

(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구  
국제사무국

(43) 국제공개일  
2017년 9월 28일 (28.09.2017)



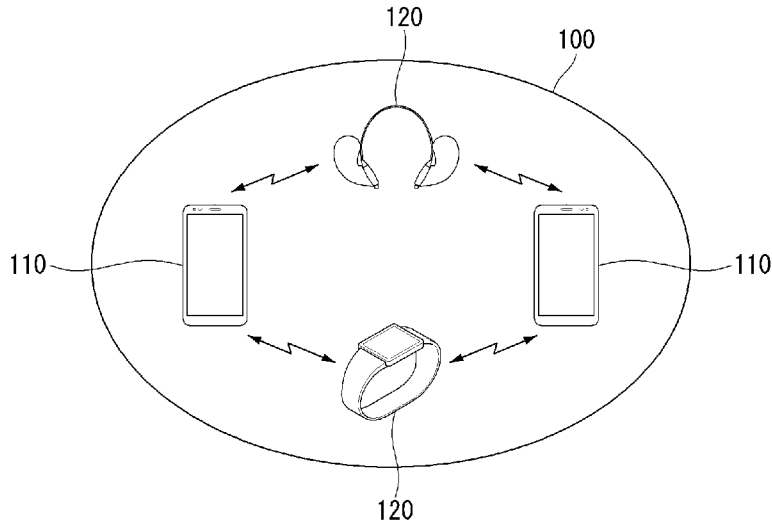
(10) 국제공개번호  
WO 2017/164618 A2

- (51) 국제특허분류: H04Q 9/04 (2006.01) H04W 76/02 (2009.01)
- (21) 국제출원번호: PCT/KR2017/003022
- (22) 국제출원일: 2017년 3월 21일 (21.03.2017)
- (25) 출원언어: 한국어
- (26) 공개언어: 한국어
- (30) 우선권정보: 62/310,847 2016년 3월 21일 (21.03.2016) US  
62/365,345 2016년 7월 21일 (21.07.2016) US
- (71) 출원인: 엘지전자(주) (LG ELECTRONICS INC.) [KR/KR]; 07336 서울시 영등포구 여의대로 128, Seoul (KR).
- (72) 발명자: 권영환 (KWON, Younghwan); 06772 서울시 서초구 양재대로 11길 19, LG 전자 특허센터, Seoul (KR).
- (74) 대리인: 특허법인 로얄 (ROYAL PATENT & LAW OFFICE); 08806 서울시 관악구 남부순환로 2072, 도원회관 빌딩 1층, 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, 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, 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, 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).

[다음 쪽 계속]

(54) Title: METHOD AND APPARATUS FOR CONTROLLING DEVICE BY USING BLUETOOTH TECHNOLOGY

(54) 발명의 명칭: 블루투스 기술을 이용하여 디바이스를 제어하기 위한 방법 및 장치



(57) Abstract: The present invention relates to: a method and an apparatus for allowing a control device to control a first device by using Bluetooth communication. According to the present invention, the method comprises the steps of: forming a Bluetooth connection with the first device; transmitting, to the first device, a read request message requesting attribute information related to a controllable operation supported by the first device; receiving, from the first device, a read response message comprising the attribute information, in response to the read request message, wherein the attribute information includes an operation field indicating an operation supported by the first device; transmitting, to the first device, a first write request message requesting a writing of an attribute for instructing a performance of a specific role on the basis of the attribute information, wherein the first write request message includes control information related to the specific role; and receiving, from the first device, a write response message in response to the first write request message, wherein the control message can include role information indicating the specific role, and parameter information indicating an operation related to the specific role.

(57) 요약서:

[다음 쪽 계속]



WO 2017/164618 A2

**공개:**

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

---

블루투스 통신을 이용하여 제어 디바이스가 제 1 디바이스를 제어하는 방법 및 장치에 관한 것이다. 본 발명에 의하면, 상기 제 1 디바이스와 블루투스 연결을 형성하는 단계; 상기 제 1 디바이스가 지원하는 제어 가능한 동작(**controllable operation**)과 관련된 특성 정보를 요청하는 판독 요청 메시지를 상기 제 1 디바이스로 전송하는 단계; 상기 판독 요청 메시지에 대한 응답으로 상기 특성 정보를 포함하는 판독 응답 메시지를 상기 제 1 디바이스로부터 수신하는 단계로서, 상기 특성 정보는 상기 제 1 디바이스가 지원하는 동작을 나타내는 동작 필드를 포함하고; 상기 특성 정보에 기초하여 상기 제 1 디바이스로 특정 역할(**role**)의 수행을 지시하기 위한 특성의 기입을 요청하는 제 1 기입 요청 메시지를 전송하는 단계로서, 상기 제 1 기입 요청 메시지는 상기 특정 역할과 관련된 제어 정보를 포함하고; 및 상기 제 1 기입 요청 메시지에 대한 응답으로 기입 응답 메시지를 상기 제 1 디바이스로부터 수신하는 단계를 포함하되, 상기 제어 정보는 상기 특정 역할을 나타내는 역할 정보 및 상기 특정 역할과 관련된 동작을 나타내는 파라미터 정보를 포함할 수 있다.

## 명세서

### 발명의 명칭: 블루투스 기술을 이용하여 디바이스를 제어하기 위한 방법 및 장치

#### 기술분야

- [1] 본 발명은 무선 통신시스템에서 근거리 기술인 블루투스를 이용하여 디바이스 간 커넥션을 형성하기 위한 방법 및 장치에 관한 것으로서, 특히 블루투스 기술을 이용하여 디바이스 간 커넥션을 형성하기 위한 방법 및 장치에 관한 것이다.

#### 배경기술

- [2] 블루투스는 근거리에서 각종 디바이스들을 무선으로 연결하여 데이터를 주고 받을 수 있는 근거리 무선 기술 규격이다. 블루투스(Bluetooth) 통신을 이용하여 두 기기 간 무선 통신을 수행하고자 하는 경우, 사용자(User)는 통신하고자 하는 블루투스(Bluetooth) 디바이스(Device)들을 검색(Discovery)하고 연결(Connection)을 요청하는 절차를 수행한다. 본 발명에서 디바이스는 기기, 장치를 의미할 수 있다.
- [3] 이때, 사용자는 블루투스 디바이스를 이용하여 사용하고자 하는 블루투스 통신방법에 따라 블루투스 디바이스를 검색한 후 연결을 수행할 수 있다.
- [4] 블루투스 통신방법에는 BR/EDR (Basic Rate/Enhanced Data Rate) 방식과 저전력 방식인 LE (Low Energy) 방식이 있다. BR/EDR 방식은 블루투스 클래식 (Bluetooth Classic)라고 호칭될 수 있다. 블루투스 클래식 방식은 베이직 레이트(Basic Rate)를 이용하는 블루투스 1.0부터 이어져온 블루투스 기술과 블루투스 2.0에서부터 지원되는 인핸스드 데이터 레이트(Enhanced Data Rate)를 이용하는 블루투스 기술을 포함한다.
- [5] 블루투스 저전력 에너지(Bluetooth Low energy, 이하 블루투스 LE라고 한다.) 기술은 블루투스 4.0부터 적용되어 적은 전력을 소모하여 수백 키로바이트(KB)의 정보를 안정적으로 제공할 수 있다. 이러한 블루투스 저전력 에너지 기술은 속성 프로토콜(Attribute Protocol)을 활용해서 디바이스(Device) 간 정보를 교환하게 된다. 이러한 블루투스 LE 방식은 헤더의 오버헤드(overhead)를 줄이고 동작을 간단하게 해서 에너지 소비를 줄일 수 있다.
- [6] 블루투스 기기들 중에는 디스플레이(Display)나 유저인터페이스(User Interface)가 없는 제품들도 있다. 다양한 종류의 블루투스 기기들과 그 중에서도 유사기술이 적용된 블루투스 기기들 간의 연결 / 관리 / 제어 / 분리 (Connection / Management / Control / Disconnection)의 복잡도가 증가하고 있다.
- [7] 또한, 블루투스는 비교적 저전력, 저비용으로 비교적 빠른 속도를 낼 수 있으나, 전송 거리가 일반적으로 최대 100m로 한정적이므로, 한정된 공간에서 사용하기 적합하다.

## 발명의 상세한 설명

### 기술적 과제

- [8] 본 발명은, 블루투스 기술을 이용하여 디바이스간 연결/페어링을 제어하기 위한 방법 및 장치를 제공함에 그 목적이 있다.
- [9] 이지 페어링 서비스(Easy pairing service)에서 기존의 컨트롤 포인트 절차에 따르면, 하나의 역할(role)에 따른 여러 동작들은 서로 밀접한 관련성이 있음에도 불구하고, 각각의 동작 또는 절차마다 개별적으로 컨트롤 포인트 절차가 수행될 것이 요구된다. 이로 인해, 관련된 동작을 지시하기 위하여 클라이언트 디바이스와 서버 디바이스간 불필요한 상호 작용(interaction)이 요구되는 문제점이 있다.
- [10] 따라서, 본 발명의 목적은 이와 같은 문제점을 해결하기 위하여 GAP 역할(role)에 기반한 컨트롤 포인트 절차의 수행 방법을 제안한다.
- [11] 또한, 본 발명의 목적은 GAP 역할에 기초하여 기존에 여러 단계를 거쳐 이루어지던 절차들을 하나의 커맨드로 구성하여 전송하는 방법을 제안한다.
- [12] 또한, 본 발명의 목적은 역할 및 이에 따른 동작들을 하나의 동작 코드로 구성하는 방법을 제안한다.
- [13] 본 명세서에서 이루고자 하는 기술적 과제들은 이상에서 언급한 기술적 과제들로 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

- [14] 본 발명의 일 양상은 블루투스 통신을 이용하여 제어 디바이스가 제 1 디바이스를 제어하는 방법에 있어서, 상기 제 1 디바이스와 블루투스 연결을 형성하는 단계; 상기 제 1 디바이스가 지원하는 제어 가능한 동작(controllable operation)과 관련된 특성 정보를 요청하는 판독 요청 메시지를 상기 제 1 디바이스로 전송하는 단계; 상기 판독 요청 메시지에 대한 응답으로 상기 특성 정보를 포함하는 판독 응답 메시지를 상기 제 1 디바이스로부터 수신하는 단계로서, 상기 특성 정보는 상기 제 1 디바이스가 지원하는 동작을 나타내는 동작 필드를 포함하고; 상기 특성 정보에 기초하여 상기 제 1 디바이스로 특정 역할(role)의 수행을 지시하기 위한 특성의 기입을 요청하는 제 1 기입 요청 메시지를 전송하는 단계로서, 상기 제 1 기입 요청 메시지는 상기 특정 역할과 관련된 제어 정보를 포함하고; 및 상기 제 1 기입 요청 메시지에 대한 응답으로 기입 응답 메시지를 상기 제 1 디바이스로부터 수신하는 단계를 포함하되, 상기 제어 정보는 상기 특정 역할을 나타내는 역할 정보 및 상기 특정 역할과 관련된 동작을 나타내는 파라미터 정보를 포함할 수 있다.
- [15] 바람직하게, 상기 동작 필드는 상기 제 1 디바이스가 지원하는 연결 타입, 역할, 모드 또는 절차 중 적어도 하나를 포함할 수 있다.

- [16] 바람직하게, 상기 파라미터 정보는 상기 제 1 디바이스가 상기 제어 디바이스로부터 요청된 동작들을 피어 디바이스(peer device)와 수행하기 위한 다수의 모드 정보 및 절차 정보를 포함할 수 있다.
- [17] 바람직하게, 상기 제 1 디바이스의 피어 디바이스(peer device)와 블루투스 LE 연결을 형성하는 단계; 및 상기 피어 디바이스의 주소가 임의 주소(random address)인 경우, 상기 피어 디바이스로부터 상기 임의 주소를 분석하기(resolve) 위한 상기 피어 디바이스의 식별자 분석 키(IRK: Identity resolving key)를 획득하는 단계를 더 포함하고, 상기 제어 정보는 상기 피어 디바이스의 식별자 분석 키를 나타내는 파라미터를 더 포함할 수 있다.
- [18] 바람직하게, 상기 제 1 디바이스의 주소가 임의 주소인 경우, 상기 제 1 디바이스로부터 상기 임의 주소를 분석하기 위한 상기 제 1 디바이스의 식별자 분석 키를 획득하는 단계; 및 상기 피어 디바이스로부터 상기 제 1 디바이스의 식별자 분석 키를 포함하는 제 2 기입 요청 메시지를 전송하는 단계를 더 포함할 수 있다.
- [19] 본 발명의 다른 일 양상은, 블루투스 통신을 이용하여 제어 디바이스에 의해 제 1 디바이스와 피어 디바이스(peer device)간 연결이 제어되는 방법에 있어서, 상기 제 1 디바이스에서 수행되는 방법은, 상기 제어 디바이스와 블루투스 연결을 형성하는 단계; 상기 제 1 디바이스가 지원하는 제어 가능한 동작(controllable operation)과 관련된 특성 정보를 요청하는 판독 요청 메시지를 상기 제어 디바이스로부터 수신하는 단계; 상기 판독 요청 메시지에 대한 응답으로 상기 특성 정보를 포함하는 판독 응답 메시지를 상기 제어 디바이스로 전송하는 단계로서, 상기 특성 정보는 상기 제 1 디바이스가 지원하는 동작을 나타내는 동작 필드를 포함하고; 상기 특성 정보에 기초하여 상기 제어 디바이스로부터 특정 역할(role)의 수행을 지시하기 위한 특성의 기입을 요청하는 기입 요청 메시지를 수신하는 단계로서, 상기 기입 요청 메시지는 상기 특정 역할과 관련된 제어 정보를 포함하고; 및 상기 기입 요청 메시지에 대한 응답으로 기입 응답 메시지를 상기 제어 디바이스로 전송하는 단계를 포함하되, 상기 제어 정보는 상기 특정 역할을 나타내는 역할 정보 및 상기 특정 역할과 관련된 동작을 나타내는 파라미터 정보를 포함할 수 있다.
- [20] 바람직하게, 상기 파라미터 정보는 상기 제 1 디바이스가 상기 제어 디바이스로부터 요청된 동작들을 상기 피어 디바이스와 수행하기 위한 다수의 모드 정보 및 절차 정보를 포함할 수 있다.
- [21] 바람직하게, 상기 제어 정보에 기초하여 피어 디바이스와 연결을 형성하는 단계를 더 포함할 수 있다.
- [22] 바람직하게, 상기 피어 디바이스의 주소가 임의 주소(random address)인 경우, 상기 제어 정보는 상기 피어 디바이스로부터 상기 임의 주소를 분석하기(resolve) 위한 상기 피어 디바이스의 식별자 분석 키(IRK: Identity resolving key)를 더 포함할 수 있다.

- [23] 바람직하게, 상기 피어 디바이스로부터 상기 임의 주소가 포함된 광고 메시지를 수신하는 단계; 상기 피어 디바이스의 식별자 분석 키를 이용하여 상기 임의 주소를 분석하는 단계; 및 상기 분석된 임의 주소 및 상기 제어 정보에 기초하여 상기 피어 디바이스와 연결을 형성하는 단계를 더 포함할 수 있다.
- [24] 본 발명의 다른 일 양상은 블루투스 통신을 이용하여 제 1 디바이스를 제어하는 제어 디바이스에 있어서, 외부와 무선 또는 유선으로 통신하기 위한 통신부; 및 상기 통신부와 기능적으로 연결되는 프로세서를 포함하되, 상기 프로세서는, 상기 제 1 디바이스와 블루투스 연결을 형성하고, 상기 제 1 디바이스가 지원하는 제어 가능한 동작(controllable operation)과 관련된 특성 정보를 요청하는 판독 요청 메시지를 상기 제 1 디바이스로 전송하고, 상기 판독 요청 메시지에 대한 응답으로 상기 특성 정보를 포함하는 판독 응답 메시지를 상기 제 1 디바이스로부터 수신하되, 상기 특성 정보는 상기 제 1 디바이스가 지원하는 동작을 나타내는 동작 필드를 포함하고, 상기 특성 정보에 기초하여 상기 제 1 디바이스로 특정 역할(role)의 수행을 지시하기 위한 특성의 기입을 요청하는 제 1 기입 요청 메시지를 전송하되, 상기 제 1 기입 요청 메시지는 상기 특정 역할과 관련된 제어 정보를 포함하고, 상기 제 1 기입 요청 메시지에 대한 응답으로 기입 응답 메시지를 상기 제 1 디바이스로부터 수신하되, 상기 제어 정보는 상기 특정 역할을 나타내는 역할 정보 및 상기 특정 역할과 관련된 동작을 나타내는 파라미터 정보를 포함할 수 있다.
- [25] 바람직하게, 상기 동작 필드는 상기 제 1 디바이스가 지원하는 연결 타입, 역할, 모드 또는 절차 중 적어도 하나를 포함할 수 있다.
- [26] 바람직하게, 상기 파라미터 정보는 상기 제 1 디바이스가 상기 제어 디바이스로부터 요청된 동작들을 피어 디바이스(peer device)와 수행하기 위한 다수의 모드 정보 및 절차 정보를 포함할 수 있다.
- [27] 바람직하게, 상기 프로세서는, 상기 제 1 디바이스의 피어 디바이스(peer device)와 블루투스 LE 연결을 형성하고, 상기 피어 디바이스의 주소가 임의 주소(random address)인 경우, 상기 피어 디바이스로부터 상기 임의 주소를 분석하기(resolve) 위한 상기 피어 디바이스의 식별자 분석 키(IRK: Identity resolving key)를 획득하고, 상기 제어 정보는 상기 피어 디바이스의 식별자 분석 키를 나타내는 파라미터를 더 포함할 수 있다.
- [28] 바람직하게, 상기 프로세서는, 상기 제 1 디바이스의 주소가 임의 주소인 경우, 상기 제 1 디바이스로부터 상기 임의 주소를 분석하기 위한 상기 제 1 디바이스의 식별자 분석 키를 획득하고, 상기 피어 디바이스로 상기 제 1 디바이스의 식별자 분석 키를 포함하는 제 2 기입 요청 메시지를 전송할 수 있다.
- 발명의 효과**
- [29] 본 발명의 일 실시예에 따른 블루투스 기술을 이용하여 디바이스를 제어하기 위한 방법에 따르면, 제어 디바이스를 통해서 다른 디바이스의 동작을 제어할 수

있는 효과가 있다.

[30] 또한, 본 발명에 따르면, 역할과 이에 관련된 동작들을 하나의 커맨드로 구성함으로써 클라이언트 디바이스와 서버 디바이스간 불필요한 상호 작용을 줄이고, 컨트롤 포인트 절차 운영의 효율성을 향상시킬 수 있다.

[31] 또한, 본 발명에 따르면 역할을 기반으로 컨트롤 포인트 절차가 수행되기 때문에, 연결 타입을 지시하기 위한 배어러 타입 서브 필드(1 byte)가 컨트롤 포인트 특성에서 삭제될 수 있다.

[32] 또한, 본 발명에 따르면 서버 디바이스(또는 GATT 서버)의 동작을 효율적으로 제어할 수 있다.

[33] 본 명세서에서 얻을 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

[34] 도 1은 본 명세서에서 제안하는 블루투스 저전력 에너지 기술을 이용하는 무선 통신 시스템의 일 예를 나타낸 개략도이다.

[35] 도 2는 본 명세서에서 제안하는 방법들을 구현할 수 있는 디바이스의 내부 블록도의 일 예를 나타낸다.

[36] 도 3는 본 명세서에서 제안하는 방법들이 적용될 수 있는 블루투스 통신 아키텍처(Architecture)의 일 예를 나타낸 도이다.

[37] 도 4는 블루투스 저전력 에너지의 GATT(Generic Attribute Profile)의 구조의 일 예를 나타낸 도이다.

[38] 도 5는 디바이스간 블루투스 LE(Low Energy)를 이용하여 커넥션을 형성하는 방법을 나타낸 흐름도이다.

[39] 도 6은 본 명세서에서 제안하는 제어 디바이스를 통해서 다른 디바이스를 제어하기 위한 방법을 간략히 나타낸 도이다.

[40] 도 7 및 도 8은 본 명세서에서 제안하는 디바이스를 제어하기 위한 서비스를 제공하기 위한 프로파일 구조의 일 예를 나타낸 도이다.

[41] 도 9는 본 발명이 적용될 수 있는 실시예로서, 컨트롤 포인트 특성의 동작을 예시하는 도면이다.

[42] 도 10은 본 발명이 적용되는 일 실시예로서, 제어 디바이스를 이용하여 디바이스간 연결을 제어하는 방법을 나타내는 흐름도이다.

[43] 도 11은 본 발명이 적용될 수 있는 일 실시예로서, 제어 디바이스를 이용하여 디바이스간 LE 연결을 제어하는 방법을 나타내는 흐름도이다.

[44] 도 12는 본 발명이 적용되는 일 실시예로서, 제어 디바이스를 이용하여 디바이스간 연결을 제어하는 방법을 나타내는 흐름도이다.

### 발명의 실시를 위한 형태

[45] 본 발명의 상술한 목적, 특징들 및 장점은 첨부된 도면과 관련된 다음의 상세한

설명을 통해 보다 분명해질 것이다. 다만, 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시 예들을 가질 수 있는 바, 이하에서는 특정 실시 예들을 도면에 예시하고 이를 상세히 설명하고자 한다. 명세서 전체에 걸쳐서 동일한 참조번호들은 원칙적으로 동일한 구성요소들을 나타낸다. 또한, 본 발명과 관련된 공지 기능 혹은 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다.

