

(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국



(10) 국제공개번호

(43) 국제공개일
2022 년 2 월 10 일 (10.02.2022) WIPO PCT

WO 2022/030656 A1

(51) 국제특허분류:

H04L 27/34 (2006.01) H04L 29/06 (2006.01)

H04L 1/00 (2006.01) H04B 1/00 (2006.01)

H04L 29/08 (2006.01)

(21) 국제출원번호: PCT/KR2020/010235

(22) 국제출원일: 2020 년 8 월 3 일 (03.08.2020)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(71) 출원인: 한국과학기술원 (KOREA ADVANCED INSTITUTE OF SCIENCE AND TECHNOLOGY) [KR/KR]; 34141 대전시 유성구 대학로 291, Daejeon (KR).

(72) 발명자: 정우재 (JEONG, Woo Jae); 34141 대전시 유성구 대학로 291, Daejeon (KR). 김성민 (KIM, Song Min); 34141 대전시 유성구 대학로 291, Daejeon (KR). 정진환 (JUNG, Jin Hwan); 34141 대전시 유성구 대학로 291, Daejeon (KR). 양석원 (YANG, Seok Won); 34141 대전시 유성구 대학로 291, Daejeon (KR). 이윤 (YI, Yung); 34141 대전시 유성구 대학로 291, Daejeon (KR).

(74) 대리인: 특허법인 아이시스 (ISIS IP LAW LLC); 06100 서울시 강남구 테헤란로63길 14, 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, 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.

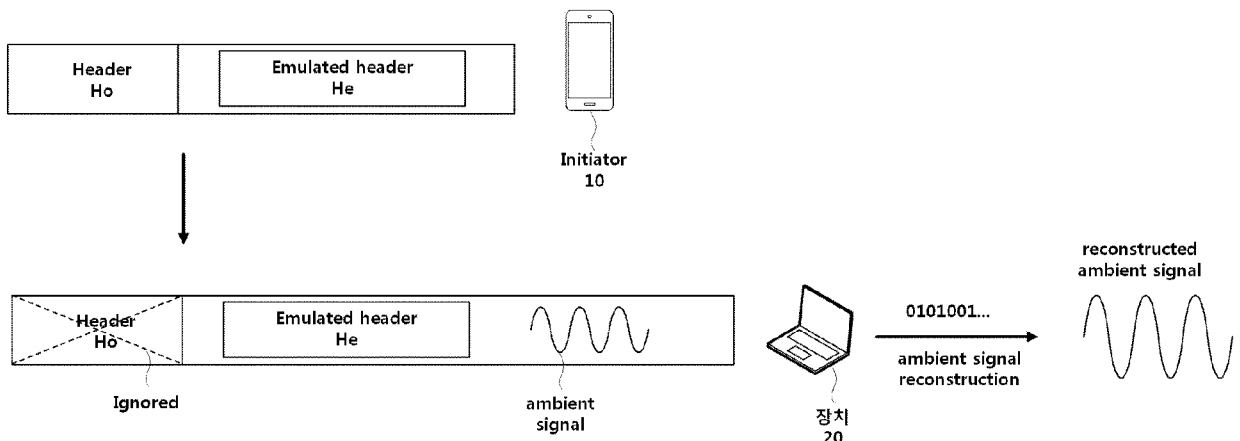
(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS,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

공개:

— 국제조사보고서와 함께 (조약 제21조(3))

(54) Title: TRANSMISSION SIDE, RECEPTION SIDE, AND METHOD FOR OPERATING WIRELESS APPARATUS COMPRISING SAME

(54) 발명의 명칭: 송신측, 수신측 및 이들을 포함하는 무선 장치 구동 방법



20 ... Apparatus

(57) Abstract: A method for operating a wireless apparatus according to the present embodiment comprises the steps of: the transmission side transmitting a header, emulated using a second protocol, concealed in a payload of a packet regulated by a first protocol; the receiving side receiving the emulated header and an ambient signal; and a bit sequence being obtained by decoding the ambient signal according to the second protocol.

(57) 요약서: 본 실시예에 의한 무선 장치 구동 방법은: 전송측이 제2 프로토콜로 에뮬레이트(emulate)된 헤더를 제1 프로토콜로 규정된 패킷(packet)의 페이로드(payload)에 은닉하여 전송하는 단계와, 수신측이 에뮬레이트된 헤더와, 주변 신호(ambient signal)를 수신하는 단계 및 주변 신호를 제2 프로토콜에 따라 디코딩하여 비트 시퀀스를 얻는 단계를 포함한다.

WO 2022/030656 A1

명세서

발명의 명칭: 송신측, 수신측 및 이들을 포함하는 무선 장치 구동 방법

기술분야

- [1] 본 기술은 송신측, 수신측 및 이들을 포함하는 무선 장치 구동 방법과 관련된다.

배경기술

- [2] 무선 장치가 폭발적으로 증가함에 따라 물리 계층 신호 분석은 네트워크 계획, 보안 및 개인 정보 보호 (예: 드론 및 스파이 캠 탐지) 및 원격 감지를 통한 모바일 상태의 간섭 최소화 등의 고유한 영역에서 유익하다. 소프트웨어 무선 장치(SDR, Software defined radio)는 이러한 서비스를 실현하는데 매우 효과적인 것으로 알려져 있지만, 고가의 하드웨어로 인해 최종 사용자가 거의 배포하거나 사용하지 못하는 실정이다. 저비용 SDR을 사용할 수 있지만 2.4GHz 이하에서 작동하여 동작 주파수 범위는 비면허 대역을 벗어난다.

발명의 상세한 설명

기술적 과제

- [3] 본 기술은 하드웨어 및 펌웨어를 변경하지 않고 상용 와이파이를 사용하는 소프트웨어 정의 라디오(SDR)와 관련된다. 본 기술은 널리 보급된 와이파이 인프라와 호환성을 갖춘 소프트웨어 라디오 장치를 이용하여 와이파이 사용자 및 가정에 전파하여 일상 생활을 향상시키고자 한다.

과제 해결 수단

- [4] 본 실시예에 의한 무선 장치 구동 방법은: 전송측이 제2 프로토콜로 에뮬레이트(emulate)된 헤더를 제1 프로토콜로 규정된 패킷(packet)의 페이로드(payload)에 은닉하여 전송하는 단계와, 수신측이 에뮬레이트된 헤더와, 주변 신호(ambient signal)를 수신하는 단계 및 주변 신호를 제2 프로토콜에 따라 디코딩하여 비트 시퀀스를 얻는 단계를 포함한다.
- [5] 본 실시예에 의한 전송측은 제2 프로토콜로 에뮬레이트(emulate)된 헤더를 제1 프로토콜에 따른 패킷의 페이로드에 은닉하여 전송한다.
- [6] 본 실시예에 의한 수신측은 제2 프로토콜로 에뮬레이트(emulate)되되, 제1 프로토콜로 규정된 패킷(packet)의 페이로드(payload)에 은닉되어 전송된 헤더 및 주변 신호(ambient signal)를 수신하고, 주변 신호를 제2 프로토콜에 따라 디코딩하여 비트 시퀀스를 얻고, 비트 시퀀스로부터 주변 신호를 재구성(reconstruction)한다.

발명의 효과

- [7] 본 기술에 의하면 주변 신호(ambient signal)를 통하여 RF 장치를 식별할 수 있고, 주변 신호의 스펙트럼 모니터링 및 주변 신호를 디코딩할 수 있다는

장점이 제공된다.

도면의 간단한 설명

- [8] 도 1은 본 실시예에 의한 방법을 개요적으로 도시한 순서도이다.
- [9] 도 2는 본 실시예에 의한 방법이 수행되는 것으로 개요적으로 도시한 개요도이다.
- [10] 도 3은 802.11g의 표준에서 정의된 와이파이(WiFi) 헤더 구조를 도시한 도면이다.
- [11] 도 4(a)는 개시자가 제공하는 40MHz, 802.11n의 패킷 구조를 도시한 도면이고, 도 4(b)는 20MHz, 802.11g의 에플레이트된 헤더의 구조를 도시한 도면이다.
- [12] 도 5(a)는 프리앰블에 포함된 10개의 슛 심볼(S)들을 도시한 도면이고, 도 5(b)는 페이로드의 심볼 구조를 개요적으로 도시한 도면이다.
- [13] 도 6(a)는 와이파이 헤더 내에 포함된 2.5 개의 룡 심볼(L)의 개요를 도시한 도면이고, 도 6(b)는 페이로드의 심볼 구조를 개요적으로 도시한 도면이다.
- [14] 도 7(a)는 페이로드에 사용된 64 QAM 포인트와 관련하여 룡 심볼과 슛 심볼을 포함하는 프리앰블 및 PHY 필드의 BPSK 콘스텔레이션 포인트를 도시한 도면이고, 도 7(b)는 슛 심볼의 에플레이션을 도시한 도면이며, 도 7(c)는 룡 심볼 및 PHY이 위치하는 점에서 가장 가까운 4 개의 지점(점선 박스)을 도시한 도면이다.
- [15] 도 8은 MAC 헤더에 사용된 16 QAM의 콘스텔레이션 매핑을 도시한 도면이다.
- [16] 도 9는 와이파이 인코딩 메커니즘과 코딩 에플레이션 메커니즘을 나타낸 도면이다.
- [17] 도 10은 개시자가 에플레이션한 와이파이 헤더의 예를 주파수 도메인으로 표시한 도면으로, 도 10(a)는 슛 심볼에 대한 에플레이션 결과를 도시하며, 도 10(b)는 16 QAM으로 변조된 MAC의 에플레이션 결과를 도시한 도면이다.
- [18] 도 11은 재구성된 신호(점선으로 도시됨)와 실제의 주변 신호(실선으로 도시됨) 사이의 오류를 도시한 도면이다.
- [19] 도 12(a)는 16 개의 QAM의 콘스텔레이션 점을 신호의 크기(즉, 신호의 전력)에 따라 3 단계(검정, 회색, 흰색)로 분류한 예를 도시한 도면이고, 도 12(b)는 신호의 워터폴(waterfall)을 도시한 도면이다.
- [20] 도 13(a)는 기준 직비 신호를 예시한 도면이고, 도 13(b)는 위상에 대한 코릴레이션 값의 변화를 도시한 도면이다.
- [21] 도 14(a)는 이상적인 신호와 위상 보상된 신호를 도시한 도면이고, 도 14(b)는 위상 보정된 직비 신호가 동일한 비트로 매핑되는 결과를 도시한 도면이다.
- [22] 도 15는 시간 영역에서 에플레이트된 신호의 형태와 이상적인 신호를 도시한 도면이다.
- [23] 도 16(a)는 본 실시예에 의한 장치와 상용 WNIC의 PRR을 도시한 도면이고, 도 16(b)는 재전송 회수에 따른 PRR을 도시한 도면이다.

- [24] 도 17(a)는 LOS 시나리오의 실험 설정을 도시한 도면이고, 도 17(b)는 LOS 시나리오에서의 PRR을 도시한 도면이다.
- [25] 도 18(a)는 개시자는 책상에 고정된 NLoS 환경에서 다양한 장치의 위치(A)-(D)를 도시한 도면이고, 도 18(b)는 각 위치별 PRR을 도시한 도면이다.
- [26] 도 19(a)는 Tx 전력이 -10 dBm에서 10 dBm으로 변할때 재구성된 직비 신호와 이상적인 직비 신호 사이의 최대 코릴레이션 값을 도시한 도면이고, 도 19(b)는 동일한 조건에서 재구성된 BLE 신호와 이상적인 BLE 신호 사이의 최대 코릴레이션 값을 도시한 도면이다.
- [27] 도 20(a) 및 도 20(b)는 각각 위에서 설명된 위상 보상을 수행하여 형성된 직비와 BLE의 위상 보정된 신호를 도시한다.
- [28] 도 21은 장치가 2.422GHz에서 전송된 BLE 신호를 캡처한 것을 도시한 도면이다.
- [29] 도 22(a), 도 22(b) 및 도 22(c)는 각각 2.410GHz 및 2.422GHz의 중심 주파수에서 캡처된 직비 신호 및 BLE 신호의 위터폴 플롯이다.
- [30] 도 23(a)와 도 23(b)는 각각 RC 자동차와 전자 레인지에서 나오는 RF 신호의 위터폴 플롯을 도시한 도면이다.
- [31] 도 24(a)는 TX 전력이 -5 dBm에서 10 dBm까지 변화할 때 개시자의 다양한 SER 성능을 도시한 도면이고, 24(b)는 SER 성능에 기초하여 10 dBm의 TX 전력에 대해 서로 다른 프레임 길이를 가진 FRR 성능을 도시한 도면이다.
- [32] 도 25는 장치 식별을 위하여 사용된 장치들을 도시한 도면이다.
- [33] 도 26은 M1-M6로 표시된 6개의 다른 모델과 3 개의 Xiaomi 8 폰 (M61-M63)의 스마트 장치 6 개를 분류한 휴대 전화 핑거 프린팅 실험 결과를 도시한 도면이다.
- [34] 도 27는 라우터 핑거 프린팅에 대한 결과를 도시한 도면이다.
- [35] 도 28은 수신기 동작 특성(ROC) 곡선을 도시한 도면이다.
- [36] 도 29는 3 개의 드론 사진이 있는 드론 실험 시나리오를 도시한다.
- [37] 도 30(a)는 장치에 의해 재구성된 Mavic Pro의 신호를 도시한 도면이고, 도 30(b)는 장치에 의해 재구성된 Solo의 신호를 도시한 도면이다.
- [38] 도 31은 USRP 및 장치에 의해 드론의 RF 신호가 캡처될 때 드론 탐지의 정확도를 도시한 도면이다
- [39] 도 32(a)는 반복 단계 수가 증가함에 따라 장치 및 USRP의 성능을 도시한 도면이고, 도 32(b)는 장치에 의해 재구성된 신호를 사용하여 드론 분류의 혼란 매트릭스를 도시한 도면이다.

발명의 실시를 위한 형태

- [40] 이하에서는 첨부된 도면들을 참조하여 본 실시예에 의한 방법을 설명한다. 도 1은 본 실시예에 의한 방법을 개요적으로 도시한 순서도이고, 도 2는 본 실시예에 의한 방법이 수행되는 것으로 개요적으로 도시한 개요도이다. 도 1 및 도 2를 참조하면, 본 실시예에 의한 방법은 개시자(initiator, 10)가 애플레이트된

와이파이 헤더(He)를 포함하는 패킷을 제공하는 단계(S10)와, 장치(20)가 주변 신호(ambient signal)를 디코딩하여 상응하는 비트 스트림을 출력하는 단계(S20)를 포함한다.

- [41] 도 3은 802.11g의 표준에서 정의된 와이파이(WiFi) 헤더 구조를 도시한다. 도 1 내지 도 3을 참조하면, 헤더는 프리앰블(preamble), PHY 및 MAC의 세 필드를 포함한다. 프리앰블(preamble)은 10 개의 쏫 심볼들과 2.5개의 롱 심볼들을 포함하며, 패킷 탐지, 동기화 및 채널 추정에 사용된다. PHY는 물리 계층 정보인 변조 타입, 코드 레이트 및 패킷 길이를 전달한다. MAC 헤더에는 프로토콜 버전 및 패킷 유형과 같은 링크 계층별 정보가 기재되어 있다. 와이파이 헤더를 수신하면, 수신기는 헤더에 지정된 변조 및 코드 레이트를 사용하여 패킷 길이 동안 헤더 이후의 페이로드(payload) 디코딩을 시작한다.
- [42] 개시자(intiator, 10)는 헤더(프리앰블, PHY, MAC 헤더)를 에뮬레이션(emulate)하고 페이로드에 은닉하여 장치(20)에 제공한다. 일 실시예로, 개시자(10)가 제공하는 패킷은 802.11n 프로토콜에 부합하는 패킷이며, 페이로드에 은닉된 헤더(He)는 802.11g 프로토콜에 따른 헤더이나, 802.11n 프로토콜에 따라 에뮬레이트되어 페이로드에 은닉된다.
- [43] 개시자(10)가 제공한 패킷을 장치(20)가 수신하나, 개시자가 제공한 원래 헤더(Ho)에 기재된 중심 주파수는 패킷의 중심 주파수가 상이하여 원래 헤더(Ho)는 무시되고, 장치(20)에서는 페이로드 내에 은닉되어 위치한 에뮬레이트된 헤더(He)에 따라 디코딩이 수행된다. 에뮬레이트된 헤더(He)에 상응하는 페이로드 디코딩은 에뮬레이트된 헤더(He)를 따르는 주변 신호(ambient signal)에 대하여 수행된다. 이에 따라 해당 주변 신호(ambient signal)를 재구성할 수 있는 출력 비트 시퀀스가 생성된다. 이하에서 보다 상세히 설명한다.
- [44] 일 실시예로, 개시자(10)는 40MHz 대역폭 802.11n으로 설정될 수 있으며, 이는 무선 네트워크 인터페이스 컨트롤러(WNIC, Wireless network interface controller)에서 일반적으로 지원된다. 40MHz 중에서 20MHz의 부분 스펙트럼이 에뮬레이트된 헤더에 사용되며 중심 주파수가 개시자와 다르다.
- [45] 도 4는 OFDM 헤더 에뮬레이션을 나타내는 도면으로, 도 4(a)는 개시자(10)가 제공하는 40MHz, 802.11n의 패킷 구조를 도시한 도면이고, 도 4(b)는 20MHz, 802.11g의 에뮬레이트된 헤더의 구조를 도시한 도면이다. 도 4(b)는 에뮬레이트된 헤더가 [-55, -3] 범위의 52 개의 쏫 심볼(가드 밴드를 제외한 16.25MHz)를 사용하는 예를 도시한다. 에뮬레이트된 헤더(He)의 중심 주파수는 와이파이 채널 2에 상응하는 2.417GHz이며 전체 40MHz의 중심 주파수와 상이하다. 따라서, 와이파이 채널 2에서 작동하는 장치(20)는 원래 헤더(Ho)를 무시하고 에뮬레이트된 헤더(He)에 따라 패킷을 디코딩한다. 설명되는 예에서, 개시자(10)는 채널 2에 상응하는 중심주파수로 802.11g 헤더를 형성하고 페이로드에 은닉하여 장치(20)에 제공하며, 장치는 채널 2로 동작한다. 그러나,

이는 실시예일 따름이며, 개시자(10)는 채널 2 이외의 다른 채널로 장치(20)과 호응하여 동작할 수 있다. 즉, 다른 채널의 장치는 다양한 개시자(10) 채널 및 에플레이션을 위한 서브 캐리어 할당에 의해 지원될 수 있다.

