reinforcement Learning), 준 지도 학습(Semi-supervised Learning)으로 분류할 수 있다.
- [230] 지도 학습은 학습 데이터에 대한 레이블(label)이 주어진 상태에서 인공 신경망을 학습시키는 방법을 의미하며, 레이블이란 학습 데이터가 인공 신경망에 입력되는 경우 인공 신경망이 추론해 내야 하는 정답(또는 결과 값)을 의미할 수 있다. 비지도 학습은 학습 데이터에 대한 레이블이 주어지지 않는 상태에서 인공 신경망을 학습시키는 방법을 의미할 수 있다. 강화 학습은 어떤 환경 안에서 정의된 에이전트가 각 상태에서 누적 보상을 최대화하는 행동 혹은 행동 순서를 선택하도록 학습시키는 학습 방법을 의미할 수 있다.

- [231] 인공 신경망 중에서 복수의 은닉층을 포함하는 심층 신경망(DNN: Deep Neural Network)으로 구현되는 머신 러닝을 딥 러닝(심층 학습, Deep Learning)이라 부르기도 하며, 딥 러닝은 머신 러닝의 일부이다. 이하에서, 머신 러닝은 딥 러닝을 포함하는 의미로 사용된다.
- [232] 또한 상술한 기술적 특징은 로봇의 무선 통신에 적용될 수 있다.
- [233] 로봇은 스스로 보유한 능력에 의해 주어진 일을 자동으로 처리하거나 작동하는 기계를 의미할 수 있다. 특히, 환경을 인식하고 스스로 판단하여 동작을 수행하는 기능을 갖는 로봇을 지능형 로봇이라 칭할 수 있다.
- [234] 로봇은 사용 목적이나 분야에 따라 산업용, 의료용, 가정용, 군사용 등으로 분류할 수 있다. 로봇은 액츄에이터 또는 모터를 포함하는 구동부를 구비하여 로봇 관절을 움직이는 등의 다양한 물리적 동작을 수행할 수 있다. 또한, 이동 가능한 로봇은 구동부에 휠, 브레이크, 프로펠러 등이 포함되어, 구동부를 통해 지상에서 주행하거나 공중에서 비행할 수 있다.
- [235] 또한 상술한 기술적 특징은 확장 현실을 지원하는 장치에 적용될 수 있다.
- [236] 확장 현실은 가상 현실(VR: Virtual Reality), 증강 현실(AR: Augmented Reality), 혼합 현실(MR: Mixed Reality)을 총칭한다. VR 기술은 현실 세계의 객체나 배경 등을 CG 영상으로만 제공하고, AR 기술은 실제 사물 영상 위에 가상으로 만들어진 CG 영상을 함께 제공하며, MR 기술은 현실 세계에 가상 객체들을 섞고 결합시켜서 제공하는 컴퓨터 그래픽 기술이다.
- [237] MR 기술은 현실 객체와 가상 객체를 함께 보여준다는 점에서 AR 기술과 유사하다. 그러나, AR 기술에서는 가상 객체가 현실 객체를 보완하는 형태로 사용되는 반면, MR 기술에서는 가상 객체와 현실 객체가 동등한 성격으로 사용된다는 점에서 차이점이 있다.
- [238] XR 기술은 HMD(Head-Mount Display), HUD(Head-Up Display), 휴대폰, 태블릿 PC, 랩탑, 데스크탑, TV, 디지털 사이니지 등에 적용될 수 있고, XR 기술이 적용된 장치를 XR 장치(XR Device)라 칭할 수 있다.
- [239] 본 명세서에 기재된 청구항들은 다양한 방식으로 조합될 수 있다. 예를 들어, 본 명세서의 방법 청구항의 기술적 특징이 조합되어 장치로 구현될 수 있고, 본 명세서의 장치 청구항의 기술적 특징이 조합되어 방법으로 구현될 수 있다. 또한, 본 명세서의 방법 청구항의 기술적 특징과 장치 청구항의 기술적 특징이 조합되어 장치로 구현될 수 있고, 본 명세서의 방법 청구항의 기술적 특징과 장치 청구항의 기술적 특징이 조합되어 방법으로 구현될 수 있다.

청구범위

- [청구항 1] 스마트홈 환경의 무선랜 시스템에서,
 피제어기기(controlee)가, 제어기기(controller)로부터 상기 피제어기기의
 검출 정보를 수신하는 단계;
 상기 피제어기기가, 상기 제어기기에 제1 정보를 요청하는 챌린지
 요청(challenge request) 메시지를 전송하는 단계;
 상기 피제어기기가, 상기 제어기기로부터 상기 제1 정보를 포함하는
 챌린지 응답(challenge response) 메시지를 수신하는 단계; 및
 상기 피제어기기가, 상기 제어기기에 챌린지 확인(challenge confirm)
 메시지를 전송하는 단계를 포함하되,
 상기 피제어기기는 제1 계정을 기반으로 상기 제1 클라우드와 연결되고,
 상기 제어기기는 제2 계정을 기반으로 제2 클라우드와 연결되고,
 상기 피제어기기의 검출 정보, 상기 챌린지 요청 메시지, 상기 챌린지
 응답 메시지 및 상기 챌린지 확인 메시지는 상기 제1 및 제2 클라우드 간
 연결을 기반으로 송수신되고,
 상기 제1 정보는 소유 증명(Proof of Possession) 값이고, 및
 상기 챌린지 확인 메시지는 상기 제1 정보를 기반으로 상기 피제어기기와
 상기 제어기기 간의 등록(commissioning)에 대한 검증 결과를 포함하는
 방법.
- [청구항 2] 제1항에 있어서,
 상기 피제어기기의 검출 정보는 제2 및 제3 정보를 포함하고,
 상기 제2 정보는 상기 피제어기기의 식별을 위한 기기 판별자(device
 discriminator 또는 Rotating Identifier) 값이고,
 상기 제3 정보는 상기 피제어기기의 BLE(Bluetooth Low Energy) MAC
 주소 값인
 방법.
- [청구항 3] 제2항에 있어서,
 상기 피제어기기가, 상기 제1 클라우드를 통해 제4 및 제5 정보를
 생성하는 단계를 더 포함하되,
 상기 제5 정보가 상기 제1 정보와 동일하면, 상기 피제어기기와 상기
 제어기기 간의 등록에 대한 검증 결과는 상기 제4 정보를 포함하고,
 상기 제5 정보가 상기 제1 정보와 다르다면, 상기 피제어기기와 상기
 제어기기 간의 등록에 대한 검증 결과는 검증 실패에 대한 이유
 코드(reason code)를 포함하고,
 상기 제4 정보는 설정(Setup) PIN(Personal Identification Number) 코드
 값이고,
 상기 제5 정보는 상기 제1 클라우드에 의해 계산된 기기 판별자 값인

- 방법.
- [청구항 4] 제3항에 있어서,
 상기 피제어기기가, 상기 제2, 상기 제4 및 제5 정보를 기반으로 상기 제어기기와 BLE 연결을 수행하는 단계;
 상기 피제어기기가, 상기 제어기기로부터 상기 BLE 연결을 통해 상기 제어기기와 연결된 AP(Access Point)의 Wi-Fi 크리덴셜(credential) 정보를 수신하는 단계;
 상기 피제어기기가, 상기 Wi-Fi 크리덴셜 정보를 기반으로 상기 AP와 연결을 수행하는 단계;
 상기 피제어기기가, 상기 제4 정보를 기반으로 상기 제어기기와 보안 세션을 설정하는 단계; 및
 상기 피제어기기가, 상기 피제어기기의 인증(attestation)을 기반으로 상기 피제어기기와 상기 제어기기 간의 등록을 완료하는 단계를 더 포함하는 방법.
- [청구항 5] 제3항에 있어서,
 상기 피제어기기가, 상기 제어기기와의 등록을 위해 상기 소유 증명 값, 상기 기기 판별자 값 및 상기 설정 PIN 코드 값을 생성하는 단계를 더 포함하되,
 상기 기기 판별자 값은 임의 숫자 생성기(Random Number Generator)에 의해 4자리 숫자로 생성되고,
 상기 설정 PIN 코드 값은 해쉬(Hash) 함수의 출력 값 중 상위 27비트의 숫자로 생성되고,
 상기 소유 증명 값은 상기 해쉬 함수의 출력 값 중 하위 12비트 또는 13비트의 숫자로 생성되고,
 상기 해쉬 함수의 입력 값은 상기 기기 판별자 값과 상기 BLE MAC 주소 값이 연결된(concatenate) 값인 방법.
- [청구항 6] 제5항에 있어서,
 상기 피제어기기가, 상기 제어기기에 상기 기기 판별자 값을 포함한 BLE 광고(BLE advertisement) 메시지를 전송하는 단계; 및
 상기 피제어기기가, 상기 BLE 광고 메시지를 기반으로 상기 제어기기와 BLE 연결을 수행하는 단계를 더 포함하되,
 상기 피제어기기의 검출 정보는 상기 BLE 연결을 기반으로 상기 제어기기에 의해 획득되는 방법.
- [청구항 7] 제1항에 있어서,
 상기 피제어기기가, 상기 제어기기로부터 상기 제1 및 제2 클라우드 간 연결을 기반으로 상기 제1 계정에 대한 정보를 수신하는 단계를 더

