(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2013 년 4 월 18 일 (18.04.2013)

WIPO | PCT

(10) 국제공개번호
WO 2013/055106 A2

(51) 국제특허분류:
H04W 12/08 (2009.01) *H04W 88/02* (2009.01)
H04W 12/06 (2009.01) *H04W 84/12* (2009.01)

(21) 국제출원번호: PCT/KR2012/008220

(22) 국제출원일: 2012 년 10 월 10 일 (10.10.2012)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
61/545,205 2011 년 10 월 10 일 (10.10.2011) US

(71) 출원인: **엘지전자 주식회사 (LG ELECTRONICS INC.)** [KR/KR]; 150-721 서울 영등포구 여의도동 20, Seoul (KR).

(72) 발명자: **이윤정 (YI, Yunjung)**; 431-080 경기도 안양시 동안구 호계 1 동 533 번지 엘지전자 특허센터, Gyeonggi-do (KR). **임재원 (LIM, Jaewon)**; 431-080 경기도 안양시 동안구 호계 1 동 533 번지 엘지전자 특허센터, Gyeonggi-do (KR). **이인선 (LEE, Insun)**; 431-080 경기도 안양시 동안구 호계 1 동 533 번지 엘지전자 특허센터, Gyeonggi-do (KR). **김봉희 (KIM, Bonghoe)**; 431-080 경기도 안양시 동안구 호계 1 동 533 번지 엘지전자 특허센터, Gyeonggi-do (KR). **김서욱 (KIM, Suhwook)**; 431-080 경기도 안양시 동안구 호계 1 동 533 번지 엘지전자 특허센터, Gyeonggi-do (KR).

(74) 대리인: **김용인 (KIM, Yong In)** 등; 138-861 서울 송파구 잠실동 175-9 현대빌딩 7 층 KBK 특허법률사무소, 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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, 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, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

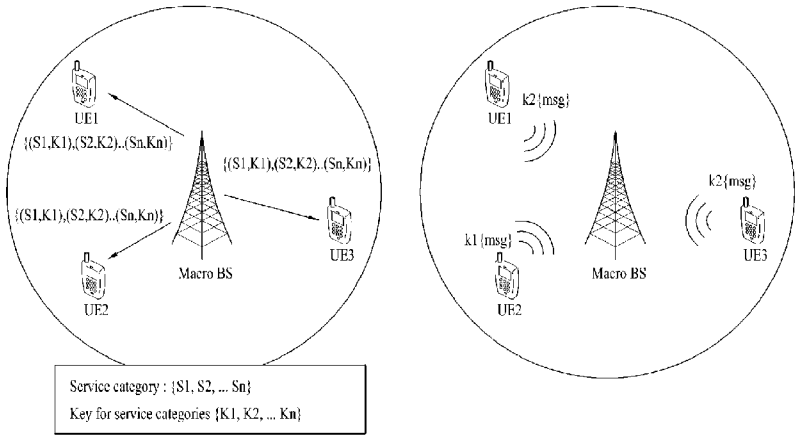
(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR),

[다음 쪽 계속]

(54) **Title**: METHOD FOR WIRELESS LOCAL AREA NETWORK (WLAN)-BASED PEER TO PEER (P2P) COMMUNICATION AND APPARATUS FOR SAME

(54) **발명의 명칭** : WLAN(WIRELESS LOCAL AREA NETWORK)-기반 P2P(PEER TO PEER) 통신을 위한 방법 및 이를 위한 장치

[Fig. 7]



(57) **Abstract**: The present invention relates to a wireless communication system. More particularly, the present invention relates to a method for performing WLAN-based P2P communication at the state where a P2P apparatus is connected to a cellular network and to a first P2P apparatus for the method. The method comprises: a step of receiving one or more pieces of key information from a cellular base station, each piece of key information including a key value corresponding to service identification information; a step of receiving an encrypted data signal from a second P2P apparatus; and a step of performing a process of attempting to decrypt said encrypted data signal using one or more keys corresponding to one or more services in which said first P2P apparatus is interested, from among said one or more pieces of key information.

(57) **요약서**:

[다음 쪽 계속]

WO 2013/055106 A2

OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

공개:

— 국제조사보고서 없이 공개하며 보고서 접수 후 이를 별도 공개함 (규칙 48.2(g))

본 발명은 무선 통신 시스템에 관한 것이다. 구체적으로, 본 발명은 셀룰러 네트워크에 연결된 상태에서 WLAN-기반 P2P 통신을 수행하는 방법 및 이를 위한 제 1 P2P 장치에 있어서, 셀룰러 기지국으로부터 하나 이상의 키 정보를 수신하되, 각각의 키 정보는 서비스 식별 정보와 대응하는 키 값을 포함하는 단계; 제 2 P2P 장치로부터 암호화된 데이터 신호를 수신하는 단계; 상기 하나 이상의 키 정보 중, 상기 제 1 P2P 장치가 관심 있는 하나 이상의 서비스에 대응하는 하나 이상의 키를 이용하여 상기 암호화된 데이터 신호의 해독화를 시도하는 위한 과정을 수행하는 단계를 포함하는 방법 및 이를 위한 장치에 관한 것이다.

명세서

발명의 명칭: WLAN(WIRELESS LOCAL AREA NETWORK)-기반 P2P(PEER TO PEER) 통신을 위한 방법 및 이를 위한 장치

기술분야

[1] 본 발명은 무선 통신 시스템에 관한 것으로서, 구체적으로 WLAN(Wireless Local Area Network)에 기반한 P2P 통신을 위한 방법 및 장치에 관한 것이다. 보다 구체적으로, 본 발명은 WLAN에 기반한 P2P 통신을 위한 이웃 발견, 데이터 통신 등을 위한 방법 및 이를 위한 장치에 관한 것이다. WLAN은 Wi-Fi(Wireless Fidelity), ZigBee, 스몰 셀(small cell)에 기반한 면허 밴드(licensed band) 등 무선 통신에 기반한 LAN(Local Area Network)를 의미한다.

배경기술

[2] 무선 통신 시스템이 음성이나 데이터 등과 같은 다양한 종류의 통신 서비스를 제공하기 위해 광범위하게 전개되고 있다. 일반적으로 무선통신 시스템은 가용한 시스템 자원(대역폭, 전송 파워 등)을 공유하여 다중 사용자와의 통신을 지원할 수 있는 다중 접속(multiple access) 시스템이다. 다중 접속 시스템의 예들로는 CDMA(Code Division Multiple Access) 시스템, FDMA(Frequency Division Multiple Access) 시스템, TDMA(Time Division Multiple Access) 시스템, OFDMA(Orthogonal Frequency Division Multiple Access) 시스템, SC-FDMA(Single Carrier Frequency Division Multiple Access) 시스템 등이 있다.

[3] 무선랜(Wireless Local Area Network, WLAN) 기술에 대한 표준은 IEEE(Institute of Electrical and Electronics Engineers) 802.11 그룹에서 개발되고 있다. IEEE 802.11a 및 b는 2.4.GHz 또는 5GHz에서 비면허 대역(unlicensed band)을 이용하고, IEEE 802.11b는 11Mbps의 전송 속도를 제공하고, IEEE 802.11a는 54 Mbps의 전송 속도를 제공한다. IEEE 802.11g는 2.4GHz에서 직교 주파수 분할 다중화(Orthogonal Frequency Division Multiplexing, OFDM)를 적용하여 54Mbps의 전송 속도를 제공한다. IEEE 802.11n은 다중입출력 OFDM(Multiple Input Multiple Output-OFDM, MIMO-OFDM)을 적용하여 300Mbps의 전송 속도를 제공한다. IEEE 802.11n은 채널 대역폭(channel bandwidth)을 40 MHz까지 지원하며, 이 경우 600Mbps의 전송 속도를 제공한다. IEEE 802.11p는 WAVE(Wireless Access in Vehicular Environments)를 지원하기 위한 표준이다. 예를 들어, 802.11p는 ITS(Intelligent Transportation Systems) 지원에 필요한 개선 사항을 제공한다. IEEE 802.11ai는 IEEE 802.11 스테이션(station, STA)의 고속 초기 링크 셋업(fast initial link setup)을 지원하기 위한 표준이다.

[4] 최근 Wi-Fi 연합(Wireless Fidelity alliance)은 Wi-Fi 기반 P2P(Peer-to-Peer) 기술(예, WFD(Wi-Fi Direct))의 발표와 함께 인증을 진행하고 있다. Wi-Fi P2P

기술은 TV, 노트북, 프린터, 카메라와 같은 휴대 기기 및 휴대 단말 등에 탑재되어 AP(Access Point) 또는 라우터와 같은 별도의 장비 없이도 단말 간 직접 통신을 통하여 기기간 컨텐츠 및 서비스를 사용할 수 있는 기반을 제공한다. Wi-Fi P2P 기술은 빠른 전송 속도를 제공함으로써 일부 영역에서 블루투스 기술을 대체할 수 있을 것으로 기대된다.

발명의 상세한 설명

기술적 과제

[5] WLAN에 기반한 P2P 통신을 효율적으로 수행하는 방법 및 이를 위한 장치를 제공하는데 있다. 본 발명의 다른 목적은 WLAN에 기반한 P2P 통신을 위한 인증/암호화를 위한 과정을 효율적으로 수행하는 방법 및 이를 위한 장치의 제공에 있다.

[6] 본 발명에서 이루고자 하는 기술적 과제들은 상기 기술적 과제로 제한되지 않으며, 언급하지 않은 또 다른 기술적 과제들은 아래의 기재로부터 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

과제 해결 수단

[7] 본 발명의 일 양상으로, 셀룰러 네트워크에 연결된 제1 P2P(Peer to Peer) 장치에서 WLAN(Wireless Local Area Network)-기반 P2P 통신을 수행하는 방법에 있어서, 셀룰러 기지국으로부터 하나 이상의 키 정보를 수신하되, 각각의 키 정보는 서비스 식별 정보와 대응하는 키 값을 포함하는 단계; 제2 P2P 장치로부터 암호화된 데이터 신호를 수신하는 단계; 상기 하나 이상의 키 정보 중, 상기 제1 P2P 장치가 관심 있는 하나 이상의 서비스에 대응하는 하나 이상의 키를 이용하여 상기 암호화된 데이터 신호의 해독화를 시도하는 위한 과정을 수행하는 단계를 포함하는 방법이 제공된다.

[8] 본 발명의 다른 양상으로, 셀룰러 네트워크에 연결되고, WLAN(Wireless Local Area Network)-기반 P2P(Peer to Peer) 통신을 수행하도록 구성된 제1 P2P 장치에 있어서, 무선 주파수(Radio Frequency, RF) 유닛; 및 프로세서를 포함하고, 상기 프로세서는 셀룰러 기지국으로부터 하나 이상의 키 정보를 수신하되, 각각의 키 정보는 서비스 식별 정보와 대응하는 키 값을 포함하고, 제2 P2P 장치로부터 암호화된 데이터 신호를 수신하며, 상기 하나 이상의 키 정보 중, 상기 제1 P2P 장치가 관심 있는 하나 이상의 서비스에 대응하는 하나 이상의 키를 이용하여 상기 암호화된 데이터 신호의 해독화를 시도하는 위한 과정을 수행하도록 구성된 제1 P2P 장치가 제공된다.

[9] 바람직하게, 상기 암호화된 데이터 신호의 수신은 상기 제2 P2P 장치에 대한 정보 또는 상기 제2 P2P 장치가 속하는 그룹에 대한 정보가 없는 상태에서 수신된다.

[10] 바람직하게, 상기 하나 이상의 키 정보에 포함된 복수의 키 값은 상기 셀룰러

기지국이 서비스를 제공하는 셀 내의 모든 혹은 같은 P2P 서비스에에 관심이 있는 P2P 장치에 동일하게 설정된다.