[46]

[47] 이하, 본 발명과 관련된 방법 및 장치에 대하여 도면을 참조하여 보다 상세하게 설명한다. 이하의 설명에서 사용되는 구성요소에 대한 접미사 "모듈" 및 "부"는 명세서 작성의 용이함만이 고려되어 부여되거나 혼용되는 것으로서, 그 자체로서 구별되는 의미 또는 역할을 갖는 것은 아니다.

[48]

[49] 도 1은 본 명세서에서 제안하는 블루투스 저전력 에너지 기술을 이용하는 무선 통신 시스템의 일 예를 나타낸 개략도이다.

[50] 무선 통신 시스템(100)은 적어도 하나의 서버 디바이스(Server Device, 120) 및 적어도 하나의 클라이언트 디바이스(Client Device, 110)를 포함한다.

[51] 서버 장치와 클라이언트 장치는 블루투스 저전력 에너지(Bluetooth Low Energy:BLE, 이하 편의상 'BLE'로 표현한다.) 기술을 이용하여 블루투스 통신을 수행한다.

[52] 먼저, BLE 기술은 블루투스 BR/EDR(Basic Rate/Enhanced Data Rate) 기술과 비교하여, 상대적으로 작은 duty cycle을 가지며 저 가격 생산이 가능하고, 저속의 데이터 전송률을 통해 전력 소모를 크게 줄일 수 있어 코인 셀(coin cell) 배터리를 이용할 경우 1년 이상 동작이 가능하다.

[53] 또한, BLE 기술에서는 디바이스 간 연결 절차를 간소화하였으며, 패키지 사이즈도 블루투스 BR/EDR 기술에 비해 작게 설계되어 있다.

[54] BLE 기술에서, (1) RF 채널수는 40개이며, (2) 데이터 전송 속도는 1Mbps를 지원하며, (3) 토폴로지는 스캐터넷 구조이며, (4) latency는 3ms 이며, (5) 최대 전류는 15mA이하이며, (6) 출력 전력은 10mW(10dBm)이하이며, (7) 휴대폰, 시계, 스포츠, 헬스케어, 센서, 기기제어 등의 어플리케이션에 주로 사용된다.

[55] 상기 서버 장치(120)는 다른 장치와의 관계에서 클라이언트 장치로 동작할 수 있고, 상기 클라이언트 장치는 다른 장치와의 관계에서 서버 장치로 동작할 수 있다. 즉, BLE 통신 시스템에서 어느 하나의 장치는 서버 장치 또는 클라이언트 장치로 동작하는 것이 가능하며, 필요한 경우, 서버 장치 및 클라이언트 장치로 동시에 동작하는 것도 가능하다.

[56] 상기 서버 장치(120)는 데이터 서비스 장치(Data Service Device), 슬레이브 디바이스(slave device) 디바이스, 슬레이브(slave), 서버, 컨덕터(Conductor), 호스트 디바이스(Host Device), 게이트웨이(Gateway), 센싱 장치(Sensing Device), 모니터링 장치(monitored device), 제 1 디바이스, 제 2 디바이스 등으로 표현될 수

있다.

- [57] 상기 클라이언트 디바이스(110)는 마스터 디바이스(master device), 마스터(master), 클라이언트, 멤버(Member), 센서 디바이스, 싱크 디바이스(Sink Device), 콜렉터(Collector), 제 3 디바이스, 제 4 디바이스 등으로 표현될 수 있다.
- [58] 서버 장치와 클라이언트 장치는 상기 무선 통신 시스템의 주요 구성요소에 해당하며, 상기 무선 통신 시스템은 서버 장치 및 클라이언트 장치 이외에도 다른 구성요소를 포함할 수 있다.
- [59] 상기 서버 장치는 클라이언트 장치로부터 데이터를 제공 받고, 클라이언트 장치와 직접 통신을 수행함으로써, 클라이언트 장치로부터 데이터 요청을 수신하는 경우, 응답을 통해 클라이언트 장치로 데이터를 제공하는 장치를 말한다.
- [60] 또한, 상기 서버 장치는 클라이언트 장치로 데이터 정보를 제공하기 위해 클라이언트 장치에게 알림(Notification) 메시지, 지시(Indication) 메시지를 보낸다. 또한, 상기 서버 장치는 상기 클라이언트 장치로 지시 메시지를 전송하는 경우, 상기 클라이언트로부터 상기 지시 메시지에 대응하는 확인(Confirm) 메시지를 수신한다.
- [61] 또한, 상기 서버 장치는 알림, 지시, 확인 메시지들을 클라이언트 디바이스와 송수신하는 과정에서 출력부(Display Unit)을 통해서 사용자에게 데이터 정보를 제공하거나 입력부(User Input Interface)를 통해 사용자로부터 입력되는 요청을 수신할 수 있다.
- [62] 또한, 상기 서버 장치는 상기 클라이언트 장치와 메시지를 송수신하는 과정에서 메모리(memory unit)로부터 데이터를 읽어 오거나 새로운 데이터를 해당 메모리에 쓸 수 있다.
- [63] 또한, 하나의 서버 장치는 다수의 클라이언트 장치들과 연결될 수 있으며, 본딩(Bonding) 정보를 활용하여 클라이언트 장치들과 쉽게 재 연결(또는 접속)이 가능하다.
- [64] 상기 클라이언트 장치 (120)는 서버 장치에게 데이터 정보 및 데이터 전송을 요청하는 장치를 말한다.
- [65] 클라이언트 장치는 상기 서버 장치로부터 알림 메시지, 지시 메시지 등을 통해 데이터를 수신하고, 지시 메시지를 상기 서버 디바이스로부터 수신하는 경우, 상기 지시 메시지에 대한 응답으로 확인 메시지를 보낸다.
- [66] 상기 클라이언트 장치도 마찬가지로 상기 서버 장치와 메시지들을 송수신하는 과정에서 출력부를 통해 사용자에게 정보를 제공하거나 입력부를 통해 사용자로부터의 입력을 수신할 수 있다.
- [67] 또한, 상기 클라이언트 장치는 상기 서버 장치와 메시지를 송수신하는 과정에서 메모리로부터 데이터를 읽어 오거나 새로운 데이터를 해당 메모리에 쓸 수 있다.
- [68] 상기 서버 장치 및 클라이언트 장치의 출력부, 입력부 및 메모리 등과 같은

- 하드웨어 구성요소에 대해서는 도 2에서 구체적으로 살펴보기로 한다.
- [69] 또한, 상기 무선 통신 시스템은 블루투스 기술을 통해 개인 영역 네트워킹(Personal Area Networking: PAN)을 구성할 수 있다. 일 예로, 상기 무선 통신 시스템에서는 디바이스 간 개인적인 피코넷(private piconet)을 확립함으로써 파일, 서류 등을 신속하고 안전하게 교환할 수 있다.
- [70] 도 2는 본 명세서에서 제안하는 방법들을 구현할 수 있는 디바이스의 내부 블록도의 일 예를 나타낸다.
- [71] 도 2에 도시된 바와 같이, 서버 디바이스는 출력부(Display Unit, 111), 입력부(User Input Interface, 112), 전력 공급부(Power Supply Unit, 113), 프로세서(Processor, 114), 메모리(Memory Unit, 115), 블루투스 인터페이스(Bluetooth Interface, 116), 다른 통신 인터페이스(Other Interface, 117) 및 통신부(또는 송수신부, 118)를 포함한다.
- [72] 상기 출력부(111), 입력부(112), 전력 공급부(113), 프로세서(114), 메모리(115), 블루투스 인터페이스(116), 다른 통신 인터페이스(117) 및 통신부(118)는 본 명세서에서 제안하는 방법을 수행하기 위해 기능적으로 연결되어 있다.
- [73] 또한, 클라이언트 디바이스는 출력부(Display Unit, 121), 입력부(User Input Interface, 122), 전력 공급부(Power Supply Unit, 123), 프로세서(Processor, 124), 메모리(Memory Unit, 125), 블루투스 인터페이스(Bluetooth Interface, 126) 및 통신부(또는 송수신부, 127)를 포함한다.
- [74] 상기 출력부(121), 입력부(122), 전력 공급부(123), 프로세서(124), 메모리(125), 블루투스 인터페이스(126), 및 통신부(127)는 본 명세서에서 제안하는 방법을 수행하기 위해 기능적으로 연결되어 있다.
- [75] 상기 블루투스 인터페이스(116, 126)는 블루투스 기술을 이용하여 디바이스들 간의 요청/응답, 명령, 알림, 지시/확인 메시지 등 또는 데이터 전송이 가능한 유닛(또는 모듈)을 말한다.
- [76] 상기 메모리(115, 125)는 다양한 종류의 디바이스에 구현되는 유닛으로서, 다양한 종류의 데이터가 저장되는 유닛을 말한다.
- [77] 상기 프로세서(114, 124)는 서버 디바이스 또는 클라이언트 디바이스의 전반적인 동작을 제어하는 모듈을 말하며, 블루투스 인터페이스 및 다른 통신 인터페이스로 메시지를 전송 요청 및 수신받은 메시지를 처리하도록 제어한다.
- [78] 상기 프로세서(114, 124)는 제어부, 제어 유닛(Control Unit), 컨트롤러 등으로 표현될 수 있다.
- [79] 상기 프로세서(114, 124)는 ASIC(application-specific integrated circuit), 다른 칩셋, 논리 회로 및/또는 데이터 처리 장치를 포함할 수 있다.
- [80] 상기 프로세서(114, 124)는 서버 디바이스로부터 광고(Advertising) 메시지를 수신하도록 상기 통신부를 제어하며, 상기 서버 디바이스로 스캔 요청(Scan Request) 메시지를 전송하고, 상기 서버 디바이스로부터 상기 스캔 요청에 대한 응답으로 스캔 응답(Scan Response) 메시지를 수신하도록 상기 통신부를

- 제어하며, 상기 서버 디바이스와 블루투스 연결 설정을 위해 상기 서버 디바이스로 연결 요청(Connect Request) 메시지를 전송하도록 상기 통신부를 제어한다.
- [81] 또한, 상기 프로세서(114,124)는 상기 연결 절차를 통해 블루투스 LE 커넥션(Connection)이 형성된 이후, 상기 서버 디바이스로부터 속성 프로토콜을 이용하여 데이터를 읽어오거나(Read), 기록(Write)할 수 있도록 상기 통신부를 제어한다.
- [82] 상기 메모리(115,125)는 ROM(read-only memory), RAM(random access memory), 플래쉬 메모리, 메모리 카드, 저장 매체 및/또는 다른 저장 장치를 포함할 수 있다.
- [83] 상기 통신부(118,127)는 무선 신호를 처리하기 위한 베이스밴드 회로를 포함할 수 있다. 실시 예가 소프트웨어로 구현될 때, 상술한 기법은 상술한 기능을 수행하는 모듈(과정, 기능 등)로 구현될 수 있다. 모듈은 메모리에 저장되고, 프로세서에 의해 실행될 수 있다.
- [84] 상기 메모리(115,125)는 프로세서(114,124) 내부 또는 외부에 있을 수 있고, 잘 알려진 다양한 수단으로 프로세서(114,124)와 연결될 수 있다.
- [85] 상기 출력부(111,121)는 디바이스의 상태 정보 및 메시지 교환 정보 등을 화면을 통해서 사용자에게 제공하기 위한 모듈을 말한다.
- [86] 상기 전력 공급부(전원 공급부, 113, 123)는 제어부의 제어 하에 외부의 전원, 내부의 전원을 인가 받아 각 구성요소들의 동작에 필요한 전원을 공급해주는 모듈을 말한다.
- [87] 앞에서 살핀 것처럼, BLE 기술에서는 작은 duty cycle을 가지며, 저속의 데이터 전송률을 통해 전력 소모를 크게 줄일 수 있다.
- [88] 상기 입력부(112,122)는 화면 버튼과 같이 사용자의 입력을 제어부에게 제공하여 디바이스의 동작을 사용자가 제어할 수 있게 하는 모듈을 말한다.
- [89] 도 3은 본 명세서에서 제안하는 방법들이 적용될 수 있는 블루투스 통신 아키텍처(Architecture)의 일 예를 나타낸 도이다.
- [90] 상기 도 3을 참고하면, 상기 도 3의 (a)는 블루투스 BR(Basic Rate)/EDR(Enhanced Data Rate)의 프로토콜 스택의 일 예를 나타내며, (b)는 블루투스 LE(Low Energy)의 프로토콜 스택의 일 예를 나타낸다.
- [91] 구체적으로, 상기 도 3의 (a)에 도시된 바와 같이, 블루투스 BR/EDR 프로토콜 스택은 호스트 컨트롤러 인터페이스(Host Controller Interface, HCI, 18)를 기준으로 상부의 컨트롤러 스택(Controller stack, 10)과 하부의 호스트 스택(Host Stack, 20)을 포함할 수 있다.
- [92] 상기 호스트 스택(또는 호스트 모듈)(20)은 2.4GHz의 블루투스 신호를 받는 무선 송수신 모듈과 블루투스 패킷을 전송하거나 수신하기 위한 하드웨어를 말하며, 상기 컨트롤러 스택(10)인 블루투스 모듈과 연결되어 블루투스 모듈을 제어하고 동작을 수행한다.

- [93] 상기 컨트롤러 스택(10)은 PHY 계층(12), 링크 컨트롤러 계층(Link Controller, 14), 링크 매니저 계층(Link Manager, 16)을 포함할 수 있다.
- [94] 상기 PHY 계층(12)은 2.4GHz 무선 신호를 송수신하는 계층으로, GFSK (Gaussian Frequency Shift Keying) modulation을 사용하는 경우 79 개의 RF 채널을 hopping 하여 데이터를 전송할 수 있다.
- [95] 상기 링크 컨트롤러 계층(14)은 Digital Signal을 전송하는 역할을 담당하며, 초당 1400번 hopping 하는 채널 시퀀스를 선택하며, 각 채널 별 625us 길이의 time slot을 전송한다.
- [96] 상기 링크 매니저 계층(16)은 LMP(Link Manager Protocol)을 활용하여 Bluetooth Connection의 전반적인 동작(link setup, control, security)을 제어한다.
- [97] 상기 링크 매니저 계층(16)은 아래와 같은 기능을 수행할 수 있다.
- [98] - ACL/SCO logical transport, logical link setup 및 control을 한다.
- [99] - Detach: connection을 중단하고, 중단 이유를 상대 디바이스에게 알려준다.
- [100] - Power control 및 Role switch를 한다.
- [101] - Security(authentication, pairing, encryption) 기능을 수행한다.
- [102] 상기 호스트 컨트롤러 인터페이스 계층(18)은 Host 모듈과 Controller 모듈 사이의 인터페이스 제공하여 Host 가 command와 Data를 Controller에게 제공하게 하며, Controller가 event와 Data를 Host에게 제공할 수 있도록 해준다.
- [103] 상기 호스트 스택(또는 호스트 모듈, 20)은 논리적 링크 제어 및 적응 프로토콜(L2CAP, 21), 속성 프로토콜(Protocol, 22), 일반 속성 프로파일(Generic Attribute Profile, GATT, 23), 일반 접근 프로파일(Generic Access Profile, GAP, 24), BR/EDR 프로파일(25)을 포함한다.
- [104] 상기 논리적 링크 제어 및 적응 프로토콜(L2CAP, 21)은 특정 프로토콜 또는 프로파일에게 데이터를 전송하기 위한 하나의 양방향 채널을 제공할 수 있다.
- [105] 상기 L2CAP(21)은 블루투스 상위에서 제공하는 다양한 프로토콜, 프로파일 등을 멀티플렉싱(multiplexing)할 수 있다.
- [106] 블루투스 BR/EDR의 L2CAP에서는 dynamic 채널 사용하며, protocol service multiplexer, retransmission, streaming mode를 지원하고, Segmentation 및 reassembly, per-channel flow control, error control을 제공한다.
- [107] 상기 일반 속성 프로파일(GATT, 23)은 서비스들의 구성 시에 상기 속성 프로토콜(22)이 어떻게 이용되는지를 설명하는 프로토콜로서 동작 가능할 수 있다. 예를 들어, 상기 일반 속성 프로파일(23)은 ATT 속성들이 어떻게 서비스들로 함께 그룹화되는지를 규정하도록 동작 가능할 수 있고, 서비스들과 연계된 특징들을 설명하도록 동작 가능할 수 있다.
- [108] 따라서, 상기 일반 속성 프로파일(23) 및 상기 속성 프로토콜(ATT, 22)은 디바이스의 상태와 서비스들을 설명하고, 특징들이 서로 어떻게 관련되며 이들이 어떻게 이용되는지를 설명하기 위하여, 특징들을 사용할 수 있다.
- [109] 상기 속성 프로토콜(22) 및 상기 BR/EDR 프로파일(25)은 블루투스 BR/EDR를

- 이용하는 서비스 (profile)의 정의 및 이들 데이터를 주고 받기 위한 application 프로토콜을 정의하며, 상기 일반 접근 프로파일(Generic Access Profile, GAP, 24)은 디바이스 발견, 연결, 및 보안 수준을 정의한다.
- [110] 상기 도 4의 (b)에 도시된 바와 같이, 블루투스 LE 프로토콜 스택은 타이밍이 중요한 무선장치 인터페이스를 처리하도록 동작 가능한 컨트롤러 스택(Controller stack, 30)과 고레벨(high level) 데이터를 처리하도록 동작 가능한 호스트 스택(Host stack, 40)을 포함한다.
- [111] 먼저, 컨트롤러 스택(30)은 블루투스 무선장치를 포함할 수 있는 통신 모듈, 예를 들어, 마이크로프로세서와 같은 프로세싱 디바이스를 포함할 수 있는 프로세서 모듈을 이용하여 구현될 수 있다.
- [112] 호스트 스택은 프로세서 모듈 상에서 작동되는 OS의 일부로서, 또는 OS 위의 패키지(package)의 인스턴스 생성(instantiation)으로서 구현될 수 있다.
- [113] 일부 사례들에서, 컨트롤러 스택 및 호스트 스택은 프로세서 모듈 내의 동일한 프로세싱 디바이스 상에서 작동 또는 실행될 수 있다.
- [114] 상기 컨트롤러 스택(30)은 물리 계층(Physical Layer, PHY, 32), 링크 레이어(Link Layer, 34) 및 호스트 컨트롤러 인터페이스(Host Controller Interface, 36)를 포함한다.
- [115] 상기 물리 계층(PHY, 무선 송수신 모듈, 32)은 2.4 GHz 무선 신호를 송수신하는 계층으로 GFSK (Gaussian Frequency Shift Keying) modulation과 40 개의 RF 채널로 구성된 frequency hopping 기법을 사용한다.
- [116] 블루투스 패킷을 전송하거나 수신하는 역할을 하는 상기 링크 레이어(34)는 3개의 Advertising 채널을 이용하여 Advertising, Scanning 기능을 수행한 후에 디바이스 간 연결을 생성하고, 37개 Data 채널을 통해 최대 257bytes의 데이터 패킷을 주고 받는 기능을 제공한다.
- [117] 상기 호스트 스택은 논리적 링크 제어 및 적응 프로토콜(L2CAP, 41), 보안 매니저(Security Manager, SM, 42), 속성 프로토콜(Attribute Protocol, ATT, 43), 일반 속성 프로파일(Generic Attribute Profile, GATT, 44), 일반 접근 프로파일(Generic Access Profile, 45), LE 프로파일(46)을 포함할 수 있다. 다만, 상기 호스트 스택(40)은 이것으로 한정되지는 않고 다양한 프로토콜들 및 프로파일들을 포함할 수 있다.
- [118] 호스트 스택은 L2CAP을 사용하여 블루투스 상위에서 제공하는 다양한 프로토콜, 프로파일 등을 다중화(multiplexing)한다.
- [119] 먼저, L2CAP(Logical Link Control and Adaptation Protocol, 41)은 특정 프로토콜 또는 프로파일에게 데이터를 전송하기 위한 하나의 양방향 채널을 제공할 수 있다.
- [120] 상기 L2CAP(41)은 상위 계층 프로토콜들 사이에서 데이터를 다중화(multiplex)하고, 패키지(package)들을 분할(segment) 및 재조립(reassemble)하고, 멀티캐스트 데이터 송신을 관리하도록 동작 가능할 수

있다.