[46] 에플레이트된 헤더(He)는 개시자가 제공한 패킷의 페이로드 내에 은닉되어 있다. 에플레이트되어 페이로드에 은닉된 헤더(He)에 의하여 심볼 불일치(symbol mismatch) 및 별도의 변조로 인한 헤더와 페이로드 사이의 콘스텔레이션 불일치(costellation mismatch) 등이 발생한다. 아래에서 설명되는 과정을 통하여 상술한 불일치를 최소화하거나 제거한다.

[47] 도 4(b)에서, PHY와 MAC 필드는 하나의 페이로드 심볼에 일대일로 매핑되어 각각 심볼 5와 6으로 표시될 수 있다. 이는 PHY와 MAC 헤더가 페이로드와 같은 3.2 μ sec 심볼 + 0.8 μ sec 사이클릭 프리픽스(CP, cyclic prefix) 심볼 구조를 공유하기 때문이다. 그러나 프리앰블(preamble) 심볼 구조는 페이로드의 심볼 구조와 다르다. 일 예로, 프리앰블에 포함된 쏫 심볼(S) 및 롱 심볼(L)의 지속 시간은 각각 0.8 μ sec 및 3.2 μ sec이다.

[48] 도 5(a)는 프리앰블에 포함된 10개의 쏫 심볼(S)들을 도시한 도면이고, 도 5(b)는 페이로드의 심볼 구조를 개요적으로 도시한 도면이다. 도 5(b)를 참조하면, 페이로드는 0.8 μ sec의 CP와 3.2 μ sec의 페이로드 심볼(payload symbol)이 연속되는 구조이다. CP는 페이로드 심볼(payload symbol) 마지막의 0.8 μ sec과 동일하다.

[49] 이러한 구조를 가지는 페이로드의 구성은 도 5(a)로 예시된 것과 같이 5 개의 0.8 μ sec 지속시간을 가지는 쏫 심볼(S)로 에플레이트될 수 있다. 즉, 도 5(a)로 예시된 것과 같이 최초 0.8 μ sec의 쏫 심볼(S)은 최후 0.8 μ sec와 동일하여 CP에 대응된다. 두 번째 내지 다섯 번째 쏫 심볼(S)들은 페이로드 심볼(payload symbol)에 대응된다. 따라서, 다섯 개의 짧은 심볼(S)들로 하나의 페이로드 심볼과 CP를 에플레이션할 수 있다.

[50] 도 6(a)는 와이파이 헤더 내에 포함된 2.5 개의 롱 심볼(L)의 개요를 도시한 도면이고, 도 6(b)는 페이로드의 심볼 구조를 개요적으로 도시한 도면이다. 도 6(a)로 예시된 것과 같이 프리앰블에는 선행하는 0.5 개 길이의 롱 심볼(L)과 두 개의 롱 심볼(L)들을 포함한다. 두 개의 롱 심볼(L)들은 서로 동일하며, 롱 심볼에서 뒤 1.6 μ sec(T1, T2)은 선행하는 0.5 개 길이의 롱 심볼(L)과 동일하다.

[51] 도 6(b)로 예시된 것과 같이 CP1은 1/2 길이의 선행하는 롱 심볼(0.5L)의 최초 0.8 μ sec 부분에 상응하며, 이는 도 6(a)의 T1에 상응한다. 마찬가지로, 도 6(a)의 롱 심볼(L)의 T2는 도 6(b)로 예시된 페이로드의 CP2에 상응한다. 각 페이로드 심볼의 마지막 0.8 μ sec는 초기 0.8 μ sec와 일치하며 페이로드 CP 요구 사항을 준수한다. 이것으로부터 2 1/2 개의 롱 심볼 시퀀스가 페이로드 심볼로 효과적으로 에플레이트 될 수 있음을 알 수 있다.

[52] 매핑된 심볼이 주어지면 콘스텔레이션(constellation) 매핑을 통해 서브 캐리어를 에플레이션한다. 일 예로, 장치(20)는 802.11g로 설정된다. 프리앰블과 PHY는 BPSK로 변조되는 반면 MAC은 16-QAM(Quadrature Amplitude

Modulation)으로 변조된다. 반대로 페이로드는 MCS(Modulation and Coding Scheme)에 따라 다양한 변조 옵션이 있다. 이들 중에서 가장 세분화된 콘스텔레이션인 64 QAM을 채택하여 콘스텔레이션 매핑의 오류를 최소화할 수 있다. 따라서, 개시자(10)는 코드 레이트 5/6 (802.11n MCS 7)의 64 QAM으로 설정된다.

- [53] 도 7(a) 내지 도 7(c)는 헤더 심볼 및 페이로드 심볼 사이의 콘스텔레이션 매핑을 설명하기 위한 도면들이다. 도 7(a)는 페이로드에 사용된 64 QAM 포인트와 관련하여 롱 심볼과 숏 심볼을 포함하는 프리앰블 및 PHY 필드의 BPSK 콘스텔레이션 포인트를 도시한다. 에플레이션 오류를 최소화하려면 코드 레이트에 의한 제한아래에서 BPSK에 가장 가까운 64 QAM 콘스텔레이션 포인트가 에플레이션을 위해 선택되어야 한다.
- [54] 도 7(b)는 숏 심볼의 에플레이션을 도시한다. 숏 심볼들은 도 7(a)로 예시된 콘스텔레이션 상에 +로 표시된 점에 위치한다. 에플레이션된 숏 심볼들은 5/6 코드 레이트에 의하여 64 QAM 포인트 당 할당된 6 비트 중 최대 4 비트에만 대응될 수 있으며 나머지 2 비트는 코딩에 의하여 생성되므로 제어할 수 없다.
- [55] 이러한 제약 조건에서 숏 심볼이 위치한 지점(+)과 가장 가까운 4 개의 지점(점선 박스)에서 공통된 4 비트를 선택하여 에플레이션 오류를 최소화할 수 있다. 이러한 매핑에 의하여 숏 심볼들은 4 개의 가장 가까운 지점(점선 박스) 중 하나로 에플레이션이 보장된다. 이것은 64 QAM의 콘스텔레이션에서 인접한 콘스텔레이션 포인트 사이는 그레이 코딩에 의하여 1 비트만 다르다는 점을 이용한다.
- [56] 롱 심볼 및 PHY도 BPSK로 변조되며, 이들은 I 축상 X로 도시된 점에 위치한다. 도 7(c)로 도시된 것과 같이 롱 심볼 및 PHY이 위치하는 점에서 가장 가까운 4 개의 지점(점선 박스)을 선택하고, 이들의 4 개의 공통 비트에 대한 에플레이션이 보장되어 에플레이션 오류를 최소화할 수 있다.
- [57] 도 8은 MAC 헤더에 사용된 16 QAM의 콘스텔레이션 매핑을 도시한다. 도 8을 참조하면, 16 QAM 콘스텔레이션 포인트 하나당 가장 가까운 4 개의 64 QAM 포인트가 매핑되며, 도 7로 예시된 실시예와 마찬가지로 4개의 공통 비트로 매핑될 수 있다. BPSK 콘스텔레이션 매핑과 마찬가지로 실제 WiFi 하드웨어 제약 조건에서도 에플레이션 오류를 최소화할 수 있다.
- [58] 도 9는 와이파이 인코딩 메커니즘과 코딩 에플레이션 메커니즘을 나타낸 도면이다. OFDM 에플레이션은 서브캐리어(subcarrier)당 6 개의 코딩된 비트를 출력 하며, 각 서브캐리어들은 64 QAM 포인트에 해당한다. 40MHz 64 QAM 802.11n으로 설정된 개시자(10)의 심볼 하나에는 108개의 숏 심볼이 있다. 이것은 Y로 표시되는 총 648 (= 108 * 6 비트/서브캐리어) 코딩된 비트로 변환된다. 도 9에서 파선 화살표로 표시된 코딩 에플레이션은 실선 화살표로 도시된 와이파이 인코딩을 통해 Y를 생성하는 사전 코딩된 비트 시퀀스 X를 찾는 것이다. 다시 말해, 주어진 Y에 대해 X를 계산하는 것으로 인터리버(Interleaver)와 컨볼루션

인코더(Convolutional Encoder)를 역 엔지니어링 하는 것이다.

- [59] Y의 코딩된 비트는 X의 540 (= 648 * 5/6 코드 레이트) 입력 비트 + 이전 심볼 Xb로부터 전달된 6 비트로부터 생성된다. P와 [Cb C]의 Galois Finite 필드 매트릭스 (GF (2))가 각각 인터리빙 및 컨볼루션 코딩 매트릭스를 나타낸다고 하자. Cb는 컨볼루션 매트릭스 Xb의 처음 6 열이다. 이어서 WiFi 인코딩은 아래의 수학적식과 같이 표현된다.

- [60] [수식1]

$$P[C_b \ C] \begin{bmatrix} X_b \\ X \end{bmatrix} = PC_b X_b + PCX = Y$$

- [61] Xb는 이전 심볼에서 제공되고 Cb와 P는 모두 와이파이 표준으로 정해진 것으로, PC_bX_b는 상수이다. 이어서 Y' = Y - PC_bX_b라 하고 수학적식 1을 선형 방정식으로 재구성하면, 아래의 수학적식 2와 같다.

- [62] [수식2]

$$(PC)X = Y'$$

- [63] PC는 648x540 매트릭스이다. 각가 4개의 선택된 비트들로 할당된 54개의 서브캐리어(20MHz)들을 에플레이트 하기 위하여 Y의 648 개의 출력 비트들 중에서 총 216개가 선택된다. 216 비트 서브벡터를 Y₂₁₆이 하고, 상응하는 PC 매트릭스를 (PC)₂₁₆ 이라하면 (PC)₂₁₆X = Y₂₁₆ 이다. 결과적으로 (PC)₂₁₆ 매트릭스는 표준에 기초한 풀 랭크(full rank) 매트릭스이므로, Y₂₁₆을 만족하는 X는 다양한 해가 존재하며 Y가 주어지면 인터리버와 컨볼루션 인코더를 고려하여 X를 얻을 수 있다.

- [64] 다양한 해 중에서 이를 만족하는 X를 찾는 방법을 하나 소개하면 다음과 같다. Y의 648 개의 출력 비트들 중에서 이전에 선택한 216개를 포함하는 540 개를 선택하여 이를 Y₅₄₀라 하고, 이에 대응하는 PC 매트릭스를 (PC)₅₄₀이라 한다. 이때 (PC)₅₄₀가 full rank가 되도록 선택 한다. 상술한 바와 유사하게 (PC)₅₄₀X = Y₅₄₀ 이다. (PC)₅₄₀는 풀 랭크(full rank)이며 정사각 매트릭스이므로 역행렬이 존재한다. 이에 X = ((PC)₅₄₀)⁻¹Y₅₄₀ 이므로 X를 구할 수 있다.

- [65] 스크램블링은 주어진 비트 시퀀스의 스크램블링 시드 시퀀스를 가진 XOR 연산이다. 즉, 와이파이 인코딩 시에는 페이로드 비트들과 스크램블링 시드로부터 얻어진 스크램블링 시퀀스와의 XOR 연산으로부터 X를 얻을 수 있다. 또한, XOR 연산의 결과인 X와 XOR 연산에 입력된 스크램블링 시퀀스를 다시 XOR 연산함으로써 페이로드 비트들을 얻을 수 있다. 일 예로, 스크램블링 시드는 상용 WNIC로부터 파악할 수 있다. 예를 들어 널리 사용되는 Atheros WNIC(예: AR9380)는 패킷 전송마다 시드를 하나씩 증가시킨다.

- [66] 도 10은 개시자(10)가 에플레이션한 와이파이 헤더의 예를 주파수 도메인으로 표시한 도면이다. 도 10(a)는 슛 심볼에 대한 에플레이션 결과를 도시하나, 롱 심볼과 PHY는 모두 BPSK로 변조되어 도 10(a)와 유사하다. 도 10(b)는 16 QAM으로 변조된 MAC의 에플레이션 결과를 도시한다. 도 10(a) 및 도 10(b)를 참조하면, 신호들은 서로 다른 콘스텔레이션 점에서 에플레이션 오류를 나타낸다.
- [67] 와이파이 표준에 따르면, 에플레이션된 와이파이 헤더의 심볼에는 세 개의 파일럿 서브 캐리어가 대응되며, 파일럿 서브 캐리어는 하드웨어에 의하여 강제되는 것으로 변경할 수 없다. 즉, 파일럿 서브캐리어 값들은 제어할 수 없어 에플레이션된 헤더와 상응하지 않는다면 오류를 발생시킬 수 있다. 따라서, 헤더 에플레이션이 시작되는 심볼 인덱스를 고려하여 오류를 최소화하여야 한다.
- [68] 에플레이션된 값과 가장 상응하는 파일럿 값의 시퀀스를 이용하여 에플레이션 오류를 최소화한다. 즉, 도 3으로 도시된 것과 같이 와이파이 헤더는 10 개의 슛 심볼, 2 1/2 개의 롱 심볼을 포함하는 프리앰블 필드와, PHY 필드 및 MAC 필드가 연속된다. 이 때, 3 번째 심볼로부터 헤더 에플레이션을 시작한다. 따라서, 앞서 도 4로 예시된 것과 같이 3, 4번째 심볼은 슛 심볼, 5, 6번째 심볼은 롱 심볼, 7번째 심볼은 PHY, 8번째 심볼은 MAC 심볼로 에플레이션 한다.
- [69] 이와 같은 방법으로 파일럿과 에플레이트된 헤더는 9 개 중 8 개 값과 일치하며, 단일한 불일치의 영향은 무시할 수 있었다. 즉, 3 번째 페이로드 심볼에서 시작하는 헤더를 에플레이션하여 파일럿 부정합(pilot mismatch)의 영향을 최소화할 수 있다.
- [70] 장치(20)는 개시자(10)가 에플레이트하고 페이로드에 은닉하여 제공한 헤더(He)에 뒤따르는 주변 신호(ambient signal)를 수집하고, 이를 802.11g의 신호 형태에 부합하도록 재구성한다. 그러나, 주변 신호(ambient signal)는 802.11g의 신호 형태에 부합한다고 할 수 없어 실제의 주변 신호와 재구성된 신호 사이에는 오차가 발생할 수 있다.
- [71] 장치(20)가 에플레이트된 헤더를 수신하면 PHY 필드에 정의된 LENGTH 기간 동안 주변 신호 수신을 시작하고 디코딩된 비트 스트림을 출력한다. 여기서 LENGTH는 와이파이에서 최대 2,304 바이트일 수 있다. 비트 시퀀스가 주어지면, 페이로드 비트와 물리 계층 신호의 일대일 매핑 관계로 인해 주변 신호(ambient signal)는 변조, 인터리빙 및 스크램블링을 포함한 와이파이 인코딩을 따라 재구성된다. 재구성된 신호와 실제 신호의 사이에는 와이파이 하드웨어에 의한 오류 및 위상 회전이 불가피하다. 이하에서는 오류의 다양한 원인과 신호 부분(예: 도 12의 흰색 상자)을 선택적으로 활용하여 원래 신호와 재구성된 신호 간의 코릴레이션을 최대화하는 방법을 설명한다.
- [72] 도 11은 재구성된 신호(점선으로 도시됨)와 실제의 주변 신호(실선으로 도시됨) 사이의 오류를 도시한다. 도 11을 참조하면, 오류가 발생하는 원인 중 하나는 도 11에서 진한 회색으로 도시된 부분의 최초 0.8 μ sec의 CP이다.

와이파이의 프로토콜에 의하여 심볼의 마지막 0.8 usec으로 최초 0.8μsec의 CP 부분이 덮어쓰기 되므로 CP에 위치하는 원래의 주변 신호는 손실된다.

- [73] 오류가 발생하는 원인 중 다른 하나는 도 11에서 연한 회색으로 도시된 경계 오류이다. 이는 심볼의 시작과 끝이 항상 같아야 하는 이산 푸리에 변환(DFT)의 순환 특성으로 인해 발생하며, 이로부터 재구성된 신호의 기호 경계가 원래 신호에서 벗어난다.

- [74] 재구성된 신호를 아래의 수학적식과 같이 표현한다면,

- [75] [수식3]

$$\sum_k X[k]e^{j2\pi kn/T}, x[0] = x[T]$$

- [76] (T는 심볼의 지속시간)

- [77] 고주파 신호가 단기간에 갑작스런 변화를 더 잘 허용하기 때문 경계 오류는 대역폭에 반비례하며, 높은 대역폭을 가질수록 더 작은 경계 오차가 발생한다. 즉, f_H 를 신호에서 가장 높은 주파수 성분(일 예로, ZigBee의 1MHz)이라 하면, 경계 오류와 CP에 의한 오류를 $1.5/f_H (= 1.5 \mu\text{sec}, \text{Zigbee})$ 로 정할 수 있으며, 이로부터 재구성된 신호와 이상적인 신호 사이의 코릴레이션으로 0.86을 얻을 수 있다.