[11] 바람직하게, 상기 암호화된 데이터 신호의 헤더는 키 식별 정보, 서비스 식별 정보 중 적어도 하나를 포함한다.

[12] 바람직하게, 상기 암호화된 데이터 신호의 헤더가 상기 제1 P2P가 관심 있는 키 또는 서비스에 관한 정보를 갖지 않는 경우, 상기 암호화된 데이터 신호는 버려지고, 상기 암호화된 데이터 신호의 헤더가 상기 제1 P2P가 관심 있는 키 또는 서비스에 관한 정보를 갖는 경우, 상기 암호화된 데이터 신호에 대한 해독화 과정이 수행된다.

[13] 바람직하게, 상기 암호화된 데이터 신호는 PHY(Physical) 계층에서 버려지고, 상기 암호화된 데이터 신호에 대한 해독화 과정은 MAC(Medium Access Control) 계층에서 수행된다.

[14] 바람직하게, 상기 하나 이상의 키 정보는 소정의 타이머가 만료되는 경우 갱신된다.

[15] 바람직하게, 상기 하나 이상의 키 정보에 대해 갱신을 요청하는 정보를 상기 셀룰러 기지국에게 전송하는 것을 더 포함한다.

발명의 효과

[16] 본 발명에 의하면, 무선 통신 시스템에서 WLAN-기반 P2P 통신을 효율적으로 수행할 수 있다. 구체적으로, WLAN-기반 P2P 통신을 위한 인증/암호화를 위한 과정을 효율적으로 수행할 수 있다.

[17] 본 발명에서 얻은 수 있는 효과는 이상에서 언급한 효과들로 제한되지 않으며, 언급하지 않은 또 다른 효과들은 아래의 기재로부터 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

[18] 본 발명에 관한 이해를 돕기 위해 상세한 설명의 일부로 포함되는, 첨부 도면은 본 발명에 대한 실시예를 제공하고, 상세한 설명과 함께 본 발명의 기술적 사상을 설명한다.

[19] 도 1a은 본 발명이 적용될 수 있는 WLAN(Wireless Local Area Network)(예, IEEE 802.11) 시스템의 구조를 예시한다.

[20] 도 1b는 액세스 장치들 및 무선 사용자 장치들을 채용하는 통신 시스템의 예시적인 동작을 나타내는 블록도이다.

[21] 도 2는 WLAN-기반 P2P(예, WFD(Wi-Fi Direct)) 네트워크를 예시한다.

[22] 도 3은 WLAN-기반 P2P 양상을 예시한다

[23] 도 4는 이웃 발견 과정을 예시한다.

[24] 도 5~6에 WLAN 인증/암호화 과정을 예시한다.

[25] 도 7~8은 본 발명에 따른 인증/암호화 과정을 예시한다.

[26] 도 9는 본 발명에 적용될 수 있는 WLAN-기반 P2P(Peer to Peer) 장치를

예시한다.

발명의 실시를 위한 형태

[27] 이하의 기술은 CDMA(code division multiple access), FDMA(frequency division multiple access), TDMA(time division multiple access), OFDMA(orthogonal frequency division multiple access), SC-FDMA(single carrier frequency division multiple access), OFDM(orthogonal frequency division multiplexing) 등과 같은 다양한 무선 접속 시스템에 사용될 수 있다. CDMA는 UTRA(Universal Terrestrial Radio Access)나 CDMA2000과 같은 무선 기술로 구현될 수 있다. TDMA는 GSM(Global System for Mobile communications)/GPRS(General Packet Radio Service)/EDGE(Enhanced Data Rates for GSM Evolution)와 같은 무선 기술로 구현될 수 있다. OFDMA는 IEEE 802.16 (WiMAX), IEEE 802-20, E-UTRA(Evolved UTRA) 등과 같은 무선 기술로 구현될 수 있다. OFDM은 IEEE 802.11등과 같은 무선 기술로 구현될 수 있다.

[28] 설명을 명확하기 위해, IEEE 802.11 (WLAN)를 위주로 기술하지만 본 발명의 기술적 사상이 이에 제한되는 것은 아니다. 예를 들어, 이하의 설명은 무선 접속 시스템들인 IEEE 802 시스템, 3GPP 시스템, 3GPP LTE 및 LTE-A(LTE-Advanced)시스템 및 3GPP2 시스템 중 적어도 하나에 개시된 표준 문서들에 의해 뒷받침될 수 있다. 즉, 본 발명의 실시예들 중 본 발명의 기술적 사상을 명확히 드러내기 위해 설명하지 않은 단계들 또는 부분들은 상기 문서들에 의해 뒷받침될 수 있다. 또한, 본 문서에서 개시하고 있는 모든 용어들은 상기 표준 문서에 의해 설명될 수 있다.

[29] 이하의 설명에서 사용되는 특정(特定) 용어들은 본 발명의 이해를 돕기 위해서 제공된 것이며, 이러한 특정 용어는 본 발명의 기술적 사상을 벗어나지 않는 범위에서 다른 형태로 변경될 수 있다. 몇몇 경우, 본 발명의 개념이 모호해지는 것을 피하기 위하여 공지의 구조 및 장치는 생략되거나, 각 구조 및 장치의 핵심기능을 중심으로 한 블록도 형식으로 도시된다. 또한, 본 명세서 전체에서 동일한 구성요소에 대해서는 동일한 도면 부호를 사용하여 설명한다. 또한, 본 명세서에서 설명되는 동작들의 순서는 변경될 수 있다. 실시예의 일부 구성이나 특징은 다른 실시예에 포함되거나 다른 실시예의 대응하는 구성 또는 특징과 교체될 수 있다.

[30] 도 1a는 본 발명이 적용될 수 있는 IEEE 802.11 시스템의 예시적인 구조를 나타내는 도면이다.

[31] IEEE 802.11 구조는 복수의 구성요소들로 구성될 수 있고, 이들의 상호작용에 의해 상위계층에 대해 트랜스패런트한 STA 이동성을 지원하는 WLAN이 제공될 수 있다. 기본 서비스 세트(Basic Service Set, BSS)는 IEEE 802.11 LAN의 기본 구성 블록에 해당할 수 있다. 도 1a는 2개의 BSS(BSS1 및 BSS2)가 존재하고 각각의 BSS각 2개의 STA를 포함하는 경우(STA1 및 STA2 는 BSS1에 포함되고,

STA3 및 STA4는 BSS2에 포함됨)를 예시한다. 여기서, STA는 IEEE 802.11 의 MAC(Medium Access Control)/PHY(Physical) 규정에 따라 동작하는 기기를 의미한다. STA는 AP(Access Point) STA(간단히, AP) 및 논-AP(논-AP) STA를 포함한다. AP는 무선 인터페이스를 통해 논-AP STA에게 네트워크(예, WLAN) 접속을 제공하는 기기에 해당한다. AP는 고정 형태 또는 이동 형태로 구성될 수 있으며, 핫-스팟(hot-spot)을 제공하는 휴대용 무선 기기(예, 랩탑 컴퓨터, 스마트 폰 등)를 포함한다. AP는 다른 무선 통신 분야에서 기지국(Base Station, BS), 노드-B(Node-B), 발전된 노드-B(Evolved Node-B; eNB), 기저 송수신 시스템(Base Transceiver System, BTS), 펨토 기지국(Femto BS) 등에 대응된다. 논-AP STA는 랩탑 컴퓨터, PDA, 무선 모뎀, 스마트 폰과 같이 일반적으로 사용자가 직접 다루는 기기에 해당한다. 논-AP STA는 단말(terminal), 무선 송수신 유닛(Wireless Transmit/Receive Unit, WTRU), 사용자 장치(User Equipment, UE), 이동국(Mobile Station, MS), 이동 단말(Mobile Terminal), 이동 가입자국(Mobile Subscriber Station, MSS) 등으로 지칭될 수 있다.

[32] 도 1a에서 BSS를 나타내는 타원은 해당 BSS에 포함된 STA들이 통신을 유지하는 커버리지 영역을 나타내는 것으로 이해될 수 있다. 이 영역을 BSA(Basic Service Area)라고 칭할 수 있다. IEEE 802.11 LAN에서 가장 기본적인 타입의 BSS는 독립적인 BSS(Independent BSS, IBSS)이다. 예를 들어, IBSS는 2개의 STA만으로 구성된 최소 형태를 가질 수 있다. 또한, 가장 단순한 형태이고 다른 구성요소들이 생략되어 있는 도 1a의 BSS(BSS1 또는 BSS2)가 IBSS의 대표적인 예시에 해당할 수 있다. 이러한 구성은 STA들이 직접 통신할 수 있는 경우에 가능하다. 또한, 이러한 형태의 LAN은 미리 계획되어서 구성되는 것이 아니라 LAN이 필요한 경우에 구성될 수 있으며, 이를 애드-혹(ad-hoc) 네트워크라고 칭할 수도 있다.

[33] STA의 켜지거나 꺼짐, STA가 BSS 영역에 들어오거나 나감 등에 의해, BSS에서STA의 멤버쉽이 동적으로 변경될 수 있다. BSS의 멤버가 되기 위해 STA는 동기화 과정을 이용하여 BSS에 참여(join)할 수 있다. BSS 기반 구조의 모든 서비스에 접속하기 위해, STA는 BSS에 연결(associated)될 수 있다.

[34] 도 1b는 액세스 장치(예, AP STA들)(102A, 102B 및 102C)들 및 무선 사용자 장치들(예, 논-AP STA들)을 채용하는 통신 시스템(100)을 예시한다.

[35] 도 1b를 참조하면, 액세스 장치들(102A-C)은 인터넷과 같은 광역 네트워크(Wide Area Network, WAN)(106)로 접속을 제공하는 스위치(104)에 연결된다. 액세스 장치들(102A-C) 각각은 시분할 다중화된 네트워크를 통해 액세스 장치의 커버리지 영역(미도시) 내의 무선 장치들에 대한 무선 접속을 제공한다. 따라서, 액세스 장치들(102A-C)은 시스템(100)의 전체 WLAN 커버리지 영역을 공동으로 제공한다. 예를 들어, 실선으로 표기된 박스에 의해 나타낸 위치에서 무선 장치(108)는 액세스 장치들(102A 및 102B)의 커버리지 영역 내에 존재할 수 있다. 따라서, 무선 장치(108)는 실선 화살표(11OA 및

11OB)와 같이 액세스 장치들(102A 및 102B) 각각으로부터 비컨들을 수신할 수 있다. 무선 장치(108)가 실선 박스로부터 파선 박스로 로밍하면, 무선 장치(108)는 액세스 장치(102C)의 커버리지 영역에 진입하고, 액세스 장치(102A)의 커버리지 영역을 나간다. 따라서, 무선 장치(108)는 파선 화살표(112A 및 112B)와 같이 액세스 장치들(102B및 102C)로부터 비컨들을 수신할 수 있다.

[36] 무선 장치(108)가 시스템(100)이 제공하는 전체 WLAN 커버리지 영역 내에서 로밍할 때, 무선 장치(108)는 어느 액세스 장치가 현재 무선 장치(108)에 대한 가장 양호한 접속을 제공하는지 결정할 수 있다. 예를 들어, 무선 장치(108)는 근접한 액세스 장치들의 비컨들을 반복적으로 스캐닝하고, 상기 비컨들 각각과 연관된 신호 강도(예, 전력)를 측정할 수 있다. 따라서, 무선 장치(108)는 최대 비컨 신호 강도에 기초해 최적의 네트워크 접속을 제공하는 액세스 장치와 연결될 수 있다. 무선 장치(108)는 최적 접속과 관련된 다른 기준을 이용할 수 있다. 예를 들어, 최적 접속은 보다 많은 바람직한 서비스(예, 컨텐츠, 데이터 레이트 등)와 연관될수 있다.