- [121] 블루투스 LE에서는 3개의 고정 채널(signaling CH을 위해 1개, Security Manager를 위해 1개, Attribute protocol을 위해 1개)을 기본적으로 사용한다. 그리고, 필요에 따라 동적 채널을 사용할 수도 있다.
- [122] 반면, BR/EDR(Basic Rate/Enhanced Data Rate)에서는 동적인 채널을 기본적으로 사용하며, protocol service multiplexer, retransmission, streaming mode 등을 지원한다.
- [123] SM(Security Manager, 42)은 디바이스를 인증하며, 키 분배(key distribution)를 제공하기 위한 프로토콜이다.
- [124] ATT(Attribute Protocol, 43)는 서버-클라이언트(Server-Client) 구조로 상대 디바이스의 데이터를 접근하기 위한 규칙을 정의한다. ATT에는 아래의 6가지의 메시지 유형(Request, Response, Command, Notification, Indication, Confirmation)이 있다.
- [125] ① Request 및 Response 메시지: Request 메시지는 클라이언트 디바이스에서 서버 디바이스로 특정 정보 요청 및 전달하기 위한 메시지이며, Response 메시지는 Request 메시지에 대한 응답 메시지로서, 서버 디바이스에서 클라이언트 디바이스로 전송하는 용도로 사용할 수 있는 메시지를 말한다.
- [126] ② Command 메시지: 클라이언트 디바이스에서 서버 디바이스로 주로 특정 동작의 명령을 지시하기 위해 전송하는 메시지로, 서버 디바이스는 Command 메시지에 대한 응답을 클라이언트 디바이스로 전송하지 않는다.
- [127] ③ Notification 메시지: 서버 디바이스에서 클라이언트 디바이스로 이벤트 등과 같은 통지를 위해 전송하는 메시지로, 클라이언트 디바이스는 Notification 메시지에 대한 확인 메시지를 서버 디바이스로 전송하지 않는다.
- [128] ④ Indication 및 Confirm 메시지: 서버 디바이스에서 클라이언트 디바이스로 이벤트 등과 같은 통지를 위해 전송하는 메시지로, Notification 메시지와는 달리, 클라이언트 디바이스는 Indication 메시지에 대한 확인 메시지(Confirm message)를 서버 디바이스로 전송한다.
- [129] 본 발명은 상기 속성 프로토콜(ATT, 43)을 사용하는 GATT 프로파일에서 긴 데이터 요청 시 데이터 길이에 대한 값을 전송하여 클라이언트가 데이터 길이를 명확히 알 수 있게 하며, UUID를 이용하여 서버로부터 특성(Characteristic) 값을 전송 받을 수 있다.
- [130] 상기 일반 접근 프로파일(45)은 블루투스 LE 기술을 위해 새롭게 구현된 계층으로, 블루투스 LE 디바이스들 간의 통신을 위한 역할 선택, 멀티 프로파일 작동이 어떻게 일어나는지를 제어하는데 사용된다.
- [131] 또한, 상기 일반 접근 프로파일(45)은 디바이스 발견, 연결 생성 및 보안 절차 부분에 주로 사용되며, 사용자에게 정보를 제공하는 방안을 정의하며, 하기와 같은 attribute의 type을 정의한다.
- [132] ① Service: 데이터와 관련된 behavior의 조합으로 디바이스의 기본적인 동작을

## 정의

- [133] ② Include: 서비스 사이의 관계를 정의
- [134] ③ Characteristics: 서비스에서 사용되는 data 값
- [135] ④ Behavior: UUID(Universal Unique Identifier, value type)로 정의된 컴퓨터가 읽을 수 있는 포맷
- [136] 상기 LE 프로파일(46)은 GATT에 의존성을 가지는 profile 들로 주로 블루투스 LE 디바이스에 적용된다. LE 프로파일(46)은 예를 들면, Battery, Time, FindMe, Proximity, Time 등이 있을 수 있으며, GATT-based Profiles의 구체적인 내용은 하기와 같다.
- [137] ① Battery: 배터리 정보 교환 방법
- [138] ② Time: 시간 정보 교환 방법
- [139] ③ FindMe: 거리에 따른 알람 서비스 제공
- [140] ④ Proximity: 배터리 정보 교환 방법
- [141] ⑤ Time: 시간 정보 교환 방법
- [142] 상기 일반 속성 프로파일(GATT, 44)은 서비스들의 구성 시에 상기 속성 프로토콜(43)이 어떻게 이용되는지를 설명하는 프로토콜로서 동작 가능할 수 있다. 예를 들어, 상기 일반 속성 프로파일(44)은 ATT 속성들이 어떻게 서비스들로 함께 그룹화되는지를 규정하도록 동작 가능할 수 있고, 서비스들과 연계된 특징들을 설명하도록 동작 가능할 수 있다.
- [143] 따라서, 상기 일반 속성 프로파일(44) 및 상기 속성 프로토콜(ATT, 43)은 디바이스의 상태와 서비스들을 설명하고, 특징들이 서로 어떻게 관련되며 이들이 어떻게 이용되는지를 설명하기 위하여, 특징들을 사용할 수 있다.
- [144]
- [145] 이하에서, 블루투스 저전력 에너지(Bluetooth Low Energy:BLE) 기술의 절차(Procedure)들에 대해 간략히 살펴보기로 한다.
- [146] BLE 절차는 디바이스 필터링 절차(Device Filtering Procedure), 광고 절차(Advertising Procedure), 스캐닝 절차(Scanning Procedure), 디스커버링 절차(Discovering Procedure), 연결 절차(Connecting Procedure) 등으로 구분될 수 있다.
- [147] 디바이스 필터링 절차(Device Filtering Procedure)
- [148] 디바이스 필터링 절차는 컨트롤러 스택에서 요청, 지시, 알림 등에 대한 응답을 수행하는 디바이스들의 수를 줄이기 위한 방법이다.
- [149] 모든 디바이스에서 요청 수신 시, 이에 대해 응답하는 것이 불필요하기 때문에, 컨트롤러 스택은 요청을 전송하는 개수를 줄여서, BLE 컨트롤러 스택에서 전력 소비가 줄 수 있도록 제어할 수 있다.
- [150] 광고 디바이스 또는 스캐닝 디바이스는 광고 패킷, 스캔 요청 또는 연결 요청을 수신하는 디바이스를 제한하기 위해 상기 디바이스 필터링 절차를 수행할 수 있다.

- [151] 여기서, 광고 디바이스는 광고 이벤트를 전송하는 즉, 광고를 수행하는 디바이스를 말하며, 광고자(Advertiser)라고도 표현된다.
- [152] 스캐닝 디바이스는 스캐닝을 수행하는 디바이스, 스캔 요청을 전송하는 디바이스를 말한다.
- [153] BLE에서는, 스캐닝 디바이스가 일부 광고 패킷들을 광고 디바이스로부터 수신하는 경우, 상기 스캐닝 디바이스는 상기 광고 디바이스로 스캔 요청을 전송해야 한다.
- [154] 하지만, 디바이스 필터링 절차가 사용되어 스캔 요청 전송이 불필요한 경우, 상기 스캐닝 디바이스는 광고 디바이스로부터 전송되는 광고 패킷들을 무시할 수 있다.
- [155] 연결 요청 과정에서도 디바이스 필터링 절차가 사용될 수 있다. 만약, 연결 요청 과정에서 디바이스 필터링이 사용되는 경우, 연결 요청을 무시함으로써 상기 연결 요청에 대한 응답을 전송할 필요가 없게 된다.
- [156] **광고 절차(Advertising Procedure)**
- [157] 광고 디바이스는 영역 내 디바이스들로 비방향성의 브로드캐스트를 수행하기 위해 광고 절차를 수행한다.
- [158] 여기서, 비방향성의 브로드캐스트는 특정 방향으로의 브로드캐스트가 아닌 전(모든) 방향으로의 브로드캐스트를 말한다.
- [159] 이와 달리, 지향성 브로드 캐스트는 특정 방향으로의 브로드캐스트를 말한다. 비방향성 브로드캐스트는 광고 디바이스와 리스닝(또는 청취) 상태에 있는 디바이스(이하, 리스닝 디바이스라 한다.) 간에 연결 절차 없이 발생한다.
- [160] 광고 절차는 근처의 개시 디바이스와 블루투스 연결을 확립하기 위해 사용된다.
- [161] 또는, 광고 절차는 광고 채널에서 리스닝을 수행하고 있는 스캐닝 디바이스들에게 사용자 데이터의 주기적인 브로드캐스트를 제공하기 위해 사용될 수 있다.
- [162] 광고 절차에서 모든 광고(또는 광고 이벤트)는 광고 물리 채널을 통해 브로드캐스트된다.
- [163] 광고 디바이스들은 광고 디바이스로부터 추가적인 사용자 데이터를 얻기 위해 리스닝을 수행하고 있는 리스닝 디바이스들로부터 스캔 요청을 수신할 수 있다. 광고 디바이스는 스캔 요청을 수신한 광고 물리 채널과 동일한 광고 물리 채널을 통해, 스캔 요청을 전송한 디바이스로 스캔 요청에 대한 응답을 전송한다.
- [164] 광고 패킷들의 일 부분으로서 보내지는 브로드캐스트 사용자 데이터는 동적인 데이터인 반면에, 스캔 응답 데이터는 일반적으로 정적인 데이터이다.
- [165] 광고 디바이스는 광고(브로드캐스트) 물리 채널 상에서 개시 디바이스로부터 연결 요청을 수신할 수 있다. 만약, 광고 디바이스가 연결 가능한 광고 이벤트를 사용하였고, 개시 디바이스가 디바이스 필터링 절차에 의해 필터링 되지 않았다면, 광고 디바이스는 광고를 멈추고 연결 모드(connected mode)로

진입한다. 광고 디바이스는 연결 모드 이후에 다시 광고를 시작할 수 있다.

[166] **스캐닝 절차(Scanning Procedure)**

[167] 스캐닝을 수행하는 디바이스 즉, 스캐닝 디바이스는 광고 물리 채널을 사용하는 광고 디바이스들로부터 사용자 데이터의 비지향성 브로드캐스트를 청취하기 위해 스캐닝 절차를 수행한다.

[168] 스캐닝 디바이스는 광고 디바이스로부터 추가적인 데이터를 요청 하기 위해, 광고 물리 채널을 통해 스캔 요청을 광고 디바이스로 전송한다. 광고 디바이스는 광고 물리 채널을 통해 스캐닝 디바이스에서 요청한 추가적인 데이터를 포함하여 상기 스캔 요청에 대한 응답인 스캔 응답을 전송한다.

[169] 상기 스캐닝 절차는 BLE 피코넷에서 다른 BLE 디바이스와 연결되는 동안 사용될 수 있다.

[170] 만약, 스캐닝 디바이스가 브로드캐스트되는 광고 이벤트를 수신하고, 연결 요청을 개시할 수 있는 개시자 모드(initiator mode)에 있는 경우, 스캐닝 디바이스는 광고 물리 채널을 통해 광고 디바이스로 연결 요청을 전송함으로써 광고 디바이스와 블루투스 연결을 시작할 수 있다.

[171] 스캐닝 디바이스가 광고 디바이스로 연결 요청을 전송하는 경우, 스캐닝 디바이스는 추가적인 브로드캐스트를 위한 개시자 모드 스캐닝을 중지하고, 연결 모드로 진입한다.

[172] **디스커버링 절차(Discovering Procedure)**

[173] 블루투스 통신이 가능한 디바이스(이하, ‘블루투스 디바이스’라 한다.)들은 근처에 존재하는 디바이스들을 발견하기 위해 또는 주어진 영역 내에서 다른 디바이스들에 의해 발견되기 위해 광고 절차와 스캐닝 절차를 수행한다.

[174] 디스커버링 절차는 비대칭적으로 수행된다. 주위의 다른 디바이스를 찾으려고 하는 블루투스 디바이스를 디스커버링 디바이스(discovering device)라 하며, 스캔 가능한 광고 이벤트를 광고하는 디바이스들을 찾기 위해 리스닝한다. 다른 디바이스로부터 발견되어 이용 가능한 블루투스 디바이스를 디스커버러블 디바이스(discoverable device)라 하며, 적극적으로 광고 (브로드캐스트) 물리 채널을 통해 다른 디바이스가 스캔 가능하도록 광고 이벤트를 브로드캐스트한다.

[175] 디스커버링 디바이스와 디스커버러블 디바이스 모두 피코넷에서 다른 블루투스 디바이스들과 이미 연결되어 있을 수 있다.

[176] **연결 절차(Connecting Procedure)**

[177] 연결 절차는 비대칭적이며, 연결 절차는 특정 블루투스 디바이스가 광고 절차를 수행하는 동안 다른 블루투스 디바이스는 스캐닝 절차를 수행할 것을 요구한다.

[178] 즉, 광고 절차가 목적이 될 수 있으며, 그 결과 단지 하나의 디바이스만 광고에 응답할 것이다. 광고 디바이스로부터 접속 가능한 광고 이벤트를 수신한 이후, 광고 (브로드캐스트) 물리 채널을 통해 광고 디바이스로 연결 요청을

전송함으로써 연결을 개시할 수 있다.

- [179] 다음으로, BLE 기술에서의 동작 상태 즉, 광고 상태(Advertising State), 스캐닝 상태(Scanning State), 개시 상태(Initiating State), 연결 상태(connection state)에 대해 간략히 살펴보기로 한다.
- [180] **광고 상태(Advertising State)**
- [181] 링크 계층(LL)은 호스트 (스택)의 지시에 의해, 광고 상태로 들어간다. 링크 계층이 광고 상태에 있을 경우, 링크 계층은 광고 이벤트들에서 광고 PDU(Packet Data Unit)들을 전송한다.
- [182] 각각의 광고 이벤트는 적어도 하나의 광고 PDU들로 구성되며, 광고 PDU들은 사용되는 광고 채널 인덱스들을 통해 전송된다. 광고 이벤트는 광고 PDU가 사용되는 광고 채널 인덱스들을 통해 각각 전송되었을 경우, 종료되거나 광고 디바이스가 다른 기능 수행을 위해 공간을 확보할 필요가 있을 경우 좀 더 일찍 광고 이벤트를 종료할 수 있다.
- [183] **스캐닝 상태(Scanning State)**
- [184] 링크 계층은 호스트 (스택)의 지시에 의해 스캐닝 상태로 들어간다. 스캐닝 상태에서, 링크 계층은 광고 채널 인덱스들을 리스닝한다.
- [185] 스캐닝 상태에는 수동적 스캐닝(passive scanning), 적극적 스캐닝(active scanning)의 두 타입이 있으며, 각 스캐닝 타입은 호스트에 의해 결정된다.
- [186] 스캐닝을 수행하기 위한 별도의 시간이나 광고 채널 인덱스가 정의되지는 않는다.
- [187] 스캐닝 상태 동안, 링크 계층은 스캔윈도우(scanWindow) 구간(duration) 동안 광고 채널 인덱스를 리스닝한다. 스캔인터벌(scanInterval)은 두 개의 연속적인 스캔 윈도우의 시작점 사이의 간격(인터벌)으로서 정의된다.
- [188] 링크 계층은 스케줄링의 충돌이 없는 경우, 호스트에 의해 지시되는 바와 같이 스캔윈도우의 모든 스캔인터벌 완성을 위해 리스닝해야한다. 각 스캔윈도우에서, 링크 계층은 다른 광고 채널 인덱스를 스캔해야한다. 링크 계층은 사용 가능한 모든 광고 채널 인덱스들을 사용한다.
- [189] 수동적인 스캐닝일 때, 링크 계층은 단지 패킷들만 수신하고, 어떤 패킷들도 전송하지 못한다.
- [190] 능동적인 스캐닝일 때, 링크 계층은 광고 디바이스로 광고 PDU들과 광고 디바이스 관련 추가적인 정보를 요청할 수 있는 광고 PDU 타입에 의존하기 위해 리스닝을 수행한다.
- [191] **개시 상태(Initiating State)**
- [192] 링크 계층은 호스트 (스택)의 지시에 의해 개시 상태로 들어간다.
- [193] 링크 계층이 개시 상태에 있을 때, 링크 계층은 광고 채널 인덱스들에 대한 리스닝을 수행한다.
- [194] 개시 상태 동안, 링크 계층은 스캔윈도우 구간 동안 광고 채널 인덱스를 리스닝한다.

[195] **연결 상태(connection state)**

[196] 링크 계층은 연결 요청을 수행하는 디바이스 즉, 개시 디바이스가 CONNECT\_REQ PDU를 광고 디바이스로 전송할 때 또는 광고 디바이스가 개시 디바이스로부터 CONNECT\_REQ PDU를 수신할 때 연결 상태로 들어간다.

[197] 연결 상태로 들어간 이후, 연결이 생성되는 것으로 고려된다. 다만, 연결이 연결 상태로 들어간 시점에서 확립되도록 고려될 필요는 없다. 새로 생성된 연결과 기 확립된 연결 간의 유일한 차이는 링크 계층 연결 감독 타임아웃(supervision timeout) 값뿐이다.

[198] 두 디바이스가 연결되어 있을 때, 두 디바이스들은 다른 역할로 활동한다.

[199] 마스터 역할을 수행하는 링크 계층은 마스터로 불리며, 슬레이브 역할을 수행하는 링크 계층은 슬레이브로 불린다. 마스터는 연결 이벤트의 타이밍을 조절하고, 연결 이벤트는 마스터와 슬레이브 간 동기화되는 시점을 말한다.

[200] 이하에서, 블루투스 인터페이스에서 정의되는 패킷에 대해 간략히 살펴보기로 한다. BLE 디바이스들은 하기에서 정의되는 패킷들을 사용한다.

[201] **패킷 포맷(Packet Format)**

[202] 링크 계층(Link Layer)은 광고 채널 패킷과 데이터 채널 패킷 둘 다를 위해 사용되는 단지 하나의 패킷 포맷만을 가진다.

[203] 각 패킷은 프리앰블(Preamble), 접속 주소(Access Address), PDU 및 CRC 4개의 필드로 구성된다.

[204] 하나의 패킷이 광고 물리 채널에서 송신될 때, PDU는 광고 채널 PDU가 될 것이며, 하나의 패킷이 데이터 물리 채널에서 전송될 때, PDU는 데이터 채널 PDU가 될 것이다.

[205] **광고 채널 PDU(Advertising Channel PDU)**

[206] 광고 채널 PDU(Packet Data Unit)는 16비트 헤더와 다양한 크기의 페이로드를 가진다.

[207] 헤더에 포함되는 광고 채널 PDU의 PDU 타입 필드는 하기 표 1에서 정의된 바와 같은 PDU 타입을 나타낸다.

[208] [표1]

PDU Type	Packet Name
0000	ADV_IND
0001	ADV_DIRECT_IND
0010	ADV_NONCONN_IND
0011	SCAN_REQ
0100	SCAN_RSP
0101	CONNECT_REQ
0110	ADV_SCAN_IND
0111-1111	Reserved

[209] 광고 PDU(Advertising PDU)

[210] 아래 광고 채널 PDU 타입들은 광고 PDU로 불리고 구체적인 이벤트에서 사용된다.

[211] ADV\_IND: 연결 가능한 비방향성 광고 이벤트

[212] ADV\_DIRECT\_IND: 연결 가능한 방향성 광고 이벤트

[213] ADV\_NONCONN\_IND: 연결 가능하지 않은 비방향성 광고 이벤트

[214] ADV\_SCAN\_IND: 스캔 가능한 비방향성 광고 이벤트

[215] 상기 PDU들은 광고 상태에서 링크 계층(Link Layer)에서 전송되고, 스캐닝 상태 또는 개시 상태(Initiating State)에서 링크 계층에 의해 수신된다.

[216] 스캐닝 PDU(Scanning PDU)

[217] 아래 광고 채널 PDU 타입은 스캐닝 PDU로 불리며, 하기에서 설명되는 상태에서 사용된다.

[218] SCAN\_REQ: 스캐닝 상태에서 링크 계층에 의해 전송되며, 광고 상태에서 링크 계층에 의해 수신된다.

[219] SCAN\_RSP: 광고 상태에서 링크 계층에 의해 전송되며, 스캐닝 상태에서 링크 계층에 의해 수신된다.

[220] 개시 PDU(Initiating PDU)

[221] 아래 광고 채널 PDU 타입은 개시 PDU로 불린다.

[222] CONNECT\_REQ: 개시 상태에서 링크 계층에 의해 전송되며, 광고 상태에서 링크 계층에 의해 수신된다.