포함하되,
 상기 제1 계정은 상기 제2 클라우드에 의해 생성된 임시 계정이고,
 상기 제1 및 제2 계정은 서로 연동되는
 방법.

- [청구항 8] 스마트홈 환경의 무선랜 시스템에서 피제어기기(controlee)에 있어서,
 메모리;
 트랜시버; 및
 상기 메모리 및 상기 트랜시버와 동작 가능하게 결합된 프로세서를
 포함하되, 상기 프로세서는:
 제어기기(controller)로부터 상기 피제어기기의 검출 정보를 수신하고;
 상기 제어기기에게 제1 정보를 요청하는 챌린지 요청(challenge request)
 메시지를 전송하고;
 상기 제어기기로부터 상기 제1 정보를 포함하는 챌린지 응답(challenge
 response) 메시지를 수신하고; 및
 상기 제어기기에게 챌린지 확인(challenge confirm) 메시지를 전송하되,
 상기 피제어기기는 제1 계정을 기반으로 상기 제1 클라우드와 연결되고,
 상기 제어기기는 제2 계정을 기반으로 제2 클라우드와 연결되고,
 상기 피제어기기의 검출 정보, 상기 챌린지 요청 메시지, 상기 챌린지
 응답 메시지 및 상기 챌린지 확인 메시지는 상기 제1 및 제2 클라우드 간
 연결을 기반으로 송수신되고,
 상기 제1 정보는 소유 증명(Proof of Possession) 값이고, 및
 상기 챌린지 확인 메시지는 상기 제1 정보를 기반으로 상기 피제어기기와
 상기 제어기기 간의 등록(commissioning)에 대한 검증 결과를 포함하는
 피제어기기.
- [청구항 9] 제8항에 있어서,
 상기 피제어기기의 검출 정보는 제2 및 제3 정보를 포함하고,
 상기 제2 정보는 상기 피제어기기의 식별을 위한 기기 판별자(device
 discriminator 또는 Rotating Identifier) 값이고,
 상기 제3 정보는 상기 피제어기기의 BLE(Bluetooth Low Energy) MAC
 주소 값인
 피제어기기.
- [청구항 10] 제9항에 있어서,
 상기 프로세서는, 상기 제1 클라우드를 통해 제4 및 제5 정보를 생성하되,
 상기 제5 정보가 상기 제1 정보와 동일하면, 상기 피제어기기와 상기
 제어기기 간의 등록에 대한 검증 결과는 상기 제4 정보를 포함하고,
 상기 제5 정보가 상기 제1 정보와 다르다면, 상기 피제어기기와 상기
 제어기기 간의 등록에 대한 검증 결과는 검증 실패에 대한 이유
 코드(reason code)를 포함하고,

상기 제4 정보는 설정(Setup) PIN(Personal Identification Number) 코드 값이고,

상기 제5 정보는 상기 제1 클라우드에 의해 계산된 기기 판별자 값인 피제어기기.

[청구항 11] 제10항에 있어서,
상기 프로세서는:
상기 제2, 상기 제4 및 제5 정보를 기반으로 상기 제어기기와 BLE 연결을 수행하고;
상기 제어기기로부터 상기 BLE 연결을 통해 상기 제어기기와 연결된 AP(Access Point)의 Wi-Fi 크리덴셜(credential) 정보를 수신하고;
상기 Wi-Fi 크리덴셜 정보를 기반으로 상기 AP와 연결을 수행하고;
상기 제4 정보를 기반으로 상기 제어기기와 보안 세션을 설정하고; 및
상기 피제어기기의 인증(attestation)을 기반으로 상기 피제어기기와 상기 제어기기 간의 등록을 완료하는
피제어기기.

[청구항 12] 제10항에 있어서,
상기 프로세서는, 상기 제어기기와의 등록을 위해 상기 소유 증명 값, 상기 기기 판별자 값 및 상기 설정 PIN 코드 값을 생성하되,
상기 기기 판별자 값은 임의 숫자 생성기(Random Number Generator)에 의해 4자리 숫자로 생성되고,
상기 설정 PIN 코드 값은 해쉬(Hash) 함수의 출력 값 중 상위 27비트의 숫자로 생성되고,
상기 소유 증명 값은 상기 해쉬 함수의 출력 값 중 하위 12비트 또는 13비트의 숫자로 생성되고,
상기 해쉬 함수의 입력 값은 상기 기기 판별자 값과 상기 BLE MAC 주소 값이 연결된(concatenate) 값인
피제어기기.

[청구항 13] 제12항에 있어서,
상기 프로세서는:
상기 제어기기에 상기 기기 판별자 값을 포함한 BLE 광고(BLE advertisement) 메시지를 전송하고; 및
상기 BLE 광고 메시지를 기반으로 상기 제어기기와 BLE 연결을 수행하되,
상기 피제어기기의 검출 정보는 상기 BLE 연결을 기반으로 상기 제어기기에 의해 획득되는
방법.

[청구항 14] 제8항에 있어서,
상기 프로세서는, 상기 제어기기로부터 상기 제1 및 제2 클라우드 간

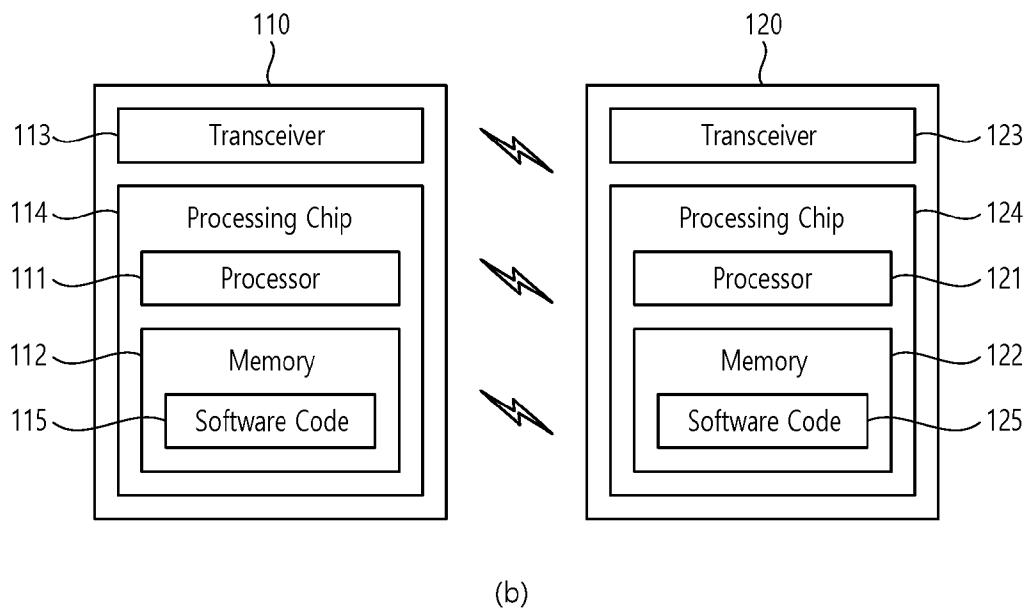
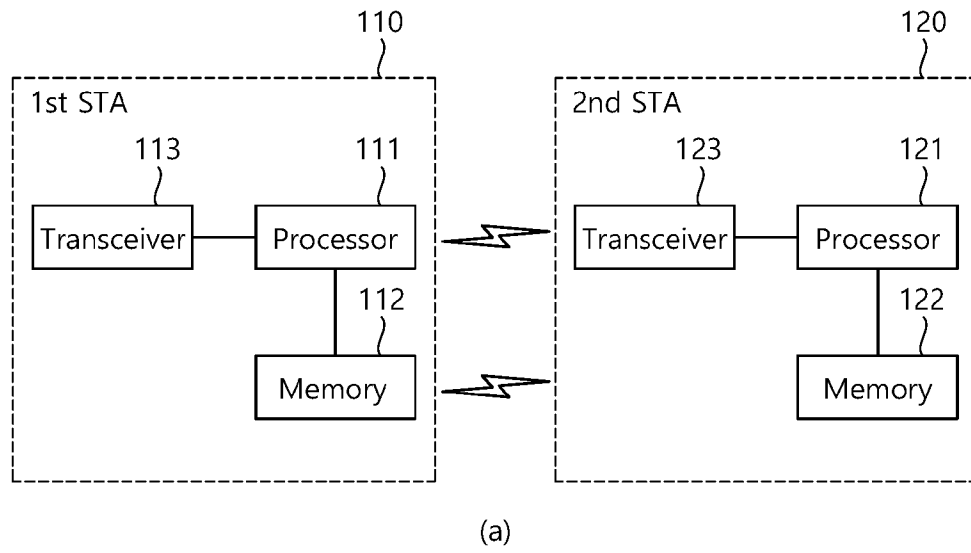
연결을 기반으로 상기 제1 계정에 대한 정보를 수신하되,
 상기 제1 계정은 상기 제2 클라우드에 의해 생성된 임시 계정이고,
 상기 제1 및 제2 계정은 서로 연동되는
 피제어기기.