[37] 도 2는 WLAN-기반 P2P(예, Wi-Fi Direct, WFD) 네트워크를 예시한다. WLAN-기반 P2P 네트워크는 Wi-Fi 장치들이 홈 네트워크, 오피스 네트워크 및 핫스팟 네트워크에 참여하지 않아도, 서로 장치-대-장치(Device to Device, D2D)(혹은, Peer to Peer, P2P) 통신을 수행할 수 있는 네트워크를 나타낸다. 이하, WLAN-기반 P2P 통신을 WLAN P2P 통신(간단히, P2P 통신) 혹은 WLAN D2D 통신(간단히, D2D 통신)이라고 지칭한다. 또한, WLAN P2P 수행 장치를 WLAN P2P 장치, 간단히 P2P 장치라고 지칭한다.

[38] 도 2를 참조하면, WLAN P2P 네트워크(200)는 제1 P2P 장치(202) 및 제2 P2P 장치(204)를 포함하는 적어도 하나의 P2P 장치를 포함할 수 있다. P2P 장치는 디스플레이 장치, 프린터, 디지털 카메라, 프로젝터 및 스마트 폰 등 WLAN (예, Wi-Fi, ZigBee , 면허 밴드에 기반한 LAN)를 지원하는 장치들을 포함한다. 또한, P2P 장치는 논-AP STA 및 AP STA를 포함한다. 도시된 예에서, 제1 P2P 장치(202)는 스마트 폰이고 제2 P2P 장치(204)는 디스플레이 장치이다. 여기서, P2P 통신은 휴대 기기 및 모바일 단말 등에 탑재되어 AP 또는 라우터와 같은 별도의 장비 없이도 단말간 직접 통신을 통하여 기기간 콘텐츠 및 서비스를 사용할 수 있는 기반을 제공하는 통신 기술을 나타낸다. 즉, P2P 네트워크 내의 P2P 장치들은 서로 직접 연결될 수 있다. 예를 들어, P2P 통신은 두 P2P 장치들간의 신호 전송 경로가 제3의 장치(예, AP) 또는 기존 네트워크(예, AP를 거쳐 WLAN에 접속)를 거치지 않고 해당 P2P 장치들간에 직접 설정된 경우를 의미할 수 있다. 여기서, 두 P2P 장치들간에 직접 설정된 신호 전송 경로는 데이터 전송 경로로 제한될 수 있다. 예를 들어, P2P 통신은 복수의 논-STA들이 AP를 거치지 않고 데이터(예, 음성/영상/문자 정보 등)를 전송하는 경우를 의미할 수 있다. 제어 정보(예, P2P 설정을 위한 자원 할당 정보, 무선 장치 식별

정보 등)를 위한 신호 전송 경로는 P2P 장치들(예, 논-AP STA-대-논-AP STA, 논-AP STA-대-AP)간에 직접 설정되거나, AP를 경유하여 두 P2P 장치들간(예, 논-AP STA-대-논-AP STA)에 설정되거나, AP와 해당 P2P 장치(예, AP-대-논-AP STA#1, AP-대-논-AP STA#2)간에 설정될 수 있다.

[39] 현재, P2P는 주로 원격 프린트, 사진 공유 등과 같은 반-정적(semi-static) 통신을 위해 사용되고 있다. 그러나, WLAN 장치의 보편화와 위치 기반 서비스 등으로 인해, P2P의 활용성은 점점 넓어지고 있다. 예를 들어, 쏘셜 채팅(예, SNS(Social Network Service)에 가입된 무선 장치들이 위치 기반 서비스에 기초해서 근접 지역의 무선 장치를 인식하고 정보를 송수신), 위치-기반 광고 제공, 위치-기반 뉴스 방송, 무선 장치간 게임 연동 등에 P2P가 활발히 사용될 것으로 예상된다. 편의상, 이러한 P2P 응용을 신규 P2P 응용이라고 지칭한다.

[40] 도 3에 신규 P2P 응용(예, 쏘셜 채팅, 위치-기반 서비스 제공, 게임 연동 등)이 적용되는 경우의 P2P 네트워크 양상을 예시하였다. 도 3을 참조하면, P2P 네트워크에서 다수의 P2P 장치들(302a~302d)이 P2P 통신(310)을 수행하며, P2P 장치의 이동에 의해 P2P 네트워크를 구성하는 P2P 장치(들)이 수시로 변경되거나, P2P 네트워크 자체가 동적/단시간적으로 새로 생성되거나 소멸될 수 있다. 이와 같이, 신규 P2P 응용 부분의 특징은 덴스(dense) 네트워크 환경에서 상당히 다수의 P2P 장치간에 동적/단시간적으로 P2P 통신이 이뤄지고 종료될 수 있다는 점이다.

[41] WLAN P2P 네트워크 구성 과정은 크게 두 과정으로 구분될 수 있다. 첫 번째 과정은 이웃 발견 과정(Neighbor Discovery, ND, procedure)이고, 두 번째 과정은 P2P 링크 설정 및 통신 과정이다. 이웃 발견 과정을 통해, P2P 장치(예, 도 2의 202)는 (자신의 무선) 커버리지 내의 다른 이웃 P2P 장치(예, 도 2의 204)를 찾고 해당 P2P 장치와의 연결(association), 예를 들어 사전-연결(pre-association)에 필요한 정보를 획득할 수 있다. 여기서, 사전-연결은 무선 프로토콜에서 제2 계층 사전-연결을 의미할 수 있다. 사전-연결에 필요한 정보는 예를 들어 이웃 P2P 장치에 대한 식별 정보 등을 포함할 수 있다.

[42] 도 4에 이웃 발견 과정을 도시하였다. 본 예는 도 2에서 P2P 장치(202)와 P2P 장치(204) 사이의 동작을 예시한다.

[43] 도 4를 참조하면, 이웃 발견 과정은 SME(Station Management Entity)/어플리케이션/사용자/벤더의 지시에 의해 개시될 수 있고(S410), 스캔 단계(scan phase)(S412)와 찾기 단계(find phase)(S414~S416)로 나눠질 수 있다. 스캔 단계(S412)는 가용한 모든 무선 채널에 대해 802.11 방식에 따라 스캔하는 동작을 포함한다. 이를 통해, P2P 장치는 최상의 동작 채널을 확인할 수 있다. 찾기 단계(S414~S416)는 청취 모드(listen)(S414)와 탐색 모드(search)(S416)를 포함하며, P2P 장치는 청취 모드(S414)와 탐색 모드(S416)를 교대로 반복한다. P2P 장치(202, 204)는 탐색 모드(S416)에서 프로브 요청 프레임(Probe request frame)을 사용하여 능동 탐색을 실시하며, 빠른 탐색을 위하여 탐색 범위를 채널

1, 6, 11(2412, 2437, 2462MHz)의 쏘셜 채널(social channel)로 한정할 수 있다. 또한, P2P 장치(202, 204)는 청취 모드(S414)에서 3개의 쏘셜 채널 중 하나의 채널만을 선택하여 수신 상태로 유지한다. 이 때, 다른 P2P 장치(예, 202)가 탐색 모드에서 전송한 프로브 요청 프레임이 수신된 경우, P2P 장치(예, 204)는 프로브 응답 프레임(probe response frame)으로 응답한다. 청취 모드(S414) 시간은 랜덤하게 주어질 수 있다(예, 100, 200, 300 TU(Time Unit)). P2P 장치는 탐색 모드와 수신 모드를 계속 반복하다 서로의 공통 채널에 도달할 수 있다. P2P 장치는 다른 P2P 장치를 발견한 후 해당 P2P 장치에 선택적으로 결합하기 위해, 프로브 요청 프레임과 프로브 응답 프레임을 사용하여 장치 타입, 제작사 또는 친근한 장치 이름을 발견/교환할 수 있다. 이웃 발견 과정을 통해 주변 P2P 장치를 발견하고 필요한 정보를 얻은 경우, P2P 장치(예, 202)는 SME/어플리케이션/사용자/벤더에게 P2P 장치 발견을 알릴 수 있다(S418)

[44] 이하, 802.11 WLAN의 인증/암호화 과정에 대해 설명한다. 도 1~4를 참조하여 설명한 바와 같이, 802.11 WLAN 프로토콜에는 두 가지 타입의 통신 구조가 존재한다. 첫 번째 통신 구조/모드(예, 도 1)에서 STA는 AP에 연결되고(associated), STA와 AP간에 통신이 수행된다. 이를 위해, 802.11 WLAN은 인증(authentication) 및 암호화(encryption) 알고리즘을 모두 지원한다. 인증 과정은 사용자 정보를 구별하여 네트워크 접속 허용/차단을 결정하는 과정을 나타낸다. 인증 과정을 걸쳐 네트워크 접속이 허용되는 경우, 무선 인터페이스를 통해 송수신되는 데이터는 암호화된다. 이로 제한되는 것은 아니지만, 인증은 AS(Authentication Server)와 STA 사이에 수행되고, AS는 키(key)를 생성하고 이를 AP에 전송한다. AS는 네트워크 접속을 위해 단말에게 인증 서비스를 수행하는 802.1x 콤포넌트를 의미하며, RADIUS(Remote Authentication Dial In User Service) 서버, AAA(Authentication, authorization, and accounting) 서버 등을 통해 구현될 수 있다. IBSS(independent BSS) 모드의 경우, AS는 AP 대신 공유 키(shared key)를 상대(peer)에게 보낼 수 있다. 키는 무선 인터페이스를 통해 전송되는 모든 데이터의 암호화(encryption)/해독화(decryption)에 사용된다. 두 번째 통신 구조/모드(예, 도 2~4)에서 STA들은 서로 피어-투-피어 방식으로 통신을 수행할 수 있다. 이 경우, 인증 및 암호화는 첫 번째 통신 구조/모드에서와 유사하게 수행될 수 있다.

[45] 도 5는 802.11 WLAN이 WEP(Wired Equivalent Privacy)을 지원하는 경우의 인증/암호화 과정을 나타낸다. WEP은 공유 키를 이용하여 인증/암호화를 수행한다.

[46] 도 5를 참조하면, 공유 키 인증 과정은 크게 4 단계(S502~S508)로 구분된다.

[47] 제1 단계: STA는 인증 요청 메시지를 AP 에게 전송한다(S502). 인증 요청 메시지는 STA 식별자(identity)를 포함한다.

[48] 제2 단계: AP는 STA에게 챌린지 텍스트(challenge text)를 전송한다(S504).

[49] 제3 단계: STA는 자신에게 설정된 64-비트 또는 128-비트 키를 이용하여 제2

단계의 챌린지 텍스트를 암호화 한 뒤, 암호화된 챌린지 텍스트를 AP에게 전송한다(S506).

[50] 제4 단계: AP는 해당 STA의 키에 대응하여 자신에게 설정된 WEP 키를 이용하여 암호화된 챌린지 텍스트를 해독한다. AP는 해독된 텍스트와 원본 텍스트를 비교한다. 두 개의 텍스트가 동일하면, AP와 STA가 동일한 WEP 키를 공유하고 있다는 것을 의미하므로 AP는 STA에게 인증 성공을 알려준다(S508). 이후, STA와 AP는 연결(association) 과정을 수행하고(S510), 무선 인터페이스를 통해 송수신되는 데이터는 공유 키를 이용하여 암호화된다. 한편, 두 개의 텍스트가 다른 경우, AP와 STA가 동일한 WEP 키를 공유하지 않는다는 것을 의미하므로 AP는 STA에게 인증 실패를 알려준다(S508). 이 경우, STA는 AP와 연결(association) 과정을 수행할 수 없다.

[51] 도 6은 802.11 WLAN이 RSN(Robust Security Network)을 지원 시의 인증/암호화 과정을 나타낸다. RSN은 TKIP(Temporal Key Integrity Protocol)와 CCMP(Counter Mode with cipher block chaining message authentication code Protocol)을 지원한다.