[223] 데이터 채널 PDU(Data Channel PDU)

- [224] 데이터 채널 PDU는 16 비트 헤더, 다양한 크기의 페이로드를 가지고, 메시지 무결점 체크(Message Integrity Check:MIC) 필드를 포함할 수 있다.
- [225] 앞에서 살펴본, BLE 기술에서의 절차, 상태, 패킷 포맷 등은 본 명세서에서 제안하는 방법들을 수행하기 위해 적용될 수 있다.
- [226] 도 4는 블루투스 저전력 에너지의 GATT Profile의 구조의 일 예를 나타낸 도이다.
- [227] 상기 도 4를 참조하면 블루투스 저전력 에너지의 프로파일 데이터(Profile Data) 교환을 위한 구조를 살펴볼 수 있다.
- [228] 구체적으로, GATT(Generic Attribute Profile)는 블루투스 LE 장치간의 서비스(Service), 특성(Characteristic)을 이용해서 데이터를 주고 받는 방법을 정의한 것이다.
- [229] 일반적으로, 페리페럴(Peripheral) 장치(예를 들면, 센서 장치)가 GATT 서버(Server)역할을 하며, 서비스(Service), 특성(Characteristic)에 대한 정의를 가지고 있다.
- [230] 데이터를 읽거나 쓰기 위해서 GATT 클라이언트는 GATT 서버로 데이터 요청을 보내게 되며, 모든 동작(Transaction)은 GATT client에서 시작되어 GATT 서버로부터 응답을 받게 된다.
- [231] 블루투스 LE에서 사용하는 GATT 기반 동작구조는 프로파일(Profile), 서비스(Service), 특성(Characteristic)에 기초하며, 상기 도 5와 같은 수직 구조를 이룰 수 있다.
- [232] 상기 프로파일(Profile) 하나 또는 그 이상의 서비스들로 구성되어 있으며, 상기 서비스는 하나 이상의 특성 또는 다른 서비스들로 구성되어 있을 수 있다.
- [233] 상기 서비스(Service)는 데이터를 논리적인 단위로 나누는 역할을 하며 하나 이상의 특성(Characteristic) 또는 다른 서비스들을 포함하고 있을 수 있다. 각 서비스는 UUID(Universal Unique Identifier)라 불리는 16bit 또는 128bit의 구분자를 가지고 있다.
- [234] 상기 특성(Characteristic)은 GATT 기반 동작 구조에서 가장 하위 단위이다. 상기 특성은 단 하나의 데이터를 포함하며, 상기 서비스와 유사하게 16 bit 또는 128 bit의 UUID를 가지고 있다.
- [235] 상기 특성은 여러 가지 정보들의 값으로 정의되고, 각각의 정보를 담기 위해서 속성(Attribute) 하나씩을 필요로 한다. 상기 특성 여러 개의 연속된 속성을 사용할 수 있다.
- [236] 상기 속성(Attribute)는 네 개의 구성 요소로 이루어지며, 아래와 같은 의미를 가진다.
- [237] - handle: 속성의 주소
- [238] - Type: 속성의 유형
- [239] - Value: 속성의 값
- [240] - Permission: 속성에 대한 접근 권한

- [241] 본 발명은 상기 GATT를 통해서 제어 디바이스가 제어하고자 하는 디바이스의 결합 정보 및 제어 가능한 동작과 관련된 정보를 획득하여 디바이스를 제어하는 방법을 제안한다.
- [242] 도 5는 디바이스간 블루투스 LE(Low Energy)를 이용하여 커넥션을 형성하는 방법을 나타낸 흐름도이다.
- [243] 상기 도 5에 도시된 바와 같이, 제 1 디바이스(300)와 제 2 디바이스(400)간 블루투스 LE 연결을 위해서 상기 제 1 디바이스(300)는 상기 제 2 디바이스에게 광고 메시지(Advertising Message)를 전송한다(S5010).
- [244] 이때, 상기 광고 메시지는 브로드캐스트 방식 또는 유니 캐스트 방식으로 전송될 수 있다.
- [245] 상기 광고 메시지는 앞에서 살펴본 바와 같이, 블루투스 LE를 활용해서 자신의 정보를 다른 디바이스에게 제공하기 위해 사용되며, 디바이스가 제공하는 서비스 정보, 사용자 정보 등 다양한 정보가 포함될 수 있다.
- [246] 상기 제 2 디바이스(400)는 상기 광고 메시지를 통해서 상기 제 1 디바이스(300)를 탐색(Discovery)할 수 있다.
- [247] 상기 제 2 디바이스(400)는 상기 광고 메시지에 포함된 정보를 확인 후, 상기 제 1 디바이스(300)에게 블루투스 LE 연결을 요청하기 위한 연결 요청 메시지(Connection request message)를 전송하고(S5020), 상기 제 1 디바이스(300)와 상기 제 2 디바이스(400)는 블루투스 LE(Low Energy) 커넥션을 형성하게 된다(S5030).
- [248] 이와 같은 방법은, 상기 제 1 디바이스(300) 및/또는 상기 제 2 디바이스(400)에 UI(User Interface)가 존재하지 않는다면, 사용자가 커넥션 형성을 제어할 수 없으며, PIN 번호 확인 및 연결 설정 제어가 불가능하다는 단점이 존재한다.
- [249] 따라서, 본 발명에서는 이와 같은 문제점을 해결하기 위해 제 3 디바이스를 이용하여 상기 제 1 디바이스(300)와 상기 제 2 디바이스(400)를 제안하기 위한 방법을 제안한다.
- [250] 도 6은 본 명세서에서 제안하는 제어 디바이스를 통해서 다른 디바이스를 제어하기 위한 방법을 간략히 나타낸 도이다.
- [251] 상기 도 6에 도시된 바와 같이, 제 1 디바이스(300)와 제 2 디바이스(400)간의 동작을 제어 하기 위해, 제 3 디바이스(500)가 필요하며, 상기 제 3 디바이스(500)는 상기 제 1 디바이스(300) 및 상기 제 2 디바이스(400)의 결합(Association)을 제어하기 위해서 새로운 제어 프로토콜이 필요하다.
- [252] 이하, 상기 제 1 디바이스(300)와 상기 제 2 디바이스(400)의 동작을 제어하기 위한 제어 디바이스를 상기 제 3 디바이스(500)라고 한다.
- [253] 이때, 상기 제 3 디바이스(500)는 디바이스들의 동작을 제어하기 위해서는 상기 디바이스들의 정보(예를 들면, 인터페이스 정보, 서비스 정보 등)를 알고 있어야 한다.
- [254] 도 7 및 도 8은 본 명세서에서 제안하는 디바이스를 제어하기 위한 서비스를

제공하기 위한 프로파일 구조의 일 예를 나타낸 도이다.

- [255] 상기 도 7 및 상기 도 8을 참조하면, 제어 디바이스가 다른 디바이스들을 제어하기 위한 서비스가 다른 서비스들의 프로파일에 함께 포함되어 있거나, 별도의 프로파일로 정의되어 있을 수 있다.
- [256] 이하, 본 발명에서 상기 제어 디바이스가 다른 디바이스들을 제어하기 위한 서비스를 이지 페어링 서비스(Easy Pairing Service)라 호칭하도록 한다.
- [257] 상기 제어 디바이스인 제 3 디바이스(300)는 상기 이지 페어링 서비스를 통해서 다른 디바이스들을 제어할 수 있다. 예를 들면, 상기 제 3 디바이스(300)는 상기 Easy Pairing Service를 통해서 제 1 디바이스(300)와 제 2 디바이스(400)간의 결합(예를 들면, 연결, 페어링 또는 본딩)과 관련된 동작들을 제어할 수 있다.
- [258] 이때, 상기 이지 페어링 서비스는 상기 도 7에 도시된 바와 같이 다른 서비스의 프로파일에 함께 포함되어 있거나, 상기 도 8에 도시된 바와 같이 별도의 프로파일로 정의될 수 있다.
- [259] 상기 도 7과 같이 상기 이지 페어링 서비스가 별도의 프로파일로 정의되지 않고 특정 서비스의 프로파일에 포함되어 있는 경우, 하나의 어플리케이션의 동작을 설명하기 편하다는 장점이 있다.
- [260] 하지만, 상기 이지 페어링 서비스를 포함하지 않는 프로파일의 서비스까지 상기 이지 페어링 서비스를 적용할 수 없으며, 디바이스간의 역할이 명확하게 정의되어 있어야 한다.
- [261] 상기 도 8과 같이 상기 이지 페어링 서비스가 별도의 프로파일로 정의되어 있는 경우, 프로파일 레벨에서 서버/클라이언트 구조가 호환 가능하며, 다른 프로파일까지 상기 이지 페어링 서비스를 확대 적용할 수 있다는 장점이 있다.
- [262]
- [263] 지원되는 페어링 기능 특성(Supported Pairing Features Characteristic)
- [264] 이 특성은 페어링 및 연결에 대한 서버의 제어 가능한 동작 정보를 제공하는데 사용된다. 서버의 동작은 블루투스 디바이스에 연결하는 디바이스 검색 및 링크 관리 측면의 일반적인 절차를 정의하는 일반 접근 프로파일(GAP: Generic Access Profile)에 정의되어 있다. 상기 특성에 의해 제공된 정보는 클라이언트가 상기 절차의 서버 동작을 제어하는데 사용된다.
- [265] 아래 표 2는 상기 지원되는 페어링 기능 특성의 필드를 보여준다.

[266] [표2]

	GAP Operations Field	EP Operations Field
Octet Order	LSO(Least Significant Octet) ... MSO(Most Significant Octet)	LSO ... MSO
Data Type	24 bits	8 bits
Size	3 octets	1 octet
Unit	None	None

[267] 특성 행동(Characteristic Behavior)

[268] 지원되는 페어링 기능 특성은 UUID «지원되는 페어링 기능» 을 사용하여 식별된다.

[269]

[270] GAP 동작 필드

[271] GAP 동작 필드는 서버에서 지원되는 일반적인 블루투스 동작을 식별한다. 상기 일반적인 동작은 블루투스 핵심 사양(specification)의 GAP 파트에서 정의된다.

[272] GAP 필드의 비트는 아래 표 3과 같이 정의될 수 있다.

[273] [표3]

Bit	Definition
0	Limited Discoverable Mode over BR/EDR transport is supported as an Acceptor
1	General Discoverable Mode over BR/EDR transport is supported as an Acceptor
2	Connectable Mode over BR/EDR transport is supported as an Acceptor
3	Bondable Mode over BR/EDR transport is supported as an Acceptor
4	Bonding Procedure over BR/EDR transport is supported as an Initiator
5	Link Establishment Procedure over BR/EDR transport is supported as an Initiator
6	BR/EDR Secure Simple Pairing is supported
7	BR/EDR Secure Connections is supported
8	Limited Discoverable Mode over LE transport is supported as a Peripheral
9	General Discoverable Mode over LE transport is supported as a Peripheral
10	Directed Connectable Mode over LE transport is supported as a Peripheral
11	Undirected Connectable Mode over LE transport is supported as a Peripheral
12	Auto Connection Establishment Procedure over LE transport is supported as a Central
13	General Connection Establishment Procedure over LE transport is supported as a Central
14	Connection Termination Procedure over LE transport is supported as a Peripheral or Central
15	Bondable Mode over LE transport is supported
16	Bonding Procedure over LE transport is supported
17	LE Secure Connections is supported
18	Secure Connection Only mode is supported. (e.g. medical device)
19	The Privacy feature is supported
20-23	Reserved for Future Use

[274] 표 3의 각 비트에 대해 서버는 지정된 동작을 지원하는 경우 비트를 1로 설정한다. 그렇지 않은 경우, 비트는 0으로 설정된다.

[275] 그리고, 서버는 미래를 위한 예약 비트를 0으로 설정한다.

[276]

[277] EP 동작 필드

[278] 이지 페어링(EP) 동작 필드는 서버에서 지원되는 선택적인 이지 페어링 기능을 식별한다.

[279] EP 동작 필드의 비트는 아래 표 4와 같이 정의될 수 있다.

[280] [표4]

Bit	Definition
0	Association Status Characteristic is supported
1	The Pairing with Confirm Value Indication and Confirm Value Relay are supported
2	The GATT Client List Characteristic is supported
3 - 7	Reserved for Future Use

[281] 표 4의 각 비트에 대해 서버는 서버가 지정된 기능을 지원하면 비트를 1로 설정한다. 그렇지 않으면 비트는 0으로 설정된다. 앞서 표 3에서 비트 18이 1로 설정된 경우, 표 4의 비트 1은 1로 설정된다.

[282] 그리고, 서버는 미래를 위한 예약 비트를 0으로 설정한다.

[283]

[284] 페어링 컨트롤 포인트 특성(Pairing Control Point Characteristic)

[285] 페어링 컨트롤 포인트 특성은 클라이언트가 서버의 페어링/연결을 관리하는데 사용된다.

[286] 페어링 컨트롤 포인트 특성의 구조는 아래 표 5와 같이 정의될 수 있다.

[287] [표5]

	Opcode	Parameters
Octet Order	None	LSO ... MSO
Data Type	8 bits	Variable
Size	1 octet	1 octet – X octets
Unit	None	None

[288] 도 9는 본 발명이 적용될 수 있는 실시예로서, 컨트롤 포인트 특성의 동작을 예시하는 도면이다.

[289] 제어 디바이스는 상기 제어 디바이스에 연결된 제 1 디바이스에 ATT 기입 요청 메시지를 전송한다(S901).

[290] 상기 기입 요청 메시지는 컨트롤 포인트 동작 코드(OP code)를 포함한다.

[291] 제 1 디바이스는 제어 디바이스로 ATT 기입 응답 메시지를 전송한다(S902).

- [292] 상기 기입 응답 메시지는 ATT 결과 값을 포함할 수 있다.
- [293] 제 1 디바이스와 제 2 디바이스는 GAP 동작을 수행한다(S903).
- [294] 즉, 제 1 디바이스와 제 2 디바이스는 제어 디바이스에 의해 요청된 GAP 동작을 수행한다.
- [295] 제 1 디바이스는 제어 디바이스로 ATT 지시 메시지를 전송한다(S904).
- [296] 상기 지시 메시지는 GAP 동작 결과에 관련된 결과 코드를 포함할 수 있다.
- [297] 제어 디바이스는 제 1 디바이스로 ATT 확인 메시지를 전송한다(S905).
- [298] 상기 확인 메시지는 ATT 결과 값을 포함할 수 있다.
- [299] 즉, 컨트롤 포인트 특성의 동작은 두 가지 GATT 절차인 Write Characteristic Value와 Characteristic Value Indications로 구성된다. 첫 번째 GATT 절차인 기입 특성 값은 서버의 GAP 동작을 요청하는 것이고, ATT 기입 응답 프로토콜 데이터 단위(PDU)는 ATT 에러 응답일 수 있는 ATT 기입 요청의 응답 PDU이다.
- [300] BR/EDR 수락자(Acceptor) 제어 절차, BR/EDR 개시자(Initiator) 제어 절차, LE 페리퍼럴(Peripheral) 제어 절차 또는 LE 센트럴(Central) 제어 절차와 같은 컨트롤 포인트 절차 중 일부는 요청된 GAP 동작을 위한 질의(Inquiry), 질의 스캔(Inquiry Scan), 페이징(Paging), 페이징 스캔(Paging Scan), 광고(Advertising) 또는 스캔(Scanning)와 같은 추가적인 Link Layer 상태를 필요로 한다. GAP 동작은 다른 장치와 상호 작용하는데 사용된다.
- [301] 서버가 절차를 수행한 후에는 특성 값 지시 절차를 사용하여 클라이언트가 요청한 GAP 동작 결과를 나타내거나 서버 확인 값을 지시한다. 따라서, 이 특성은 지시를 위해 클라이언트 특성 설명자(Descriptor)를 통해 구성되고 서버는 클라이언트에게 지시하여야 한다.
- [302]
- [303] 페어링 컨트롤 포인트 절차 요구 사항(Pairing Control Point Procedure Requirements)
- [304] 아래 표 6은 페어링 컨트롤 포인트 절차(Opcode 및 파라미터) 요구 사항을 나타낸다.

[305] [표6]

Opcode Value	Procedure	Requirement	Parameters	Applicable Response Values	Response Parameter
0x00	Reserved for Future Use				
0x01	BR/EDR Acceptor Control	C1	Operations & Peer Device ID	Success	
0x02	BR/EDR Initiator Control	C1	Operations & Peer Device ID	Success	
0x03	LE Peripheral Control	C2	Operations & Peer Device ID & Peer Device IRK	Success	
0x04	LE Central Control	C2	Operations & Peer Device ID & Peer Device IRK	Success	
0x05	Association Termination	Optional	Peer Device ID & Bearers & Operations	Success	
0x06	Confirm Value Indication	C3	Device Address, Random Value, Confirm Value	Success	
0x07	Confirm Value Relay	C3	Device Address, Random Value, Confirm Value	Success	
0x08	Control Point Response Indication	Mandatory	Request Opcode, Response Code		
0x09	Select Association Status Bank	C4	Bank Counter	Success, Not Supported Bank	
0x0A	Select Client List Bank	C5	Bank Counter	Success, Not Supported Bank	
0x0B-0xFF	Reserved for Future Use				

[306] C1: 서버가 BR/EDR 트랜스포트(transport)를 지원하는 경우 필수이다.

[307] C2: 서버가 LE 트랜스포트를 지원하는 경우 필수이다.

[308] C3: 서버가 보안 연결 전용 모드를 지원하는 경우 필수이다. 그 후, 앞서 표 3의 비트 6, 비트 7 및 비트 17 중 적어도 하나의 비트가 1로 설정된다.

[309] C4: 모든 연관(Association) 정보에 대해 512 바이트 이상이 지원되는 경우 필수이다.

[310] C5: 모든 클라이언트 목록 정보에 대해 512 바이트 이상이 지원되는 경우 필수이다.

[311]

[312] 페어링 컨트롤 포인트 특성 행동(Pairing Control Point Characteristic Behavior)

[313] 페어링 컨트롤 포인트 특성은 클라이언트가 GATT Write Characteristic Value 서브 절차를 사용하여 서버의 동작을 명령하는 메커니즘을 제공하는 것이다. 프로시저는 해당 opcode의 컨텍스트 내에서 유효한 파라미터 다음에 오는 동작을 나타내는 opcode가 포함된 값을 기입하여 트리거(trigger)된다.

[314] 이러한 절차가 성공적으로 완료되면, 서버는 성공 결과 코드와 함께 컨트롤 포인트 응답 지시를 사용하여 클라이언트에게 지시해야 한다. 절차가 성공적으로 완료되지 않은 경우, 서버는 에러 응답 코드와 함께 컨트롤 포인트 응답 지시를 사용하여 클라이언트에게 지시해야 한다.

[315]

[316] BR/EDR 수락자 컨트롤 절차 행동(Acceptor Control Procedure Behavior)

[317] 이 절차는 서버가 지원되는 페어링 기능 특성(supported pairing feature characteristic)에서 GAP 동작 필드(비트 0, 비트 1, 비트 2 및 비트 3)에서 알려진(언어지는) 수락자 역할(role)을 지원하는 경우에 지원된다.

[318] BR/EDR 트랜스포트를 통해 수락자 역할은 디바이스 검색 및 연결 성립 절차에 대한 개시자의 요청을 수락한다.

[319] 수락자가 제한된 검색 가능 모드(Limited Discoverable Mode) 또는 일반 검색 가능 모드(General Discoverable Mode)에 있는 경우, 수락자가 개시자 장치에 의해 검색된다. 그렇지 않은 경우, 개시자의 질의에 응답하지 않기 때문에 수락자가 검색되지 않는다.

[320] 수락자가 연결 가능 모드(Connectable Mode)에 있으면, 수락자는 개시자로부터 링크 설립 절차를 수락하여 그들 사이에 BR/EDR 링크 연결을 만든다. 그렇지 않은 경우, 수락자는 개시자에게 응답하지 않으므로 개시자와 연결하지 않는다. 수락자가 개시자와 페어링 프로세스를 수행하면, 링크 연결을 생성한 후 개시자와 하나 이상의 공유된 비밀 키를 생성한다.

[321] 수락자가 본딩 모드(Bonding Mode)에 있는 경우, 서버는 신뢰된 디바이스 쌍을 형성하기 위해 후속 연결에 대한 페어링 프로세스 후에 생성된 키를 저장해야 한다.

[322] 이러한 컨트롤 포인트 메시지는 서버의 가능한 동작을 제어하기 위한 추가적인 파라미터가 필요하다. 파라미터는 아래 표 7에서와 같이 동작 필드와 선택적 피어 디바이스 ID 필드로 구성된다.

[323] [표7]

	Operation	Peer Device ID
Octet Order	LSO ... MSO	LSO ... MSO
Data Type	8 bits	48 bits
Size	1 octet	6 octets
Unit	None	None

[324] 동작 필드는 제한된 검색 가능 모드, 일반 검색 가능 모드, 연결 가능 모드, 본딩 모드, 확인 값 지시(Confirm Value Indication) 및 확인 값 릴레이(Confirm Value Relay)를 위한 비트 기반 정보이다. 피어 디바이스 ID 필드는 피어 디바이스를 결정하기 위한 선택적 필드이다.

[325] 상기 동작 필드는 표 8과 같이 정의될 수 있다.

[326] [표8]

Bit	Definition of Operation
0-1	Server shall operate the Discoverable Mode.  00b: Non-Discoverable Mode  01b: Limited Discoverable Mode  10b: General Discoverable Mode  11b: Reserved for Future Use
2	Server shall operate the Connectable Mode.
3	Server shall operate the Bondable Mode.
4	Server shall operate with a Peer Device whose Bluetooth Address is same as the following Peer Device ID field.
5	Server shall indicate its Confirm Value to Client with Confirm Value Indication.
6	Server shall receive the Confirm Value of the peer Server via the Client with the Confirm Value Relay.
7	Reserved for Future Use

[327] 서버는 표 8의 동작 서브 필드의 비트 0, 비트 1, 비트 2 및 비트 3에 정의된 바와 같이, 검색 가능 모드, 연결 가능 모드 및 본딩 가능 모드(Bondable Mode)로 설정된다. 서버는 이러한 비트에서 미래 사용을 위해 예약된 값으로 설정되서는 안된다.

[328] 비트 4가 1로 설정된 경우, 서버는 다음 피어 디바이스 ID 필드 값의 디바이스 주소를 피어 디바이스와 수락자 동작을 수행해야 한다. 그렇지 않으면, 피어 디바이스 ID 필드는 존재하지 않고, 서버는 모든 장치의 요청을 수락할 수 있다.

[329] 비트 5가 1로 설정된 경우, 서버는 확인 값을 피어 서버로 릴레이할 클라이언트에게 확인 값을 지시해야 한다. 그렇지 않으면, 서버는 확인 값을 표시하지 않는다.

[330] 비트 6이 1로 설정된 경우, 서버는 확인 값 릴레이와 함께 클라이언트를 통해

피어 서버의 확인 값을 수신한다. 그렇지 않으면, 서버는 클라이언트로부터 확인 값 릴레이를 받지 못한다.

[331] 미래 사용을 위해 예약된 비트는 0으로 설정되어야 한다.

[332]

[333] **BR/EDR 개시자 컨트롤 절차 행동(Initiator Control Procedure Behavior)**

[334] 이 절차는 서버가 지원되는 페어링 기능 특성의 GAP 동작 필드(비트 4 및 비트 5)에서 알려진(언어지는) 개시자 역할을 지원하는 경우에 지원된다.

[335] BR/EDR 트랜스포트를 통해, 개시자 역할은 수락자 디바이스에 링크 설립 절차(Link Establishment Procedure) 및 본딩 절차(Bonding procedure)를 시작한다.

[336] 이 컨트롤(제어) 절차는 서버의 가능한 동작을 제어하기 위한 추가적인 파라미터가 필요하다.