- [청구항 15] 적어도 하나의 프로세서(processor)에 의해 실행됨을 기초로 하는 명령어(instruction)를 포함하는 적어도 하나의 컴퓨터로 읽을 수 있는 기록매체(computer readable medium)에 있어서,
 제어기기(controller)로부터 상기 피제어기기의 검출 정보를 수신하는 단계;
 상기 제어기기에게 제1 정보를 요청하는 챌린지 요청(challenge request) 메시지를 전송하는 단계;
 상기 제어기기로부터 상기 제1 정보를 포함하는 챌린지 응답(challenge response) 메시지를 수신하는 단계; 및
 상기 제어기기에게 챌린지 확인(challenge confirm) 메시지를 전송하는 단계를 포함하되,
 피제어기기(controlee)는 제1 계정을 기반으로 상기 제1 클라우드와 연결되고,
 상기 제어기기는 제2 계정을 기반으로 제2 클라우드와 연결되고,
 상기 피제어기기의 검출 정보, 상기 챌린지 요청 메시지, 상기 챌린지 응답 메시지 및 상기 챌린지 확인 메시지는 상기 제1 및 제2 클라우드 간 연결을 기반으로 송수신되고,
 상기 제1 정보는 소유 증명(Proof of Possession) 값이고, 및
 상기 챌린지 확인 메시지는 상기 제1 정보를 기반으로 상기 피제어기기와 상기 제어기기 간의 등록(commissioning)에 대한 검증 결과를 포함하는 기록매체.

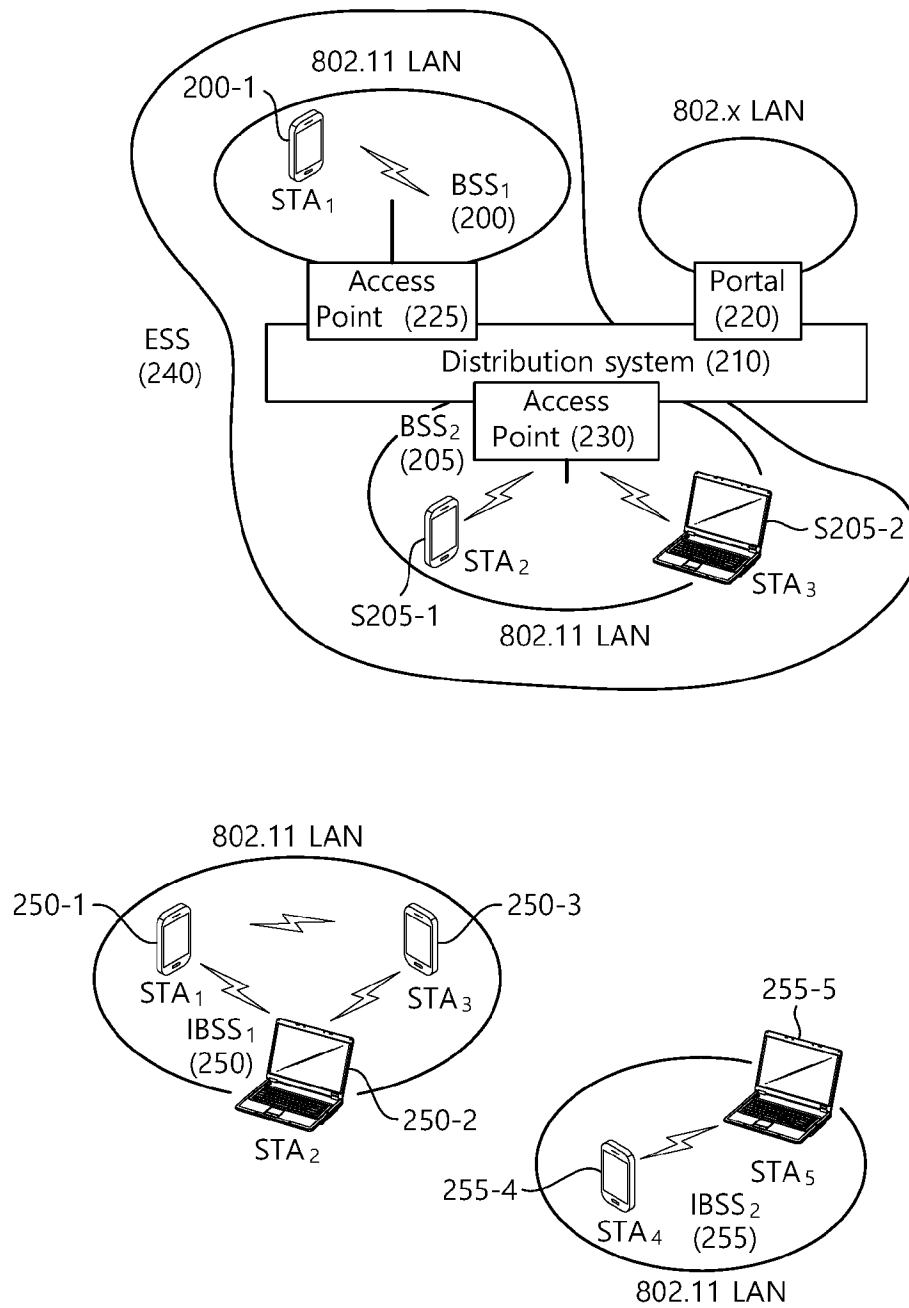
- [청구항 16] 스마트홈 환경의 무선랜 시스템에서 장치에 있어서,
 메모리; 및
 상기 메모리와 동작 가능하게 결합된 프로세서를 포함하되, 상기 프로세서는:
 제어기기(controller)로부터 상기 피제어기기의 검출 정보를 수신하고;
 상기 제어기기에게 제1 정보를 요청하는 챌린지 요청(challenge request) 메시지를 전송하고;
 상기 제어기기로부터 상기 제1 정보를 포함하는 챌린지 응답(challenge response) 메시지를 수신하고; 및
 상기 제어기기에게 챌린지 확인(challenge confirm) 메시지를 전송하되,
 피제어기기(controlee)는 제1 계정을 기반으로 상기 제1 클라우드와 연결되고,
 상기 제어기기는 제2 계정을 기반으로 제2 클라우드와 연결되고,

상기 피제어기기의 검출 정보, 상기 챌린지 요청 메시지, 상기 챌린지 응답 메시지 및 상기 챌린지 확인 메시지는 상기 제1 및 제2 클라우드 간 연결을 기반으로 송수신되고,
상기 제1 정보는 소유 증명(Proof of Possession) 값이고, 및
상기 챌린지 확인 메시지는 상기 제1 정보를 기반으로 상기 피제어기와 상기 제어기기 간의 등록(commissioning)에 대한 검증 결과를 포함하는 장치.