- [78] 파일럿 서브캐리어에서의 주변 잡음으로 인해 재구성된 신호도 위상 회전된다. 와이파이는 I, Q 축을 회전함으로써 수신된 파일럿 서브캐리어와 기준값 사이의 위상차를 보상하여 위상 에러를 제거한다. 그러나, 장치(20)에서 파일럿 서브캐리어는 주변 노이즈로 채워져 재구성된 심볼에 임의의 위상 회전이 발생한다. 위상 회전은 일부 애플리케이션(예: 디코딩)에서 문제가 될 수 있으나, 다른 애플리케이션(예: RF 지문 및 스펙트럼 모니터링)에서는 문제되지 않는다.

- [79] 재구성된 신호는 원래의 신호에 근사하여 기기 고유의 특성을 그대로 유지한다. 이것은 재구성된 신호가 RF 장치의 식별(RF fingerprinting)에 사용될 수 있음을 나타낸다. 임의의 심볼 위상 회전에도 불구하고, 전체 심볼은 고정된 위상 시프트에 의해 회전되어, 서브 캐리어들 사이의 상대 위상이 원래 신호와 일치하도록 유지된다.

- [80] 진폭은 위상 회전에 영향을 받지 않는다. 다시 말해, 애플리케이션된 신호의 서브 캐리어들 사이의 진폭 및 상대 위상은 원래 신호의 물리 계층 서명을 직접 반영한다. 장치는 이러한 속성을 활용하여 범용 와이파이를 사용하여 다양한 장치를 식별할 수 있는 RF 핑거 프린팅을 가능하게 한다.

- [81] 도 12를 참조하여 본 실시예를 이용하여 스펙트럼 모니터링을 수행하는 예를 설명한다. 도 12는 스펙트럼 분석에 사용될 수 있는 신호의 워터폴(waterfall)을 도시한 도면이다. 스펙트럼 모니터링은 세분화된 전력 측정을 통해 무선 채널의 다양한 활동을 조사한다. 전력은 위상 회전에 영향을 받지 않기 때문에,

재구성된 신호는 별도의 처리 없이 직접 사용될 수 있다. 전력 측정의 정밀도는 재구성된 신호의 변조 방식에 크게 좌우된다. 도 12(a)는 16 개의 QAM의 콘스텔레이션 점을 신호의 크기(즉, 신호의 전력)에 따라 3 단계(검정, 회색, 흰색)로 분류한 예를 도시한다. 더 높은 차수 QAM (예: 64 QAM의 경우 10 단계)을 채택하면 정밀도를 향상시킬 수 있다.

- [82] 도 12(a)에서 분류된 신호를 도 12(b)와 같이 시간-주파수에 따라 도시하여 스펙트럼 모니터링을 수행할 수 있다. 도 12(b)는 4 번째 심볼에서 시작하여 0.192ms 길이의 신호를 캡처하여 얻은 16 QAM의 재구성된 신호에서 얻은 워터폴 플롯이다. 신호가 위치하는 서브캐리어 인덱스로부터, 이 신호는 각각 약 2.422GHz(= BLE 채널 9)의 중심 주파수 및 1MHz 대역폭을 갖는 BLE로 식별된다. 도 12(b)로부터 본 실시예에 따른 방법으로 각각 심볼 지속 시간으로 4 μ sec의 타이밍 정밀도 및 서브캐리어 간격으로 312.5KHz의 주파수 정밀도를 가지는 스펙트럼 모니터링을 수행할 수 있다.
- [83] 스펙트럼 모니터링은 무선 신호의 방식, 중심 주파수, 지속 시간 및 도착 시간을 포함한 무선 신호 특성을 식별할 수 있다. 이러한 정보로부터 신호를 디코딩할 수 있다. 이하에서는 도 13 내지 도 14를 참조하여 본 실시예에 의한 방법으로 주변 신호(ambient signal)에 대한 디코딩을 수행하는 과정을 설명한다. 일 예로, 주변 신호(ambient signal)은 직비 신호를 예시한다. 도 13(a)는 기준 직비 신호를 예시한 도면이고, 도 13(b)는 위상에 대한 코릴레이션 값의 변화를 도시한 도면이다. 직비를 포함하는 일반적인 인코딩이 위상을 활용한다는 점에서 신호 디코딩 과정에서는 위상 회전을 보상해야 한다. 직비 신호가 나타내는 데이터에 관계없이 임의의 직비 신호에 포함된 공통 신호 특성을 이용하여 위상을 보상한다. +/- 하프 사인(half-sine)형 직비 신호에 의하여 임의의 직비 신호의 절대값(즉, 동 위상 성분 및 직교 성분에 대해 11를 취함)을 취하면 도 13(a)와 같이 표시될 수 있다. 이 신호를 위상 보상에 대한 기준 신호로 활용한다. 먼저 재구성된 신호의 절대값을 취하고, θ 만큼 위상 회전을 수행한다. 이어서 도 13(a)의 기준 신호와 코릴레이션(correlation)을 연산하며, 서로 다른 θ 에 대하여 코릴레이션 연산을 수행하며, 이는 아래의 수학식으로 표시될 수 있다.

[84] [수식4]

$$\operatorname{argmax}_{\theta} \operatorname{Corr}(R(t), |I\{x(t)e^{j\theta}\}| + j|Q\{x(t)e^{j\theta}\}|)$$

- [85] $R(t)$ 와 $x(t)$ 는 각각 참조 신호 및 위상이 회전된 신호이며, θ 는 일 예로, $\pi/8$ 만큼 증가시킨다. 이것은 $-\theta$ 의 심볼 위상 회전을 보상한다. 도 13(b)는 $(3\pi)/4$ 및 $\pi+(3\pi)/4$ 에서 0.93의 최대 코릴레이션 연산값을 얻을 수 있는 것을 도시한다. 이러한 결과는 신호의 절대값은 위상이 π 만큼 시프트된 것과 동일하기

때문이다. 즉, $|x(-t)e^{j0}| = |x(t)e^{j0}|$ 이고, 이는 직교 성분도 동일하다.

[86] 직비의 DSSS(Direct Sequence Spread Spectrum)를 활용하여 도 13(b)에서 도시된 두 피크 중에서 선택한다. 즉, DSSS에는 신호 시퀀스들이 미리 정의되어 있으며, 미리 정의된 신호 시퀀스에는 서로 반전된 관계인 신호 시퀀스는 포함되지 않는다. 따라서, DSSS에 정의된 신호 시퀀스는 두 후보 중 하나 (즉, $(3\pi)/4$ 및 $\pi + (3\pi)/4$)만 포함하며, 정의된 신호 시퀀스를 선택함으로써 심볼 위상 회전을 보정할 수 있다.

[87] 도 14(a)는 이상적인 신호와 위상 보상된 신호를 도시하고, 도 14(b)는 위상 보정된 직비 신호가 동일한 비트로 매핑되는 결과를 도시한다. 직비에서, 시계 방향 또는 반시계 방향 위상 편이는 1 또는 0을 나타내며, 여기서 위상 보상된 신호는 정확한 비트(즉, 2 개의 연속적인 비트)로 디코딩된다. 또한 DSSS 신호 시퀀스에 매핑하여 CP와 경계 오류의 영향을 동시에 보상할 수 있다.

[88]

[89] 평가(Evaluation)

[90] 다양한 상황에서 본 실시예를 평가하기 위해 광범위한 실험을 수행하였다. 실험 환경은 개시자(10)와 장치(20)로 구성되며 개시자(10)는 에플레이트된 헤더를 포함하는 40MHz WiFi 패킷을 WiFi 채널 4에서 1MHz 시프트된 2.426GHz로 전송한다. 장치(20)는 2.417GHz(와이파이 채널 2)에서 에플레이트된 헤더를 수신한다. 개시자(10)로 상용 WNIC Atheros AR9380 및 USRP B210을 사용하였으며, 장치(20)로 D-Link DWA-192 및 Alfa AWUS036ACM을 사용하였다.

[91] 개시자(10)와 장치(20) 사이의 거리에 따라 에플레이트된 헤더의 형태와 PRR(Packet Reception Rate) 성능 측면에서 본 기술의 기본 성능을 평가한다. 개시자와 장치로 각각 AR9380, Alfa AWUS036ACM을 각각 사용하였다.

[92] 도 15는 시간 영역에서 에플레이트된 신호의 형태와 이상적인 신호를 도시한다. 에플레이션 오차에도 불구하고 에플레이션된 신호와 이상적인 신호들 사이에는 높은 유사성을 가지는 것을 확인할 수 있다. 따라서, 상용 WiFi 수신기는 에플레이트된 헤더를 감지하고 디코딩할 수 있다.

[93] PRR(Packet Reception Rate)을 평가하기 위해 개시자는 전송 전력(TX 전력) 18dBm 으로 40MHz 802.11n 패킷을 전송하도록 하였다. 패킷은 16 QAM, 3/4의 코드 레이트의 페이로드를 포함하며, 페이로드는 802.11g 에플레이트된 헤더를 포함한다. AR 9380 및 USRP를 개시자로 사용하여, 40MHz 802.11n 패킷에 에플레이트된 헤더를 은닉하여 전송하였다. 장치는 개시자와 2m 떨어져 에플레이트된 헤더를 수신하였다.

[94] 도 16(a)는 본 실시예에 의한 장치와 상용 WNIC의 PRR을 도시한 도면이고, 도 16(b)는 재전송 회수에 따른 PRR을 도시한 도면이다. 도 16(a)을 참조하면, 상용 WNIC은 PRR이 최대 67 % 인 반면 개시자로 사용된 USRP는 최대 62 %에 불과한 것을 도시한다. 개시자인 USRP의 PRR은 CSMA / CA(Carrier-Sense Multiple

Access with Collision Avoidance)를 수행하지 않기 때문에 상용 WNIC의 PRR보다 낮다. 이 PRR 성능은 도 16(b)로 도시된 것과 같이 재전송을 통해 향상될 수 있다. 에플레이트된 헤더를 4 회 이상 재전송함으로써 99 % 이상의 PRR 성능을 달성할 수 있다.

- [95] 도 17(a)는 LOS 시나리오의 실험 설정을 도시한 도면이고, 도 17(b)는 LOS 시나리오에서의 PRR을 도시한 도면이다. 다양한 시나리오에서 SDR-Lite의 성능을 검증하기 위해 PRR 평가를 위해 가시 거리 (LoS)와 비가시 거리 (NLoS)를 모두 고려한다. 먼저, 도 17(a)과 같이 LOS 시나리오에서 TX 전력이 18 dBm일 때 개시자와 장치 사이의 거리가 멀어짐에 따라 PRR을 측정한다. 도 17(b)에 도시된 것과 같이 가장 가까운 거리(1m)에서 측정된 PRR 성능은 최대 67 % 인 반면, 10m에서 SNR이 저하됨에 따라 PRR은 52 %로 감소하였다. 그러나 에플레이트된 헤더를 5 번 재전송하면 PRR이 10m에서 최대 95%에 도달하였다.
- [96] 도 18(a)는 개시자(10)는 책상에 고정된 NLoS 환경에서 다양한 장치(20)의 위치(A)-(D)를 도시한다. 도 18(b)는 각 위치별 PRR을 도시한 도면이다. 도 18(b)로 도시된 것과 같이 (C)와 (D)의 PRR은 각각 52 %와 55 % 인 반면, (A)와 (B)의 경우 PRR은 각각 47 %, 52 %이다. 이것은 (A)와 (B)의 위치가 다른 위치보다 개시자(10)로부터 더 멀리 있기 때문이며, 에플레이트된 헤더를 다시 전송하면 NLoS 시나리오의 모든 사용자가 95 %의 PRR을 얻을 수 있다.
- [97] AR 9380이 전송한 에플레이트된 헤더 신호 및 CC2650이 전송한 ZigBee 신호를 USRP를 사용하여 기록한 다음 연결된 신호를 편의상 USRP에서 장치로 전송하였다. 도 19(a)는 Tx 전력이 -10 dBm에서 10 dBm으로 변할때 재구성된 직비 신호와 이상적인 직비 신호 사이의 최대 코릴레이션 값을 도시한다. 도 19(b)는 동일한 조건에서 재구성된 BLE 신호와 이상적인 BLE 신호 사이의 최대 코릴레이션 값을 도시한 도면이다. 도 19(a)와 도 19(b)에서 도시된 바와 같이 신호 대 잡음비 (SNR)가 충분히 높을 때 직비의 최대 코릴레이션 값과 BLE의 최대 코릴레이션 값은 각각 0.86과 0.85에 도달하였다. 실험 결과로부터 장치에 의해 수신된 신호가 도 20으로 예시된 것과 같이 원래 신호를 복구하기 위해 성공적으로 재구성될 수 있음을 나타낸다.
- [98] 도 20(a) 및 도 20(b)는 각각 위에서 설명된 위상 보상을 수행하여 형성된 직비와 BLE의 위상 보정된 신호를 도시한다. 도시된 바와 같이, 실선으로 도시된 재구성된 신호와 점선으로 도시된 이상적인 신호는 높은 유사성을 나타내므로, 재구성된 신호로부터 원래의 페이로드를 디코딩할 수 있다.
- [99] 이하에서는 도 21 내지 도 23을 참조하여 본 실시예를 이용하여 주변 신호의 스펙트럼을 분석하는 방법을 설명한다. AR 9380 또는 USRP를 개시자(10)로 사용하고, D-Link DWA-192를 장치(20)로 사용하여 ISM 대역에서 RF 스펙트럼을 모니터링 할 수 있다. 직비/ BLE 장치로 표준을 준수하는 CC2650을 사용하였다.
- [100] RF 스펙트럼을 분석하기 위해, 장치가 다양한 RF 활동에 대해 워터폴

플로팅(plotting)을 수행하여 RF 신호의 전력을 측정할 수 있다. 개시자(10)가 보낸 에플레이트된 헤더를 수신하면 장치(20)는 2.417GHz, 20MHz 대역폭에서 RF 스펙트럼을 모니터링한다. 도 21은 장치(20)가 2.422GHz에서 전송된 BLE 신호를 캡처한 것을 도시한다. 여기서 X 축은 WiFi 심볼 단위(4 μ sec)로 표시된 시간 영역을 나타내고 Y 축은 서브 캐리어 단위 (0.3125kHz)의 주파수 영역을 나타낸다.

- [101] 장치에 의하여 측정된 RF 전력은 에플레이트된 헤더의 전력에 따라 다르다. 에플레이트된 헤더의 전력이 미치는 영향을 평가하기 위해 에플레이트된 헤더 및 직비/BLE 신호를 USRP에 기록한 다음 에플레이트된 헤더 대 BLE / ZigBee의 전력비를 16:1에서 1.6:1로 변경하여 장치로 전송하였다.
- [102] 도 22(a), 도 22(b) 및 도 22(c)는 각각 2.410GHz 및 2.422GHz의 중심 주파수에서 캡처된 직비 신호 및 BLE 신호의 워터폴 플롯이다. 도 22(a), 도 22(b) 및 도 22(c)에서 에플레이트된 헤더의 전력이 감소함에 따라 각 플롯에는 직비 및 BLE 신호의 보다 자세한 전력 레벨이 표시된다. 장치(20)가 RF 신호를 수신하면 RF 신호의 전력을 적절한 QAM 포인트에 매핑하기 위해 RF 신호에 가까운 에플레이트된 헤더의 전력을 제어해야 한다.
- [103] 본 실시예를 이용하여 비무선 프로토콜 신호도 모니터링할 수 있다. 동일한 실험 설정으로 장치를 통해 무선 제어(Remote Control) 차량과 전자 레인지(microwave oven)에서 RF 신호를 캡처한다. 도 23(a)와 도 23(b)는 각각 RC 자동차와 전자 레인지에서 나오는 RF 신호의 워터폴 플롯을 도시한다. 장치(20)가 RF 스펙트럼을 모니터링하여 다양한 RF 신호가 있는 환경에서 더 나은 스펙트럼 효율을 위해 네트워크를 관리할 수 있는 것을 알 수 있다.
- [104] 이하에서는 본 기술로 직비 신호를 디코딩하는 것을 설명한다. SER(Symbol Error Rate) 및 FRR(Frame Reception Rate)을 평가한다. 자세한 분석을 위해 개시자(10)로 USRP B210을 사용하여 에플레이트된 헤더 및 직비 신호를 기록하고 장치를 사용하여 ZigBee 신호를 재구성하고 디코딩한다.
- [105] SER 및 FRR을 평가하기 위해 개시자인 USRP에 의해 기록된 에플레이트된 헤더 및 직비 신호를 다른 TX 전력을 가진 장치로 전송한다. 개시자(10)와 장치(20) 사이의 거리를 2m로 설정하였다. 도 24(a)는 TX 전력이 -5 dBm에서 10 dBm까지 변화할 때 개시자(10)의 다양한 SER 성능을 도시한다. 목표 신호의 전력을 고려하여 에플레이트된 헤더의 전력을 제어해야하므로 에플레이트된 헤더와 직비 신호의 전력비를 16 : 1로 설정했다.
- [106] 10dBm TX 전력을 사용하면 SER 성능을 최대 95 %까지 달성할 수 있었으며 SER 성능은 -5dBm의 TX 전력에 대해 80 %이었다. 도 24(b)는 SER 성능에 기초하여 10 dBm의 TX 전력에 대해 서로 다른 프레임 길이를 가진 FRR 성능을 도시한다. 4 바이트가 있는 프레임의 경우 FRR 성능은 64 %이고 프레임 길이가 길어질수록 FRR은 감소한다. 이 결과는 장치가 직비 심볼 및 프레임을 디코딩하여 와이파이 장치를 직비 디코더(예 : 모바일 IoT 리더)로 변환할 수

있음을 나타낸다.