[52] 도 6을 참조하면, 키 분배를 위해 4개 상태(phase)가 존재한다(S602~S608).

[53] 보안 능력 발견(security capabilities discovery)(S602): AP는 네트워크 보안 능력을 STA에게 광고(advertise)한다. 통신 수행 가능성이 있는 대상이 보안 능력 발견을 통해 결정될 수 있다.

[54] 802.1X 인증(authentication)(S604): AS에서 네트워크 허가 정책 결정(network admission policy decisions)을 집중화한다(centralize). STA와 AS를 상호 인증한다. 인증의 효과로 마스터 키가 생성된다. 마스터 키는 긍정 접속 결정을 나타낸다. 또한, 접속 인증 토큰(token)으로서 PMK(Pairwise Master Key)가 생성된다. PMK는 802.11 매체에 대한 승인을 나타낸다.

[55] RADIUS-기반 키 분배(key distribution)(S606): AS는 PMK를 STA의 AP로 (복사하지 않고) 옮긴다.

[56] 802.1X 관리(management)(S608): PMK를 STA 및 AP에 바인드한다(bind). AP와 STA가 모두 PMK를 소유하고 있음을 확인한다. 프레쉬(fresh) PTK(Pairwise Transient Key)를 생성하고, PTK 사용을 동기화하며, GTK(Group Transient Key)를 분배한다. PTK는 KCK(Key Confirmation Key), KEK(Key Encryption Key), TK(Temporal Key)의 모음이다. KCK는 PMK를 AP, STA에 바인드하는데 사용되며, PMK 소유를 증명하는데 사용된다. KEK는 GTK 분배에 사용된다. TK는 데이터 암호화에 사용된다. 본 과정은 PMK를 이용한 4-way 핸드쉐이크에 의해 수행된다.

[57] 상기 과정에 의해 키 분배가 완료되면, AP와 STA 사이에 무선 인터페이스를 통해 전송되는 데이터는 암호화 키(예, TK)를 통해 암호화된다.

[58] 도 5 및 6을 참조하여 설명한 기존의 802.11 WLAN 보안 메카니즘에 따르면, 인증 및 키 분배(key distribution)를 위해 STA, AP 및 AS간에 수많은 패킷이 교환되므로 높은 오버헤드가 발생한다. 이러한 오버헤드는 기존의 정적

네트워크 구조(예, 도 1)에서는 문제가 없을 수 있다. 그러나, P2P 네트워크의 경우(예, 도 2~4), 단말들이 지속적으로 이동하고 단말간의 세션(session)이 매우 짧은 시간 동안만 유지되므로, 기존의 높은 오버헤드는 바람직하지 않을 수 있다. 특히, 쏘셜 채팅, 온라인 게임, 위치-기반 광고, 위치-기반 뉴스 등과 같은 신규 P2P 응용의 경우(도 3), 덴스(dense) 네트워크 환경에서 상당히 다수의 P2P 장치간에 동적/단시간적으로 P2P 통신이 이뤄질 수 있다. 이로 인해, STA의 무선 범위 내에 높은 수의 세션 및 사용자가 존재할 수 있고, 인증/암호화에 따른 오버헤드 문제는 보다 중요할 수 있다.

[59] 따라서, P2P 통신의 효율적 수행을 위해, 인증 및 연결(association)을 포함하는 데이터 세션 설정에 필요한 오버헤드를 극단적으로 최소화 하는 것이 바람직할 수 있다. 또한, P2P 통신에서는, 별도의 명시적 연결 과정이 일어나지 않을 수 있으므로, 패킷-기반 인증 및 암호화를 제공하는 것이 필요할 수 있다.

[60] **실시예: 셀룰러 네트워크를 이용한 키 분배**

[61] 이하, 도면을 참조하여, 인증/암호화를 위해 효율적으로 키 관리/분배하는 과정에 대해 설명한다. 구체적으로, 본 발명은 셀룰러 네트워크를 이용하여 P2P 통신을 위한 키를 관리/분배하는 방법을 제안한다. 앞에서 언급한 바와 같이, 기존의 방식(도 5~6)에 따르면 P2P 장치는 네트워크에 참여하거나 네트워크를 생성하는 경우 매번 인증 과정을 요구하고, 또한 매번 여러 단계의 키 분배 과정을 거칠 수 있다. 이러한 이유는 네트워크 처음 참여/생성 시 해당 P2P 장치에 대한 인증 상태를 알 수 없기 때문이다. 그러나, 본 발명에서 제안하는 바와 같이, 셀룰러 네트워크(예, (셀룰러) 기지국)를 이용하여 P2P 통신용 키를 P2P 장치들에게 분배하는 경우, 해당 P2P 장치들은 (셀룰러 네트워크에 연결돼 있는 한) 셀룰러 네트워크 내에서 인증이 이뤄진 상태를 의미한다. 따라서, 셀룰러 네트워크로부터 키를 분배 받은 P2P 장치들 간에 P2P 통신(예, 쏘셜 채팅 등)을 수행할 경우, P2P 통신을 위한 추가적인 인증/키 분배 과정을 생략할 수 있다. 정리하면, 셀룰러 네트워크(예, 기지국)로부터 P2P 통신용 키를 분배 받은 P2P 장치는 셀룰러 네트워크에 의해 이미 인증된 상태이므로, 이후에 새롭게 P2P 네트워크에 참여하더라도 해당 P2P용 키를 사용하는 경우에는 인증 과정을 생략하여, 보다 효율적으로 P2P 통신을 수행하는 것이 가능하다.

[62] 이하, 셀룰러 네트워크를 통해 WLAN P2P용 키를 분배하는 2가지 방안에 대해 예시한다. 이하에서 P2P 장치는 셀룰러 통신 모듈과 WLAN 통신 모듈(예, Wi-Fi, ZigBee, 스몰 셀(small cell)에 기반한 면허 밴드(licensed band) 용 통신 모듈)을 모두 구비하고 있다고 가정하고, 편의상 STA/단말과 혼용한다. 또한, 이하의 설명에서 특별히 다른 언급이 없는 한, P2P 장치는 셀룰러 네트워크에 접속된 상태라고 가정한다.

[63] **방안 1: P2P 그룹 키 분배**

[64] 본 예는 P2P를 위한 그룹 키 분배 과정에 대해 예시한다. 여기서, 그룹 키는 P2P를 위한 서비스 카테고리 별로 할당될 수 있다. 본 예에 따르면, 셀룰러

네트워크의 기지국(셀룰러 기지국)은 셀 내의 STA/단말에게 {서비스 카테고리, 키} 리스트를 전송한다. 따라서, {서비스 카테고리, 키} 리스트는 셀 내의 하나 혹은 복수의 STA/단말에게 공유되며, 이들 키는 P2P 서비스 발견 및 통신을 위해 사용된다. 여기서, {서비스 카테고리, 키} 리스트는 (STA/단말이 관심 있는 서비스에 기초하여) STA/단말-특정(specific), STA/단말 그룹-특정, 셀-특정 방식으로 전송될 수 있다. 기지국이 STA/단말-특정(specific), STA/단말 그룹-특정하게 {서비스 카테고리, 키} 리스트를 전송하기 위해, 셀 내의 STA/단말들은 자신이 관심 있는 하나 이상의 서비스에 대한 정보(예, 서비스 리스트)를 미리 셀룰러 기지국에게 전송할 수 있다.

[65] 본 예에 따르면, 서비스 카테고리에 대응하여 키가 할당되므로, P2P 통신은 서비스 카테고리에 기반하여 수행된다. 즉, 동일한 서비스 카테고리(즉, 동일한 키)를 사용하는 복수의 STA/단말들간에 P2P 통신이 수행되며, P2P를 수행하는 STA/단말들은 서로에 대해 알 필요가 없다. 따라서, STA/단말은 프락시머티(proximity)에 있는 다른 STA/단말에 대한 정보 또는 다른 STA/단말이 속하는 그룹에 대한 정보를 모르는 상태에서 프락시머티(proximity)에 있는 하나 이상의 다른 STA/단말과 P2P 통신을 수행하는 것이 가능하다. 이와 같이, P2P 통신을 수행하는 주체에 대한 익명성(anonymous)을 보장함으로써, 실제 P2P 그룹을 형성하는 과정을 거치지 않더라도 안전한(secure) P2P 서비스 그룹을 형성하는 것이 가능하다. 즉, 기지국에서 셀 내의 STA/단말에게 {서비스 카테고리, 키} 리스트를 전송함으로써, STA/단말은 P2P 통신용 키를 획득할 뿐만 아니라, 어떤 P2P 서비스 그룹에 속하는 과정을 거치지 않더라도 해당 P2P 서비스 그룹에 속한 경우의 동작을 수행할 수 있다.

[66] 도 7는 본 예에 따른 그룹 키 분배/관리 과정을 예시한다. 도 7을 참조하면, 그룹 키 관리/분배 과정 및 그에 따른 P2P 통신은 다음과 같이 수행될 수 있다.

[67] 제1 단계; STA/단말이 쏘셜 P2P 서비스 참여에 관심이 있는 경우, 상기 STA/단말은 기지국에게 P2P 그룹 키(예, 쏘셜 P2P 키)의 리스트를 요청할 수 있다. 이로 제한되는 것은 아니지만, 서비스 카테고리, 해당 카테고리에 대한 ID (S1, S2, ..., Sn)(n: 1 이상의 정수), 서비스 카테고리에 대한 설명은 표 1과 같이 주어질 수 있다.

[68] 표 1

[Table 1]

ID	Service Category	Description
0	Social P2P chatting	STA/UE talk to each other (unicast or multicast) (similar to Kakao talk)
1	Socail Advertisement	STA/UE broadcasts advertisement information such as coupons, weekly ad, special deals, etc
2	Social map	STA/UE exchange data for location-dependent information such as local restaurant review, theater movie list, etc
3	On-line gaming	STA/UE participate on-line multi-party gaming without accessing a centralized game server
4-255	Reserved	

[69] 제2 단계: P2P 그룹 키 리스트에 대한 요청을 수신 후, 기지국은 셀 내에서 지원되는 서비스 카테고리에 대해 (서비스 카테고리 식별 정보(예, ID), 키) 리스트를 STA/단말에게 전송한다({S1,K1),(S2,K2),...,(Sn,Kn)}).

[70] 제3 단계: STA/단말은 특정 서비스 카테고리에 속하는 메시지를 그룹 키를 이용하여 암호화/해독화를 수행할 수 있다. 구체적으로, STA/단말이 서비스 카테고리 Si를 위한 메시지를 전송하는 경우, STA/단말은 서비스 카테고리 Si에 대응하는 키 Ki로 해당 메시지를 암호화할 수 있다. 이와 대응하여, STA/단말이 서비스 카테고리 Si를 위한 메시지를 수신하거나 해당 서비스를 탐색하는 경우, STA/단말은 서비스 카테고리 Si에 대응하는 키 Ki로 수신 메시지의 해독을 시도할 수 있다. 즉, STA/단말은 관심이 있는 서비스 카테고리에 대응하는 키만을 이용하여 수신 메시지의 해독을 시도할 수 있다. 이 경우, STA/단말이 복수의 서비스 카테고리에 속하는 메시지를 수신하려는 경우, STA/단말은 해당하는 복수의 키를 이용하여 수신 메시지의 해독을 시도할 수 있다. 또한, 그룹 키를 이용한 서비스 탐색/메시지 검출을 보다 용이하게 하기 위하여, 그룹 키에 관한 정보(혹은, 서비스 카테고리, 서비스 카테고리 ID)가 메시지 헤더에 포함될 수 있고, 이를 통해 상대 STA/단말은 원치 않는 그룹(혹은 서비스 카테고리)에 대한 데이터를 용이하게 필터링 할 수 있다. 구체적으로, 원치 않는 그룹(혹은 서비스 카테고리)에 대한 데이터는 PHY(Physical) 계층에서 필터링 되고, 필터링 되지 않은 데이터는 MAC(Medium Access Control) 계층에서 해독화 될 수 있다. 본 예에 따라, 서비스 그룹에 할당된 키를 공유한 P2P 통신을 이용할 경우, 한 STA/단말은 대상 STA/단말의 정보(예 STA/단말 ID) 또는 대상 STA/단말이 속하는 그룹에 관한 정보를 알지 못하더라도 데이터를 전송/수신할 수 있다.