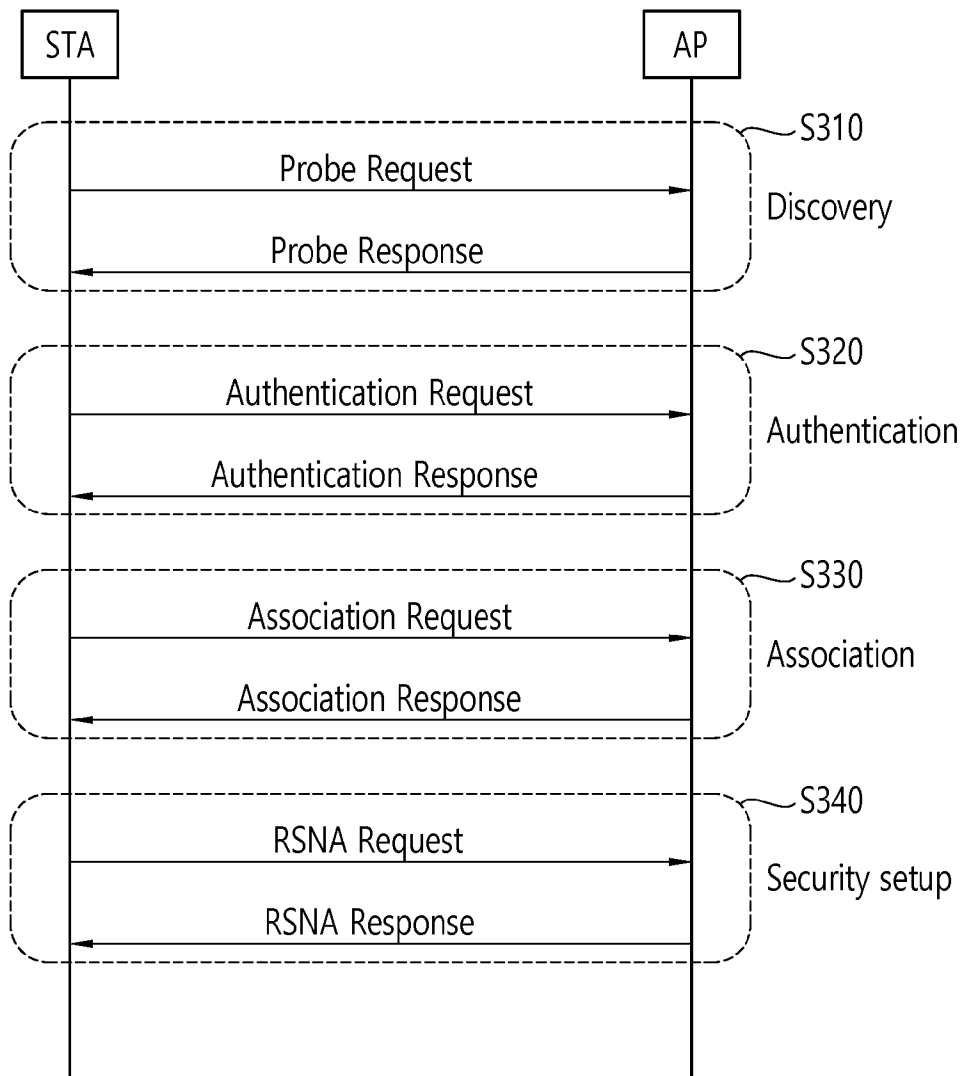
[도 1]



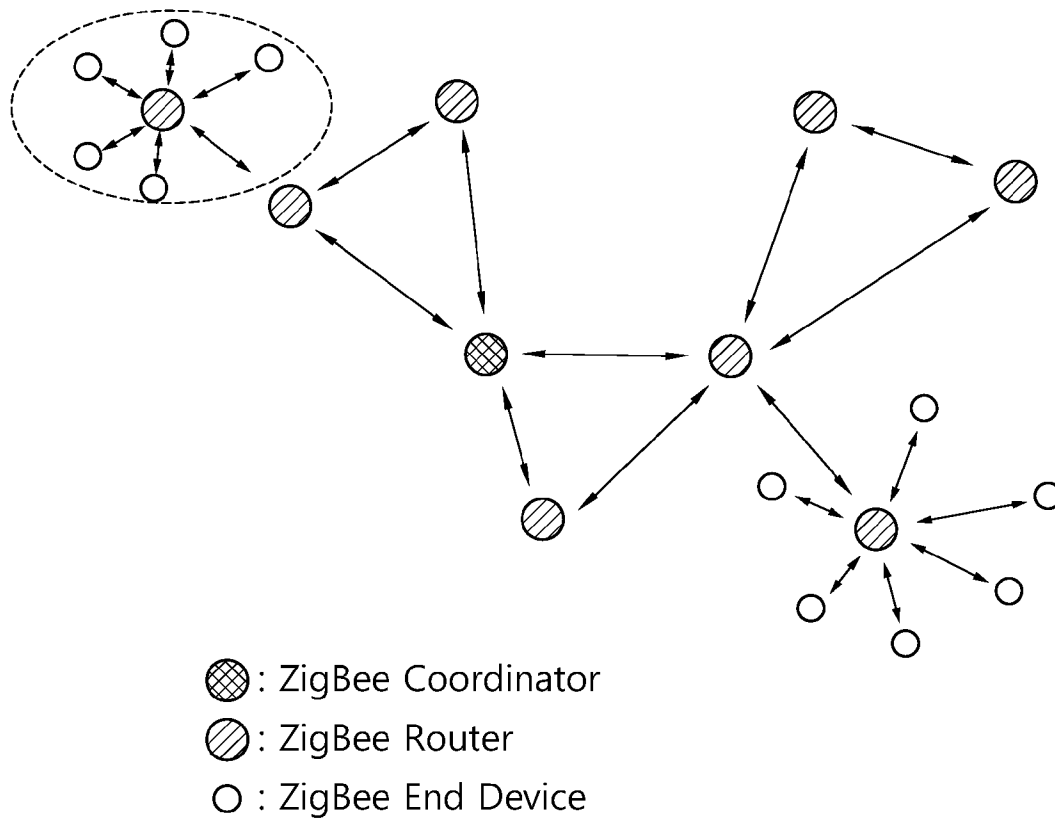
[도2]



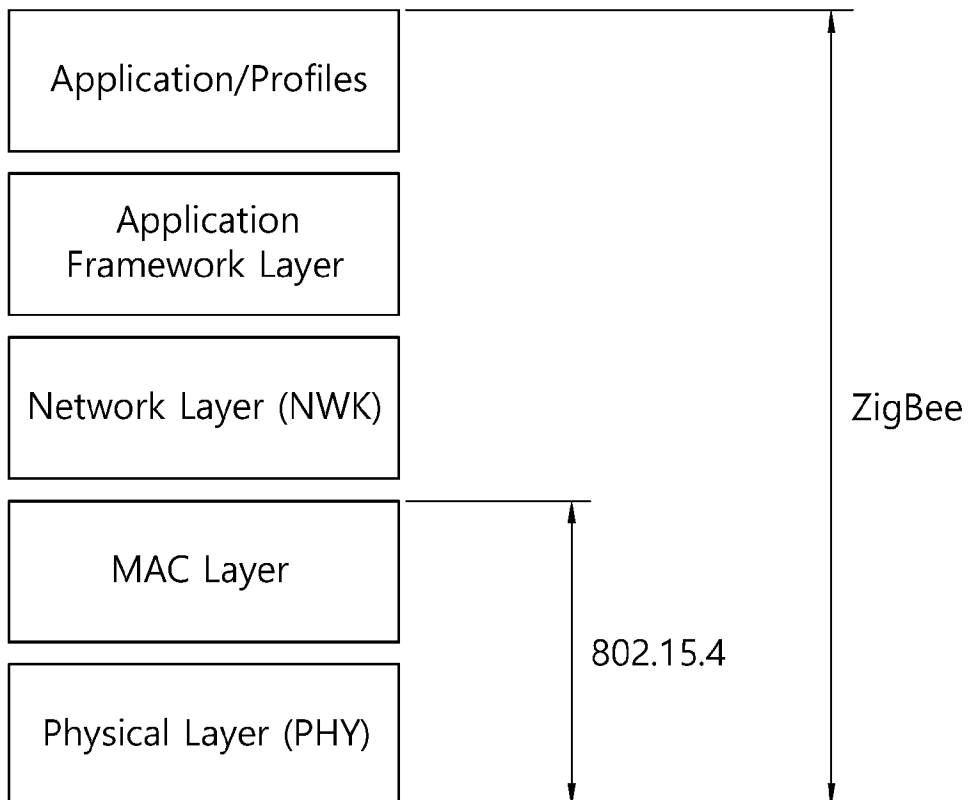
[도3]