[107] 프레임 과도 상태(frame transient state)를 이용하여 장치가 캡처한 RF 서명을 사용하는 장치 식별 응용을 설명한다. 프레임 과도 상태는 각 프레임의 시작과 끝에서 관찰되며 하드웨어 제조 프로세스와 결합에 의해 결정된다. 프레임 과도 상태는 신호가, 일 예로, 어느 한 레벨에서 다른 레벨로 변화할 때 형성되는 오버슈트(overshoot)의 개수 및 레벨 대비 오버슈트의 피크의 퍼센트 및/또는 변화에 필요한 스텝(step)등을 포함할 수 있다. 이러한 특징은 장치가 속한 동일한 모델 중에서도 장치에 따라 고유할 수 있다. 결과적으로, 이러한 프레임 과도 기능은 휴대 전화 및 와이파이 AP를 포함하여 다양한 와이파이 장치를 식별(identification) 및/또는 핑거 프린팅(finger-printing)하는데 사용될 수 있다.

[108] 아래의 표 1은 실험에 사용된 와이파이 장치를 요약한 표이다. 도 25는 장치 식별을 위하여 사용된 장치들을 도시한 도면이다. 장치에 대한 핑거프린팅 과정에서 장치(20) 및 USRP의 성능을 비교하기 위해 장치(20) 및 개시자를 설정하여 이러한 장치에서 와이파이 신호의 프레임 과도 상태를 캡처한다.

[109] [표1]

Model	Quantity	Type
Honor View 10 (M1)	1	Smart device
iPad Pro (M2)	1	Smart device
iPhone 5s (M3)	1	Smart device
Moto G4 (M4)	1	Smart device
Moto G5 (M5)	1	Smart device
Xiaomi 8 (M6)	3	Smart device
TP-Link Archer A7 (A1)	1	Router
Netgear R7000 (A2)	1	Router
Raspberry Pi 0 (A3)	1	Router
Raspberry Pi 3 (A4)	1	Router
TP-Link WR841N (A5)	4	Router

[110] 장치 식별에는 교육 과정 및 테스트 과정이 필요하다. USRP 및 장치(20)에서 캡처한 과도 신호(transient signal)를 훈련 세트로 사용한다. 여기서 USRP 및 장치(20)의 각 과도 신호의 길이는 각각 200 및 64 데이터 포인트이다. 이어서, 또 다른 200 개의 샘플을 테스트 세트로 캡처하고 인공 지능(Artificial intelligence)를 이용하여 이러한 과도 신호의 장치 레이블을 예측한다. 일 예로, 인공 지능은 SVM (support vector machine) 알고리즘, linear regression, logistic regression, neural networks 중 어느 하나일 수 있다.

[111] 도 26은 M1-M6로 표시된 6개의 다른 모델과 3 개의 Xiaomi 8 폰 (M6¹-M6³)의 스마트 장치 6 개를 분류한 휴대 전화 핑거 프린팅 실험 결과를 도시한 도면이다. 도 27는 라우터 핑거 프린팅에 대한 결과를 도시한 도면이다. 라우터에서 핑거 프린팅 실험에서는 5 개의 서로 다른 모델(A1-A5) 라우터와 4 개의 TP-Link WR841N 라우터 (A5¹-A5⁴)를 분류하였다.

[112] 분류 정확도 및 식별 정확도는 서로 다른 장치 모델을 분류하고 동일한 모델로

개별 장치를 식별하는 정확도를 나타낸다. 도 28 및 도 29로 도시된 결과는 훈련 샘플 수가 증가함에 따라 정확도가 증가하는 것을 도시한다. 장치(20)는 충분한 훈련 샘플이 주어지면 USRP와 매우 유사한 장치 분류 정확도를 얻을 수 있다.

[113] 그러나 동일한 모델들 중에서 장치를 식별하는 과정에서, 장치(20)는 USRP의 정확도와 비교하여 낮은 정확도를 보여준다. 하지만, 이러한 열화는 재구성 과정에서 필연적인 신호 왜곡에 의하여 형성된 것이다. 100 개의 교육 프레임을 사용하면 스마트 폰과 라우터의 장치 식별 정확도가 94 %를 초과하여 현저하게 상승한다.

[114] 도 28은 수신기 동작 특성(ROC) 곡선을 도시한다. 프레임 과도(frame transient) 특성은 불량 AP를 탐지하는 데 사용될 수 있다. 두 개의 TP-Link WR841N 라우터를 합법적인 AP로 사용하고 각 장치에 대한 훈련 세트로 장치(20)를 통해 100 개의 일시적 샘플을 캡처한다. 이어서 다른 TP-Link WR841N 라우터와 Raspberry Pi Zero를 두 개의 불량 AP로 선택하고 인공지능을 이용하여 불량 AP를 탐지한다. 이 때, 인공지능은 k-nearest-neighbor(kNN) 알고리즘일 수 있다.

[115] 도 28을 참조하면, 불량 AP의 모델이 합법적인 AP와 다른 경우에는 높은 탐지 정확도를 달성하는 것을 확인할 수 있다. 특히 장치(20)는 99 %의 실제 양성률과 3 % 미만의 잘못된 양성률로 Raspberry Pi rogue AP를 감지할 수 있었다. 그러나 불량 AP의 모델이 합법적인 AP와 동일한 경우(즉, WR841N) 탐지 성능이 저하되었다.

[116] 본 기술의 또 다른 응용으로 분야로 드론 검출기가 있을 수 있다. 상업용 드론과 컨트롤러는 메시지 교환(예: 제어, 비디오 스트리밍)에 ISM 대역을 사용한다. 이 평가에서는 Intel Aero, DJI Mavic Pro 및 3Dr Solo의 3 가지 대표적인 드론 모델을 선택하였다. Intel Aero 및 DJI Mavic Pro는 독점 프로토콜을 사용하고 3DR Solo는 WiFi 표준을 채택하였다. 드론 검출을 위해 RF 핑거 프린팅을 수행하는 인공지능을 도입하였다. 일 예로, 인공지능은 Supervised learning인 SVM, linear regression, logistic regression, neural networks, DNN(Deep Neural Network)중 어느 하나일 수 있다.

[117] 도 29는 3 개의 드론 사진이 있는 드론 실험 시나리오를 도시한다. 시계열(time series) RF 신호를 분석하기 위해 인공지능을 사용하였으며, 일 예로, 인공지능은 1D CNN(Convolutional Neural Network) 아키텍처를 가진다. 이 평가에서 우리는 (i) 드론 존재 감지와 (ii) 드론 모델 분류의 두 가지 작업을 수행하였다.

[118] 드론 존재 감지 작업에서는 2.4GHz 스펙트럼을 스캔하여 RF 신호를 기반으로 드론을 감지하였다. 드론 모델 분류는 드론의 RF 신호를 검사하여 드론 모델을 분류하는 것이다. 보편적 SDR 장치인 USRP와 장치(20)를 모두 사용하여 2.4GHz 스펙트럼을 스캔하고 DNN의 입력으로 RF 신호를 캡처한다. 두 작업에서 USRP 또는 장치(20)가 드론 신호를 캡처할 때의 정확도 성능을 비교하였다.

[119] 도 30(a)는 장치(20)에 의해 재구성된 Mavic Pro의 신호를 도시한 도면이고, 도 30(b)는 장치(20)에 의해 재구성된 Solo의 신호를 도시한 도면이다. 도시된 바와

같이, 예를 들어 Mavic Pro 및 Solo와 같이 상이한 드론 모델이 일반적으로 상이한 PHY 표준 또는 변조를 채택하기 때문에, 이들의 특성이 재구성된 신호에서 유지된다.

- [120] DNN(Deep Neural Network)을 학습시키기 위해 600 개의 드론 RF 신호 샘플과 600 개의 노이즈 샘플을 수집하였다. 각 RF 신호 샘플은 64 개의 동위상(In-phase) 및 직교(Quadrature) 포인트로 구성된다 (도 30 참조). 모든 RF 신호의 진폭이 정규화되므로 각 신호의 다른 RF 게인이 DNN 결과에 영향을 미치지 않는다. 학습 후, 본 기술의 정확도 성능을 평가하기 위해 다른 400 개의 테스트 샘플을 사용하였다.
- [121] 도 31은 USRP 및 장치에 의해 드론의 RF 신호가 캡처될 때 드론 탐지의 정확도를 도시한다(회색으로 표시된 부분은 5 개의 랜덤 시드를 갖는 표준 편차를 나타냄). 훈련 반복 단계의 수가 증가함에 따라 개시자에 의한 탐지 정확도는 99.6 %의 정확도로 수렴한다. 장치는 더 많은 단계를 수렴해야 하는 반면 USRP와 비교하여 유사한 성능인 97 %를 얻을 수 있었다. 장치의 16 QAM 매핑으로 인해 원래 신호의 약간의 변동이 양자화될 수 있지만 DNN은 더 많은 훈련 단계를 통해 드론의 신호를 구별할 수 있다.
- [122] DNN을 통해 RF 신호를 분석하여 3 개의 드론 모델을 분류할 수 있었다. 존재 탐지 실험과 유사하게, 각각의 무인 항공기에서 훈련을 위해 450 샘플과 테스트를 위해 200 샘플을 수집하였다.
- [123] 도 32(b)는 장치에 의해 재구성된 신호를 사용하여 드론 분류의 혼란 매트릭스를 도시한다. Y 축은 실제 드론 모델이고 X 축은 DNN에 의해 예측된 모델이다. 3Dr Solo 드론은 다른 RF 신호와 크게 다른 WiFi 신호만 사용하기 때문에 오류없이 분류 할 수 있다.
- [124] 도 32(a)는 반복 단계 수가 증가함에 따라 장치 및 USRP의 성능을 도시한다. USRP 성능은 99.3 %의 정확도를 달성하는 반면 장치는 드론 모델을 93.7 %의 정확도로 분류할 수 있었다. Solo 드론의 와이파이 신호와 비교하여 장치에서 Aero 및 Mavic Pro 드론의 RF 신호를 재구성 하였을때 이들은 유사하므로, RF 신호를 구별하는 것은 어려운 작업이다. 장치가 달성한 분류 성능은 93.7 %이지만, 이 분류는 DNN에 4 μ s 샘플을 제공하여 수행된다. 따라서 여러 샘플을 수집하여 정확도를 더욱 향상시킬 수 있다.
- [125]
- [126] 본 발명에 대한 이해를 돕기 위하여 도면에 도시된 실시 예를 참고로 설명되었으나, 이는 실시를 위한 실시예로, 예시적인 것에 불과하며, 당해 분야에서 통상적 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시 예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호범위는 첨부된 특허청구범위에 의해 정해져야 할 것이다.

청구범위

- [청구항 1] 무선 장치 구동 방법으로, 상기 무선 장치 구동 방법은:
전송측이 제2 프로토콜로 에뮬레이트(emulate)된 헤더를 제1 프로토콜로 규정된 패킷(packet)의 페이로드(payload)에 은닉하여 전송하는 단계와,
수신측이 상기 에뮬레이트된 헤더와, 주변 신호(ambient signal)를 수신하는 단계 및
상기 주변 신호를 상기 제2 프로토콜에 따라 디코딩하여 비트 시퀀스를 얻는 단계를 포함하는 무선 장치 구동 방법.
- [청구항 2] 제1항에 있어서,
상기 에뮬레이트된 헤더의 중심 주파수는 상기 제1 프로토콜로 규정된 패킷으로 지정된 중심 주파수와 상이한 무선 장치 구동 방법.
- [청구항 3] 제1항에 있어서,
상기 제1 프로토콜은 802.11n이고,
상기 제2 프로토콜은 802.11g인 무선 장치 구동 방법.
- [청구항 4] 제1항에 있어서,
상기 에뮬레이트된 헤더는 10개의 쏫 심볼들, 2.5개의 룡 심볼들을 포함하는 프리앰블 필드와, PHY 필드 및 MAC 필드를 포함하며,
상기 10개의 쏫 심볼들은 두 개의 페이로드 심볼로 에뮬레이트되고,
상기 2.5개의 룡 심볼들은 두 개의 페이로드 심볼로 에뮬레이트되며,
상기 PHY 필드와 상기 MAC 필드는 각각 하나의 페이로드 심볼로 에뮬레이트 되는 무선 장치 구동 방법.
- [청구항 5] 제1항에 있어서,
상기 에뮬레이트된 헤더는 프리앰블 필드 및 PHY 필드를 포함하며,
상기 전송측은 상기 프리앰블 필드 및 PHY 필드를 64 QAM(64 Quadrature Amplitude Modulation)으로 콘스텔레이션 매핑하여 BPSK(Binary Phase Shift Keying)로 전송하되,
상기 수신측은 상기 프리앰블 필드 및 PHY 필드를 BPSK(Binary Phase Shift Keying)로 콘스텔레이션 매핑하여 디코딩하는 무선 장치 구동 방법.
- [청구항 6] 제1항에 있어서,
상기 에뮬레이트된 헤더는 MAC 필드를 더 포함하며,
상기 전송측은 상기 MAC 필드를 64 QAM으로 콘스텔레이션 매핑하여 16 QAM으로 전송하되,
상기 수신측은 상기 MAC 필드를 16 QAM으로 콘스텔레이션 매핑하여 디코딩하는 무선 장치 구동 방법.
- [청구항 7] 제5항 및 제6항 중 어느 한 항에 있어서,
상기 64 QAM으로 콘스텔레이션 매핑하여 디코딩하는 단계는,
상기 64 QAM으로 콘스텔레이션 중 인접하는 네 개의 콘스텔레이션

포인트에 공통되는 4 비트(bit)로 디코딩하여 수행하는 무선 장치 구동 방법.

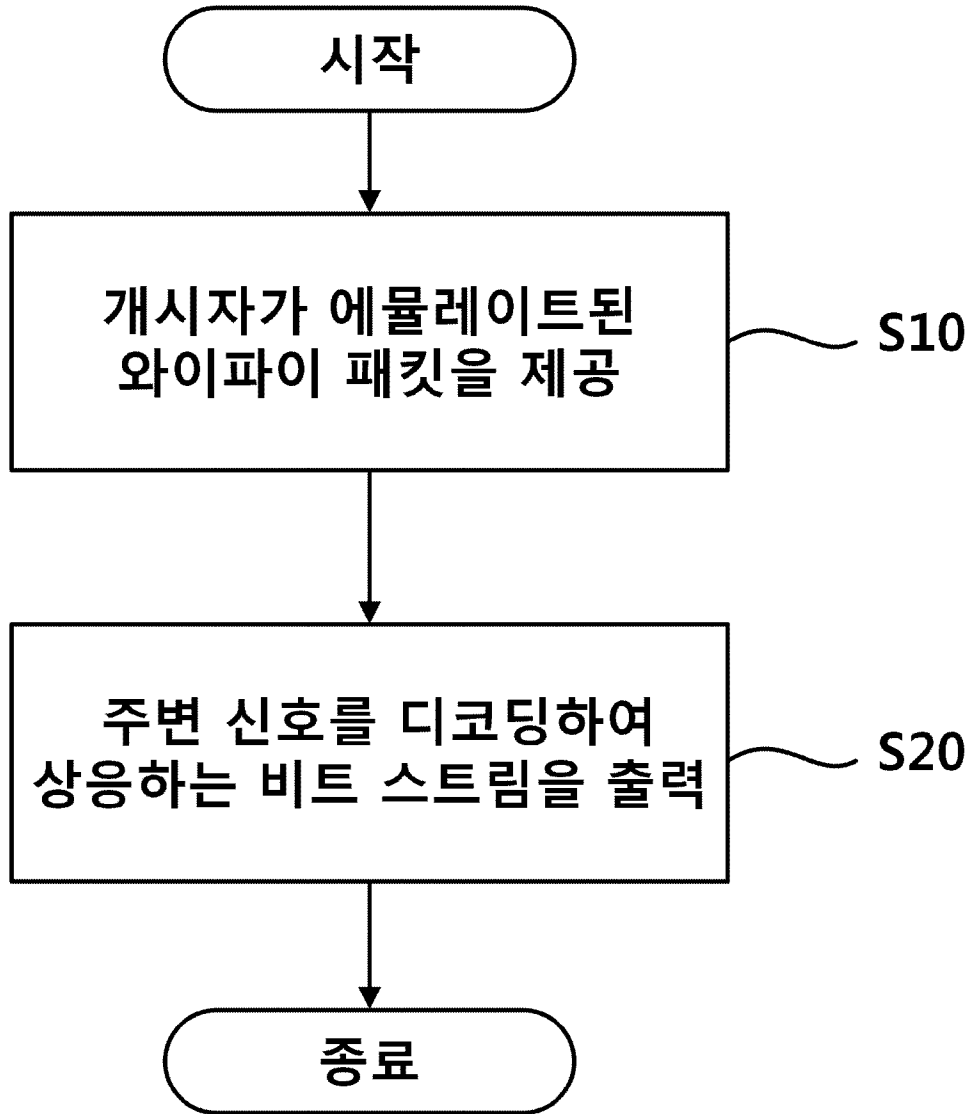
- [청구항 8] 제1항에 있어서,
상기 무선 장치 구동 방법은,
상기 비트 시퀀스로부터 상기 주변 신호를 재구성(reconstruction)하는 단계를 더 포함하는 무선 장치 구동 방법.
- [청구항 9] 제8항에 있어서,
상기 무선 장치 구동 방법은,
스펙트럼 모니터링 단계를 더 포함하며, 상기 스펙트럼 모니터링 단계는,
상기 재구성된 주변 신호의 크기에 따라 분류하는 단계와,
분류된 상기 주변 신호를 시간 축과 주파수 축에 따라 플로팅하여 워터폴 플롯(waterfall plot)을 형성하는 단계를 포함하는 무선 장치 구동 방법.
- [청구항 10] 제9항에 있어서,
상기 스펙트럼 모니터링 단계는,
상기 전송측이 상기 에뮬레이트(emulate)된 헤더를 전송하는 전력을 조절하면서 수행하는 무선 장치 구동 방법.
- [청구항 11] 제8항에 있어서,
상기 무선 장치 구동 방법은,
상기 주변 신호를 제공하는 RF 장치를 식별하는 식별 단계를 더 포함하며, 상기 식별 단계는,
상기 RF 장치별 상기 재구성된 상기 주변 신호의 프레임 파도 상태 특징을 인공지능(AI, Artificial Intelligence)에 학습시키는 단계와,
학습된 상기 인공지능에 재구성된 주변 신호를 제공하여 상기 인공지능이 제공된 상기 주변 신호에 상응하는 RF 장치를 식별(identify)하는 단계를 포함하는 무선 장치 구동 방법.
- [청구항 12] 제11항에 있어서,
상기 RF 장치는
드론(drone), 휴대단말, 라우터(router) 및 영상 통신 장비 중 어느 하나인 무선 장치 구동 방법.
- [청구항 13] 제8항에 있어서,
상기 주변 신호를 재구성하는 단계는,
위상 오차를 제거하는 단계를 더 포함하며, 상기 위상 오차를 제거하는 단계는,
상기 재구성된 상기 주변 신호의 위상을 변화시키면서 기준 신호와 코릴레이션 연산을 수행하는 단계 및
상기 코릴레이션 연산값이 제일 큰 위상을 선택하는 단계를 포함하는 무선 장치 구동 방법.
- [청구항 14] 제13항에 있어서,

상기 코릴레이션 연산값이 제일 큰 위상을 선택하는 단계는,
상기 코릴레이션 연산값이 제일 큰 위상을 가지는 상기 주변 신호 중,
규정에 부합하는 위상을 가지는 주변 신호를 선택하여 수행하는 무선
장치 구동 방법.