[337] 파라미터는 아래 표 9과 같이 동작 필드와 피어 디바이스 ID 필드로 구성될 수 있다.

[338] [표9]

	Operation	Peer Device ID
Octet Order	LSO ... MSO	LSO ... MSO
Data Type	8 bits	48 bits
Size	1 octet	6 octets
Unit	None	None

[339] BR/EDR 수락자 제어 절차와 달리, 상기 절차에서는 피어 디바이스 ID 필드를 사용하여 서버가 연결할 대상을 식별한다.

[340] 동작 필드는 링크 설립 절차(Link Establishment Procedure), 본딩 절차(Bonding Procedure), 확인 값 지시(Confirm Value Indication) 및 확인 값 릴레이(Confirm Value Relay)에 대한 비트 기반 정보이다. 각 동작은 이 필드의 별도 비트에 매핑된다.

[341] 상기 동작 필드는 아래 표 10과 같이 정의될 수 있다.

[342] [표10]

Bit	Definition of Operations
0	Server shall perform the Link Establishment Procedure.
1	Server shall perform the Bonding Procedure.
2	Server shall indicate its Confirm Value to Client with Confirm Value Indication.
3	Server shall receive the Confirm Value of the peer Server via the Client with the Confirm Value Relay.
4-7	Reserved for Future Use

[343] 표 10의 각 비트에 대해 서버는 각 비트가 1로 설정된 경우 각 작업을 수행한다. 그렇지 않으면, 서버가 각 작업을 수행하지 않는다.

[344] 미래 사용을 위해 예약된 비트는 0으로 설정된다.

[345]

[346] LE 페리퍼럴 컨트롤 절차 행동(Peripheral Control Procedure Behavior)

[347] 이 절차는 서버가 지원되는 페어링 기능 특성에서 GAP 동작 필드(비트 8, 비트 9, 비트 10 및 비트 11)에서 알려진(얻어지는) 페리퍼럴 역할을 지원하는 경우에 지원된다.

[348] LE 트랜스포트를 통해, 페리퍼럴 역할의 디바이스는 센트럴 역할의 디바이스가 검색하도록 광고하고 센트럴 역할의 연결 요청을 수락한다. 따라서, 광고 동작은 검색 가능 모드(Discoverable mode) 및 연결 가능 모드(Connectable mode)와 관련된다. 서버가 다이렉트 연결 가능 광고 모드(directed connectable advertising mode)에 있으면, 서버는 광고 메시지에서 식별된 센트럴 디바이스로부터 연결 요청을 수신한다. 서버가 언다이렉트 연결 가능 광고(undirected connectable advertising) 모드에 있으면, 서버는 모든 센트럴 디바이스로부터 연결 요청을 받을 수 있다.

[349] 검색 가능 모드(Discoverable Mode), 연결 가능 모드(Connectable Mode) 및 개인 정보 보호 모드(Privacy Mode)와 같은 서버의 광고 동작은 클라이언트에 의해 제어된다. 일반 검색 가능 모드(General Discoverable Mode) 및 제한된 검색 가능 모드(Limited Discoverable Mode)에서 서버의 광고 지속 시간은 클라이언트에 의해 제어된다. 클라이언트는 서버가 광고하는 동안 다이렉트 연결 가능 모드 또는 언다이렉트 연결 가능 모드를 사용하는지 여부를 제어한다. 클라이언트는

광고하는 동안 서버가 랜덤 어드레스(Random Address)를 사용하는지 여부를 제어한다. 또한, 클라이언트는 서버가 피어 디바이스에 연결된 후, 서버의 페어링 및 본딩 동작을 제어한다.

[350] 이러한 동작을 구성하기 위해, 이 절차는 표 11과 같이 동작 필드와 선택적인 피어 디바이스 ID 필드 및 선택적인 피어 디바이스 IRK(Identify Resolving Key) 필드를 포함하는 파라미터가 필요하다.

[351] 피어 디바이스 ID는 동작 필드에서 직접 연결 모드가 선택되는 경우 제공된다.

[352] [표11]

	Operation	Peer Device ID	Peer Device IRK
Octet Order	LSO ... MSO	LSO ... MSO	LSO ... MSO
Data Type	16 bits	48 bits	128 bits
Size	2 octets	6 octets	16 octets
Unit	None	None	None

[353] 동작 필드는 검색 가능 모드, 연결 가능 모드, 개인 정보 보호 모드, 본딩 가능 모드, 확인 값 지시, 릴레이 값 지시, 아이덴티티 분석 키 동작에 대한 비트 기반 정보이다. 동작 필드는 아래의 표 12와 같이 정의될 수 있다.

[354] [표 12]

Bit	Definition of Operations
0-1	Server operates the Discoverable Mode. 00b: Non-Discoverable Mode 01b: Limited Discoverable Mode 10b: General Discoverable Mode 11b: Reserved for Future Use
2	Reserved for Future Use
3-4	Server shall operate the Connectable Mode. 00b: Non-Connectable Mode 01b: Directed Connectable Mode 10b: Undirected Connectable Mode 11b: Reserved for Future Use
5	Reserved for Future Use
6-7	Server shall use the following address type for its Advertiser's Address. 00b: Public Device Address 01b: Static Device Address 10b: Non-Resolvable Private Address 11b: Resolvable Private Address
8	Reserved for Future Use
9	Server shall operate the Bondable Mode. 0b: Non-Bondable Mode 1b: Bondable Mode
10	Server shall indicate its Confirm Value to Client with Confirm Value Indication.
11	Server shall receive the Confirm Value of the peer Server via the Client with the Confirm Value Relay.
12	Identity Resolving Key of the Peer Device is attached.
13-16	Reserved for Future Use

[355] 표 12를 참조하면, 서버는 동작 서브 필드의 비트 0과 비트 1에 정의된 바와 같이 검색 가능 모드로 설정될 수 있다. 서버는 이 비트에서 미래 사용을 위해 예약된 값으로 설정되지 않는다.

[356] 서버는 동작 서브 필드의 비트 3과 비트 4에 의해 정의된 바와 같이 연결 가능 모드로 설정될 수 있다. 값이 01b 인 경우, 서버는 피어 디바이스 ID 필드의 값을 개시자의 주소로 사용하여 직접 연결 모드로 동작할 수 있다. 서버는 이

비트에서 미래 사용을 위해 예약된 값으로 설정되지 않는다.

- [357] 서버는 동작 서브 필드의 비트 6과 비트 7에 정의된 바와 같이 광고자의 주소 유형을 광고한다. 서버가 분석 가능한 주소 전용 특성(Resolvable Private Address Only Characteristic)을 가지는 경우, 서버는 분석 가능한 개인 주소(resolvable private address)로 광고한다. 피어 디바이스에 ID 분석 가능 키(Identity Resolvable Key)가 없으면, 피어 디바이스는 이 서버의 광고를 무시할 수 있다.
- [358] 서버는 동작 서브 필드의 비트 9에 정의된 바와 같이 본딩 가능 모드(Bondable Mode)로 설정될 수 있다. 그렇지 않으면, 서버는 본딩 가능 모드로 설정되지 않습니다.
- [359] 비트 10이 1로 설정된 경우 서버는 클라이언트에게 확인 값을 피어 서버(peer Server)로 중계(릴레이)할 확인 값을 지시한다. 그렇지 않으면 서버는 확인 값을 지시하지 않는다.
- [360] 비트 11이 1로 설정된 경우 서버는 확인 값 릴레이와 함께 클라이언트를 통해 피어 서버의 확인 값을 수신한다. 그렇지 않으면 서버는 클라이언트로부터 확인 값 릴레이를 수신하지 않는다.
- [361] 비트 12가 1로 설정된 경우 서버는 피어 디바이스 ID의 IRK 값인 피어 디바이스 IRK(Identity Resolving Key) 필드를 수신한다. 서버는 피어 디바이스 ID, 피어 디바이스 IRK 및 로컬 IRK를 해당 장치의 분석 목록(resolving list)에 추가한다. 그렇지 않으면, 서버는 피어 디바이스 IRK 필드를 수신하지 않는다.
- [362] 미래를 위해 예약된 비트는 0으로 설정된다.
- [363]
- [364] LE 센트럴 컨트롤 절차 행동(Central Control Procedure Behavior)
- [365] 이 절차는 서버가 지원되는 페어링 기능 특성의 GAP 동작 필드(비트 12 및 비트 13)에서 알려진(얻어지는) 센트럴 역할을 지원하는 경우에 지원된다.
- [366] LE 트랜스포트를 통해 센트럴 역할의 디바이스는 페리퍼럴의 광고를 수신하고 주변 장치로 연결 요청을 전송하여 연결을 형성한다. 연결 설립 절차(Connection Establishment Procedure), 본딩 절차(Bonding Procedure), 확인 값 지시(Confirm Value Indication) 및 확인 값 릴레이(Confirm Value Relay)와 같은 서버의 동작 절차는 클라이언트에 의해 제어된다. 서버의 연결 설립 절차는 자동 연결 설립(Auto Connection Establishment) 또는 일반 연결 설립 절차(General Connection Establishment Procedure)로 구성되는 동작으로 클라이언트에 의해 제어된다.
- [367] 서버의 자동 연결 설립 절차를 사용하면 이 절차를 수행 한 후 서버가 클라이언트 상호 작용(interaction) 없이 특정 LE 디바이스에 자동적으로 연결할 수 있다. 그러나, 일반 연결 설정을 사용하면 서버가 이 절차로 특정 LE 장치와 한 번 연결할 수 있다. 그 후, 본딩 절차, 확인 값 지시 또는 확인 값 릴레이와 같은 서버의 동작은 서버에 링크 계층 연결이 설립된 후 클라이언트에 의해 제어될 수 있다.

[368] 이러한 동작을 구성하기 위해, 이 절차는 아래의 표 13과 같이 동작 필드, 피어 디바이스 ID 필드 및 선택적인 피어 디바이스 IRK가 포함된 파라미터가 필요하다. 피어 디바이스 ID 필드는 연결할 블루투스 디바이스의 디바이스 주소이다.

[369] [표13]

	Operations	Peer Device ID	Peer Device IRK
Octet Order	LSO ... MSO	LSO ... MSO	LSO ... MSO
Data Type	16 bits	48 bits	128 bits
Size	2 octets	6 octets	16 octets
Unit	None	None	None

[370] 상기 동작은 아래의 표 14와 같이 정의될 수 있다.

[371] [표14]

Bit	Definition of Operations
0-1	Server shall operate the Connection Establishment Procedure.  00b: Auto Connection Establishment Procedure  01b: General Connection Establishment Procedure  10b-11b: Reserved for Future Use
2	Server shall operate the Bondable Procedure.
3	Server shall indicate its Confirm Value to Client with Confirm Value Indication.
4	Server shall receive the Confirm Value of the peer Server via the Client with the Confirm Value Relay.
5-6	Server shall use the following address type for its Initiator Address.  00b: Public Device Address  01b: Static Device Address  10b: Non-Resolvable Private Address  11b: Resolvable Private Address
7	Identity Resolving Key of the Peer Device is attached.
8-15	Reserved for Future Use

[372] 표 14를 참조하면 서버는 동작 서브 필드의 비트 0과 비트 1에 의해 정의된 바와 같이 연결 설립 절차(Connection Establishment Procedure)로 설정될 수 있다. 만약, 그 값이 00b(자동 연결 설립 절차)인 경우, 서버는 LE 트랜스포트를 통해 특정 디바이스와 자동으로 연결을 형성한다. 이 절차는 호스트와 상호 작용하지 않고 컨트롤러 부분에서 동작한다. 따라서, 서버는 이 컨트롤 포인트 메시지를 수신한 후, 클라이언트와 상호 작용 없이 특정 디바이스와 자동으로 연결할 수 있다. 만약, 그 값이 01b(일반 연결 설립 절차)인 경우, 서버는 이 컨트롤 포인트 절차에 따라 한 번 연결을 생성한다. 서버는 이 비트에서 미래 사용을 위해 예약된 값으로 설정되지 않는다.

[373] 비트 2가 1로 설정된 경우, 서버는 페어링 프로세스 후 피어 디바이스와의 다음

연결을 위한 본딩 정보를 저장하기 위해 본딩 절차를 시작한다.

- [374] 비트 3이 1로 설정된 경우, 서버는 클라이언트에 확인 값을 피어 서버로 중계할 확인 값을 지시할 수 있다. 그렇지 않으면 서버는 클라이언트에 확인 값을 나타내지 않을 수 있다.
- [375] 비트 4가 1로 설정된 경우 서버는 클라이언트로부터 확인 값 릴레이가 있는 피어 서버의 확인 값을 수신할 수 있다. 그렇지 않으면 서버는 클라이언트로부터 확인 값 릴레이를 수신하지 않을 수 있다.
- [376] 서버는 동작 서브 필드의 비트 5와 비트 6에 정의된 바와 같이, 해당 개시자의 주소 유형을 이용하여 개시할 수 있다. 서버가 분석 가능한 개인 주소 전용 특성을 가지고 있는 경우, 서버는 분석 가능한 개인 주소로 초기화해야 한다. 피어 디바이스에 ID 분석 가능 키가 없는 경우, 피어 디바이스는 이 서버의 연결 요청을 무시할 수 있다.
- [377] 비트 7이 1로 설정된 경우 서버는 이 절차에서 피어 디바이스 ID의 IRK 값을 포함하는 피어 장치 IRK 필드를 수신할 수 있다. 서버는 피어 디바이스 ID, 피어 디바이스 IRK 및 로컬 IRK를 분석 목록에 추가할 수 있다. 그렇지 않으면, 서버는 ID 분석 키 필드를 수신하지 않는다.
- [378]
- [379] 기존의 컨트롤 포인트 절차는 동작에 기반하여 수행된다. 즉, GAP 동작을 기반으로 각각의 모드 또는 절차에 따라 개별적으로 컨트롤 포인트 절차가 수행된다.
- [380] 구체적으로, 기존의 방법에 따르면 검색 가능 모드 셋업 절차(Discoverable Mode Setup Procedure), 연결 가능 모드 셋업 절차(Connectable Mode Setup Procedure), 연결 요청 절차(Connection Request Procedure), 연결 종료(Connection Termination)의 각 단계 별로 개별적인 커맨드(또는 컨트롤 포인트 특성)가 제어 디바이스에 의해 전송된다.
- [381] 즉, 기존의 하나의 역할에 따른 여러 동작들은 서로 밀접한 관련성이 있음에도 불구하고, 각각의 동작 또는 절차마다 컨트롤 포인트 절차가 수행되어야 한다. 이로 인해, 관련된 동작을 지시하기 위하여 클라이언트 디바이스와 서버 디바이스간 불필요한 상호 작용(interaction)이 요구되는 문제점이 있다.
- [382] 예를 들어, 검색 모드 셋업 절차(Discovery Mode Setup Procedure) (즉, 일반 또는 제한된 검색 가능 모드)와 연결 모드 셋업 절차(Connectable Mode Setup Procedure)(즉, 다이렉트 또는 언다이렉트(Undirected) 연결 가능 모드)는 LE 페리퍼럴 디바이스의 광고와 관련된 동작임에도 불구하고, 동작 단계 별로 별도의 커맨드가 전송된다. 이로 인해, LE 페리퍼럴 디바이스의 광고 동작을 지시하기 위하여 클라이언트 디바이스와 서버 디바이스간 불필요한 상호 작용이 요구되고, 컨트롤 포인트 절차 운영의 효율성이 저하된다.
- [383] 또한, 앞서 예시한 절차 또는 모드 외에 개인 정보 보호 모드(Privacy mode)를 수행하기 위하여 마찬가지로 별도의 커맨드 전송이 요구되는 문제점이 있다.

- [384] 본 발명에서는 이와 같은 문제점을 해결하기 위하여 GAP 역할(role)에 기반한 컨트롤 포인트 절차를 제안한다.
- [385] GAP 역할에 기초하여 기존의 여러 절차(또는 단계)에 거쳐 이루어지던 커맨드를 한번에 전송함으로써 효율적인 제어가 가능하도록 할 수 있다.
- [386] GAP 역할은 검색부터 연결 성립까지 디바이스의 동작을 정의한다. 예를 들어, GAP 역할은 다음과 같이 정의될 수 있다.
- [387] 1) BR/EDR 역할
- [388] - 개시자(또는 이니시에이터)(Initiator): 디바이스의 검색을 개시하기 위한 질의(inquiry) 메시지를 전송하고, 이에 대한 응답 메시지를 수신한다.
- [389] - 수락자(또는 액셉터)(Acceptor): 개시자로부터 질의 메시지를 수신하고, 질의 메시지에 대한 응답 메시지를 전송한다.
- [390] 2) LE 역할
- [391] - 페리퍼럴(Peripheral): 광고를 전송하며, 센트럴로부터 연결 요청을 수신한다.
- [392] - 센트럴(Central): 페리퍼럴로부터 광고를 수신하고, 수신된 광고에 기초하여 페리퍼럴에 대하여 연결 요청을 전송한다.
- [393] 즉, 본 명세서에서 제안하는 방법에 따르면, 제어 디바이스(즉, 클라이언트 디바이스)는 제 1 디바이스(즉, 서버 디바이스)의 복수 개의 동작들을 하나의 커맨드로 제어할 수 있다.
- [394] 또한, 역할을 기반으로 컨트롤 포인트 절차를 수행하기 때문에, 연결 타입(BR/EDR 트랜스포드 또는 LE 트랜스포드)를 지시하기 위한 베어러 필드가 컨트롤 포인트 특성에서 삭제될 수 있다. 예를 들어, 이 경우 Opcode 값의 범위는 256일 수 있다.
- [395] 일 실시예에서, 동작 코드 Opcode(또는 컨트롤 포인트 특성)는 각 역할(BR/EDR 개시자, BR/EDR 수락자, LE 페리퍼럴, LE 센트럴) 별로 정의될 수 있다. 그리고, Opcode는 GAP 역할과 각각의 GAP 역할에 기초한 복수 개의 동작들을 지시하는 파라미터를 포함할 수 있다.
- [396] 다시 말해, Opcode는 GAP 역할을 지시하는 역할 필드와 복수개의 동작들을 나타내는 파라미터 필드를 포함할 수 있다. 그리고 상기 파라미터의 파라미터들에 의해 각각의 동작들이 독립적인 비트(bit)로 지시될 수 있다.
- [397] 이하에서, 하나의 컨트롤 포인트 절차로서 디바이스의 역할 및 동작을 제어하기 위하여 GAP 역할 별로 컨트롤 포인트 특성(또는 Opcode)를 구성하는 방법을 설명한다.
- [398]
- [399] - BR/EDR 수락자 역할
- [400] BR/EDR 수락자 역할을 제어하는 절차는 하나의 Opcode로 구성될 수 있다. 그리고, 상기 Opcode는 제 1 디바이스(즉, 서버 디바이스)의 가능한 동작들을 제어하기 위한 추가적인 파라미터를 포함할 수 있다. 상기 절차는 상기 제 1 디바이스가 지원되는 페어링 기능 특성의 GAP 동작 필드에서 수락자 역할을

- 지원하는 것으로 지시되는 경우에 지원될 수 있다.
- [401] 이때, BR/EDR 수락자 역할을 제어하기 위한 Opcode는 검색 가능 모드(Discoverable mode) 동작, 연결 가능 모드(Connectable mode) 동작 및/또는 본딩 가능 모드(Bondable mode) 동작을 지시하는 파라미터들을 포함할 수 있다. 이때, 각 동작은 별도 비트에 매핑될 수 있다.
- [402] 여기서, 검색 가능 모드(Discoverable mode)는 검색 불가능 모드(Non-Discoverable mode), 제한된 검색 가능 모드(Limited Discoverable Mode) 또는 일반 검색 가능 모드(General Discoverable Mode)로 구분될 수 있다.
- [403] 만약, 수락자가 제한된 검색 가능 모드(Limited Discoverable Mode) 또는 일반 검색 가능 모드(General Discoverable Mode)에 있는 경우, 수락자가 개시자 장치에 의해 검색될 수 있다. 그렇지 않은 경우, 개시자의 질의에 응답하지 않기 때문에 수락자가 검색되지 않을 수 있다.
- [404] 만약, 수락자가 연결 가능 모드(Connectable Mode)에 있는 경우, 수락자는 개시자로부터 링크 설립 절차를 수락하여 그들 사이에 BR/EDR 링크 연결을 형성할 수 있다. 그렇지 않은 경우, 수락자는 개시자에게 응답하지 않으므로 개시자와 연결을 형성하지 않을 수 있다.
- [405] 수락자가 페어링 프로세스를 수행하면, 링크 연결을 생성한 후 개시자와 하나 이상의 공유된 비밀 키를 생성할 수 있다.
- [406] 만약, 수락자가 본딩 모드(Bonding Mode)에 있는 경우, 서버는 신뢰된 디바이스 쌍을 형성하기 위해 후속 연결에 대한 페어링 프로세스 후에 생성된 키를 저장할 수 있다.
- [407]
- [408] - BR/EDR 개시자 역할
- [409] BR/EDR 개시자 역할을 제어하는 절차는 하나의 Opcode로 구성될 수 있다. 그리고 상기 Opcode는 제 1 디바이스(즉, 서버 디바이스)의 가능한 동작들을 제어하기 위한 추가적인 파라미터를 포함할 수 있다. 상기 절차는 제 1 디바이스가 지원되는 페어링 기능 특성의 GAP 동작 필드에서 개시자 역할을 지원하는 것으로 지시되는 경우에 지원될 수 있다.
- [410] BR/EDR 개시자 역할을 제어하기 위한 Opcode는 링크 설립 절차(Link Establishment Procedure), 본딩 절차(Bonding Procedure) 및/또는 페어링 절차(Pairing Procedure) 동작을 지시하는 파라미터들을 포함할 수 있다. 이때, 각 동작은 별도 비트에 매핑될 수 있다.
- [411] 예를 들어, 제어 디바이스는 BR/EDR 개시자 역할을 지시하는 Opcode에 링크 설립 절차를 나타내는 파라미터 필드를 1 값으로 설정하고, 본딩 절차를 나타내는 파라미터 필드를 1 값으로 설정하고, 개시자 역할의 디바이스로 컨트롤 포인트 기입 요청 메시지를 전송하는 경우, 개시자 역할의 디바이스는 BR/EDR 트랜스퍼트를 통해 수락자 디바이스에 링크 설립 절차 및 본딩 절차를 시작할 수 있다.