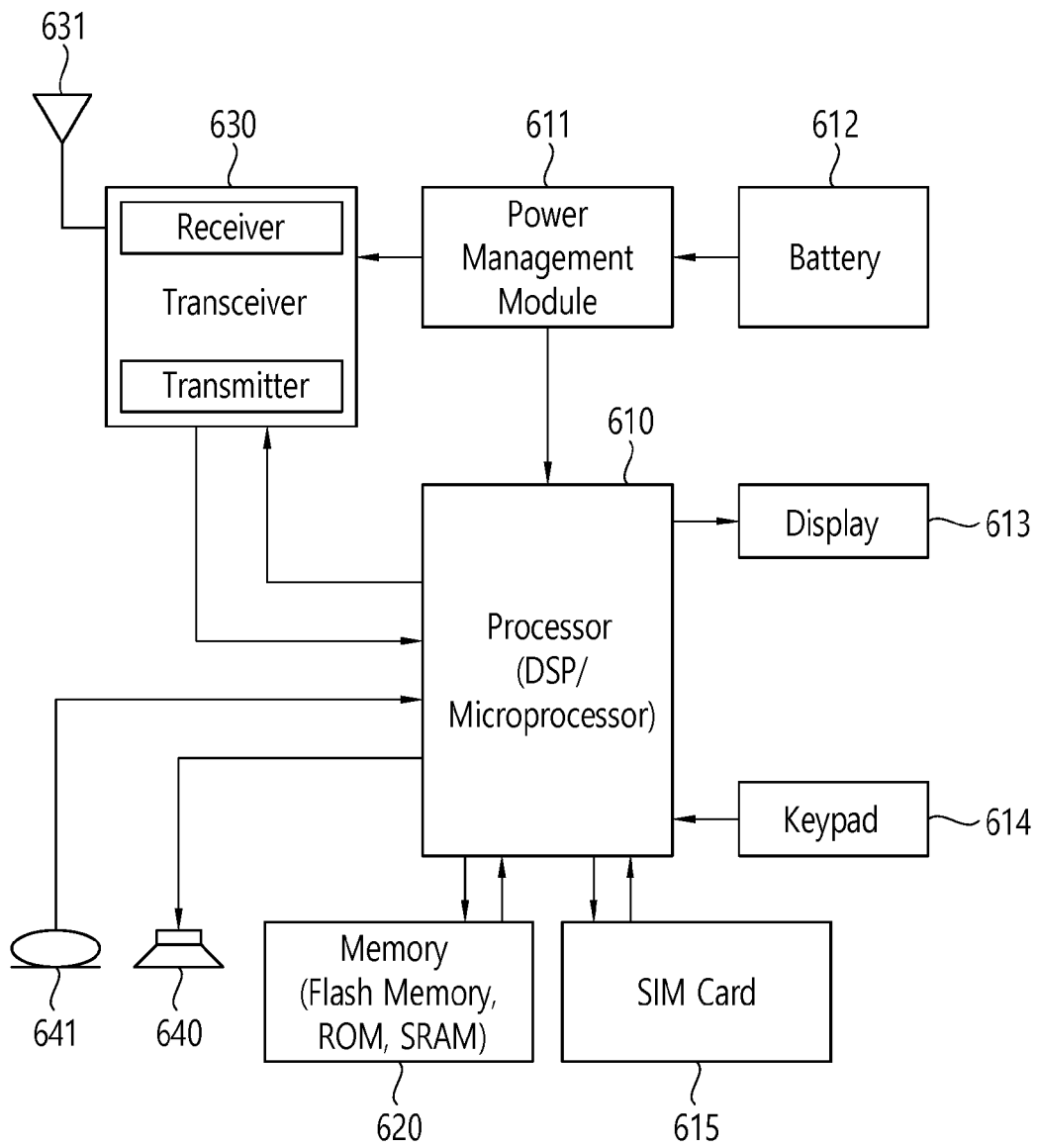
[도4]



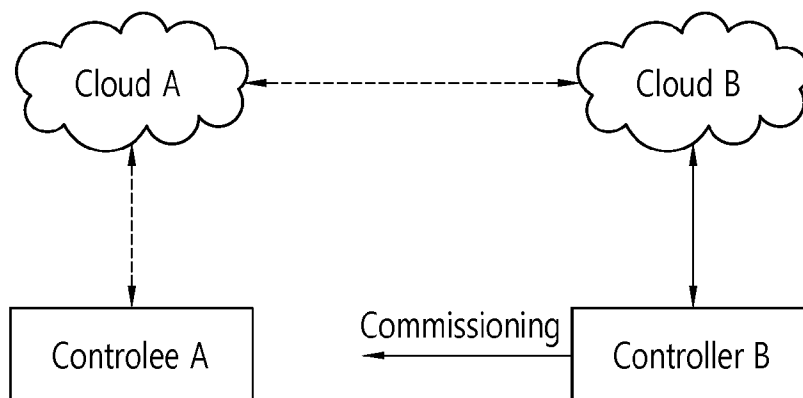
[도5]



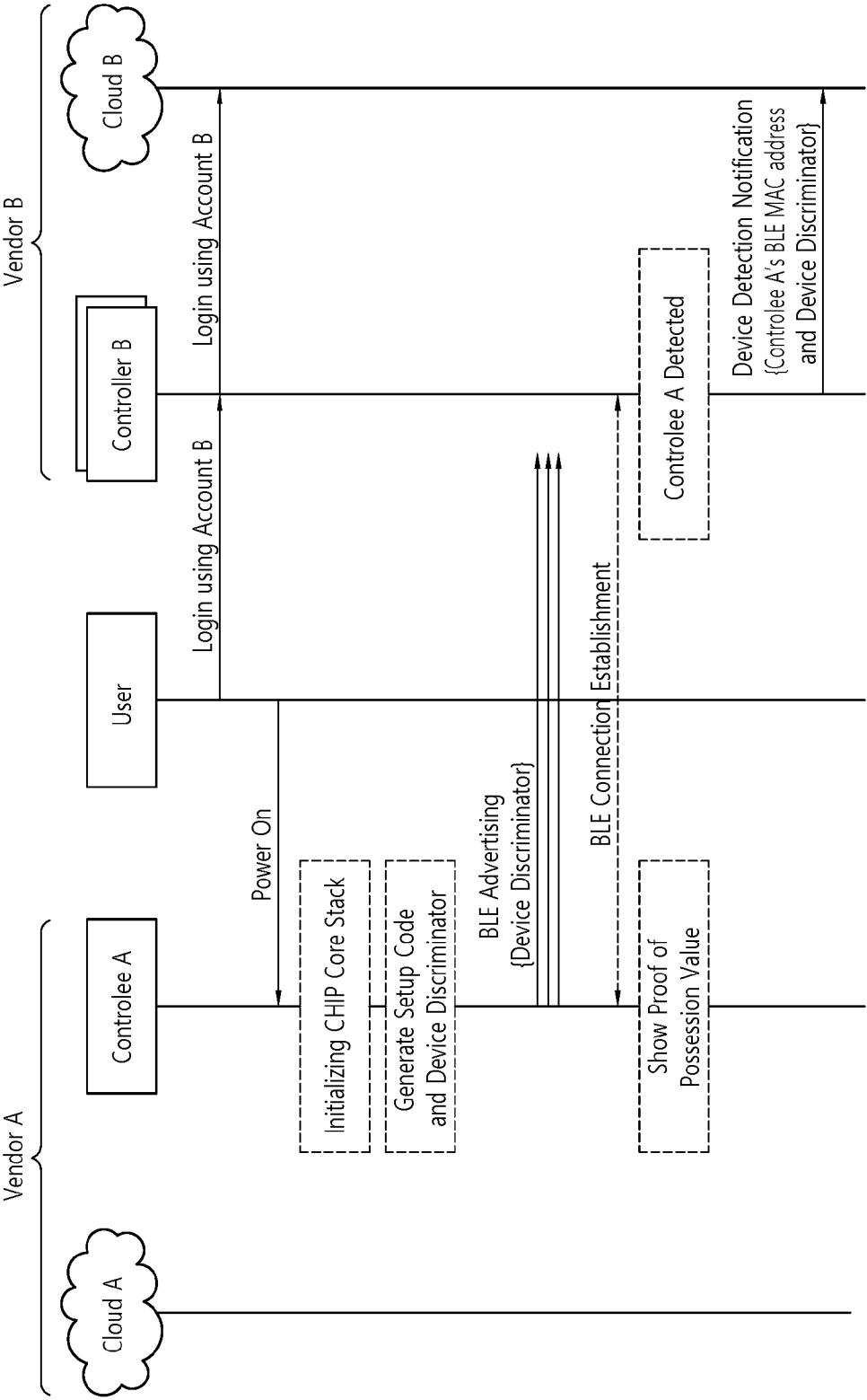
[도6]