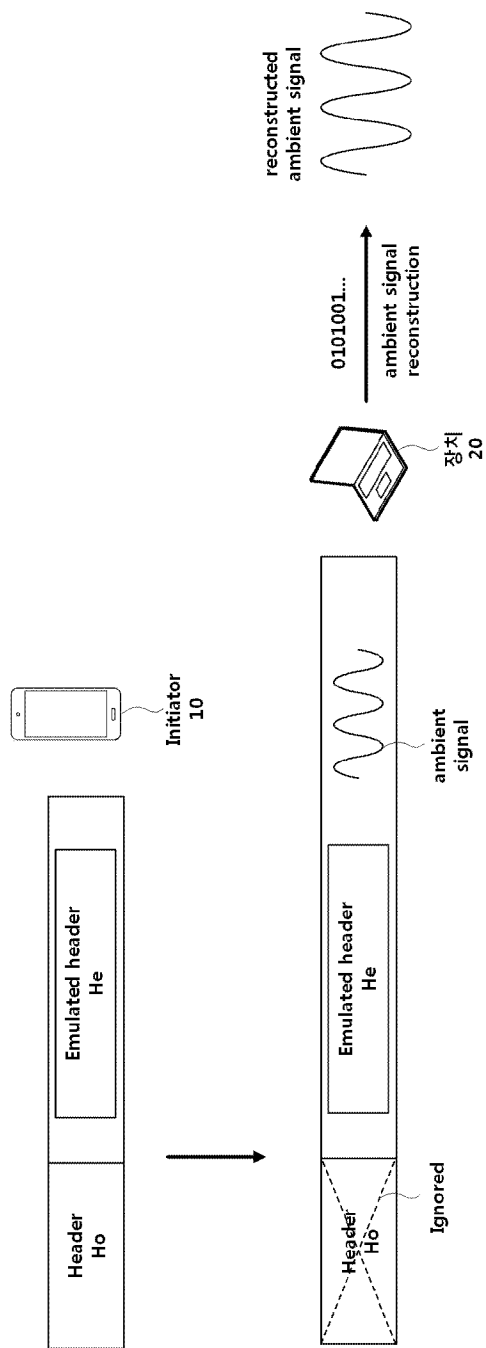
- [청구항 15] 제2 프로토콜로 에뮬레이트(emulate)된 헤더를 제1 프로토콜에 따른
패킷의 페이로드에 은닉하여 전송하는 전송측(transmission side).
- [청구항 16] 제15항에 있어서,
상기 제1 프로토콜은 802.11n이고,
상기 제2 프로토콜은 802.11g인 전송측.
- [청구항 17] 제15항에 있어서,
상기 에뮬레이트된 헤더는 10개의 슛 심볼들, 2.5개의 롱 심볼들을
포함하는 프리앰블 필드와, PHY 필드 및 MAC 필드를 포함하며,
상기 10개의 슛 심볼들은 두 개의 제1 프로토콜에 따른 페이로드 심볼로
에뮬레이트되고,
상기 2.5개의 롱 심볼들은 두 개의 제1 프로토콜에 따른 페이로드 심볼로
에뮬레이트되며,
상기 PHY 필드와 상기 MAC 필드는 각각 하나의 제1 프로토콜에 따른
페이로드 심볼로 에뮬레이트 되는 전송측.
- [청구항 18] 제15항에 있어서,
상기 에뮬레이트된 헤더는 프리앰블 필드 및 PHY 필드를 포함하며,
상기 전송측은 상기 프리앰블 필드 및 PHY 필드를 BPSK(Binary Phase
Shift Keying)로 전송하는 전송측.
- [청구항 19] 제2 프로토콜로 에뮬레이트(emulate)되되, 제1 프로토콜로 규정된
패킷(packet)의 페이로드(payload)에 은닉되어 전송된 헤더 및 주변
신호(ambient signal)를 수신하고,
상기 주변 신호를 상기 제2 프로토콜에 따라 디코딩하여 비트 시퀀스를
얻고,
상기 비트 시퀀스로부터 상기 주변 신호를 재구성(reconstruction)하는
수신측.
- [청구항 20] 제19항에 있어서,
상기 수신측은,
상기 제1 프로토콜로 규정된 패킷의 헤더를 무시(ignore)하는 수신측.
- [청구항 21] 제19항에 있어서,
상기 제1 프로토콜은 802.11n이고,
상기 제2 프로토콜은 802.11g인 수신측.
- [청구항 22] 제19항에 있어서,
상기 수신측은,
상기 재구성된 주변 신호를 크기에 따라 분류하는 단계와,

분류된 상기 주변 신호를 시간 축과 주파수 축에 따라 플로팅하여 워터폴 플롯(waterfall plot)을 형성하여 상기 주변 신호의 스펙트럼을 모니터링하는 수신측.

[도1]

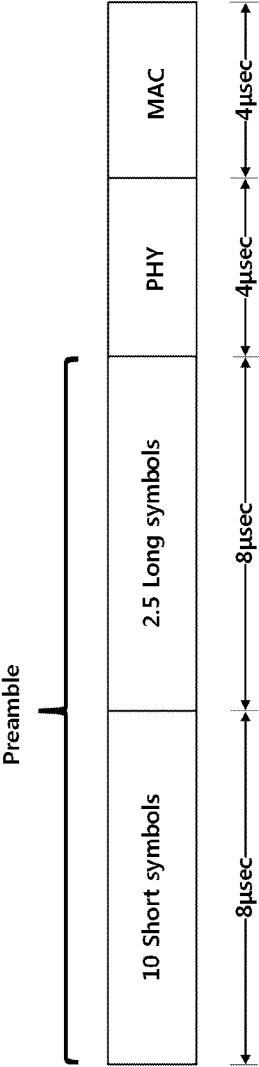


[도2]

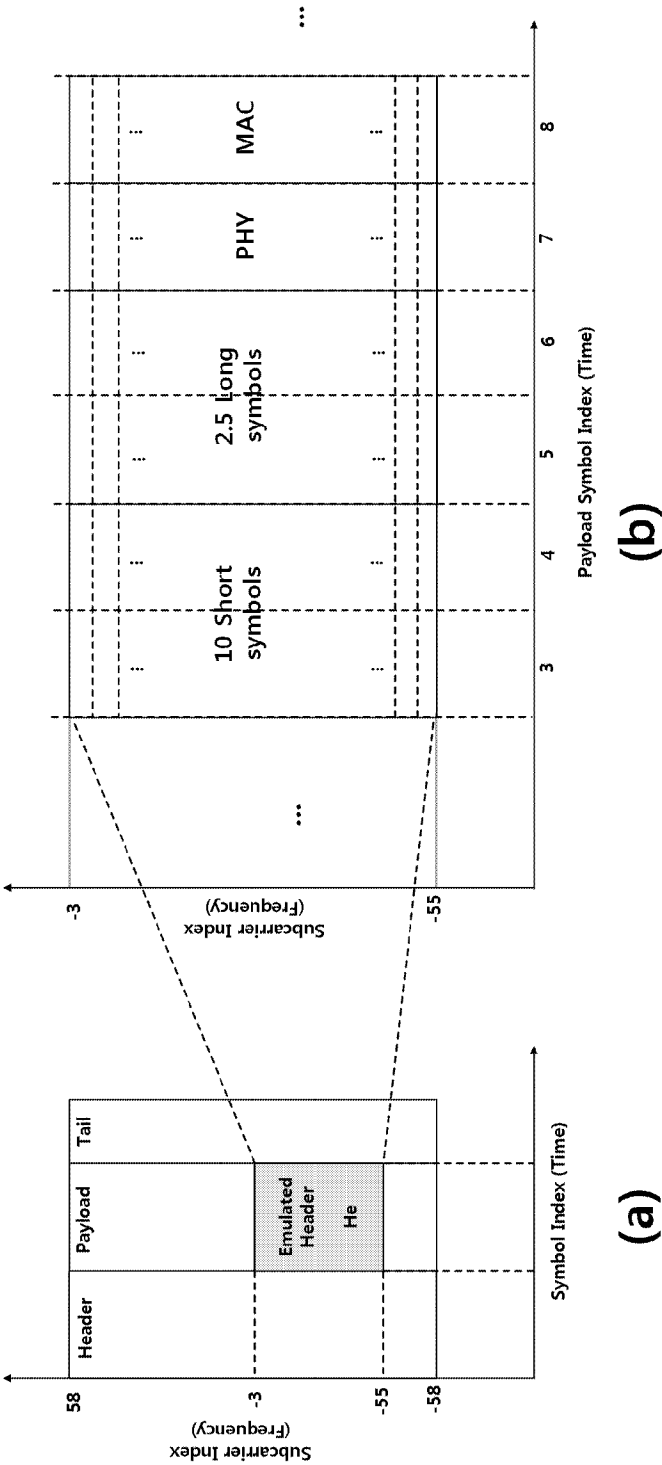


[도3]

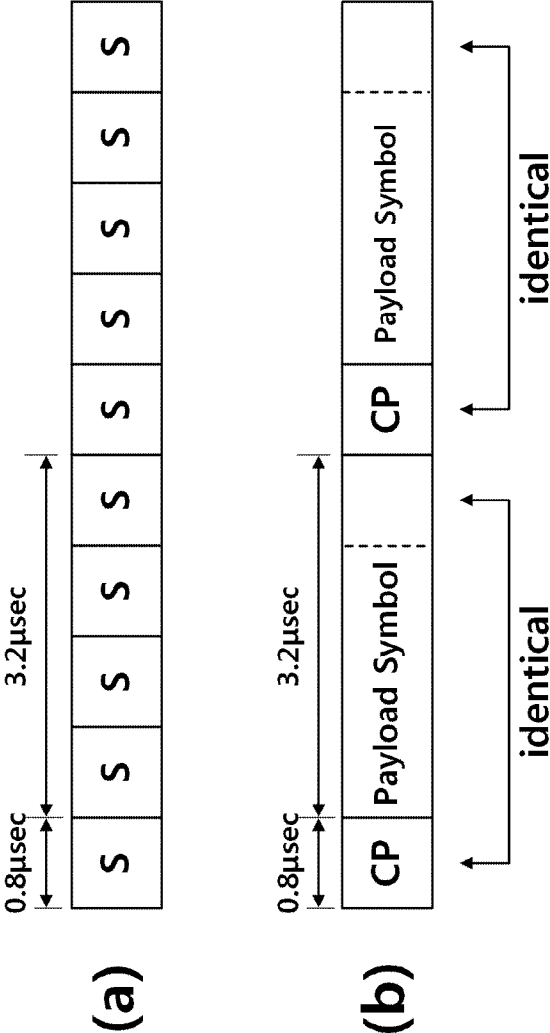
<Prior art>



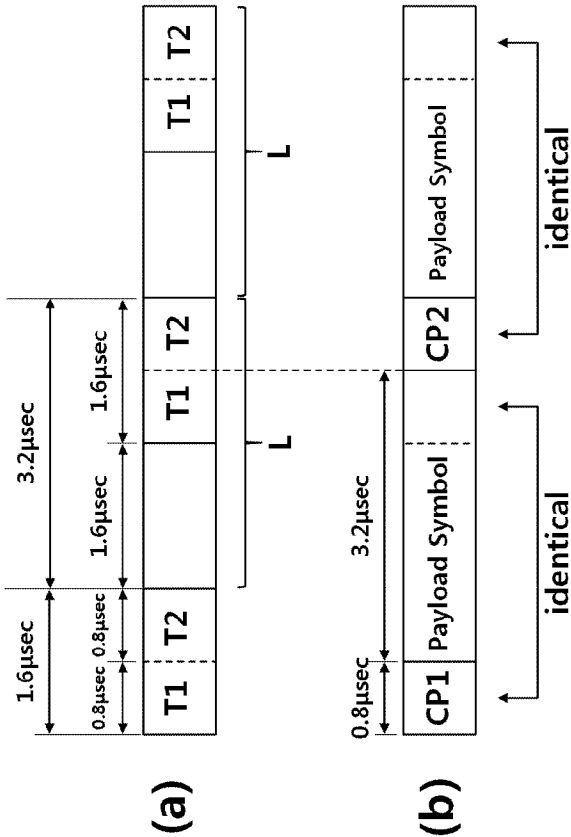
[도4]



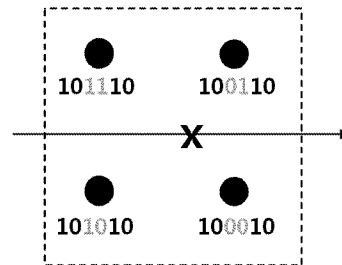
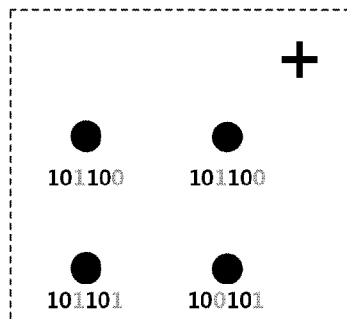
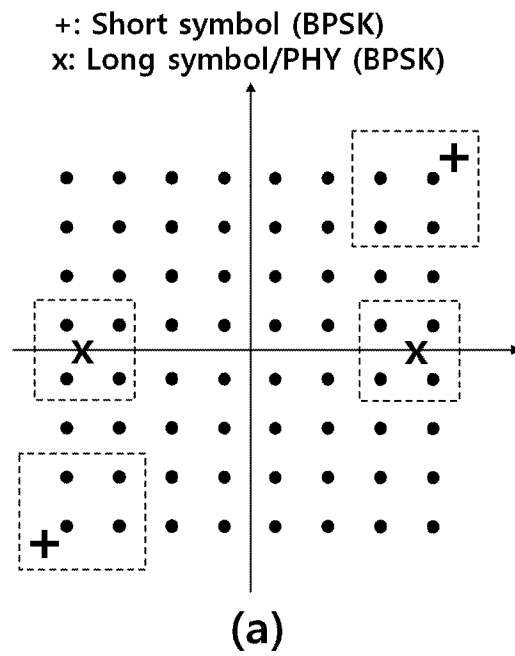
[도5]



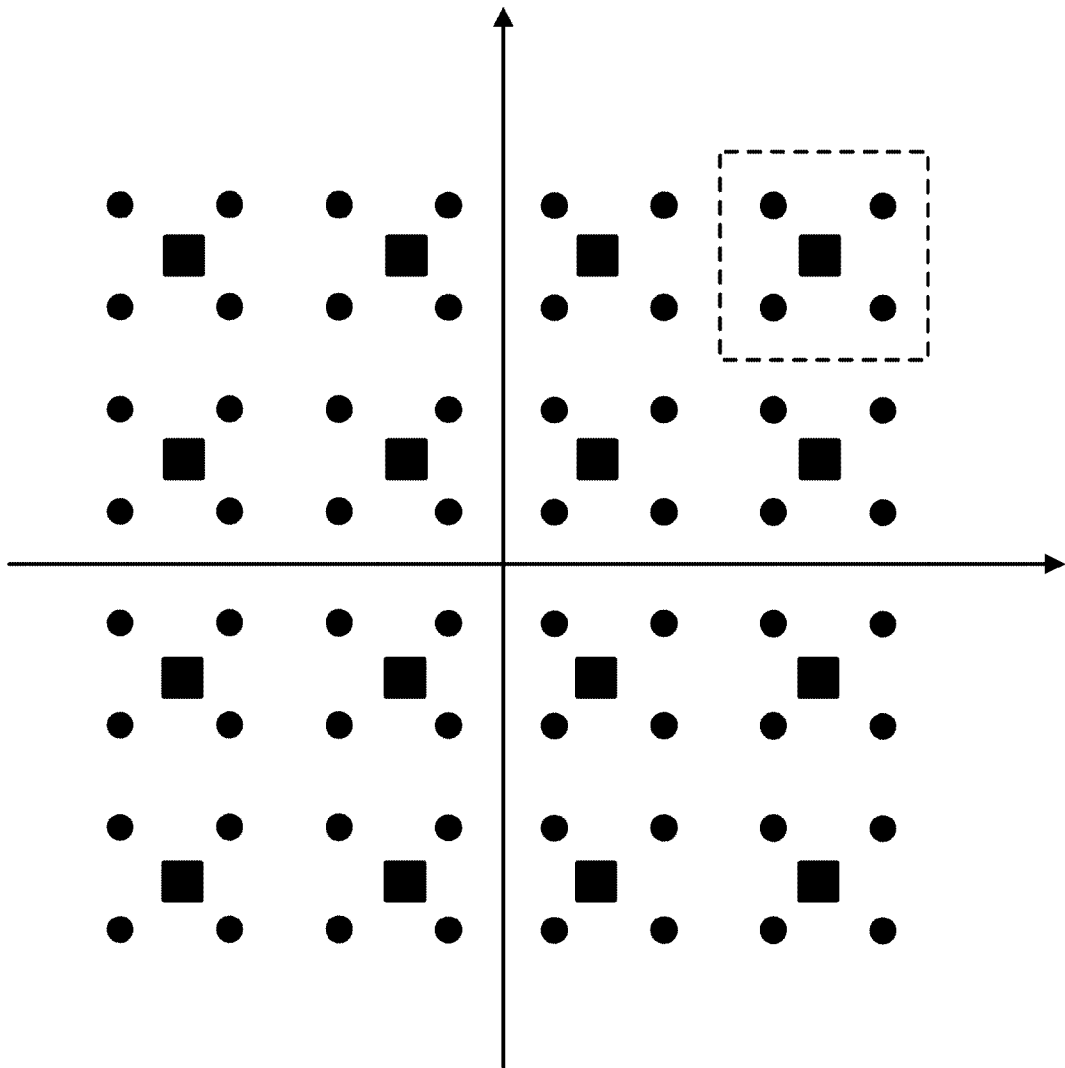
[도6]