[71] 본 예에서 제안하는 그룹 키는 소정 조건에 따라 갱신될 수 있다. 예를 들어,

기지국은 STA/단말에게 그룹 키를 제공하고 "KEY EXPIRATION" 타이머를 세팅할 수 있다. "KEY EXPIRATION" 타이머는 STA/단말에게 그룹 키를 전송한 뒤 T 시간 이후에 만료될 수 있다. "KEY EXPIRATION" 타이머가 만료될 경우, 기지국은 그룹 키를 재생성하고 (서비스 카테고리 ID, 갱신된 키) 리스트를 STA/단말에게 전송할 수 있다. 또한, STA/단말은 기지에게 그룹 키(예, 쏘셜 P2P 키)의 갱신을 요청하고, 기지국은 이를 고려하여 그룹 키 갱신할 수 있다. STA/단말은 기지에게 그룹 키의 갱신을 요청하는 것은 단말 내에 설정된 타이머가 만료된 경우에 이뤄질 수 있다. 이 경우, 타이머는 그룹 키를 제공 받은 경우에 동작하여 T1 시간 이후에 만료될 수 있다.

[72] **방안 2: P2P를 위한 개별 키 분배**

[73] 방안 1의 그룹 키 메카니즘을 정리하면 다음의 특징이 있다: (1) 셀룰러 네트워크에서 인증된 어떤 STA/단말도 셀 내에서 지원되는 모든 서비스 또는 그룹의 메시지를 암호화/해독화 할 수 있도록 그룹 키를 제공, (2) 원치 않는 그룹(혹은 서비스 카테고리)에 대한 데이터는 PHY(Physical) 계층에서 필터링 되고, 필터링 되지 않은 데이터는 MAC(Medium Access Control) 계층에서 해독화, (3) 서비스 카테고리에 대응하는 그룹 키에 기반하여 P2P 통신을 수행하므로 상대 STA/단말에 대한 정보 없이도 데이터 송수신이 가능하다.

[74] 그러나, 방안 1의 경우, 셀 내 모든 STA/단말에 의해 키가 공유되므로 P2P통신에서 프라이버시가 제공되지 못한다. 따라서, 본 방안에서는 셀룰러 네트워크를 이용하여 안전한(secure) P2P 연결을 제공하는 방법에 대해 설명한다. 본 방안에서는 셀 내 STA/단말은 기존 이웃 발견 과정(예, 도 4)을 통해 P2P 통신이 가능한 셀 내 다른 STA/단말의 존재 및 식별 정보(예, STA/단말 ID)를 알고 있다고 가정한다.

[75] 도 8에 본 예에 따른 개별 키 분배/관리 과정을 예시하였다. 여기서, 개별 키는 P2P 피어(peer)들(즉, 2개의 STA/단말)이 공유하는 키, 또는 제한된 수 또는 제한된 그룹의 STA/단말들만이 공유하는 키를 의미할 수 있다. 도 8을 참조하면, 개별 키 관리/분배 과정 및 그에 따른 P2P 통신은 다음과 같이 수행될 수 있다.

[76] 제1 단계; STA/단말(예, UE1)은 특정 STA/단말(예, UE3)과의 P2P 연결을 원하는 경우, 기지국에게 UE3과의 P2P 세션을 위한 키를 요청할 수 있다. 이를 위해, 키 요청 메시지는 상대 STA/단말에 대한 식별 정보(예, STA/단말 ID), 원하는 서비스(예, 쏘셜 채팅)에 대한 정보(예, 표 1의 ID 정보)를 포함할 수 있다. 서비스에 따라 불특정 STA/단말과 P2P 연결이 형성돼도 괜찮은 경우(예, 온라인 대전 게임), 상대 STA/단말에 대한 식별 정보(예, STA/단말 ID)는 생략되거나, 미리 정해진 특정 값으로 설정될 수 있다.

[77] 제2 단계: UE1으로부터 P2P 키를 요청 받은 후, 기지국은 UE1 및 UE3에게 각 피어의 공개(public) 키를 제공한다. 도면을 참조하면, UE1의 개인(private) 키 K_UE1이 UE3에게 제공/공개되고, UE3의 개인 키 K_UE3이 UE1에게 제공/공개된다. UE3은 UE1이 요청한 STA/단말일 수이거나, 서비스 종류에 따라

기지국이 임의로 선정한 STA/단말일 수 있다.

[78] 제3 단계: STA/단말은 공개 키를 이용해 데이터를 암호화하고, 상대 STA/단말은 자신의 개인 키를 이용해 수신 데이터를 해독화한다. 도면을 참조하면, UE1은 공개 키 K_UE3을 이용해 전송 데이터를 암호화하고, UE3은 개인 키 K_UE3을 이용해 수신 데이터를 해독화한다. 반대로, UE3은 공개 키 K_UE1을 이용해 전송 데이터를 암호화하고, UE1은 개인 키 K_UE1을 이용해 수신 데이터를 해독화한다.

[79] 공개 키를 STA/단말이 요청한 경우에만 제공하는 것은, STA/단말 피어의 개수에 비해 설정되는 P2P 세션의 개수가 적은 경우 보다 효율적일 수 있다.

[80] 도 9는 본 발명에 적용될 수 있는 WLAN P2P 장치를 예시한다.

[81] 도 9를 참조하면, WLAN-기반 P2P 네트워크는 제1 P2P 장치(110) 및 제2 P2P 장치(120)을 포함한다. 제1 P2P 장치(110)는 프로세서(112), 메모리(114) 및 무선 주파수(Radio Frequency, RF) 유닛(116)을 포함한다. 프로세서(112)는 본 발명에서 제안한 절차 및/또는 방법들을 구현하도록 구성될 수 있다. 메모리(114)는 프로세서(112)와 연결되고 프로세서(112)의 동작과 관련한 다양한 정보를 저장한다. RF 유닛(116)은 프로세서(112)와 연결되고 무선 신호를 송신 및/또는 수신한다. RF 유닛(116)은 셀룰러 통신 모듈과 WLAN 통신 모듈(예, Wi-Fi, ZigBee, 스몰 셀(small cell)에 기반한 면허 밴드(licensed band) 용 통신 모듈)을 모두 포함한다. 제2 P2P 장치(120)는 프로세서(122), 메모리(124) 및 RF 유닛(126)을 포함한다. 프로세서(122)는 본 발명에서 제안한 절차 및/또는 방법들을 구현하도록 구성될 수 있다. 메모리(124)는 프로세서(122)와 연결되고 프로세서(122)의 동작과 관련한 다양한 정보를 저장한다. RF 유닛(126)은 프로세서(122)와 연결되고 무선 신호를 송신 및/또는 수신한다. RF 유닛(126)은 셀룰러 통신 모듈과 WLAN 통신 모듈(예, Wi-Fi, ZigBee, 스몰 셀(small cell)에 기반한 면허 밴드(licensed band) 용 통신 모듈)을 모두 포함한다. 제1 P2P 장치(110) 및/또는 제2 P2P 장치(120)는 단일 또는 다중 안테나를 가질 수 있다.

[82] 이상 설명된 실시예들은 본 발명의 구성요소들과 특징들이 소정 형태로 결합된 것들이다. 각 구성요소 또는 특징은 별도의 명시적 언급이 없는 한 선택적인 것으로 고려되어야 한다. 각 구성요소 또는 특징은 다른 구성요소나 특징과 결합되지 않은 형태로 실시될 수 있다. 또한, 일부 구성요소들 및/또는 특징들을 결합하여 본 발명의 실시예를 구성하는 것도 가능하다. 본 발명의 실시예들에서 설명되는 동작들의 순서는 변경될 수 있다. 어느 실시예의 일부 구성이나 특징은 다른 실시예에 포함될 수 있고, 또는 다른 실시예의 대응하는 구성 또는 특징과 교체될 수 있다. 특허청구범위에서 명시적인 인용 관계가 있지 않은 청구항들을 결합하여 실시예를 구성하거나 출원 후의 보정에 의해 새로운 청구항으로 포함시킬 수 있음은 자명하다.

[83] 본 발명에 따른 실시예는 다양한 수단, 예를 들어, 하드웨어, 펌웨어(firmware), 소프트웨어 또는 그것들의 결합 등에 의해 구현될 수 있다. 하드웨어에 의한

구현의 경우, 본 발명의 일 실시예는 하나 또는 그 이상의 ASICs(application specific integrated circuits), DSPs(digital signal processors), DSPDs(digital signal processing devices), PLDs(programmable logic devices), FPGAs(field programmable gate arrays), 프로세서, 콘트롤러, 마이크로 콘트롤러, 마이크로 프로세서 등에 의해 구현될 수 있다.

[84] 펌웨어나 소프트웨어에 의한 구현의 경우, 본 발명의 일 실시예는 이상에서 설명된 기능 또는 동작들을 수행하는 모듈, 절차, 함수 등의 형태로 구현될 수 있다. 소프트웨어 코드는 메모리 유닛에 저장되어 프로세서에 의해 구동될 수 있다. 상기 메모리 유닛은 상기 프로세서 내부 또는 외부에 위치하여, 이미 공지된 다양한 수단에 의해 상기 프로세서와 데이터를 주고 받을 수 있다.

[85] 본 발명은 본 발명의 특징을 벗어나지 않는 범위에서 다른 특정한 형태로 구체화될 수 있음은 당업자에게 자명하다. 따라서, 상기의 상세한 설명은 모든 면에서 제한적으로 해석되어서는 아니되고 예시적인 것으로 고려되어야 한다. 본 발명의 범위는 첨부된 청구항의 합리적 해석에 의해 결정되어야 하고, 본 발명의 등가적 범위 내에서의 모든 변경은 본 발명의 범위에 포함된다.

산업상 이용가능성

[86] 본 발명은 P2P 통신, 구체적으로 WLAN-기반 P2P 통신을 위한 장치에 사용될 수 있다.

청구범위

[청구항 1] 셀룰러 네트워크에 연결된 제1 P2P(Peer to Peer) 장치에서 WLAN(Wireless Local Area Network)-기반 P2P 통신을 수행하는 방법에 있어서,
셀룰러 기지국으로부터 하나 이상의 키 정보를 수신하되, 각각의 키 정보는 서비스 식별 정보와 대응하는 키 값을 포함하는 단계;
제2 P2P 장치로부터 암호화된 데이터 신호를 수신하는 단계;
상기 하나 이상의 키 정보 중, 상기 제1 P2P 장치가 관심 있는 하나 이상의 서비스에 대응하는 하나 이상의 키를 이용하여 상기 암호화된 데이터 신호의 해독화를 시도하는 위한 과정을 수행하는 단계를 포함하는 방법.

[청구항 2] 제1항에 있어서,
상기 암호화된 데이터 신호의 수신은 상기 제2 P2P 장치에 대한 정보 또는 상기 제2 P2P 장치가 속하는 그룹에 대한 정보가 없는 상태에서 수신되는 방법.

[청구항 3] 제1항에 있어서,
상기 하나 이상의 키 정보에 포함된 복수의 키 값은 상기 셀룰러 기지국이 서비스를 제공하는 셀 내의 모든 P2P 장치 또는 동일한 P2P 서비스에 관심이 있는 P2P 장치에 동일하게 설정되는 방법.