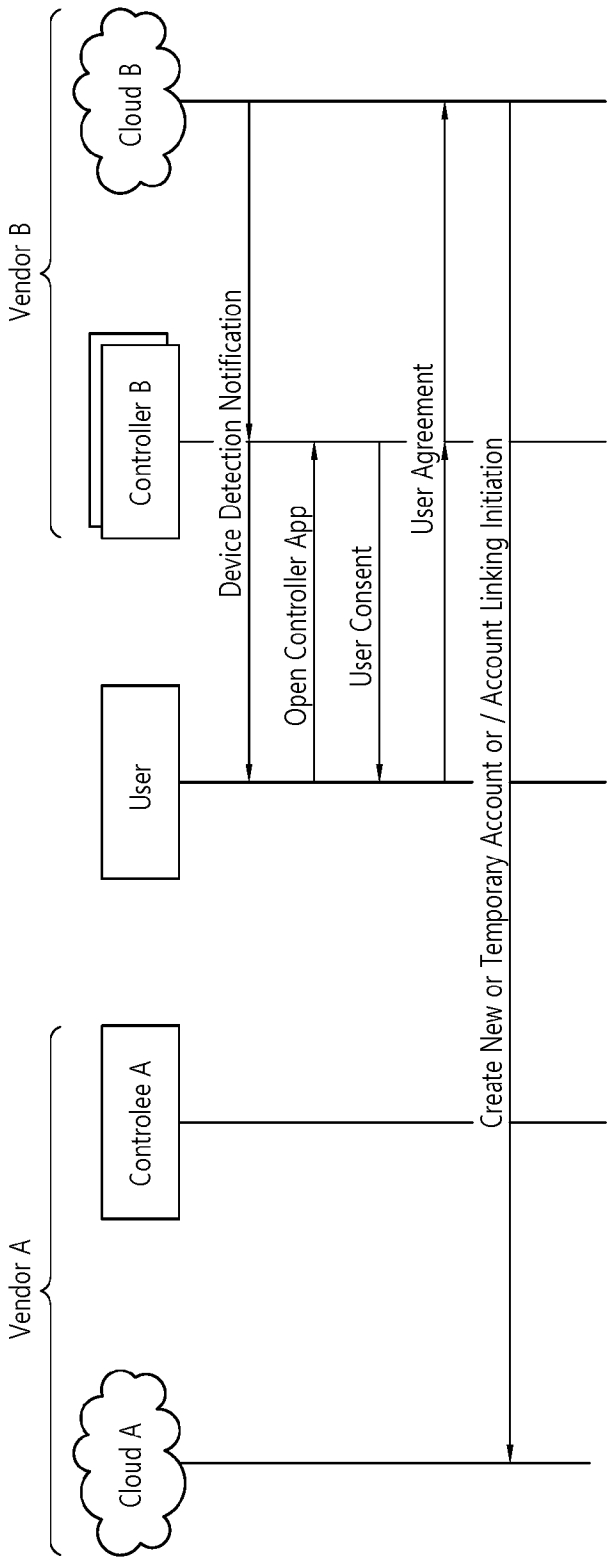
[도7]



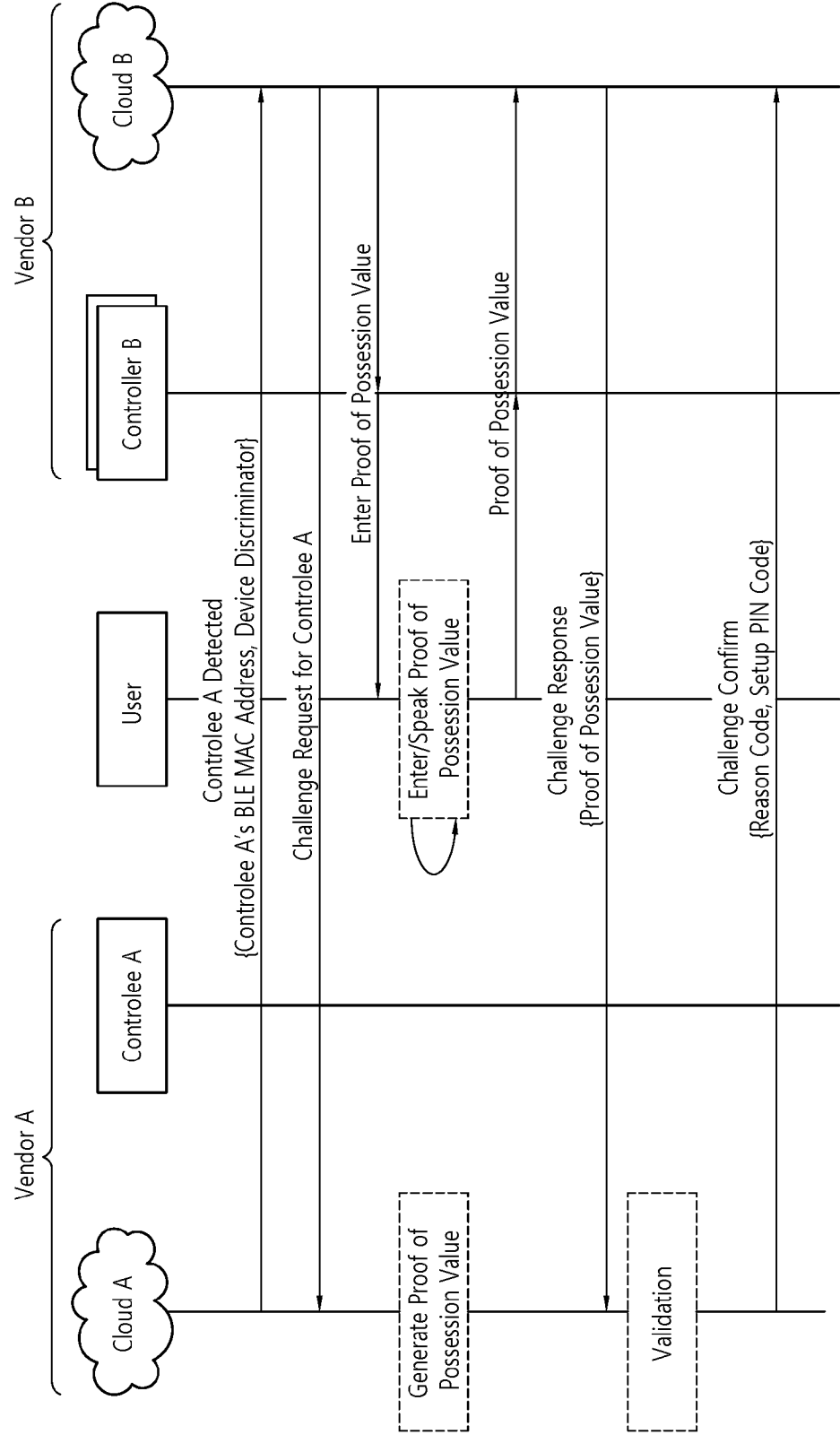
[도8]