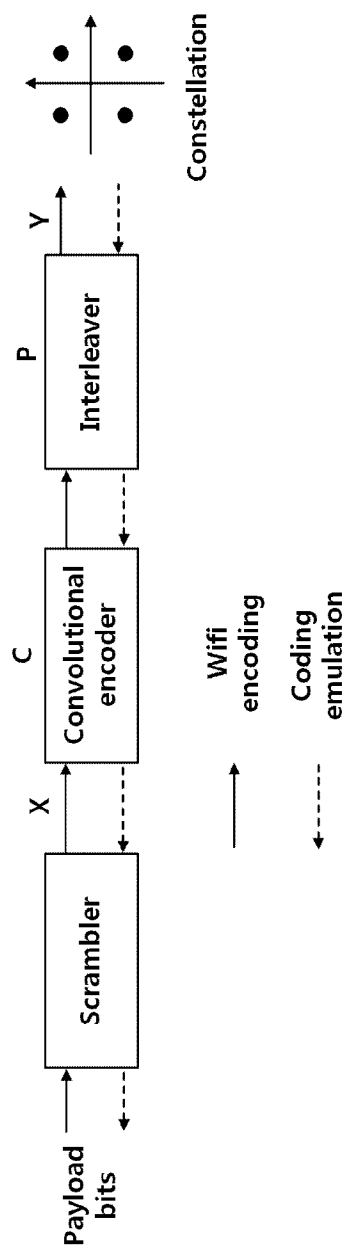
[도7]



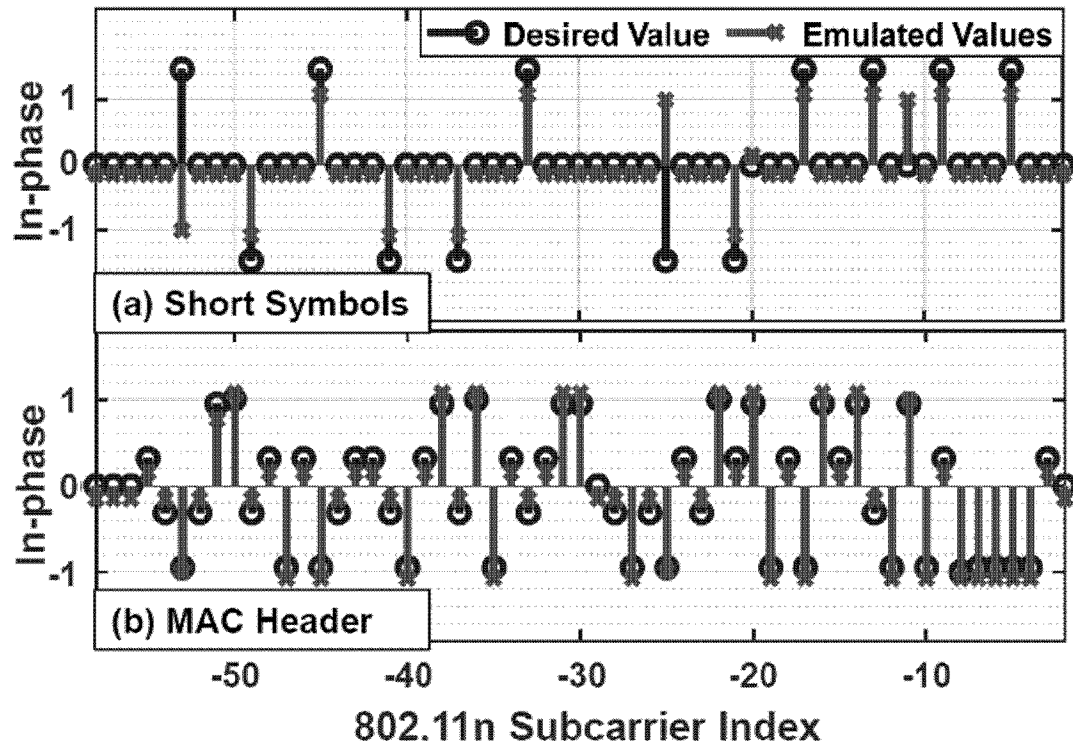
[도8]

■: MAC (16 QAM)

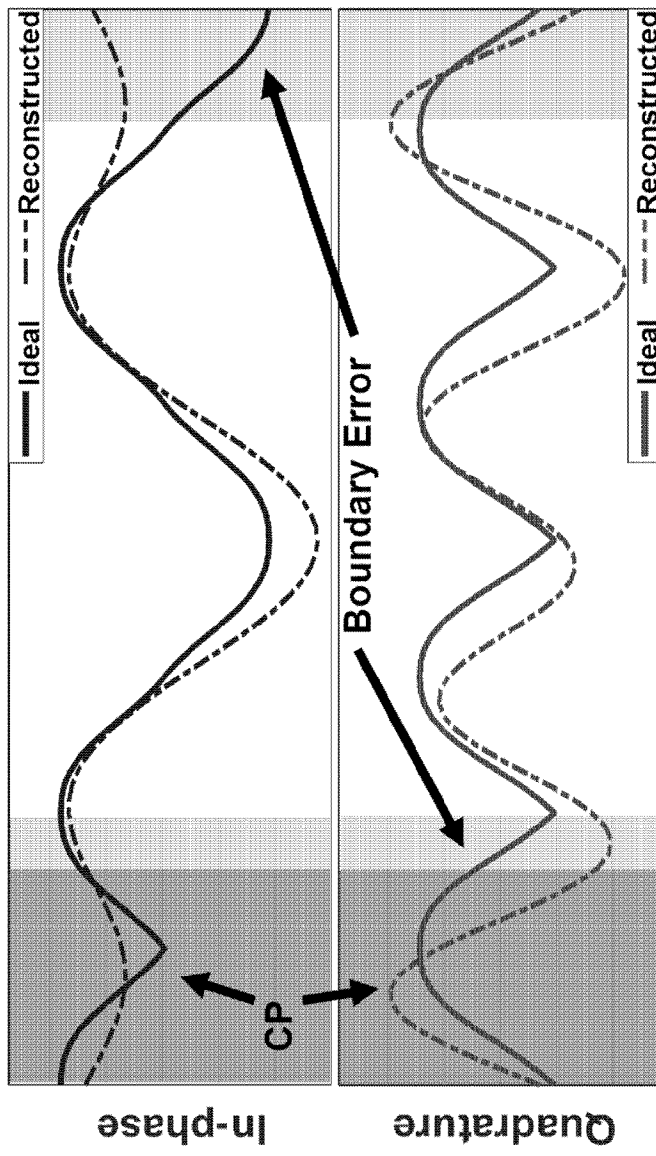
[도9]



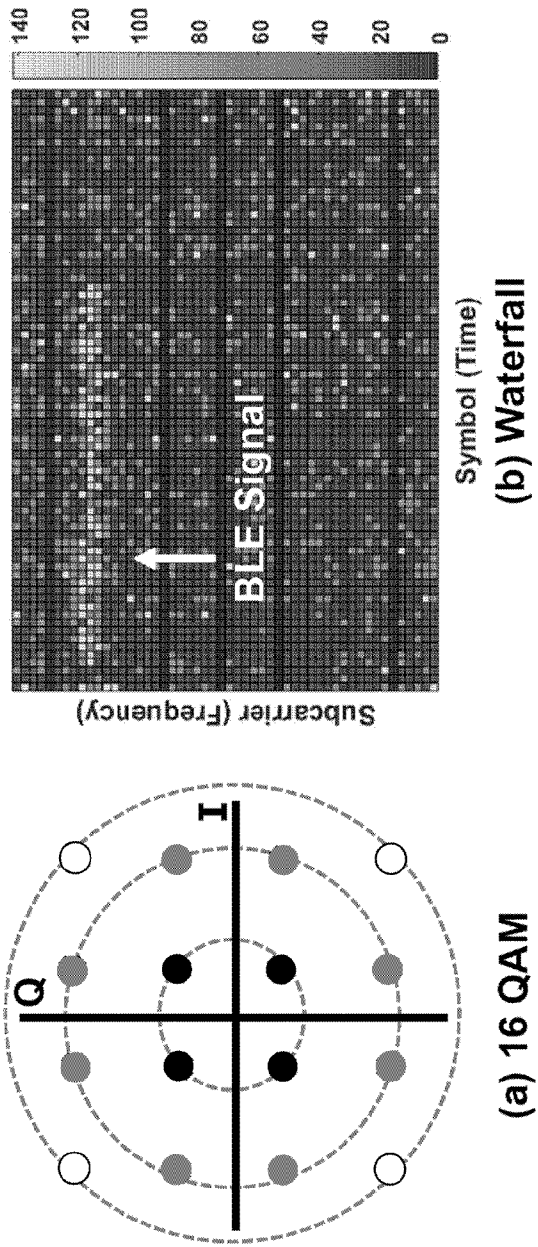
[도10]



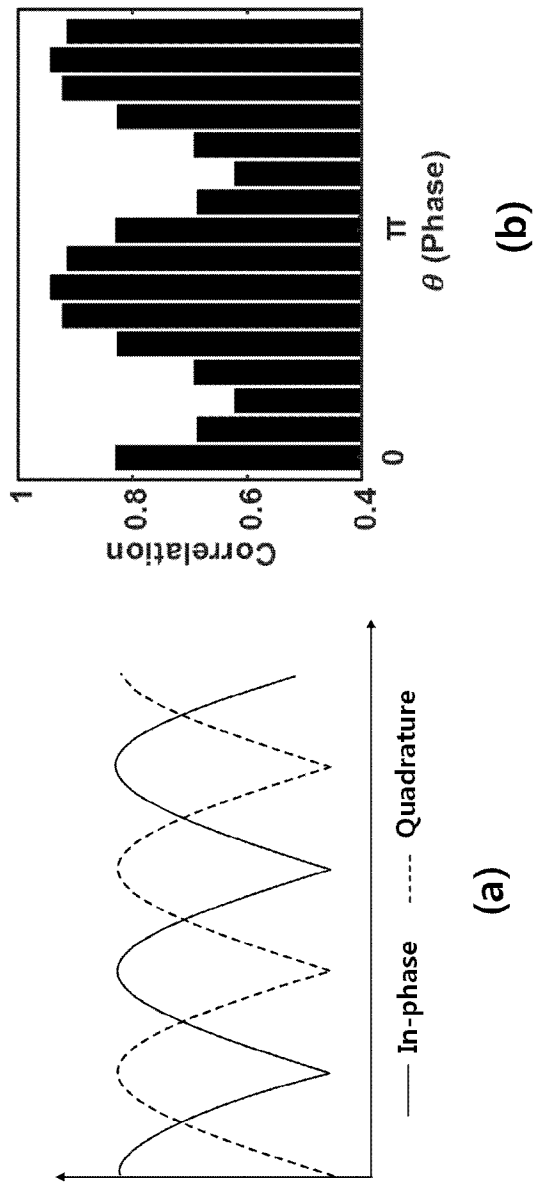
[도11]



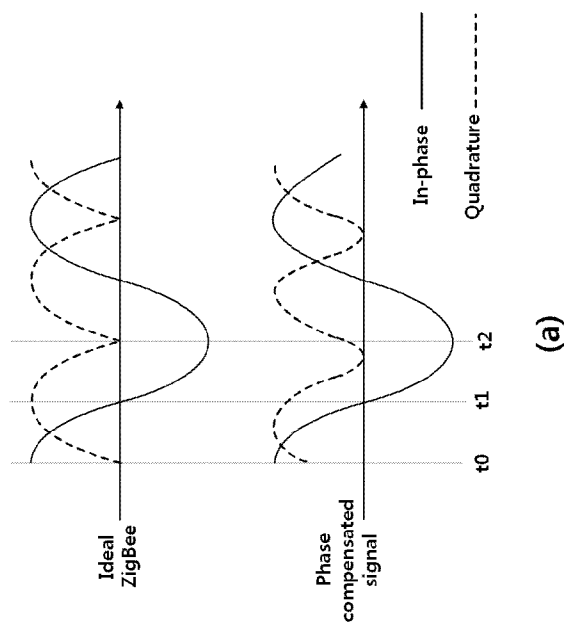
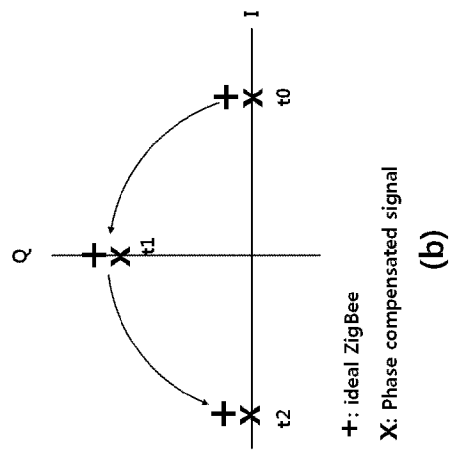
[도12]



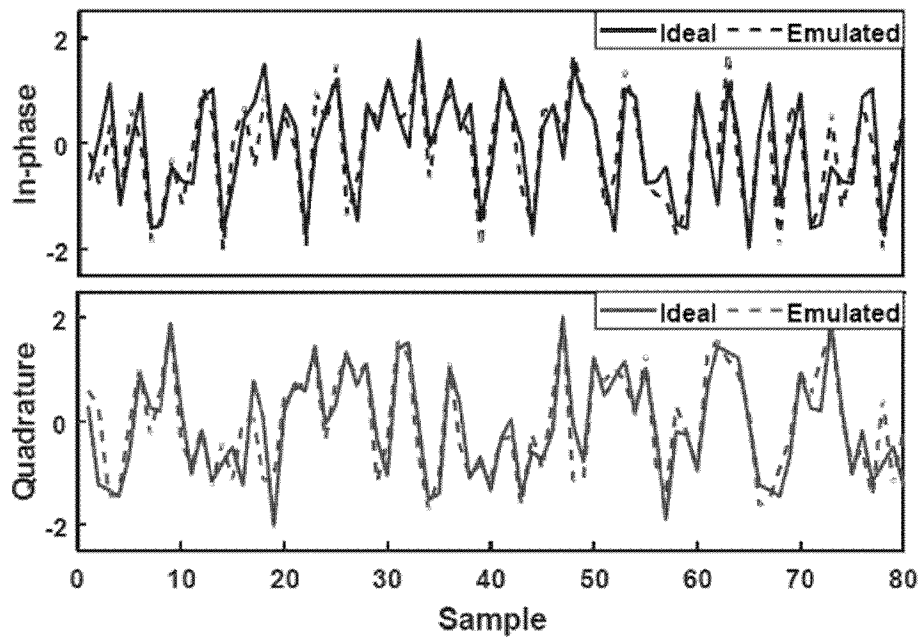
[도13]



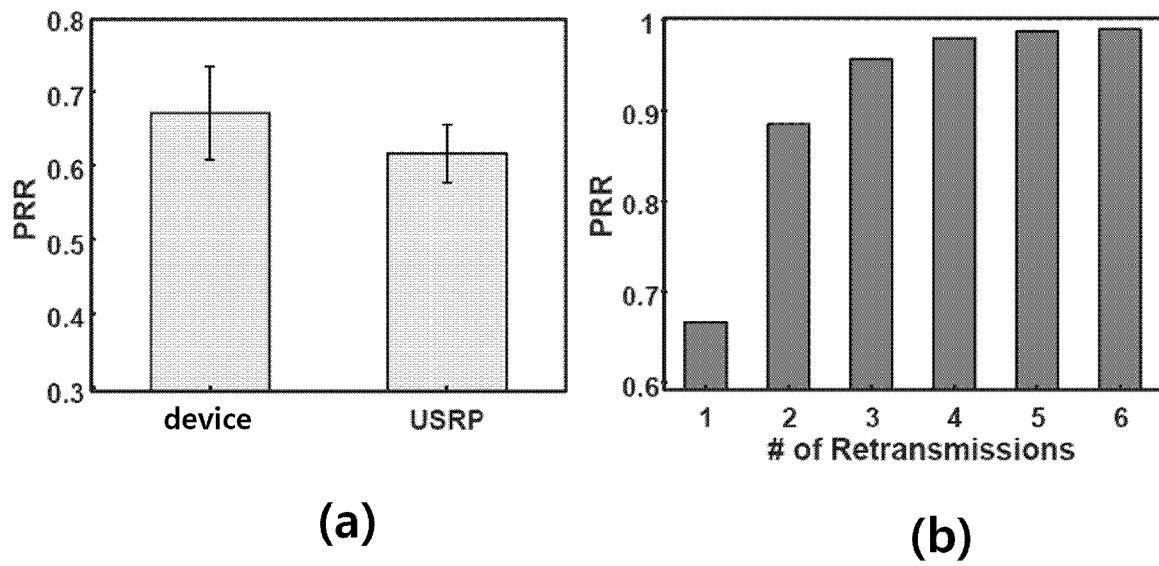
[도14]