[청구항 4] 제1항에 있어서,
상기 암호화된 데이터 신호의 헤더는 키 식별 정보, 서비스 식별 정보 중 적어도 하나를 포함하는 방법.

[청구항 5] 제4항에 있어서,
상기 암호화된 데이터 신호의 헤더가 상기 제1 P2P가 관심 있는 키 또는 서비스에 관한 정보를 갖지 않는 경우, 상기 암호화된 데이터 신호는 버려지고,
상기 암호화된 데이터 신호의 헤더가 상기 제1 P2P가 관심 있는 키 또는 서비스에 관한 정보를 갖는 경우, 상기 암호화된 데이터 신호에 대한 해독화 과정이 수행되는 방법.

[청구항 6] 제5항에 있어서,
상기 암호화된 데이터 신호는 PHY(Physical) 계층에서 버려지고,
상기 암호화된 데이터 신호에 대한 해독화 과정은 MAC(Medium Access Control) 계층에서 수행되는 방법.

[청구항 7] 제1항에 있어서,
상기 하나 이상의 키 정보는 소정의 타이머가 만료되는 경우 갱신되는 방법.

[청구항 8] 제1항에 있어서,

상기 하나 이상의 키 정보에 대해 갱신을 요청하는 정보를 상기 셀룰러 기지국에게 전송하는 단계를 더 포함하는 방법.

[청구항 9] 셀룰러 네트워크에 연결되고, WLAN(Wireless Local Area Network)-기반 P2P(Peer to Peer) 통신을 수행하도록 구성된 제1 P2P 장치에 있어서,
무선 주파수(Radio Frequency, RF) 유닛; 및
프로세서를 포함하고,
상기 프로세서는 셀룰러 기지국으로부터 하나 이상의 키 정보를 수신하되, 각각의 키 정보는 서비스 식별 정보와 대응하는 키 값을 포함하고, 제2 P2P 장치로부터 암호화된 데이터 신호를 수신하며, 상기 하나 이상의 키 정보 중, 상기 제1 P2P 장치가 관심 있는 하나 이상의 서비스에 대응하는 하나 이상의 키를 이용하여 상기 암호화된 데이터 신호의 해독화를 시도하는 위한 과정을 수행하도록 구성된 제1 P2P 장치.

[청구항 10] 제9항에 있어서,
상기 암호화된 데이터 신호의 수신은 상기 제2 P2P 장치에 대한 정보 또는 상기 제2 P2P 장치가 속하는 그룹에 대한 정보가 없는 상태에서 수신되는 제1 P2P 장치.

[청구항 11] 제9항에 있어서,
상기 하나 이상의 키 정보에 포함된 복수의 키 값은 상기 셀룰러 기지국이 서비스를 제공하는 셀 내의 모든 P2P 장치 또는 동일한 P2P 서비스에 관심이 있는 P2P 장치에 동일하게 설정되는 제1 P2P 장치.

[청구항 12] 제9항에 있어서,
상기 암호화된 데이터 신호의 헤더는 키 식별 정보, 서비스 식별 정보 중 적어도 하나를 포함하는 제1 P2P 장치.

[청구항 13] 제12항에 있어서,
상기 암호화된 데이터 신호의 헤더가 관심 있는 키 또는 서비스에 관한 정보를 갖지 않는 경우, 상기 암호화된 데이터 신호는 버려지고,
상기 암호화된 데이터 신호의 헤더가 관심 있는 키 또는 서비스에 관한 정보를 갖는 경우, 상기 암호화된 데이터 신호에 대한 해독화 과정이 수행되는 제1 P2P 장치.

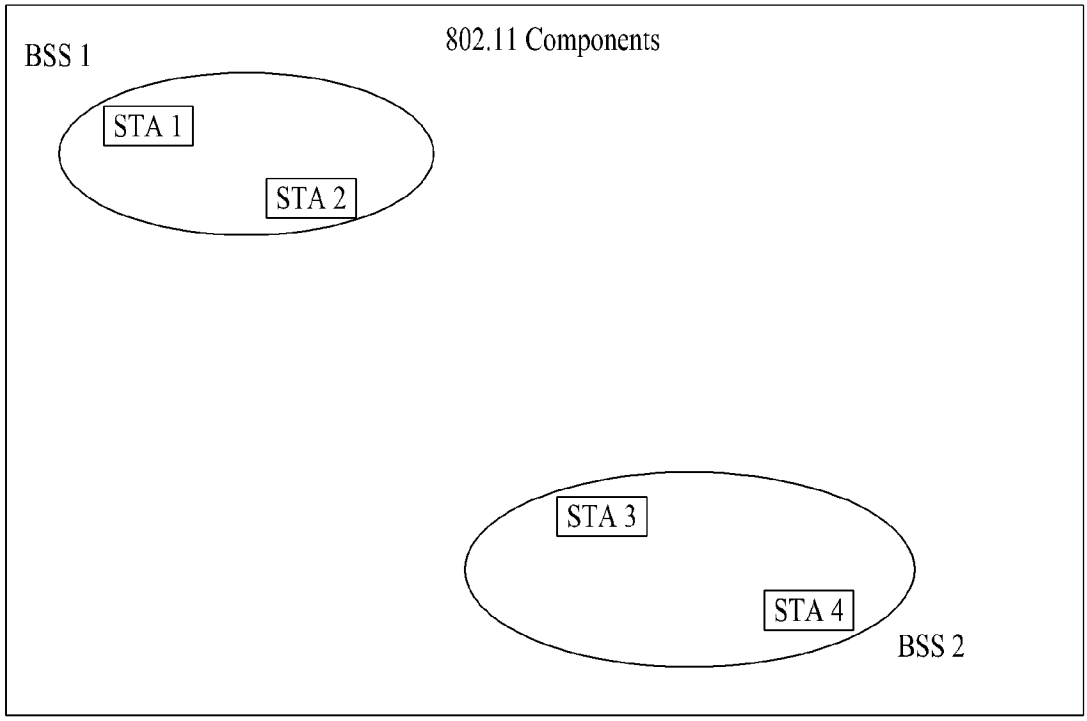
[청구항 14] 제13항에 있어서,
상기 암호화된 데이터 신호는 PHY(Physical) 계층에서 버려지고,
상기 암호화된 데이터 신호에 대한 해독화 과정은 MAC(Medium Access Control) 계층에서 수행되는 제1 P2P 장치.

[청구항 15] 제9항에 있어서,

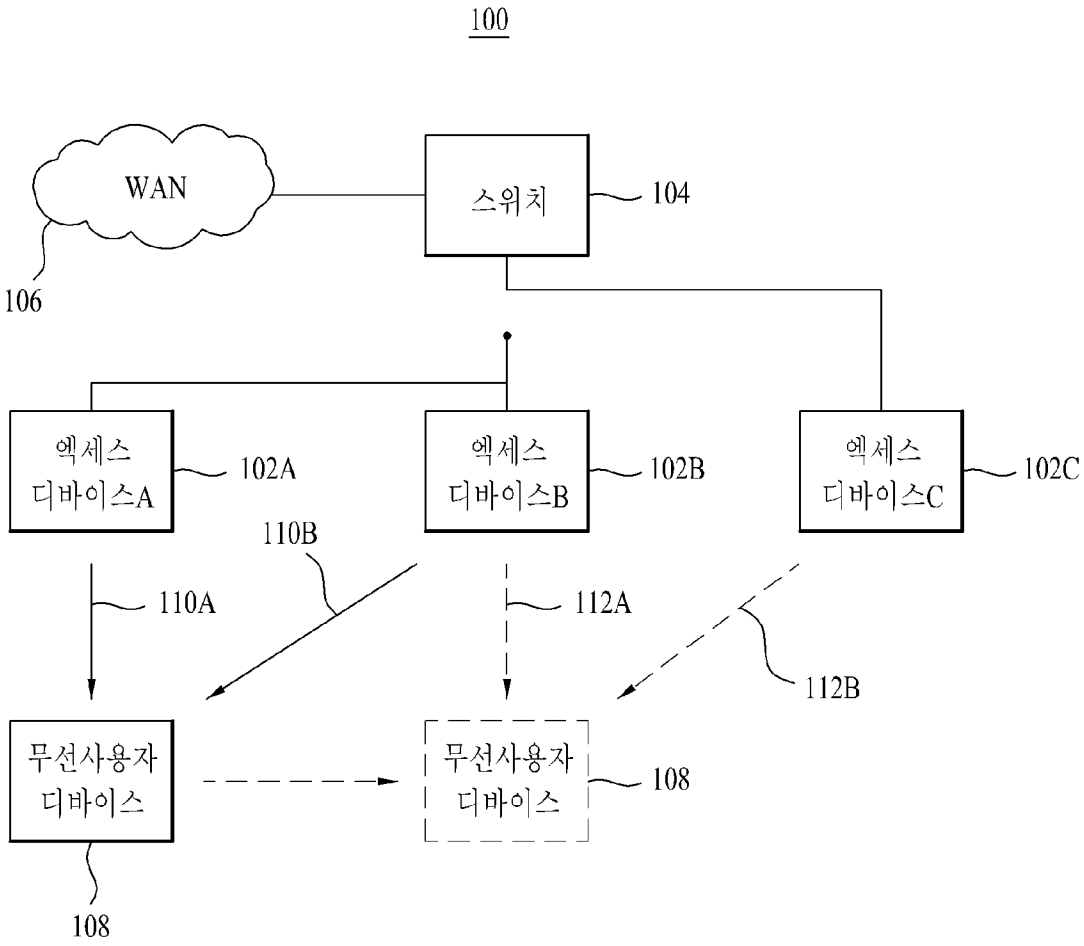
상기 하나 이상의 키 정보는 소정의 타이머가 만료되는 경우 갱신되는 제1 P2P 장치.

[청구항 16] 제9항에 있어서,
상기 프로세서는 또한 상기 하나 이상의 키 정보에 대해 갱신을 요청하는 정보를 상기 셀룰러 기지국에게 전송하도록 구성된 제1 P2P 장치.

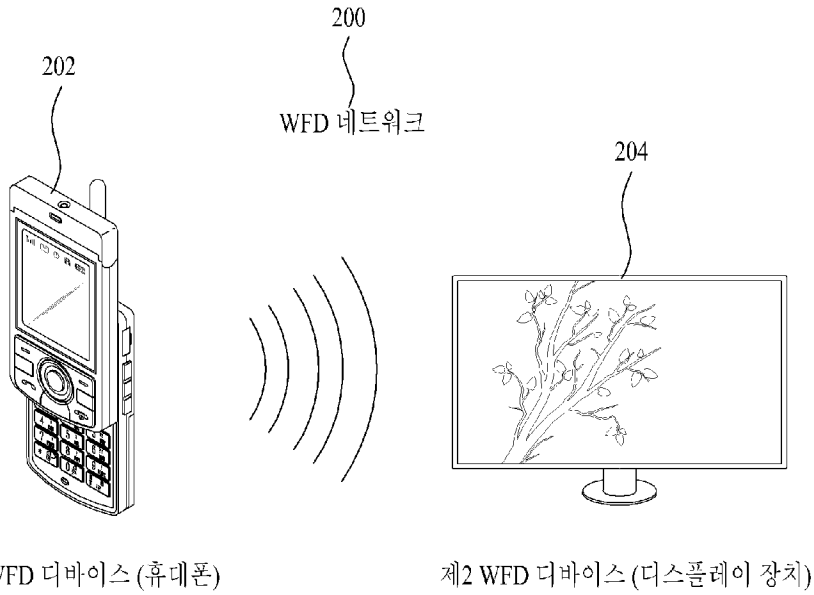
[Fig. 1a]