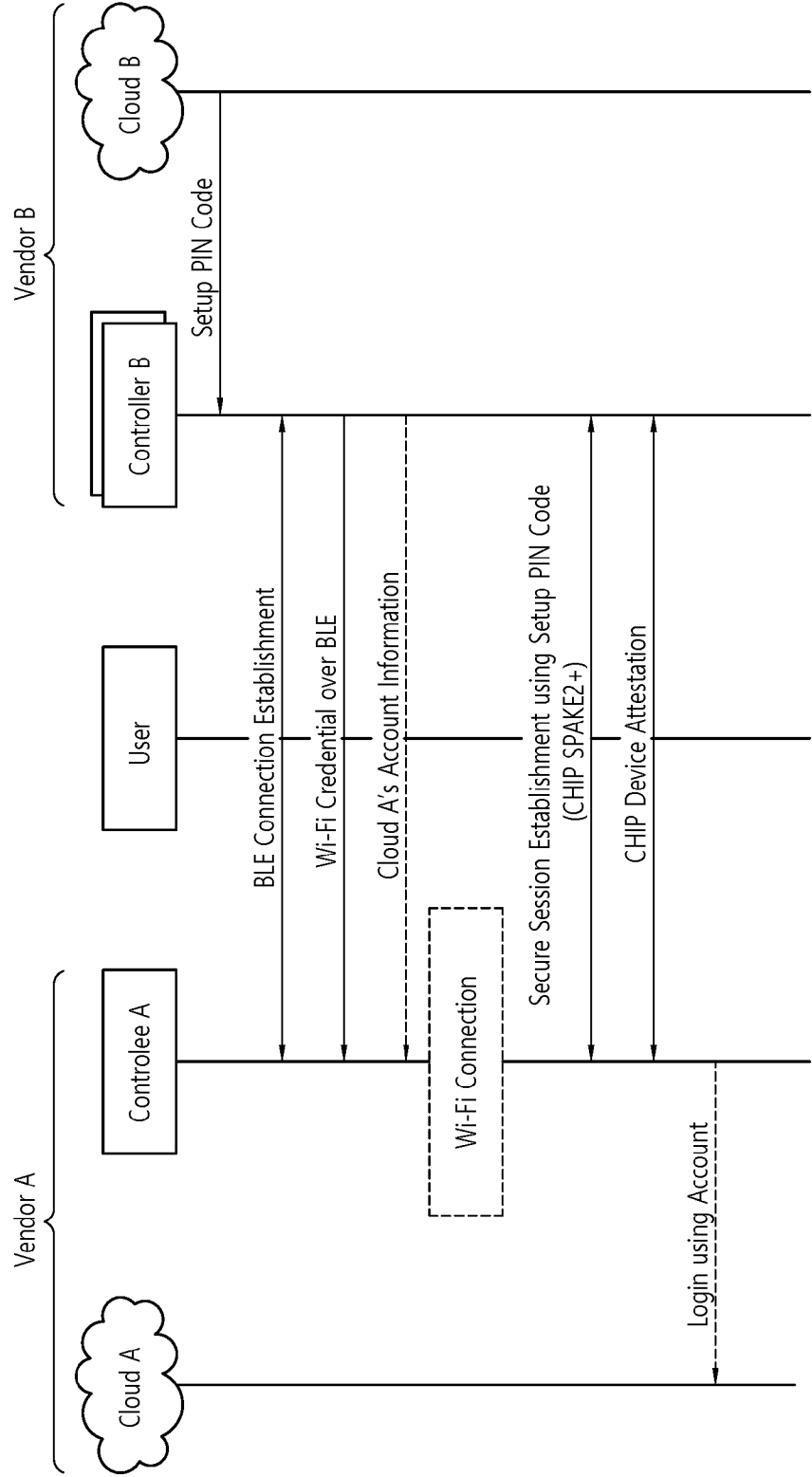
[도9]



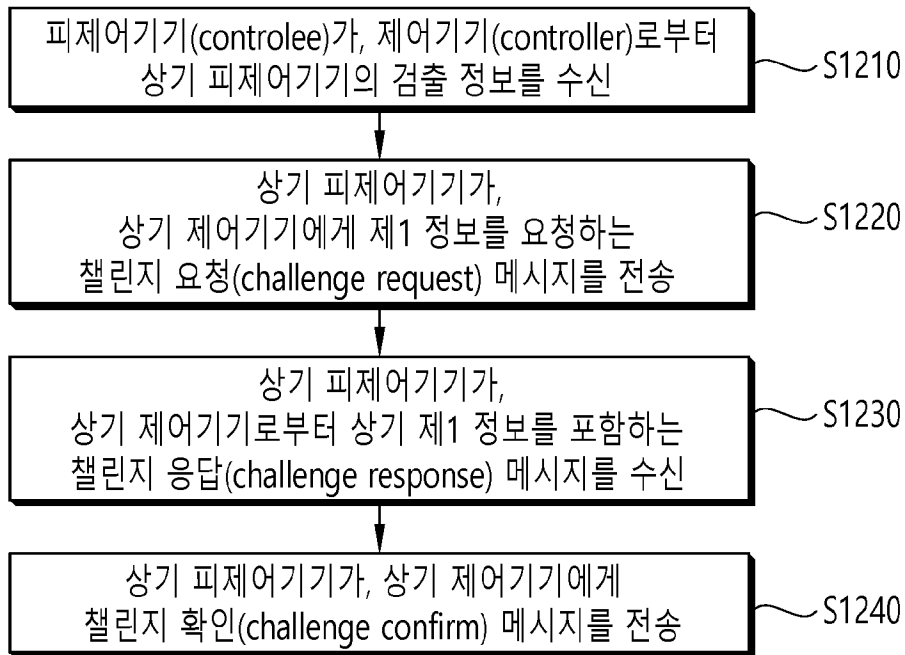
[도10]



[도11]



[도12]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2021/017482

A. CLASSIFICATION OF SUBJECT MATTER**H04L 61/00**(2022.01)i; **H04L 9/40**(2022.01)i; **H04L 9/32**(2006.01)i; **H04W 4/80**(2018.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L 61/00(2022.01); H04L 12/28(2006.01); H04L 29/06(2006.01); H04L 29/08(2006.01); H04L 9/32(2006.01);
H04W 76/10(2018.01)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean utility models and applications for utility models: IPC as above
Japanese utility models and applications for utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & keywords: 클라우드(cloud), 피제어기기(controlee), 챌린지 확인(challenge confirm), 소유
증명(proof of possession), 등록(commissioning)**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2016-0156614 A1 (HCL TECHNOLOGIES LIMITED) 02 June 2016 (2016-06-02) See paragraphs [0029]-[0034]; claim 7; and figures 1 and 2a.	1-16
A	KR 10-2020-0098561 A (MOCANA CORPORATION) 20 August 2020 (2020-08-20) See paragraphs [0036]-[0037]; claim 1; and figures 1-3.	1-16
A	KR 10-2015-0122199 A (QUALCOMM INCORPORATED) 30 October 2015 (2015-10-30) See paragraphs [0067]-[0072]; claim 1; and figure 6.	1-16
A	US 2019-0364096 A1 (INTEL CORPORATION) 28 November 2019 (2019-11-28) See paragraphs [0023]-[0029]; claim 29; and figure 1.	1-16
A	KR 10-2016-0146346 A (SAMSUNG ELECTRONICS CO., LTD.) 21 December 2016 (2016-12-21) See paragraphs [0083]-[0099]; claim 1; and figure 3a.	1-16



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“D” document cited by the applicant in the international application

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search

23 February 2022

Date of mailing of the international search report

25 February 2022

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
Government Complex-Daejeon Building 4, 189 Cheongsaro, Seo-gu, Daejeon 35208