[412]

[413] - LE 페리퍼럴 역할

[414] LE 페리퍼럴 역할을 제어하는 절차는 하나의 Opcode로 구성될 수 있다. 그리고 상기 Opcode는 제 1 디바이스(즉, 서버 디바이스)의 가능한 동작들을 제어하기 위한 추가적인 파라미터를 포함할 수 있다. 상기 절차는 상기 제 1 디바이스가 지원되는 페어링 기능 특성의 GAP 동작 필드에서 페리퍼럴 역할을 지원하는 것으로 지시되는 경우에 지원될 수 있다.

[415] LE 페리퍼럴 역할을 제어하기 위한 Opcode는 검색 가능 모드(Discoverable mode) 동작, 연결 가능 모드(Connectable mode) 동작, 프라이버시 모드(Privacy mode) 동작 및/또는 본딩 가능 모드(Bondable mode) 동작을 지시하는 파라미터들을 포함할 수 있다. 이때, 각 동작은 별도 비트에 매핑될 수 있다.

[416] LE 페리퍼럴의 광고 동작은 검색 가능 모드(Discoverable mode) 및 연결 가능 모드(Connectable mode)와 관련된다. 여기서, 검색 가능 모드는 일반 검색 가능 모드(General Discoverable Mode) 및 제한된 검색 가능 모드(Limited Discoverable Mode)로 구분될 수 있다. 그리고, 연결 가능 모드는 다이렉트 연결 가능 광고(mode)와 언다이렉트 연결 가능 광고(undirected connectable advertising) 모드로 구분될 수 있다.

[417] 만약, 페리퍼럴이 다이렉트 연결 가능 광고 모드(directed connectable advertising mode)에 있는 경우, 페리퍼럴은 광고 메시지에서 식별된 센트럴 디바이스로부터 연결 요청을 수신한다.

[418] 만약, 페리퍼럴이 언다이렉트 연결 가능 광고(undirected connectable advertising) 모드에 있는 경우, 페리퍼럴은 모든 센트럴 디바이스로부터 연결 요청을 받을 수 있다.

[419] 검색 가능 모드(Discoverable Mode), 연결 가능 모드(Connectable Mode) 및 개인 정보 보호 모드(Privacy Mode)와 같은 페리퍼럴(즉, 서버)의 광고 동작은 클라이언트에 의해 제어될 수 있다.

[420] 또한, 일반 검색 가능 모드(General Discoverable Mode) 및 제한된 검색 가능 모드(Limited Discoverable Mode)에서 서버의 광고 지속 시간은 클라이언트에 의해 제어될 수 있다.

[421] 클라이언트는 서버(즉, 페리퍼럴)가 광고하는 동안 다이렉트 연결 가능 모드 또는 언다이렉트 연결 가능 모드를 사용하는지 여부를 제어할 수 있다. 또한, 클라이언트는 광고하는 동안 서버가 랜덤 어드레스(Random Address)를 사용하는지 여부를 제어할 수 있다. 또한, 클라이언트는 서버가 피어 디바이스에 연결된 후, 서버의 페어링 및 본딩 동작을 제어할 수 있다.

[422] 이러한 동작을 구성하기 위해, 앞서 설명한 표 11과 같이 동작 필드와 선택적인 피어 디바이스 ID 필드 및 선택적인 피어 디바이스 IRK(Identify Resolving Key) 필드를 포함하는 파라미터가 필요할 수 있다. 여기서, 피어 디바이스 ID는 다이렉트 연결 모드가 선택되는 경우 제공된다. 상기 피어 디바이스의 IRK를

이용한 개인 정보 보호 모드(Privacy Mode) 동작은 자세히 후술한다.

[423]

[424] - LE 센트럴 역할

[425] LE 센트럴 역할을 제어하는 절차는 하나의 Opcode로 구성될 수 있다. 그리고 상기 Opcode는 제 1 디바이스(즉, 서버 디바이스)의 가능한 동작들을 제어하기 위한 추가적인 파라미터를 포함할 수 있다. 상기 절차는 상기 제 1 디바이스가 지원되는 페어링 기능 특성의 GAP 동작 필드에서 센트럴 역할을 지원하는 것으로 지시되는 경우에 지원될 수 있다.

[426] LE 센트럴 역할을 제어하기 위한 Opcode는 연결 설립 절차(Connection Establishment procedure) 및/또는 본딩 가능 절차(Bondable procedure) 동작을 지시하는 파라미터들을 포함할 수 있다. 이때, 각 동작은 별도 비트에 매핑될 수 있다.

[427] 여기서, 연결 설립 절차는 자동 연결 설립 절차(Auto Connection Establishment Procedure) 또는 일반 연결 설립 절차(General Connection Establishment Procedure)로 구분될 수 있다.

[428] 센트럴에서 자동 연결 설립 절차가 수행되는 경우, 센트럴은 클라이언트와 상호 작용(interaction) 없이 특정 LE 디바이스에 자동적으로 연결할 수 있다. 즉, 센트럴은 상기 자동 연결 설립 절차를 지시하는 컨트롤 포인트 메시지를 수신한 후, 클라이언트와 추가적인 상호 작용 없이 특정 디바이스와 자동으로 연결할 수 있다. 그러나, 일반 연결 설립 절차가 수행되는 경우, 센트럴은 상기 일반 연결 설립 절차를 수행한 후, 본딩 절차와 같은 동작은 링크 계층 연결이 설립된 후에 클라이언트에 의해 제어될 수 있다. 즉, 센트럴은 상기 일반 연결 설립 절차를 지시하는 컨트롤 포인트 메시지를 수신한 후, 컨트롤 포인트 절차에 따라 한 번 연결을 생성한다.

[429] 이러한 동작을 구성하기 위해, 이 절차는 앞서 설명한 표 13과 같이 동작 필드, 피어 디바이스 ID 필드 및 선택적인 피어 디바이스 IRK가 포함된 파라미터가 필요할 수 있다. 여기서, 피어 디바이스 ID 필드는 연결을 수행할 상대 블루투스 디바이스의 디바이스 주소를 나타낸다.

[430] 본딩 모드(또는 절차)를 지시하는 비트가 1로 설정된 경우, 제 1 디바이스는 페어링 프로세스 후 피어 디바이스와의 다음 연결을 위한 본딩 정보를 저장하기 위해 본딩 절차를 시작할 수 있다.

[431]

[432] 이상에서, 컨트롤 포인트 절차에서 이용되는 GAP 역할에 기반한 Opcode의 구조를 설명하였다. 이하에서 상기 Opcode를 이용하여 디바이스간 페어링/연결을 제어하는 방법을 구체적으로 설명한다.

[433] 도 10은 본 발명이 적용되는 일 실시예로서, 제어 디바이스를 이용하여 디바이스간 연결을 제어하는 방법을 나타내는 흐름도이다.

[434] 제어 디바이스는 제 1 디바이스와 블루투스 연결을 형성할 수 있다(S1001).

- [435] 상기 블루투스 연결을 블루투스 BR/EDR 방식 또는 블루투스 LE 방식으로 형성될 수 있다.
- [436] 제어 디바이스는 제 1 디바이스로 제 1 디바이스가 지원하는 동작과 관련된 특성 정보를 요청하는 판독 요청 메시지를 전송하고(S1002), 제 1 디바이스는 상기 판독 요청 메시지에 대한 응답으로 상기 특성 정보를 포함하는 판독 응답 메시지를 상기 제어 디바이스로 전송한다(S1003).
- [437] 즉, 컨트롤 포인트 절차에 앞서 제어 디바이스(또는 클라이언트 디바이스)는 제 1 디바이스(또는 서버 디바이스)로부터 페어링 및 연결에 대한 제 1 디바이스의 제어 가능한 동작 정보를 수신한다. 상기 특성에 의해 제공된 정보는 제어 디바이스가 상기 제 1 디바이스의 역할 및 동작을 제어하는데 사용된다.
- [438] 또한, 상기 특성 정보는 상기 제 1 디바이스가 지원하는 동작을 나타내는 동작 필드를 포함할 수 있다. 그리고, 상기 동작 필드는 상기 제 1 디바이스가 지원하는 연결 타입, 역할, 모드 또는 절차 중 적어도 하나를 포함할 수 있다.
- [439] 제어 디바이스는 상기 특성 정보에 기초하여 상기 제 1 디바이스로 특정 역할(role)의 수행을 지시하기 위한 특성의 기입을 요청하는 기입 요청 메시지를 전송한다(S1004).
- [440] 상기 특성은 클라이언트 디바이스가 서버의 페어링 및 연결을 관리하는데 사용되는 페어링 컨트롤 포인트 특성일 수 있다.
- [441] 상기 기입 요청 메시지는 상기 특정 역할과 관련된 제어 정보를 포함할 수 있다. 그리고, 상기 제어 정보는 상기 특정 역할을 나타내는 역할 정보 및 상기 특정 역할과 관련된 동작을 나타내는 파라미터 정보를 포함할 수 있다.
- [442] 다시 말해, 제 1 디바이스를 제어하기 위한 컨트롤 포인트 특성의 구조는 상기 제 1 디바이스의 역할을 지시하는 역할 정보와 상기 역할에 관련된 동작들을 지시하는 파라미터들을 포함하여 구성될 수 있다.
- [443] 여기서, 상기 특정 역할은 블루투스 BR/EDR의 억셉터(Acceptor), 블루투스 BR/EDR의 이니시에이터(Initiator), 블루투스 LE의 페리퍼럴(Periphral) 및 블루투스 LE의 센트럴(Central) 중 어느 하나일 수 있다.
- [444] 또한, 상기 파라미터 정보는 제 1 디바이스가 제어 디바이스로부터 요청된 동작들을 피어 디바이스(peer device)와 수행하기 위한 다수의 모드 정보 및/또는 절차 정보를 포함할 수 있다.
- [445] 구체적으로, 제 1 디바이스의 역할이 BR/EDR의 억셉터(Acceptor)인 경우, 상기 제어 정보는 검색 가능 모드(Discoverable mode) 동작, 연결 가능 모드(Connectable mode) 동작 및 본딩 가능 모드(Bondable mode) 동작을 지시하는 파라미터들을 포함할 수 있다.
- [446] 또한, 제 1 디바이스의 역할이 BR/EDR의 이니시에이터(Initiator)인 경우, 상기 제어 정보는 링크 설립 절차(Link Establishment procedure) 및 본딩 절차(Bonding procedure)를 지시하는 파라미터들을 포함할 수 있다.
- [447] 또한, 제 1 디바이스의 역할이 블루투스 LE의 페리퍼럴(Periphral)인 경우, 상기

제어 정보는 검색 가능 모드(Discoverable mode) 동작, 연결 가능 모드(Connectable mode) 동작 및 본딩 가능 모드(Bondable mode) 동작을 지시하는 파라미터들을 포함할 수 있다.

- [448] 또한, 제 1 디바이스의 역할이 블루투스 LE의 센트럴(Central)인 경우, 상기 제어 정보는 연결 설립 절차(Connection Establishment procedure) 및 본딩 가능 절차(Bondable procedure) 동작을 지시하는 파라미터들을 포함할 수 있다.
- [449] 제 1 디바이스는 상기 기입 요청 메시지에 대한 응답으로 기입 응답 메시지를 제어 디바이스로 전송한다(S1005).
- [450] 상기 기입 응답 메시지는 상기 기입 요청에 따른 특정 역할의 수행 결과를 나타내는 결과 코드를 포함할 수 있다.
- [451]
- [452] 본 발명에 따르면, 역할과 이에 관련된 동작들을 하나의 커맨드로 구성함으로써(예를 들어, 블루투스 LE의 광고 절차와 관련된 동작(또는 모드)인 검색 가능 모드(Discoverable Mode)와 연결 가능 모드(Connectable Mode)를 하나의 커맨드를 통해 지시함으로써) 클라이언트 디바이스와 서버 디바이스 간 불필요한 상호 작용을 줄이고, 컨트롤 포인트 절차 운영의 효율성을 향상시킬 수 있다.
- [453] 또한, 본 발명에 따르면 역할을 기반으로 컨트롤 포인트 절차가 수행되기 때문에, 연결 타입(BR/EDR 트랜스포트 또는 LE 트랜스포트)를 지시하기 위한 베어러 타입 서브 필드(1 byte)가 컨트롤 포인트 특성에서 삭제될 수 있다.
- [454] 또한, 본 발명에 따르면 서버 디바이스(또는 GATT 서버)의 동작을 효율적으로 제어할 수 있다.
- [455]
- [456] 도 11은 본 발명이 적용될 수 있는 일 실시예로서, 제어 디바이스를 이용하여 디바이스 간 LE 연결을 제어하는 방법을 나타내는 흐름도이다.
- [457] 도 11을 참조하면, 제 1 디바이스에 대하여 LE 센트럴 역할 및 이에 관련된 동작들을 수행하도록 지시하는 경우를 가정한다.
- [458] 제어 디바이스는 제 1 디바이스로부터 광고 메시지를 수신한다(S1101).
- [459] 제어 디바이스는 상기 광고 메시지에 기초하여 상기 제 1 디바이스로 연결 요청 메시지를 전송한다(S1102).
- [460] 제어 디바이스는 제 1 디바이스로 페어링 기능 특성을 요청하는 판독 요청 메시지를 전송한다(S1103).
- [461] 즉, 제어 디바이스는 제 1 디바이스로 상기 제 1 디바이스가 지원하는 지원 가능한 동작 정보를 요청하기 위하여 판독 요청 메시지를 전송한다.
- [462] 제 1 디바이스는 제어 디바이스로 상기 페어링 기능 특성을 포함하는 판독 응답 메시지를 전송한다(S1104).
- [463] 즉, 제 1 디바이스는 제어 디바이스로 상기 제 1 디바이스가 지원하는 동작들에 관련된 정보를 전송한다. 이 경우, 상기 판독 응답 메시지는 상기 제 1

디바이스가 지원하는 동작을 나타내는 동작 필드를 포함할 수 있고, 상기 동작 필드는 상기 제 1 디바이스가 지원하는 연결 타입, 역할 모드 또는 절차 중 적어도 하나를 포함할 수 있다.

- [464] 제어 디바이스는 제 1 디바이스로 센트럴 역할 및 이에 관련된 동작들의 수행을 지시하는 페어링 컨트롤 포인트 특성의 기입을 요청하는 기입 요청 메시지를 전송하고(S1105), 상기 제 1 디바이스는 상기 기입 요청 메시지에 대한 응답으로 기입 응답 메시지를 전송한다(S1106).
- [465] 전술한 바와 같이, LE 센트럴 역할을 제어하기 위한 Opcode는 연결 설립 절차(Connection Establishment procedure) 및/또는 본딩 가능 절차(Bondable procedure) 동작을 지시하는 파라미터들을 포함할 수 있다. 이때, 각 동작은 별도 비트에 매핑될 수 있다.
- [466] 페리퍼럴 역할 및 이에 관련된 동작들을 명령하는 경우에도 앞서 설명한 S1101 내지 S1106 단계와 동일한 절차로 컨트롤 포인트 절차가 수행될 수 있다.
- [467] 즉, 제어 디바이스는 제 2 디바이스로부터 광고 메시지를 수신한다(S1107). 제어 디바이스는 상기 광고 메시지에 기초하여 상기 제 2 디바이스로 연결 요청 메시지를 전송한다(S1108). 제어 디바이스는 제 2 디바이스로 페어링 기능 특성을 요청하는 관독 요청 메시지를 전송한다(S1109). 제 2 디바이스는 제어 디바이스로 상기 페어링 기능 특성을 포함하는 관독 응답 메시지를 전송한다(S1110). 제어 디바이스는 제 2 디바이스로 페리퍼럴 역할 및 이에 관련된 동작들의 수행을 지시하는 페어링 컨트롤 포인트 특성의 기입을 요청하는 기입 요청 메시지를 전송하고(S1111), 상기 제 2 디바이스는 상기 기입 요청 메시지에 대한 응답으로 기입 응답 메시지를 전송한다(S1112).
- [468] 여기서, LE 페리퍼럴 역할을 제어하기 위한 Opcode는 검색 가능 모드(Discoverable mode) 동작, 연결 가능 모드(Connectable mode) 동작, 프라이버시 모드(Privacy mode) 동작 및/또는 본딩 가능 모드(Bondable mode) 동작을 지시하는 파라미터들을 포함할 수 있고, 각 동작은 별도 비트에 매핑될 수 있다.
- [469] 상기 S1107 내지 S1112 단계는 선택적인 단계로서, 생략될 수 있다. 즉, 제어 디바이스는 LE 센트럴 역할을 수행하는 디바이스 또는 LE 페리퍼럴 역할을 수행하는 디바이스에 대하여 컨트롤 포인트 절차를 수행할 수 있지만, 반드시 제 1 디바이스(또는 서버 디바이스) 및 제 2 디바이스(또는 피어 디바이스) 모두에 대하여 컨트롤 포인트 절차를 수행하여야 하는 것은 아니다.
- [470] 이후, 상기 제 1 디바이스와 상기 제 2 디바이스는 상기 제어 디바이스로부터 수신한 컨트롤 포인트 특성에 기초하여 연결 절차를 수행한다.
- [471] 구체적으로, 제 2 디바이스는 제 1 디바이스로 광고 메시지를 전송한다(S1113).
- [472] 상기 제 2 디바이스가 제어 디바이스로부터 LE 페리퍼럴 역할 및 이에 관련된 동작들을 지시하는 컨트롤 포인트 특성의 기입 응답 요청 메시지를 수신한 경우, 상기 제 2 디바이스는 상기 컨트롤 포인트를 기반으로 하여 광고 메시지를

- 전송할 수 있다.
- [473] 제 1 디바이스와 제 2 디바이스는 상기 광고 메시지 및 제어 디바이스로부터 수신한 컨트롤 포인트에 기초하여 연결을 형성한다(S1114).
- [474] 제 1 디바이스 및/또는 제 2 디바이스는 제어 디바이스로 지시 메시지를 전송한다(S1115).
- [475] 상기 지시 메시지는 제 1 디바이스와 제 2 디바이스간의 연결 절차 수행 결과를 나타내는 결과 코드를 포함할 수 있다.
- [476]
- [477] 전술한 바와 같이, 제어 디바이스는 제 1 디바이스가 개인 정보 보호 모드(Privacy Mode)로 동작하도록 지시할 수 있다. 이하에서 IRK를 이용한 컨트롤 포인트 절차를 살펴 본다.
- [478] LE 트랜스포트(transport)에서 블루투스 주소의 타입은 공공 디바이스 주소(public device address)와 임의 디바이스 주소(random device address)로 나뉘질 수 있다. 여기서, 임의 디바이스 주소는 고정 디바이스 주소(static device address)와 전용 디바이스 주소(private device address)로 나뉘질 수 있다.
- [479] 그리고, 상기 전용 디바이스 주소는 분석 가능하지 않은 경우(non-resolvable)와 분석 가능한 경우(resolvable)로 나뉘지는데, 상기 전용 디바이스 주소가 분석 가능한 경우, IRK(identity resolving key)(식별자 분석 키)가 필요하다.
- [480] 상기 IRK는 RPA(resolvable private address)를 생성하거나 분석하기 위해서 필요하다. 또한, IRK 쌍(pair)은 로컬 디바이스 및 피어 디바이스가 서로 상대방의 디바이스 주소를 분석하기 위하여 사용될 수 있다.
- [481] 임의 주소인 디바이스의 주소는 IRK가 있는 경우에만 분석할 수 있다.
- [482] 제 1 디바이스(즉, 서버 디바이스)의 지원 가능한 동작을 나타내기 위한 지원되는 페어링 기능(supported pairing feature) 특성을 통해 상기 제 1 디바이스는 프라이버시 기능의 지원 여부를 제어 디바이스에 지시할 수 있다.
- [483] 또한, 페어링 컨트롤 포인트를 이용하여 LE 페리퍼럴과 LE 센트럴의 연결/페어링을 관리할 수 있다.
- [484] LE 페리퍼럴 또는 LE 센트럴을 제어할 때, 피어 디바이스의 주소(또는 ID)가 RPA인 경우, 상기 페어링 컨트롤 포인트에 피어 디바이스의 IRK가 추가될 수 있다.
- [485] LE 페리퍼럴 역할의 디바이스가 분석 가능한 주소 전용 특성(Resolvable Private Address Only Characteristic)을 가지는 경우, LE 페리퍼럴 역할의 디바이스는 분석 가능한 개인 주소(resolvable private address)로 광고할 수 있다. 만약 피어 디바이스에 IRK가 없으면, 피어 디바이스는 상기 LE 페리퍼럴 역할의 디바이스의 광고를 무시할 수 있다.
- [486] 만약, 프라이버시 모드가 제어 디바이스로부터 지시되는 경우, 제 1 디바이스는 피어 디바이스 ID의 IRK 값을 나타내는 피어 디바이스 IRK를 수신한다. 상기 피어 디바이스 IRK 필드는 전술한 컨트롤 포인트 Opcode에 포함될 수 있다.