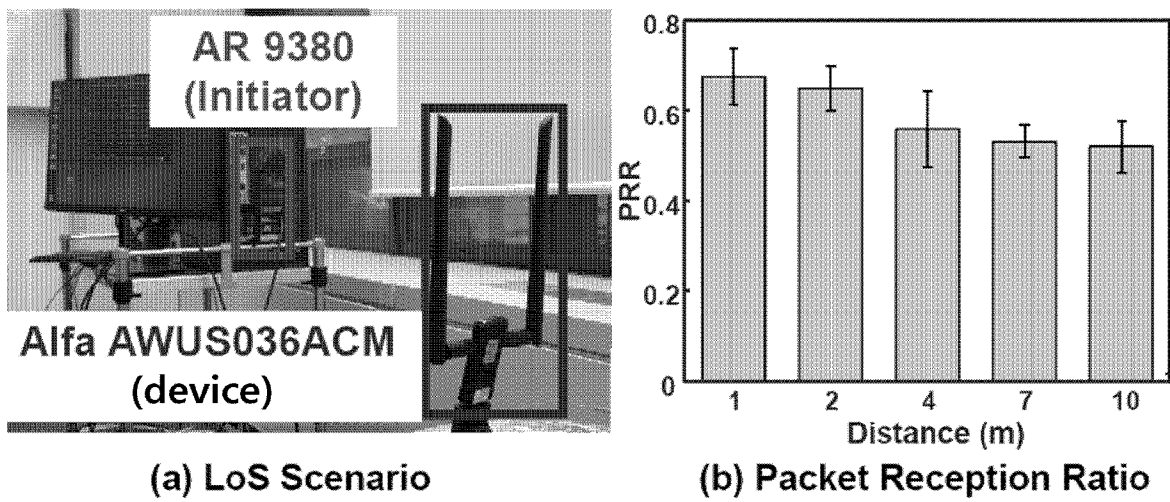
[도15]



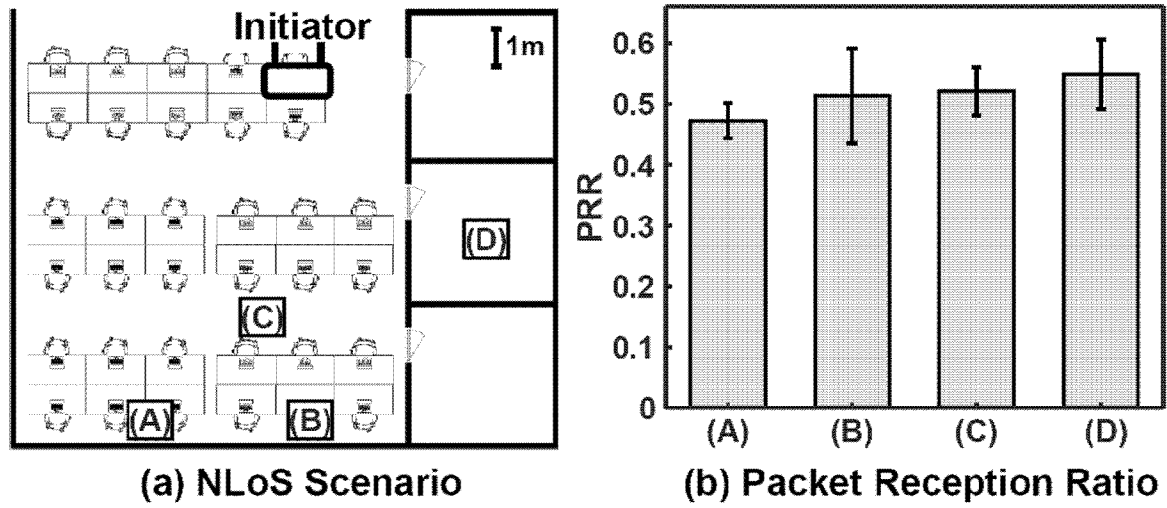
[도16]



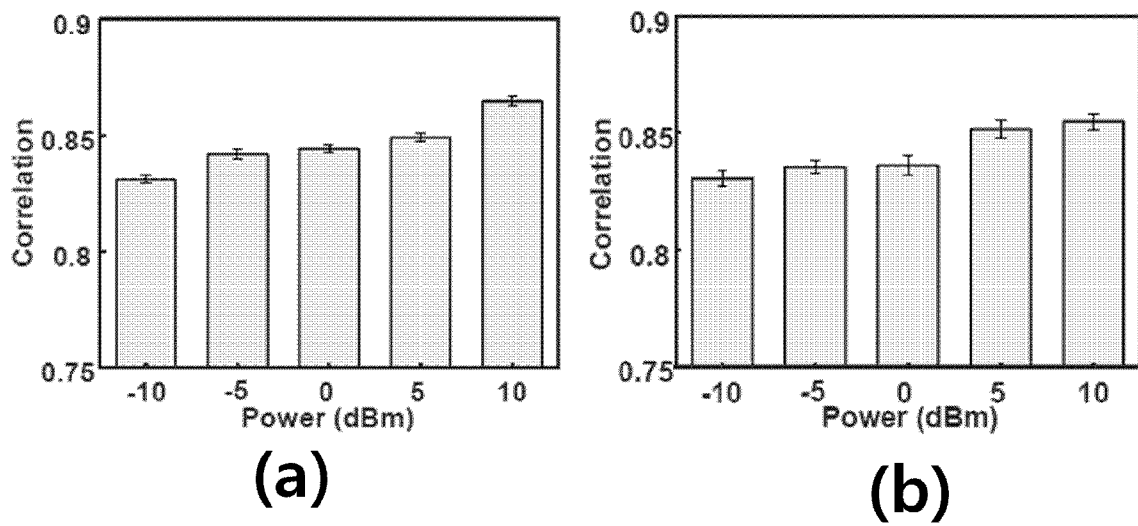
[도17]



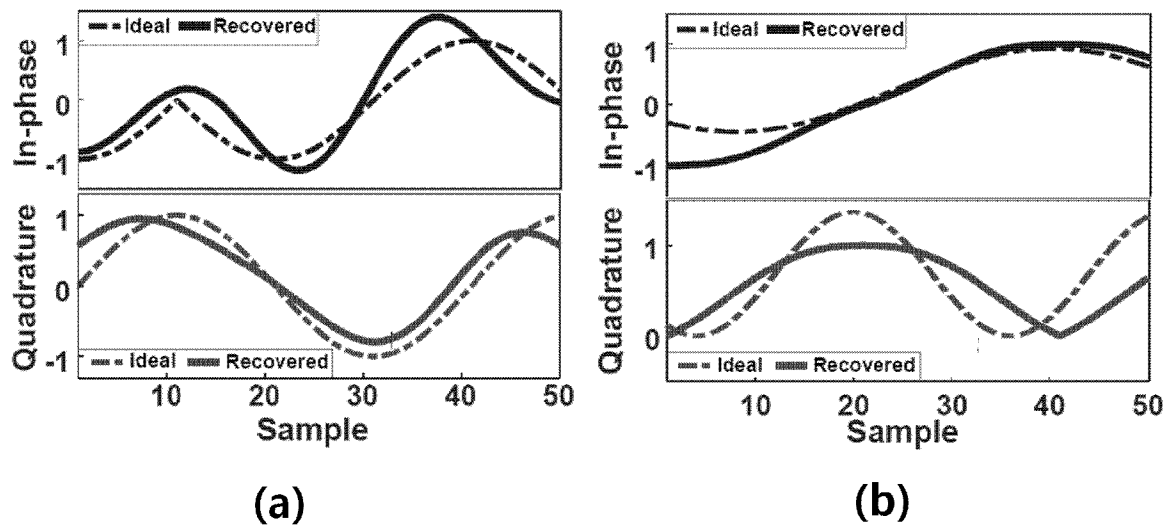
[도18]



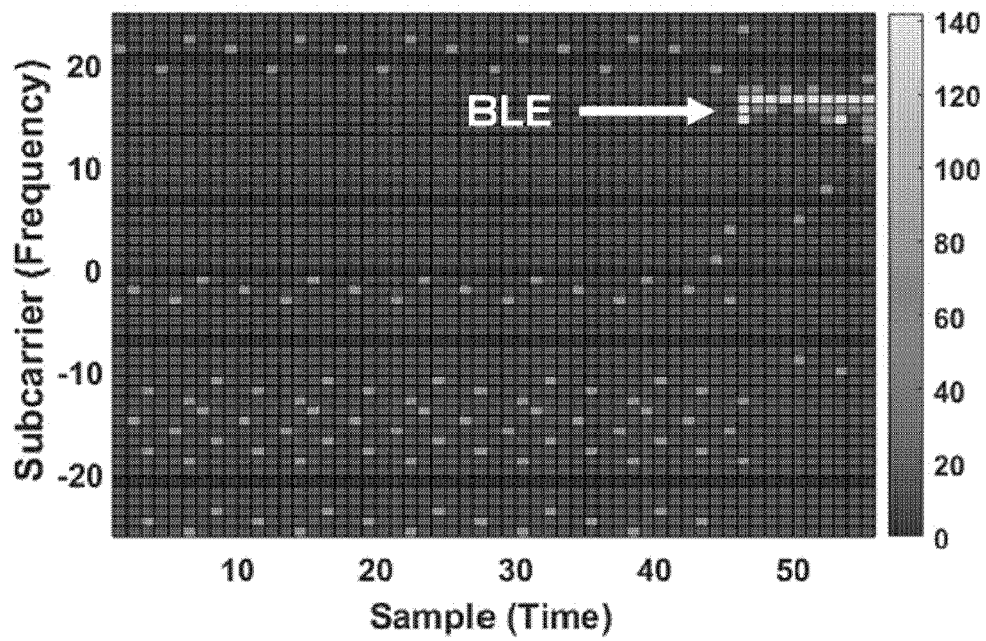
[도19]



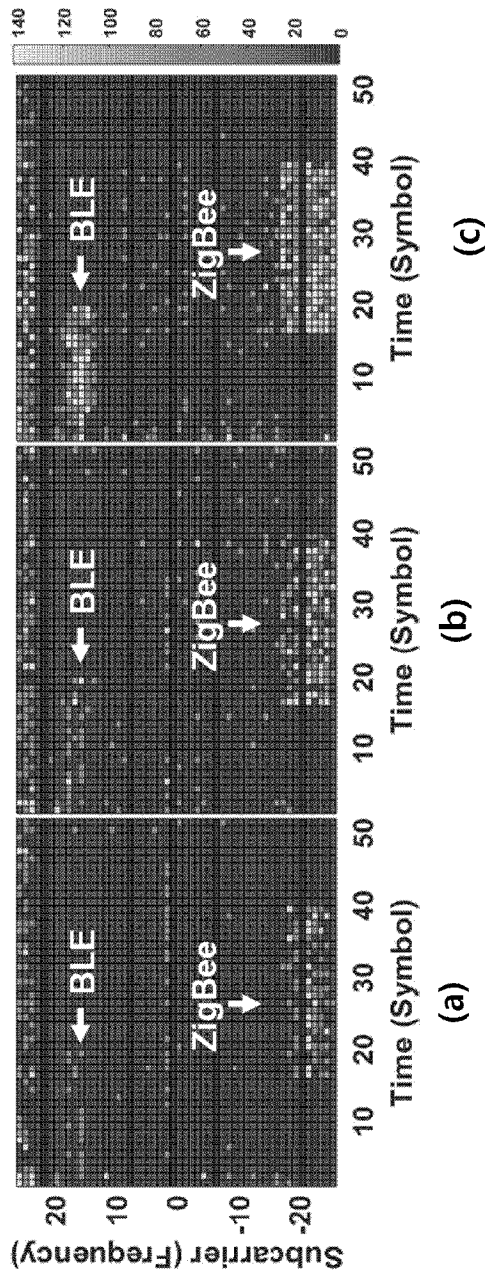
[도20]



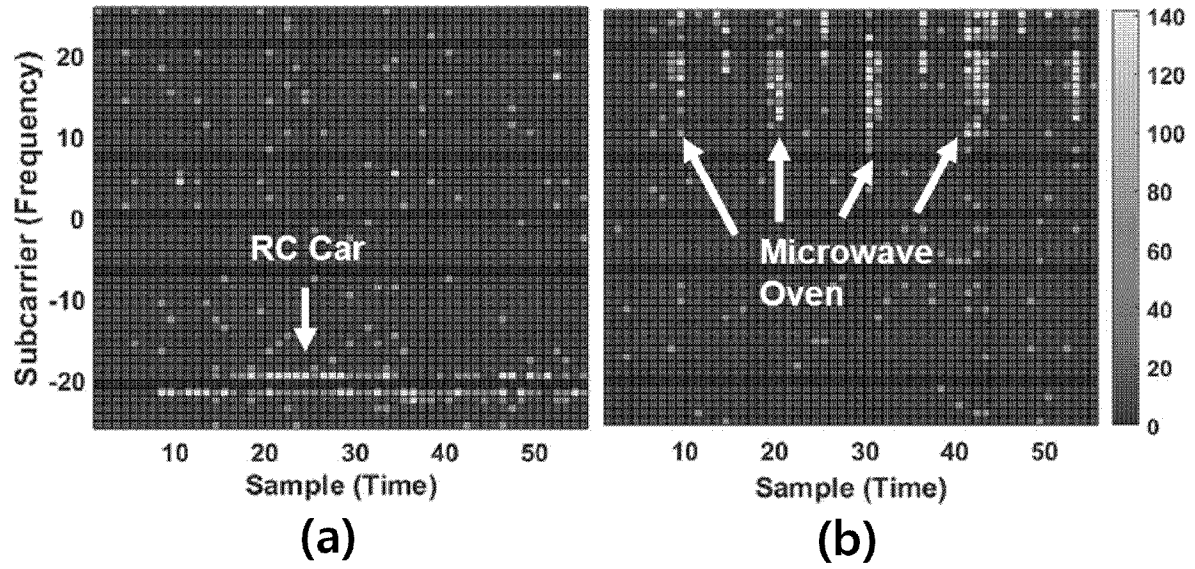
[도21]



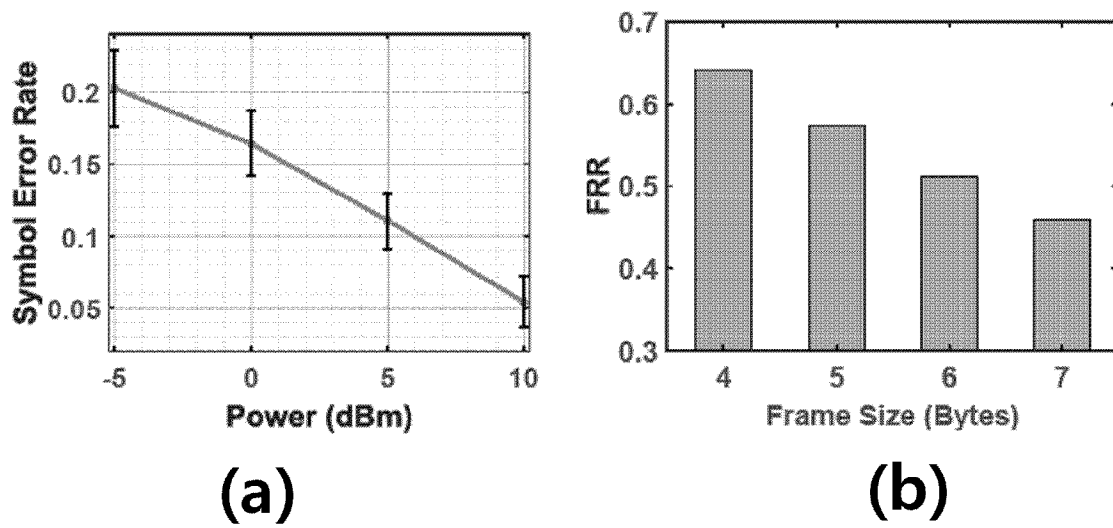
[도22]



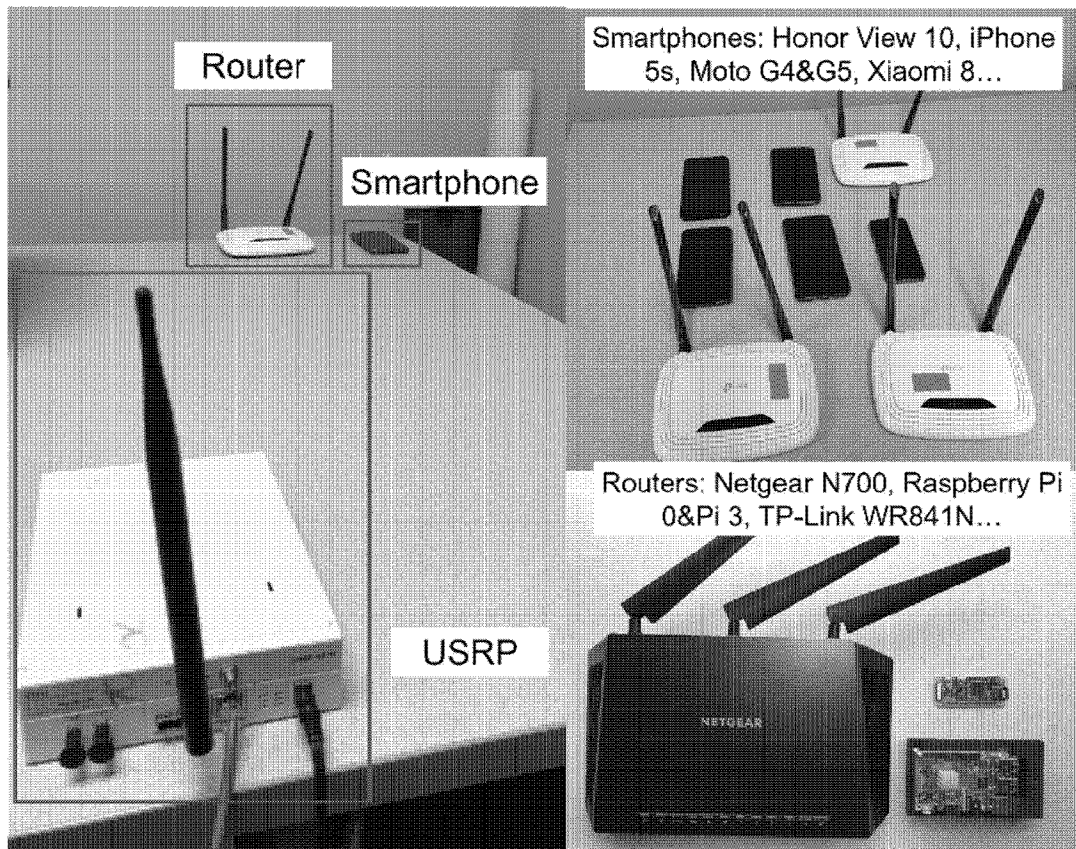
[도23]