Facsimile No. +82-42-481-8578

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/KR2021/017482

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
US	2016-0156614	A1	02 June 2016	None			
KR	10-2020-0098561	A	20 August 2020	EP	3718036	A1	07 October 2020
				EP	3718036	A4	22 December 2021
				EP	3718252	A1	07 October 2020
				EP	3718252	A4	12 January 2022
				EP	3718282	A1	07 October 2020
				EP	3718282	A4	11 August 2021
				JP	2021-504865	A	15 February 2021
				JP	2021-505097	A	15 February 2021
				JP	2021-505098	A	15 February 2021
				KR	10-2020-0097744	A	19 August 2020
				KR	10-2020-0099543	A	24 August 2020
				US	10057243	B1	21 August 2018
				US	10162968	B1	25 December 2018
				US	10469480	B2	05 November 2019
				US	10505920	B2	10 December 2019
				US	10657261	B2	19 May 2020
				US	10979419	B2	13 April 2021
				US	2019-0163912	A1	30 May 2019
				US	2019-0166116	A1	30 May 2019
				US	2019-0166117	A1	30 May 2019
				US	2020-0067915	A1	27 February 2020
				US	2020-0242249	A1	30 July 2020
				WO	2019-108435	A1	06 June 2019
				WO	2019-108436	A1	06 June 2019
				WO	2019-108438	A1	06 June 2019
KR	10-2015-0122199	A	30 October 2015	CN	105075185	A	18 November 2015
				CN	105075185	B	16 November 2018
				EP	2959643	A1	30 December 2015
				JP	2016-515328	A	26 May 2016
				TW	201448524	A	16 December 2014
				TW	I530120	B	11 April 2016
				US	2014-0241354	A1	28 August 2014
				US	9853826	B2	26 December 2017
				WO	2014-131038	A1	28 August 2014
US	2019-0364096	A1	28 November 2019	CN	102118430	A	06 July 2011
				CN	102118430	B	16 September 2015
				CN	105024865	A	04 November 2015
				CN	105024865	B	04 June 2019
				EP	2336886	A2	22 June 2011
				EP	2336886	A3	06 June 2012
				EP	3306473	A1	11 April 2018
				JP	2011-129117	A	30 June 2011
				KR	10-1227267	B1	28 January 2013
				KR	10-2011-0069732	A	23 June 2011
				US	10298665	B2	21 May 2019
				US	11044305	B2	22 June 2021
				US	2011-0153727	A1	23 June 2011
				US	2015-0120822	A1	30 April 2015
				US	2018-0013819	A1	11 January 2018

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/KR2021/017482

Patent document cited in search report				Publication date (day/month/year)			Patent family member(s)			Publication date (day/month/year)		
							US	8924569	B2	30 December 2014		
							US	9749398	B2	29 August 2017		
KR	10-2016-0146346	A	21 December 2016	KR	10-2340917	B1	20 December 2021					
							US	10172167	B2	01 January 2019		
							US	2016-0366708	A1	15 December 2016		

A. 발명이 속하는 기술분류(국제특허분류(IPC)) H04L 61/00(2022.01)i; H04L 9/40(2022.01)i; H04L 9/32(2006.01)i; H04W 4/80(2018.01)i		
B. 조사된 분야 조사된 최소문헌(국제특허분류를 기재) H04L 61/00(2022.01); H04L 12/28(2006.01); H04L 29/06(2006.01); H04L 29/08(2006.01); H04L 9/32(2006.01); H04W 76/10(2018.01) 조사된 기술분야에 속하는 최소문헌 이외의 문헌 한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC 일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC 국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우)) eKOMPASS(특허청 내부 검색시스템) & 키워드: 클라우드(cloud), 피제어기기(controlee), 챌린지 확인(challenge confirm), 소유 증명(proof of possession), 등록(commissioning)		
C. 관련 문헌		
카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
A	US 2016-0156614 A1 (HCL TECHNOLOGIES LIMITED) 2016.06.02 단락 [0029]-[0034]; 청구항 7; 및 도면 1, 2a	1-16
A	KR 10-2020-0098561 A (모카나 코포레이션) 2020.08.20 단락 [0036]-[0037]; 청구항 1; 및 도면 1-3	1-16
A	KR 10-2015-0122199 A (헬캡 인코포레이티드) 2015.10.30 단락 [0067]-[0072]; 청구항 1; 및 도면 6	1-16
A	US 2019-0364096 A1 (INTEL CORPORATION) 2019.11.28 단락 [0023]-[0029]; 청구항 29; 및 도면 1	1-16
A	KR 10-2016-0146346 A (삼성전자주식회사) 2016.12.21 단락 [0083]-[0099]; 청구항 1; 및 도면 3a	1-16
☐ 추가 문헌이 C(계속)에 기재되어 있습니다. ☒ 대응특허에 관한 별지를 참조하십시오.		
* 인용된 문헌의 특별 카테고리: “A” 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌 “D” 본 국제출원에서 출원인이 인용한 문헌 “E” 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌 “L” 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌 “O” 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌 “P” 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌 “T” 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌 “X” 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다. “Y” 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다. “&” 동일한 대응특허문헌에 속하는 문헌		
국제조사의 실제 완료일 2022년02월23일(23.02.2022)		국제조사보고서 발송일 2022년02월25일(25.02.2022)
ISA/KR의 명칭 및 우편주소 대한민국 특허청 (35208) 대전광역시 서구 청사로 189, 4동 (둔산동, 정부대전청사) 팩스 번호 +82-42-481-8578		심사관 양정록 전화번호 +82-42-481-5709

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
US 2016-0156614 A1	2016/06/02	없음	
KR 10-2020-0098561 A	2020/08/20	EP 3718036 A1	2020/10/07
		EP 3718036 A4	2021/12/22
		EP 3718252 A1	2020/10/07
		EP 3718252 A4	2022/01/12
		EP 3718282 A1	2020/10/07
		EP 3718282 A4	2021/08/11
		JP 2021-504865 A	2021/02/15
		JP 2021-505097 A	2021/02/15
		JP 2021-505098 A	2021/02/15
		KR 10-2020-0097744 A	2020/08/19
		KR 10-2020-0099543 A	2020/08/24
		US 10057243 B1	2018/08/21
		US 10162968 B1	2018/12/25
		US 10469480 B2	2019/11/05
		US 10505920 B2	2019/12/10
		US 10657261 B2	2020/05/19
		US 10979419 B2	2021/04/13
		US 2019-0163912 A1	2019/05/30
		US 2019-0166116 A1	2019/05/30
		US 2019-0166117 A1	2019/05/30
		US 2020-0067915 A1	2020/02/27
		US 2020-0242249 A1	2020/07/30
		WO 2019-108435 A1	2019/06/06
		WO 2019-108436 A1	2019/06/06
		WO 2019-108438 A1	2019/06/06
KR 10-2015-0122199 A	2015/10/30	CN 105075185 A	2015/11/18
		CN 105075185 B	2018/11/16
		EP 2959643 A1	2015/12/30
		JP 2016-515328 A	2016/05/26
		TW 201448524 A	2014/12/16
		TW I530120 B	2016/04/11
		US 2014-0241354 A1	2014/08/28
		US 9853826 B2	2017/12/26
		WO 2014-131038 A1	2014/08/28
US 2019-0364096 A1	2019/11/28	CN 102118430 A	2011/07/06
		CN 102118430 B	2015/09/16
		CN 105024865 A	2015/11/04
		CN 105024865 B	2019/06/04
		EP 2336886 A2	2011/06/22
		EP 2336886 A3	2012/06/06
		EP 3306473 A1	2018/04/11
		JP 2011-129117 A	2011/06/30
		KR 10-1227267 B1	2013/01/28
		KR 10-2011-0069732 A	2011/06/23
		US 10298665 B2	2019/05/21
		US 11044305 B2	2021/06/22
		US 2011-0153727 A1	2011/06/23
		US 2015-0120822 A1	2015/04/30
		US 2018-0013819 A1	2018/01/11

국 제 조 사 보 고 서
대응특허에 관한 정보

국제출원번호

PCT/KR2021/017482

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
		US 8924569 B2	2014/12/30
		US 9749398 B2	2017/08/29
KR 10-2016-0146346 A	2016/12/21	KR 10-2340917 B1	2021/12/20
		US 10172167 B2	2019/01/01
		US 2016-0366708 A1	2016/12/15