- [487] 제 1 디바이스는 피어 디바이스 ID, 피어 디바이스 IRK 및 로컬 IRK를 해당 장치의 분석 목록(resolving list)에 추가할 수 있다.
- [488] 도 12는 본 발명이 적용되는 일 실시예로서, 제어 디바이스를 이용하여 디바이스간 연결을 제어하는 방법을 나타내는 흐름도이다.
- [489] 도 12를 참조하면, 제 1 디바이스에 대하여 LE 센트럴 역할 및 이에 관련된 동작들을 수행하도록 지시하는 경우를 가정한다.
- [490] 제어 디바이스는 제 1 디바이스와 블루투스 LE 연결을 형성하고, 상기 제 1 디바이스의 IRK를 획득한다(S1201). 마찬가지로 제어 디바이스는 제 2 디바이스와 LE 연결을 형성하고, 상기 제 2 디바이스의 IRK를 획득한다(S1202).
- [491] 제어 디바이스는 상기 제 1 디바이스 및/또는 상기 제 2 디바이스의 주소가 임의 주소인 경우, 블루투스 LE 연결을 형성 후에 상기 제 1 디바이스 및/또는 상기 제 2 디바이스로부터 IRK를 획득할 수 있다.
- [492] 또는, 제어 디바이스는 상기 제 1 디바이스 및 상기 제 2 디바이스간의 프라이버시 모드를 통한 연결을 제어하기 위하여 각 디바이스와 RPA를 생성하고 IRK를 수신(또는 획득)할 수도 있다.
- [493] 제어 디바이스는 제 1 디바이스 및 제 2 디바이스와 지원되는 페어링 기능 절차를 수행한다(S1203).
- [494] 즉, 제어 디바이스는 제 1 디바이스 및 제 2 디바이스로 제어 가능한 동작들에 관련된 정보를 요청하기 위하여 지원되는 페어링 기능 특성을 포함하는 판독 요청 메시지를 전송하고, 상기 제 1 디바이스 및 상기 제 2 디바이스는 상기 판독 요청 메시지에 대한 응답으로 판독 응답 메시지를 전송한다.
- [495] 제어 디바이스는 상기 제 1 디바이스에 상기 제 2 디바이스(즉, 피어 디바이스)의 IRK가 포함된 페어링 컨트롤 포인트 특성의 기입을 요청하는 기입 요청 메시지를 전송한다(S1204).
- [496] 상기 기입 요청 메시지는 상기 제 1 디바이스에 대하여 LE 센트럴 역할을 수행하도록 지시하는 역할 정보가 포함될 수 있다.
- [497] 제어 디바이스는 상기 제 2 디바이스에 상기 제 1 디바이스의 IRK가 포함된 페어링 컨트롤 포인트 특성의 기입을 요청하는 기입 요청 메시지를 전송한다(S1205).
- [498] 상기 기입 요청 메시지는 상기 제 2 디바이스에 대하여 LE 페리퍼럴 역할을 수행하도록 지시하는 역할 정보가 포함될 수 있다.
- [499] 제 2 디바이스는 RPA가 포함된 광고 메시지를 제 1 디바이스로 전송한다(S1206).
- [500] 상기 광고 메시지를 수신한 제 1 디바이스는 상기 제 2 디바이스의 IRK를 가지고 있기 때문에, 상기 RPA(또는 임의 주소)를 분석할 수 있다.
- [501] 제 1 디바이스는 상기 광고 메시지 및 상기 분석된 상기 제 2 디바이스의 주소를 이용하여 자신의 RPA가 포함된 연결 요청 메시지를 제 2 디바이스로 전송한다(S1207).

- [502] 상기 연결 요청 메시지를 수신한 제 2 디바이스는 상기 제 1 디바이스의 IRK를 가지고 있기 때문에, 상기 RPA(또는 임의 주소)를 분석할 수 있다.
- [503] 제 1 디바이스와 제 2 디바이스는 연결을 형성하고(S1208), 상기 제어 디바이스로 기입 응답 메시지를 전송한다(S1209, 1210).
- [504] 상기 기입 응답 메시지는 상기 기입 요청에 따른 특정 역할의 수행 결과를 나타내는 결과 코드를 포함할 수 있다.
- [505]
- [506] 나아가, 설명의 편의를 위하여 각 도면을 나누어 설명하였으나, 각 도면에 서술되어 있는 실시 예들을 병합하여 새로운 실시 예를 구현하도록 설계하는 것도 가능하다. 그리고, 당업자의 필요에 따라, 이전에 설명된 실시 예들을 실행하기 위한 프로그램이 기록되어 있는 컴퓨터에서 판독 가능한 기록 매체를 설계하는 것도 본 발명의 권리범위에 속한다.
- [507] 본 명세서에 따른 방향 기반 기기 검색 방법은 상기한 바와 같이 설명된 실시 예들의 구성과 방법이 한정되게 적용될 수 있는 것이 아니라, 상기 실시 예들은 다양한 변형이 이루어질 수 있도록 각 실시 예들의 전부 또는 일부가 선택적으로 조합되어 구성될 수도 있다.
- [508] 한편, 본 명세서의 방향 기반 기기 검색 방법은 네트워크 디바이스에 구비된 프로세서가 읽을 수 있는 기록매체에 프로세서가 읽을 수 있는 코드로서 구현하는 것이 가능하다. 프로세서가 읽을 수 있는 기록매체는 프로세서에 의해 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록장치를 포함한다. 프로세서가 읽을 수 있는 기록 매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광 데이터 저장장치 등이 있으며, 또한, 인터넷을 통한 전송 등과 같은 캐리어 웨이브의 형태로 구현되는 것도 포함한다. 또한, 프로세서가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산방식으로 프로세서가 읽을 수 있는 코드가 저장되고 실행될 수 있다.
- [509] 또한, 이상에서는 본 명세서의 바람직한 실시 예에 대하여 도시하고 설명하였지만, 본 명세서는 상술한 특정의 실시 예에 한정되지 아니하며, 청구범위에서 청구하는 본 발명의 요지를 벗어남이 없이 당해 발명이 속하는 기술분야에서 통상의 지식을 가진 자에 의해 다양한 변형실시가 가능한 것은 물론이고, 이러한 변형실시들은 본 발명의 기술적 사상이나 전망으로부터 개별적으로 이해해서는 안 될 것이다.
- [510] 그리고, 당해 명세서에서는 물건 발명과 방법 발명이 모두 설명되고 있으며, 필요에 따라 양 발명의 설명은 보충적으로 적용될 수가 있다.

[511]

### 산업상 이용가능성

- [512] 이상, 전술한 본 발명의 바람직한 실시예는, 예시의 목적을 위해 개시된 것으로,

당업자라면 이하 첨부된 특허청구범위에 개시된 본 발명의 기술적 사상과 그 기술적 범위 내에서, 다양한 다른 실시예들을 개량, 변경, 대체 또는 부가 등이 가능할 것이다.

## 청구범위

- [청구항 1] 블루투스 통신을 이용하여 제어 디바이스가 제 1 디바이스를 제어하는 방법에 있어서,  
 상기 제 1 디바이스와 블루투스 연결을 형성하는 단계;  
 상기 제 1 디바이스가 지원하는 제어 가능한 동작(controllable operation)과 관련된 특성 정보를 요청하는 판독 요청 메시지를 상기 제 1 디바이스로 전송하는 단계;  
 상기 판독 요청 메시지에 대한 응답으로 상기 특성 정보를 포함하는 판독 응답 메시지를 상기 제 1 디바이스로부터 수신하는 단계로서,  
 상기 특성 정보는 상기 제 1 디바이스가 지원하는 동작을 나타내는 동작 필드를 포함하고;  
 상기 특성 정보에 기초하여 상기 제 1 디바이스로 특정 역할(role)의 수행을 지시하기 위한 특성의 기입을 요청하는 제 1 기입 요청 메시지를 전송하는 단계로서,  
 상기 제 1 기입 요청 메시지는 상기 특정 역할과 관련된 제어 정보를 포함하고; 및  
 상기 제 1 기입 요청 메시지에 대한 응답으로 기입 응답 메시지를 상기 제 1 디바이스로부터 수신하는 단계를 포함하되,  
 상기 제어 정보는 상기 특정 역할을 나타내는 역할 정보 및 상기 특정 역할과 관련된 동작을 나타내는 파라미터 정보를 포함하는 방법.
- [청구항 2] 제 1 항에 있어서,  
 상기 동작 필드는 상기 제 1 디바이스가 지원하는 연결 타입, 역할, 모드 또는 절차 중 적어도 하나를 포함하는 방법
- [청구항 3] 제 1 항에 있어서,  
 상기 파라미터 정보는 상기 제 1 디바이스가 상기 제어 디바이스로부터 요청된 동작들을 피어 디바이스(peer device)와 수행하기 위한 다수의 모드 정보 및 절차 정보를 포함하는 방법.
- [청구항 4] 제 1항에 있어서,  
 상기 제 1 디바이스의 피어 디바이스(peer device)와 블루투스 LE 연결을 형성하는 단계; 및  
 상기 피어 디바이스의 주소가 임의 주소(random address)인 경우, 상기 피어 디바이스로부터 상기 임의 주소를 분석하기(resolve) 위한 상기 피어 디바이스의 식별자 분석 키(IRK: Identity resolving key)를 획득하는 단계를 더 포함하고,  
 상기 제어 정보는 상기 피어 디바이스의 식별자 분석 키를 나타내는 파라미터를 더 포함하는 방법.
- [청구항 5] 제 4항에 있어서,

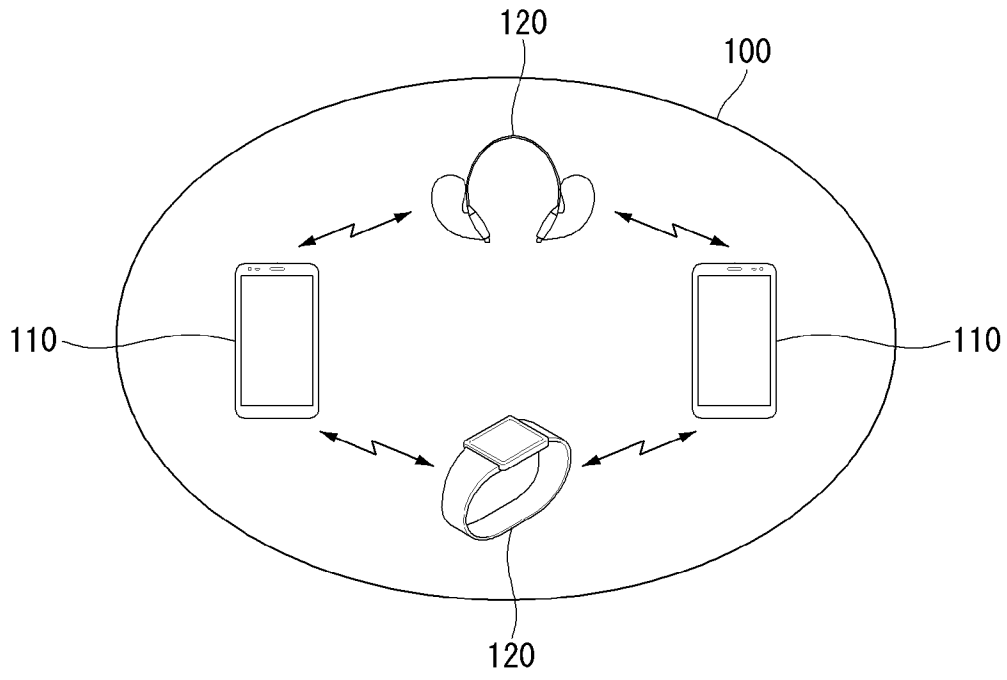
- 상기 제 1 디바이스의 주소가 임의 주소인 경우, 상기 제 1 디바이스로부터 상기 임의 주소를 분석하기 위한 상기 제 1 디바이스의 식별자 분석 키를 획득하는 단계; 및  
상기 피어 디바이스로 상기 제 1 디바이스의 식별자 분석 키를 포함하는 제 2 기입 요청 메시지를 전송하는 단계를 더 포함하는 방법.
- [청구항 6] 블루투스 통신을 이용하여 제어 디바이스에 의해 제 1 디바이스와 피어 디바이스(peer device)간 연결이 제어되는 방법에 있어서, 상기 제 1 디바이스에서 수행되는 방법은,  
상기 제어 디바이스와 블루투스 연결을 형성하는 단계;  
상기 제 1 디바이스가 지원하는 제어 가능한 동작(controllable operation)과 관련된 특성 정보를 요청하는 판독 요청 메시지를 상기 제어 디바이스로부터 수신하는 단계;  
상기 판독 요청 메시지에 대한 응답으로 상기 특성 정보를 포함하는 판독 응답 메시지를 상기 제어 디바이스로 전송하는 단계로서,  
상기 특성 정보는 상기 제 1 디바이스가 지원하는 동작을 나타내는 동작 필드를 포함하고;  
상기 특성 정보에 기초하여 상기 제어 디바이스로부터 특정 역할(role)의 수행을 지시하기 위한 특성의 기입을 요청하는 기입 요청 메시지를 수신하는 단계로서,  
상기 기입 요청 메시지는 상기 특정 역할과 관련된 제어 정보를 포함하고;  
및  
상기 기입 요청 메시지에 대한 응답으로 기입 응답 메시지를 상기 제어 디바이스로 전송하는 단계를 포함하되,  
상기 제어 정보는 상기 특정 역할을 나타내는 역할 정보 및 상기 특정 역할과 관련된 동작을 나타내는 파라미터 정보를 포함하는 방법.
- [청구항 7] 제 6항에 있어서,  
상기 파라미터 정보는 상기 제 1 디바이스가 상기 제어 디바이스로부터 요청된 동작들을 상기 피어 디바이스와 수행하기 위한 다수의 모드 정보 및 절차 정보를 포함하는 방법.
- [청구항 8] 제 6항에 있어서,  
상기 제어 정보에 기초하여 피어 디바이스와 연결을 형성하는 단계를 더 포함하는 방법.
- [청구항 9] 제 6항에 있어서,  
상기 피어 디바이스의 주소가 임의 주소(random address)인 경우, 상기 제어 정보는 상기 피어 디바이스로부터 상기 임의 주소를 분석하기(resolve) 위한 상기 피어 디바이스의 식별자 분석 키(IRK: Identity resolving key)를 더 포함하는 방법.
- [청구항 10] 제 9항에 있어서,

- 상기 피어 디바이스로부터 상기 임의 주소가 포함된 광고 메시지를 수신하는 단계;  
 상기 피어 디바이스의 식별자 분석 키를 이용하여 상기 임의 주소를 분석하는 단계; 및  
 상기 분석된 임의 주소 및 상기 제어 정보에 기초하여 상기 피어 디바이스와 연결을 형성하는 단계를 더 포함하는 방법.
- [청구항 11] 블루투스 통신을 이용하여 제 1 디바이스를 제어하는 제어 디바이스에 있어서,  
 외부와 무선 또는 유선으로 통신하기 위한 통신부; 및  
 상기 통신부와 기능적으로 연결되는 프로세서를 포함하되, 상기 프로세서는,  
 상기 제 1 디바이스와 블루투스 연결을 형성하고,  
 상기 제 1 디바이스가 지원하는 제어 가능한 동작(controllable operation)과 관련된 특성 정보를 요청하는 판독 요청 메시지를 상기 제 1 디바이스로 전송하고,  
 상기 판독 요청 메시지에 대한 응답으로 상기 특성 정보를 포함하는 판독 응답 메시지를 상기 제 1 디바이스로부터 수신하되,  
 상기 특성 정보는 상기 제 1 디바이스가 지원하는 동작을 나타내는 동작 필드를 포함하고,  
 상기 특성 정보에 기초하여 상기 제 1 디바이스로 특정 역할(role)의 수행을 지시하기 위한 특성의 기입을 요청하는 제 1 기입 요청 메시지를 전송하되,  
 상기 제 1 기입 요청 메시지는 상기 특정 역할과 관련된 제어 정보를 포함하고,  
 상기 제 1 기입 요청 메시지에 대한 응답으로 기입 응답 메시지를 상기 제 1 디바이스로부터 수신하되,  
 상기 제어 정보는 상기 특정 역할을 나타내는 역할 정보 및 상기 특정 역할과 관련된 동작을 나타내는 파라미터 정보를 포함하는 장치.
- [청구항 12] 제 11 항에 있어서,  
 상기 동작 필드는 상기 제 1 디바이스가 지원하는 연결 타입, 역할, 모드 또는 절차 중 적어도 하나를 포함하는 장치.
- [청구항 13] 제 11 항에 있어서,  
 상기 파라미터 정보는 상기 제 1 디바이스가 상기 제어 디바이스로부터 요청된 동작들을 피어 디바이스(peer device)와 수행하기 위한 다수의 모드 정보 및 절차 정보를 포함하는 장치.
- [청구항 14] 제 11항에 있어서, 상기 프로세서는,  
 상기 제 1 디바이스의 피어 디바이스(peer device)와 블루투스 LE 연결을 형성하고,

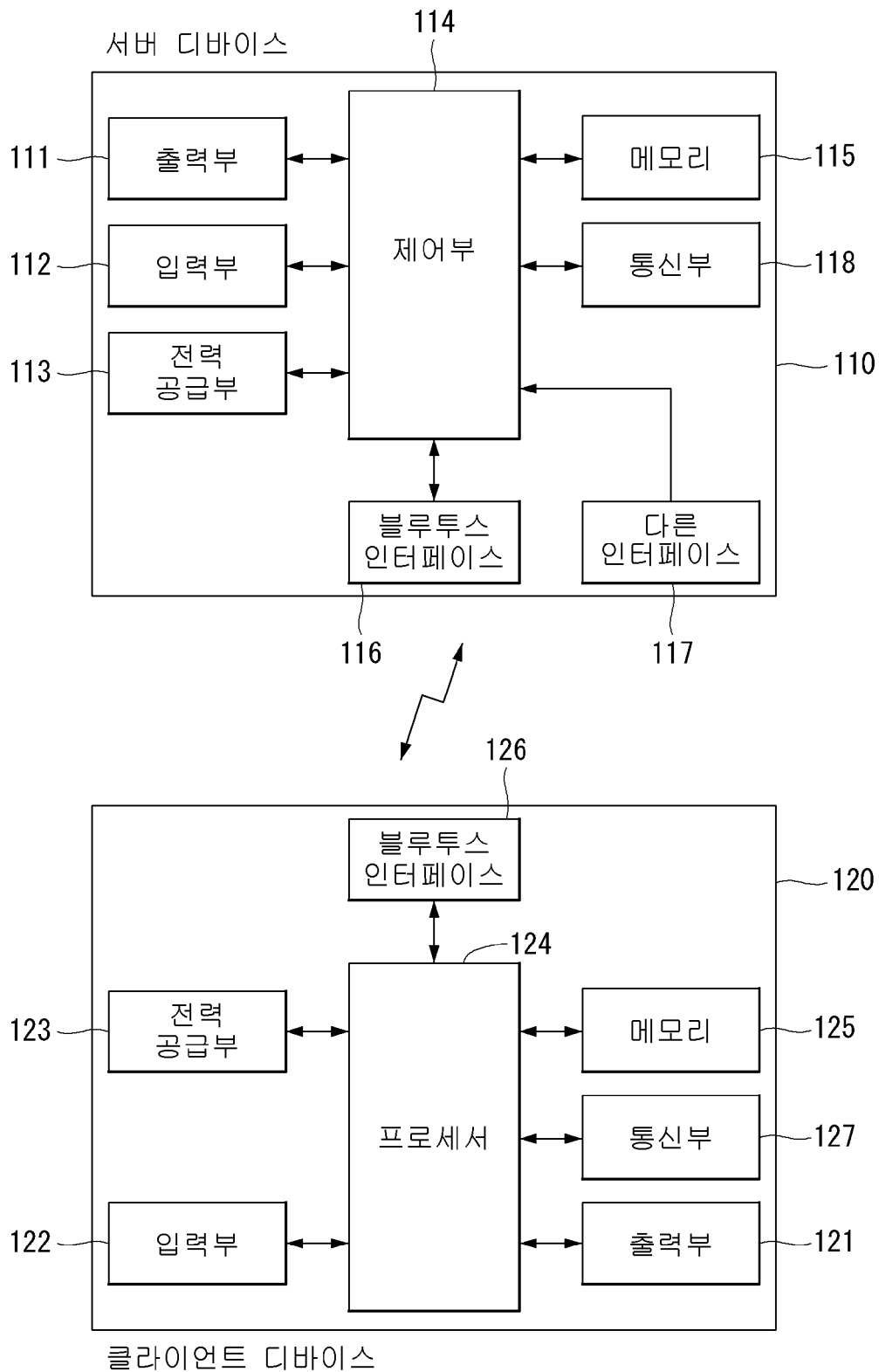
상기 피어 디바이스의 주소가 임의 주소(random address)인 경우, 상기 피어 디바이스로부터 상기 임의 주소를 분석하기(resolve) 위한 상기 피어 디바이스의 식별자 분석 키(IRQ: Identity resolving key)를 획득하고, 상기 제어 정보는 상기 피어 디바이스의 식별자 분석 키를 나타내는 파라미터를 더 포함하는 장치.