802.11 Components
BSS 1
STA 1
STA 2
STA 3
STA 4
BSS 2

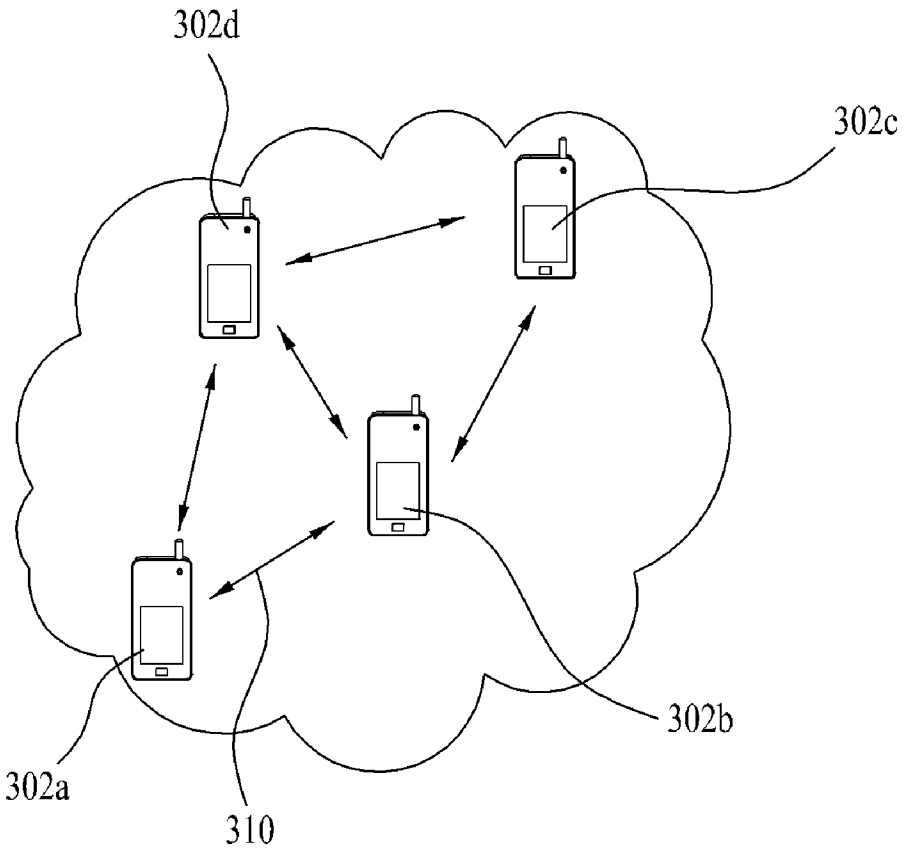
[Fig. 1b]


100
WAN
106
스위치
104
엑세스 디바이스A
102A
엑세스 디바이스B
102B
엑세스 디바이스C
102C
110B
110A
112A
112B
무선사용자 디바이스
108
무선사용자 디바이스
108

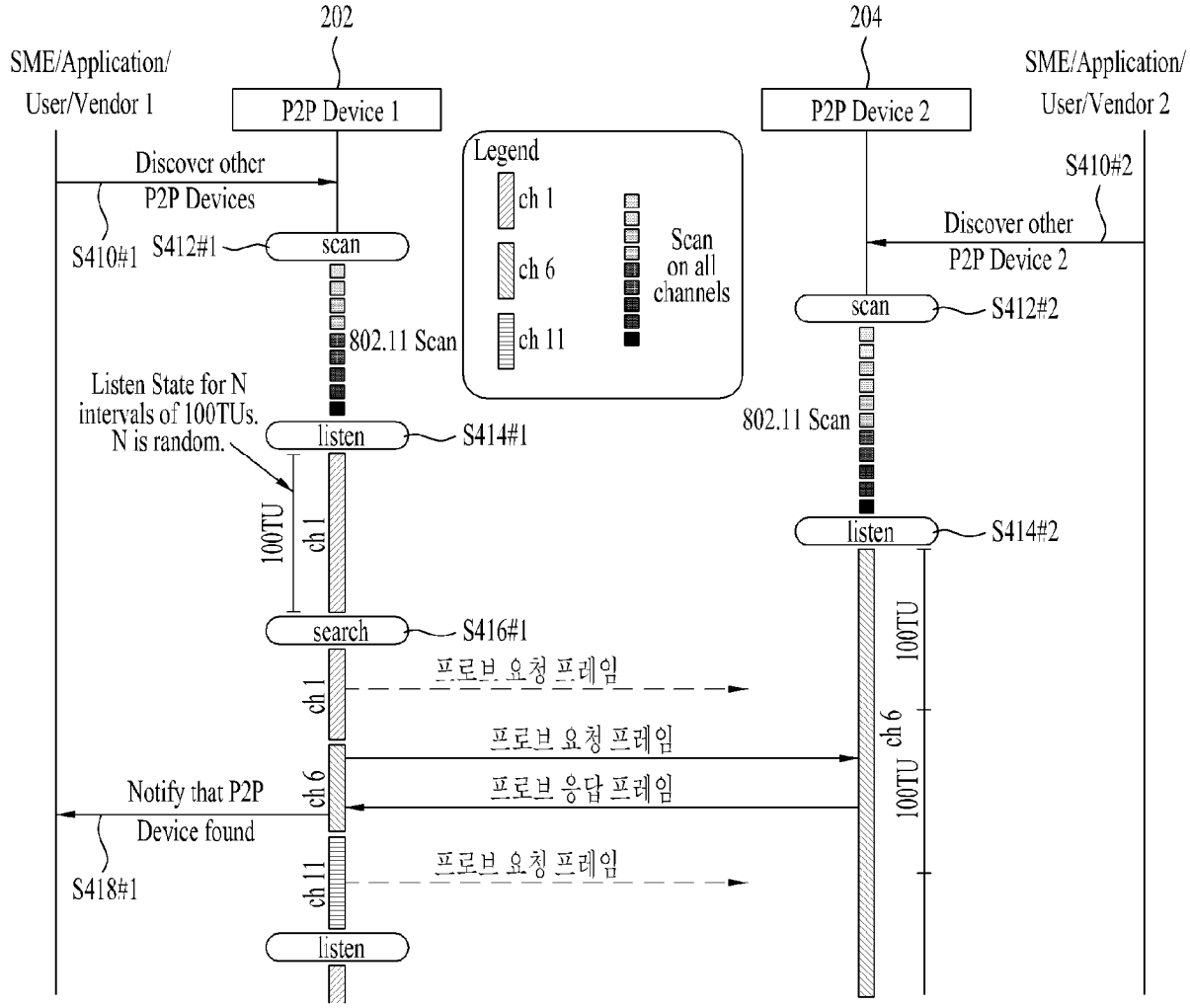
[Fig. 2]


200
202
WFD 네트워크
204
제1 WFD 디바이스 (휴대폰)
제2 WFD 디바이스 (디스플레이 장치)

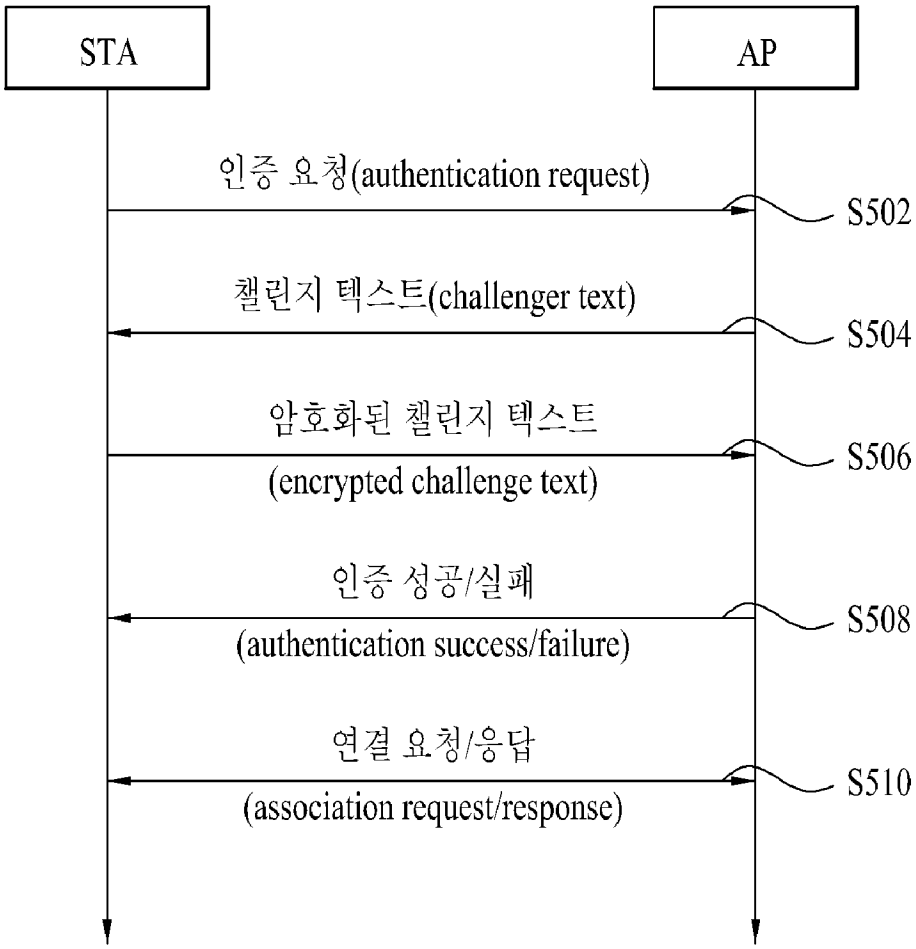
[Fig. 3]


302d
302c
302b
302a
310

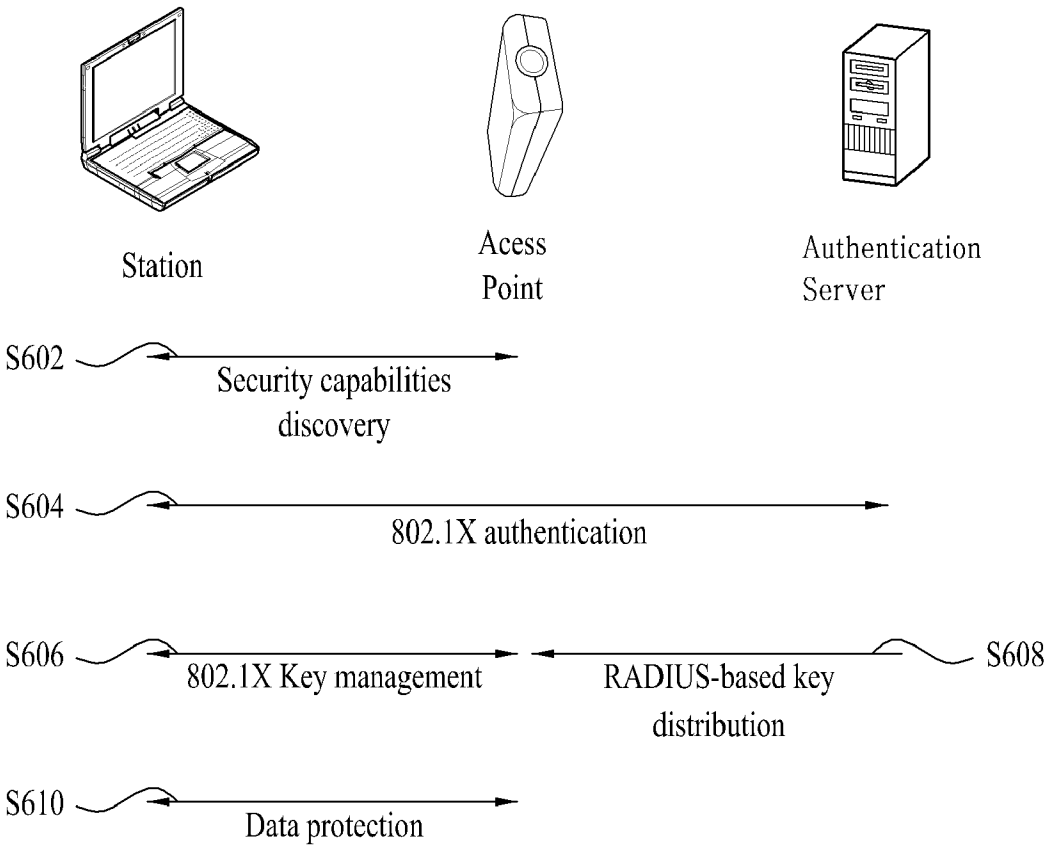
[Fig. 4]