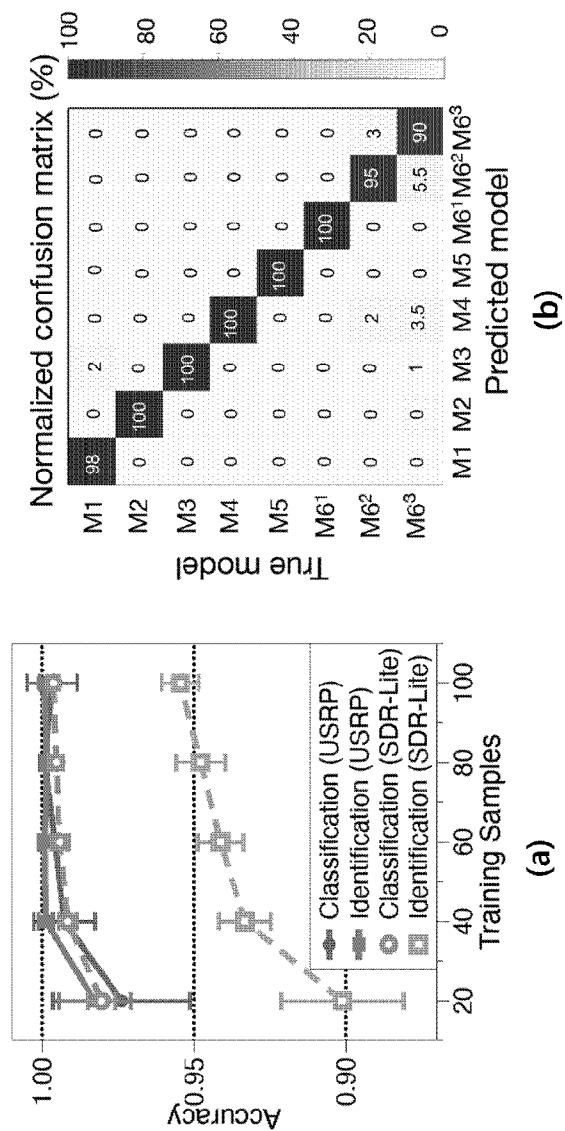
[도24]



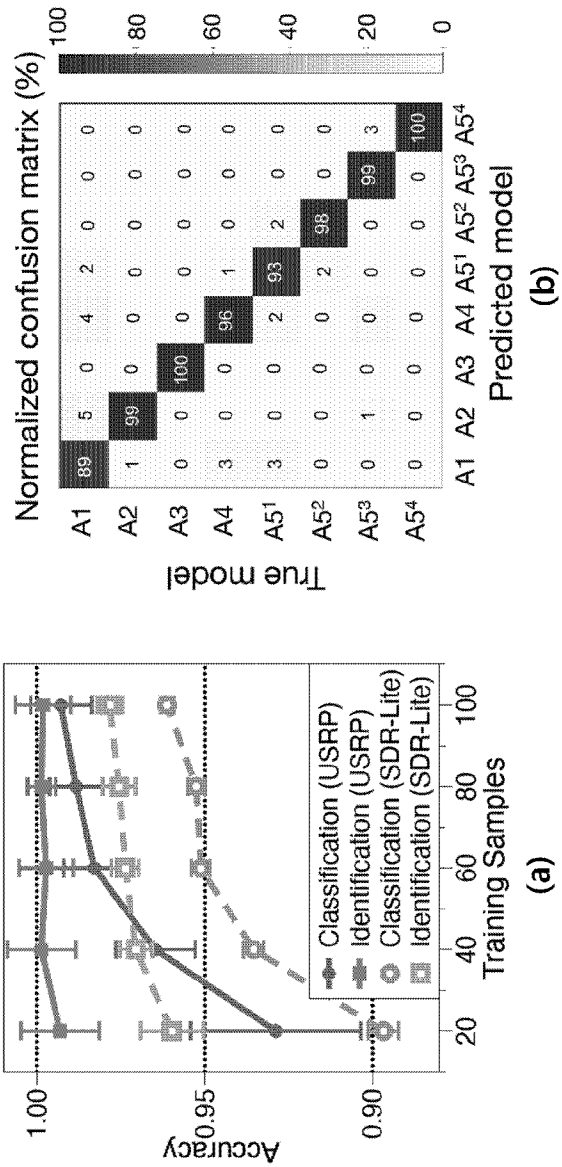
[도25]



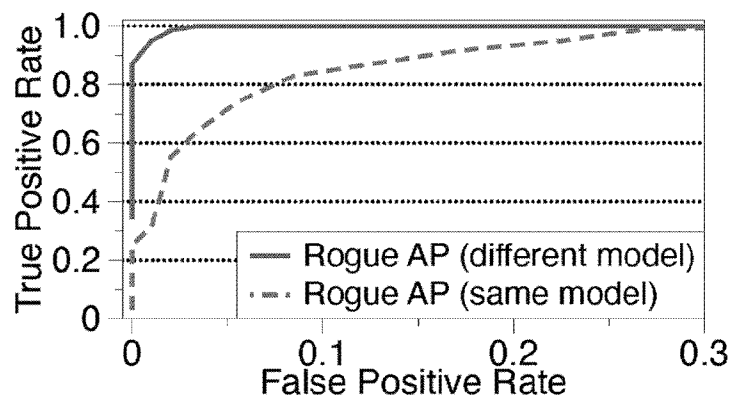
[도26]



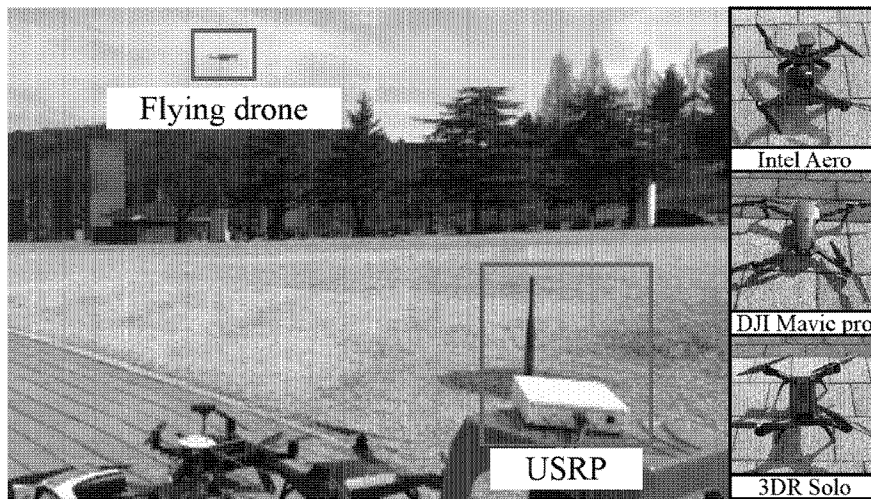
[도27]



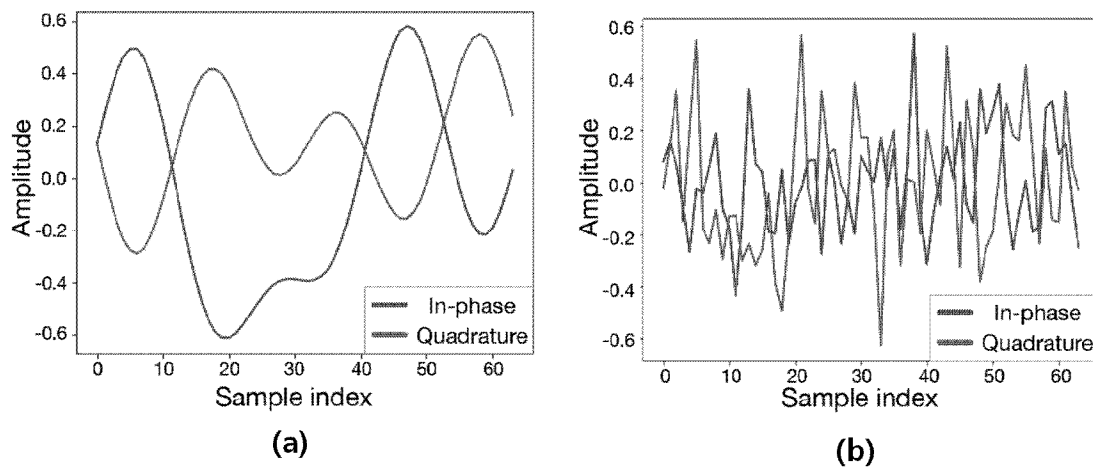
[도28]



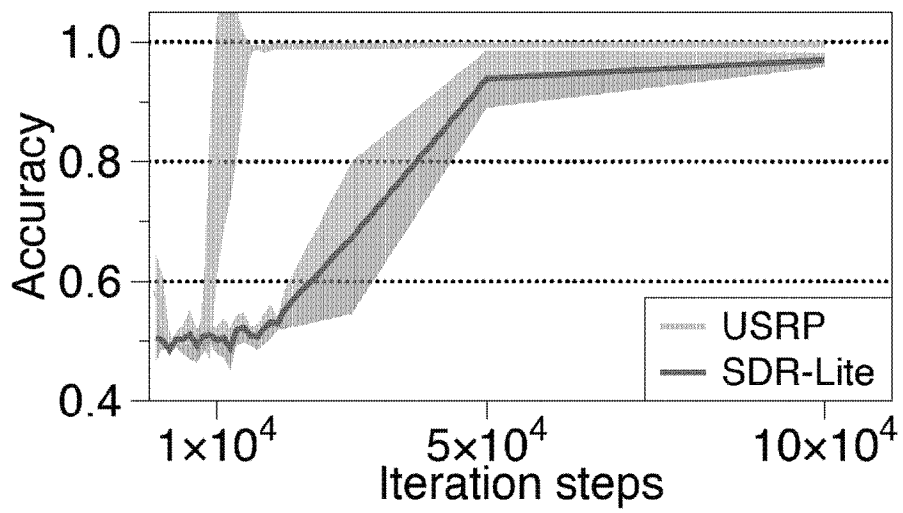
[도29]



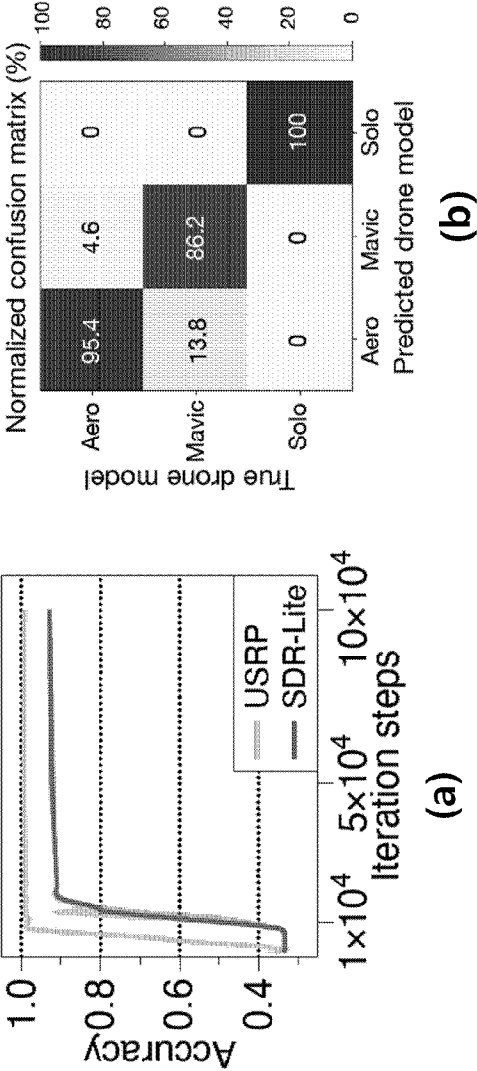
[도30]



[도31]



[도32]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2020/010235

A. CLASSIFICATION OF SUBJECT MATTER**H04L 27/34(2006.01)i; H04L 1/00(2006.01)i; H04L 29/08(2006.01)i; H04L 29/06(2006.01)i; H04B 1/00(2006.01)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 27/34(2006.01); G01R 23/16(2006.01); G01S 3/04(2006.01); H04L 12/70(2013.01); H04L 12/801(2013.01);
H04W 16/26(2009.01)

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: 제1-제2 프로토콜(first and second protocols), 에뮬레이트(emulate), 페이로드(payload), 헤더(header), 주변 신호(ambient signal), 신호 재구성(signal reconstruction)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	LI, Zhijun et al. WEBe: Physical-Layer Cross-Technology Communication via Emulation. In: MobiCom '17: Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking. October 2017, pp. 2-14. See pages 3-12; and figures 1-16 and 24.	15-18 1-14,19-22
Y	LIU, Vincent et al. Ambient Backscatter: Wireless Communication Out of Thin Air. In: SIGCOMM 13. Proceedings of the ACM SIGCOMM 2013 conference on SIGCOMM. August 2013, pp. 39-50. See pages 39-46; and figure 1.	1-14,19-22
Y	US 2013-0113659 A1 (MORGAN, David) 09 May 2013 (2013-05-09) See paragraph [0066]; and figure 9.	9,10,22
Y	JP 2016-152453 A (HITACHI LTD.) 22 August 2016 (2016-08-22) See paragraphs [0032], [0108] and [0157].	11,12



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

28 April 2021

Date of mailing of the international search report

28 April 2021

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

International application No.

PCT/KR2020/010235

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2013-541242 A (ZTE CORP.) 07 November 2013 (2013-11-07) See paragraphs [0006]-[0008] and [0058]-[0060]; and figure 1.	1-22

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/KR2020/010235

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
US	2013-0113659	A1	09 May 2013	EP	2534495	A1	19 December 2012
				EP	2534495	B1	24 April 2019
				US	9116186	B2	25 August 2015
				WO	2011-098810	A1	18 August 2011
JP	2016-152453	A	22 August 2016	None			
JP	2013-541242	A	07 November 2013	CN	102377470	A	14 March 2012
				CN	102377470	B	12 August 2015
				EP	2605572	A1	19 June 2013
				JP	5763767	B2	12 August 2015
				WO	2012-019504	A1	16 February 2012

A. 발명이 속하는 기술분류(국제특허분류(IPC)) H04L 27/34(2006.01)i; H04L 1/00(2006.01)i; H04L 29/08(2006.01)i; H04L 29/06(2006.01)i; H04B 1/00(2006.01)i		
B. 조사된 분야 조사된 최소문헌(국제특허분류를 기재) H04L 27/34(2006.01); G01R 23/16(2006.01); G01S 3/04(2006.01); H04L 12/70(2013.01); H04L 12/801(2013.01); H04W 16/26(2009.01) 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: 제1-제2 프로토콜(first and second protocols), 에뮬레이트(emulate), 페이로드(payload), 헤더(header), 주변신호(ambient signal), 신호 재구성(signal reconstruction)		
C. 관련 문헌		
카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
X Y	ZHIJUN LI 등, WEBee: Physical-Layer Cross-Technology Communication via Emulation, In: MobiCom '17: Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking, 2017.10, pp. 2-14 페이지 3-12; 및 도면 1-16, 24	15-18 1-14,19-22
Y	VINCENT LIU 등, Ambient Backscatter: Wireless Communication Out of Thin Air, In: SIGCOMM 13, Proceedings of the ACM SIGCOMM 2013 conference on SIGCOMM, 2013.08, pp. 39-50 페이지 39-46; 및 도면 1	1-14,19-22
Y	US 2013-0113659 A1 (DAVID MORGAN) 2013.05.09 단락 [0066]; 및 도면 9	9,10,22
Y	JP 2016-152453 A (HITACHI LTD.) 2016.08.22 단락 [0032], [0108], [0157]	11,12
A	JP 2013-541242 A (ZTE CORP.) 2013.11.07 단락 [0006]-[0008], [0058]-[0060]; 및 도면 1	1-22
☐ 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 2021년04월28일(28.04.2021)		국제조사보고서 발송일 2021년04월28일(28.04.2021)
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

국 제 조 사 보 고 서
대응특허에 관한 정보

국제출원번호

PCT/KR2020/010235

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
US 2013-0113659 A1	2013/05/09	EP 2534495 A1	2012/12/19
		EP 2534495 B1	2019/04/24
		US 9116186 B2	2015/08/25
		WO 2011-098810 A1	2011/08/18
JP 2016-152453 A	2016/08/22	없음	
JP 2013-541242 A	2013/11/07	CN 102377470 A	2012/03/14
		CN 102377470 B	2015/08/12
		EP 2605572 A1	2013/06/19
		JP 5763767 B2	2015/08/12
		WO 2012-019504 A1	2012/02/16