202
204
SME/Application/
User/Vendor 1
P2P Device 1
P2P Device 2
SME/Application/
User/Vendor 2
Legend
ch 1
ch 6
ch 11
Scan on all channels
Discover other
P2P Devices
S410#1
S412#1
scan
802.11 Scan
S410#2
Discover other
P2P Device 2
scan
S412#2
802.11 Scan
Listen State for N intervals of 100TUs. N is random.
listen
S414#1
listen
S414#2
100TU
ch 1
search
S416#1
프로브 요청 프레임
프로브 요청 프레임
프로브 응답 프레임
Notify that P2P Device found
S418#1
프로브 요청 프레임
ch 6
ch 11
100TU
100TU
listen

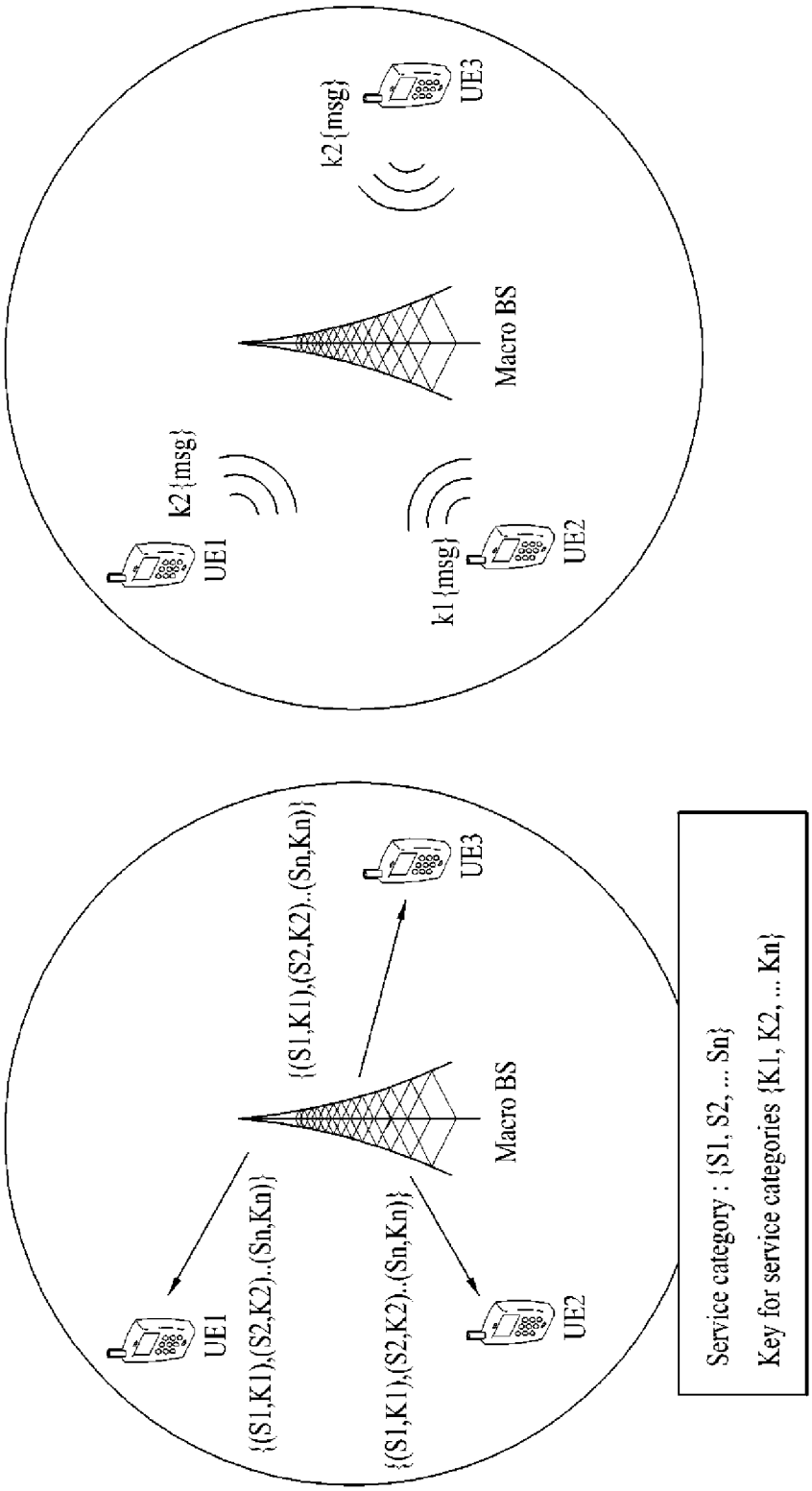
[Fig. 5]


STA
AP
인증 요청(authentication request)
S502
챌린지 텍스트(challenger text)
S504
암호화된 챌린지 텍스트
(encrypted challenge text)
S506
인증 성공/실패
(authentication success/failure)
S508
연결 요청/응답
(association request/response)
S510

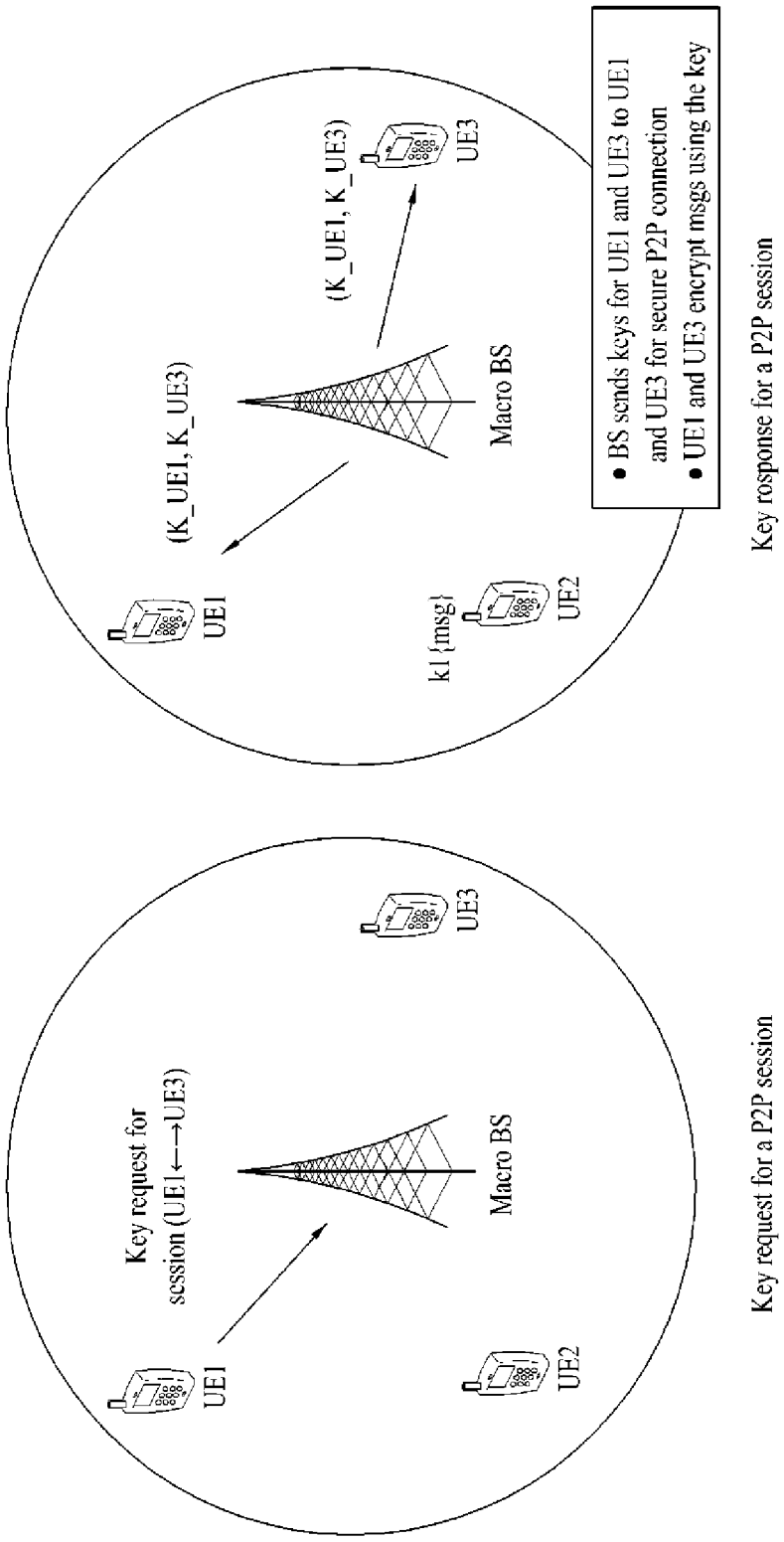
[Fig. 6]


Station
Acess Point
Authentication Server
S602
Security capabilities discovery
S604
802.1X authentication
S606
802.1X Key management
S608
RADIUS-based key distribution
S610
Data protection

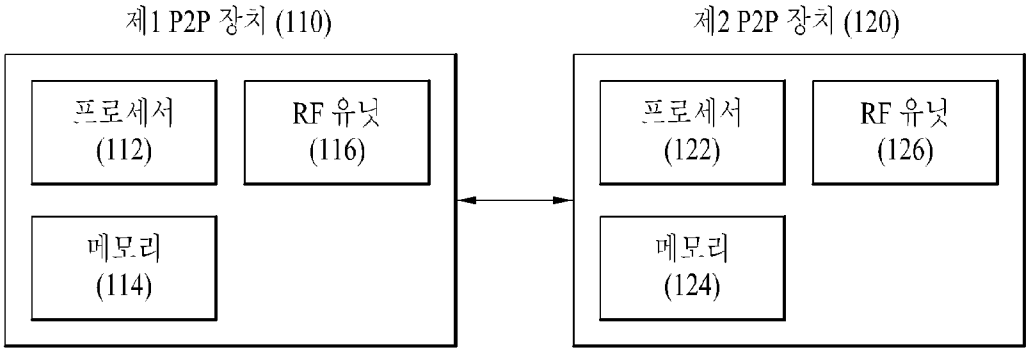
[Fig. 7]


k2{msg}
UE3
Macro BS
k2{msg}
UE1
k1{msg}
UE2
{(S1,K1),(S2,K2)..(Sn,Kn)}
UE3
Macro BS
UE1
{(S1,K1),(S2,K2)..(Sn,Kn)}
{(S1,K1),(S2,K2)..(Sn,Kn)}
UE2
Service category : {S1, S2, ... Sn}
Key for service categories {K1, K2, ... Kn}

[Fig. 8]


Key request for a P2P session
Key request for session (UE1←→UE3)
UE1
Macro BS
UE3
UE2
Key response for a P2P session
(K_UE1, K_UE3)
UE1
Macro BS
(K_UE1, K_UE3)
UE3
k1{msg}
UE2
• BS sends keys for UE1 and UE3 to UE1 and UE3 for secure P2P connection
• UE1 and UE3 encrypt msgs using the key

[Fig. 9]


제1 P2P 장치 (110)
프로세서 (112)
RF 유닛 (116)
메모리 (114)
제2 P2P 장치 (120)
프로세서 (122)
RF 유닛 (126)
메모리 (124)