- [청구항 15] 제 14항에 이어서, 상기 프로세서는, 상기 제 1 디바이스의 주소가 임의 주소인 경우, 상기 제 1 디바이스로부터 상기 임의 주소를 분석하기 위한 상기 제 1 디바이스의 식별자 분석 키를 획득하고, 상기 피어 디바이스로 상기 제 1 디바이스의 식별자 분석 키를 포함하는 제 2 기입 요청 메시지를 전송하는 장치.

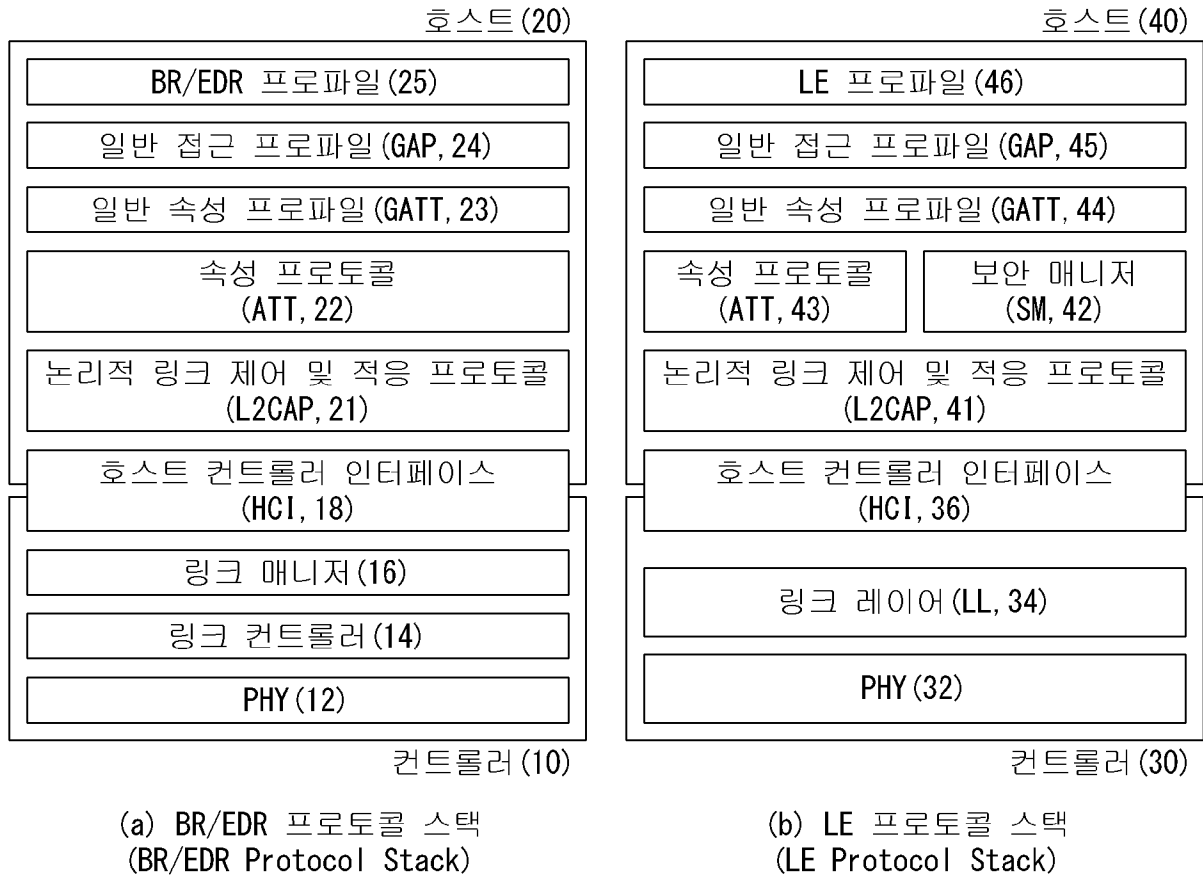
[도 1]



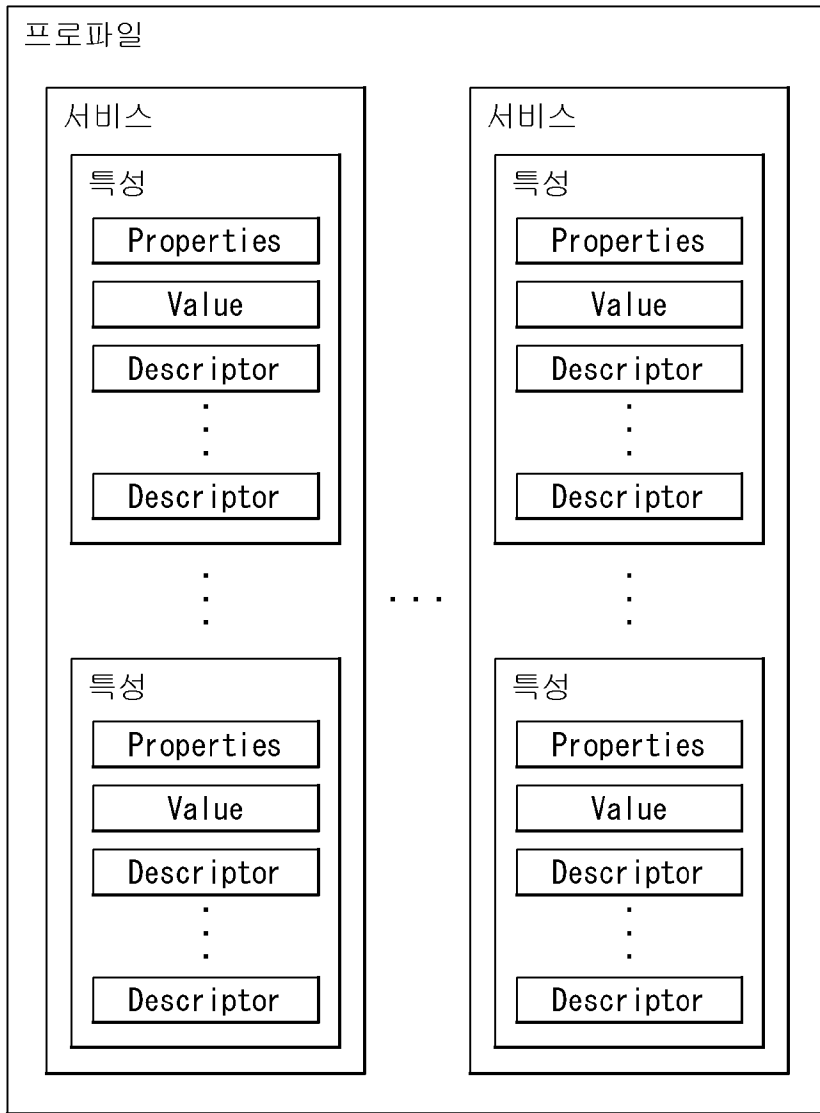
[도2]



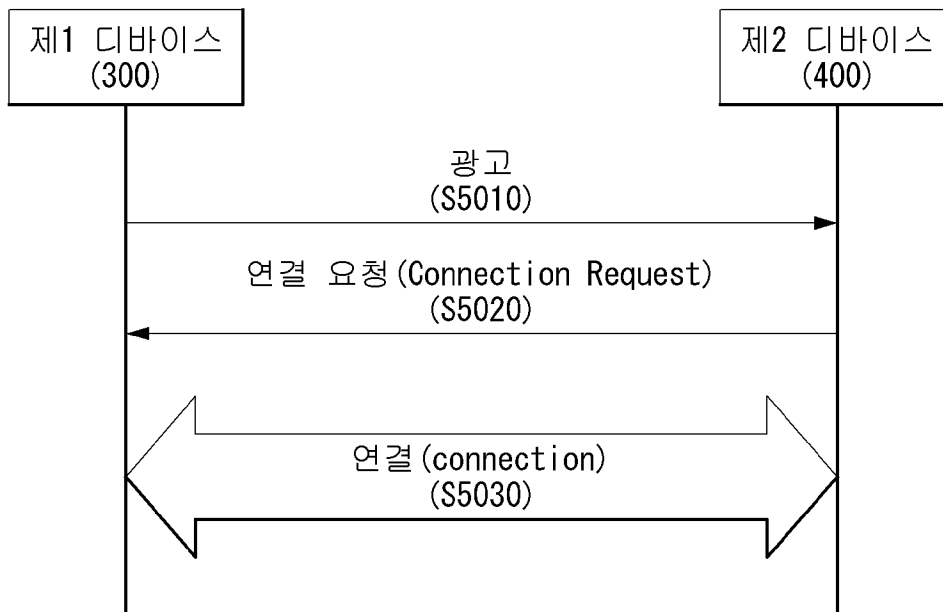
[도3]



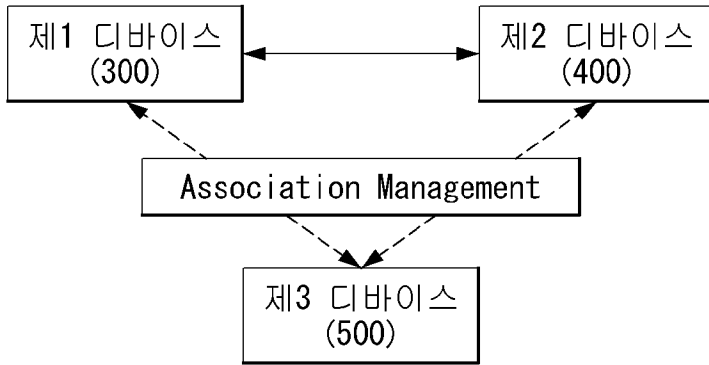
[도4]



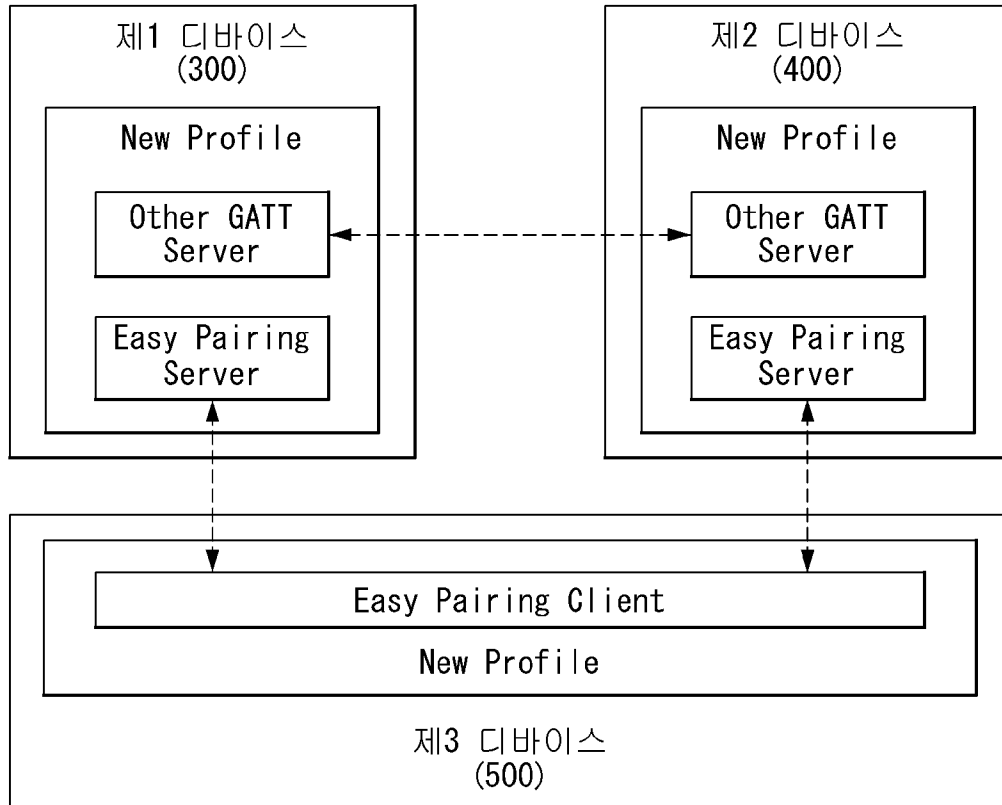
[도5]



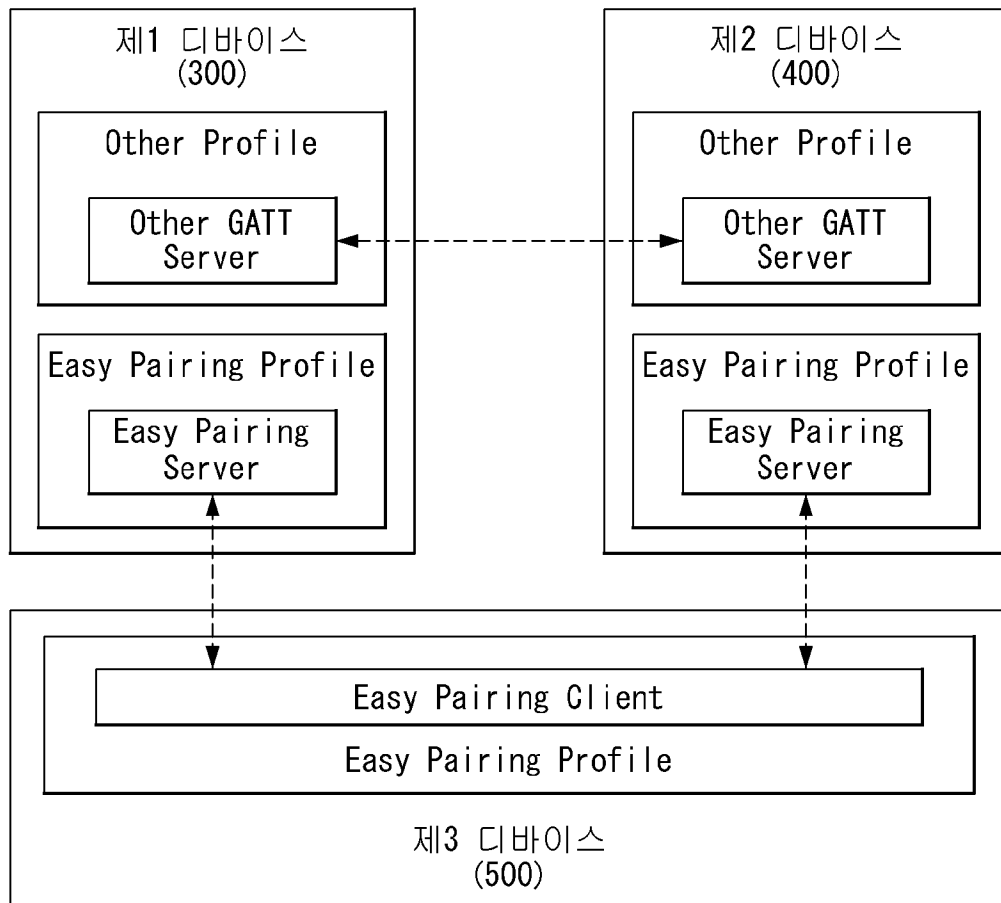
[도6]



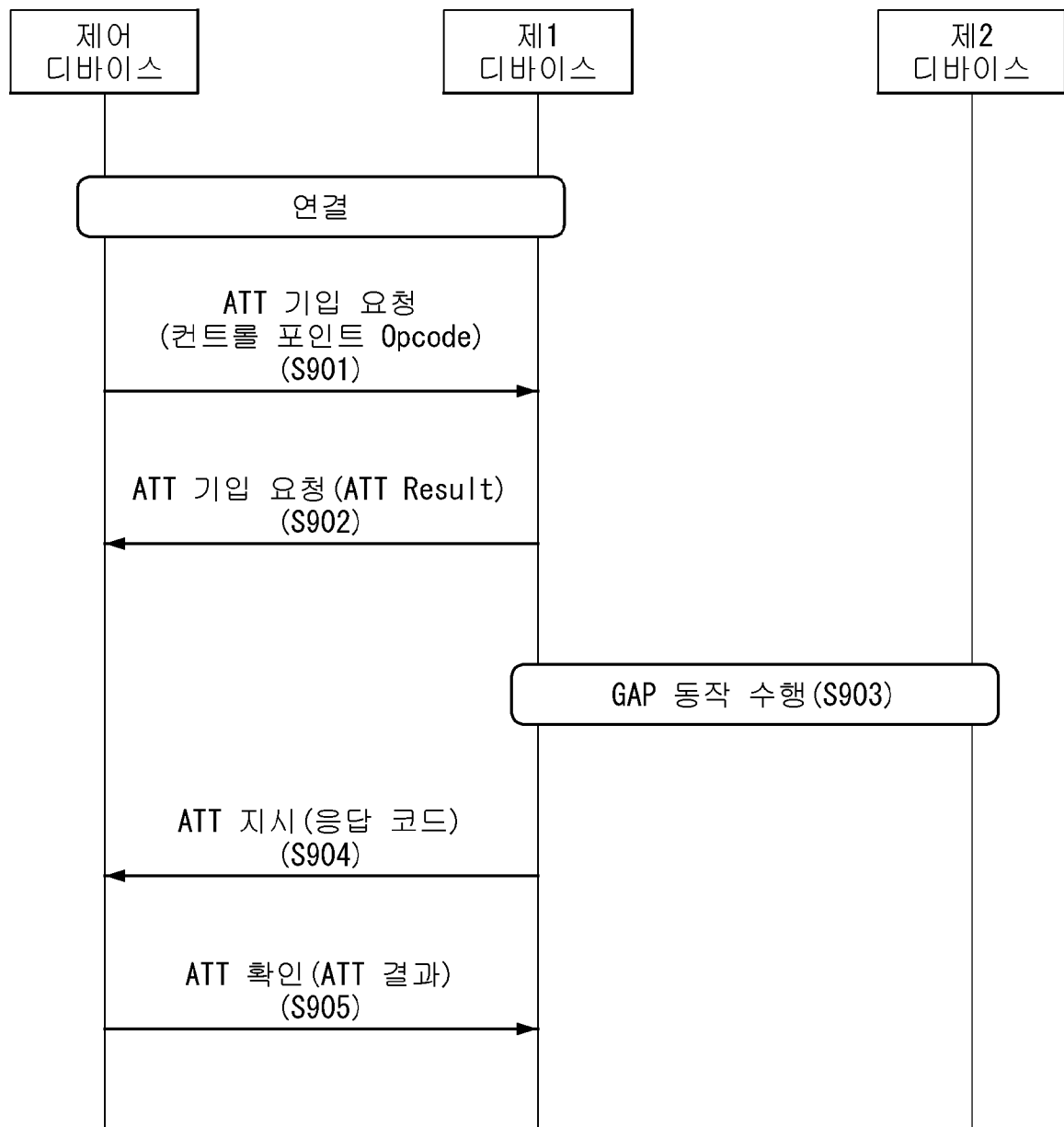
[도7]



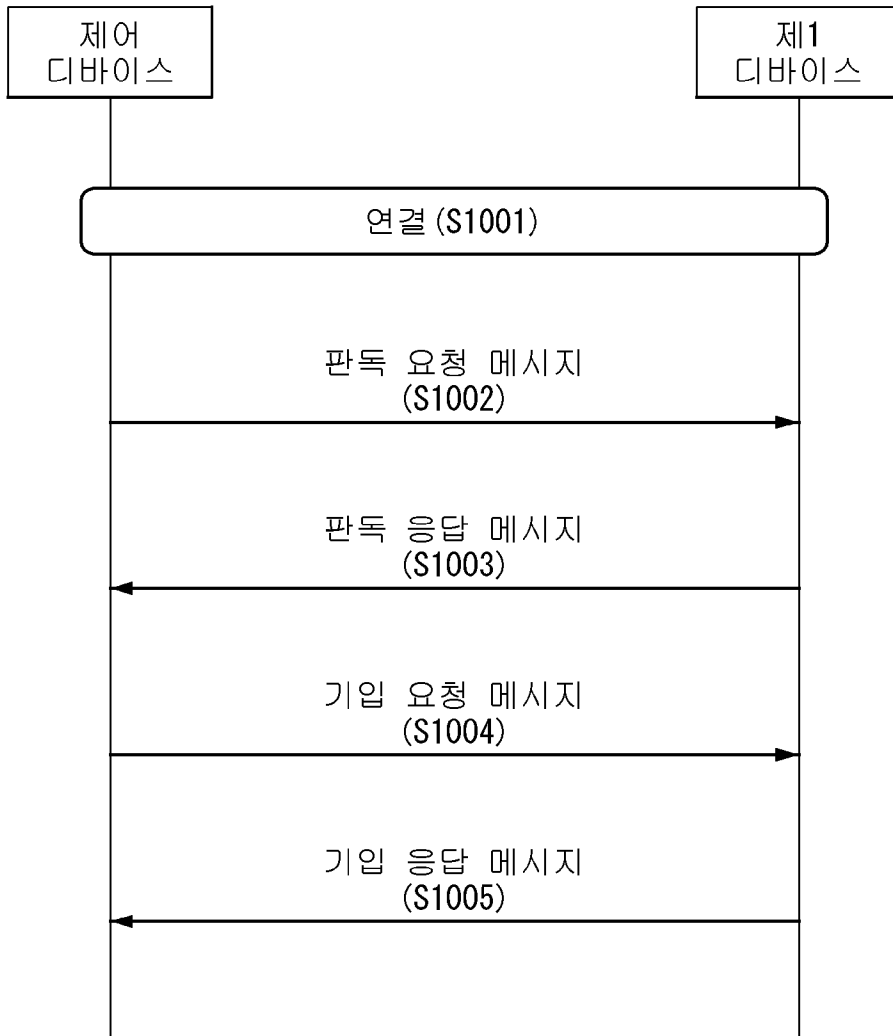
[도8]



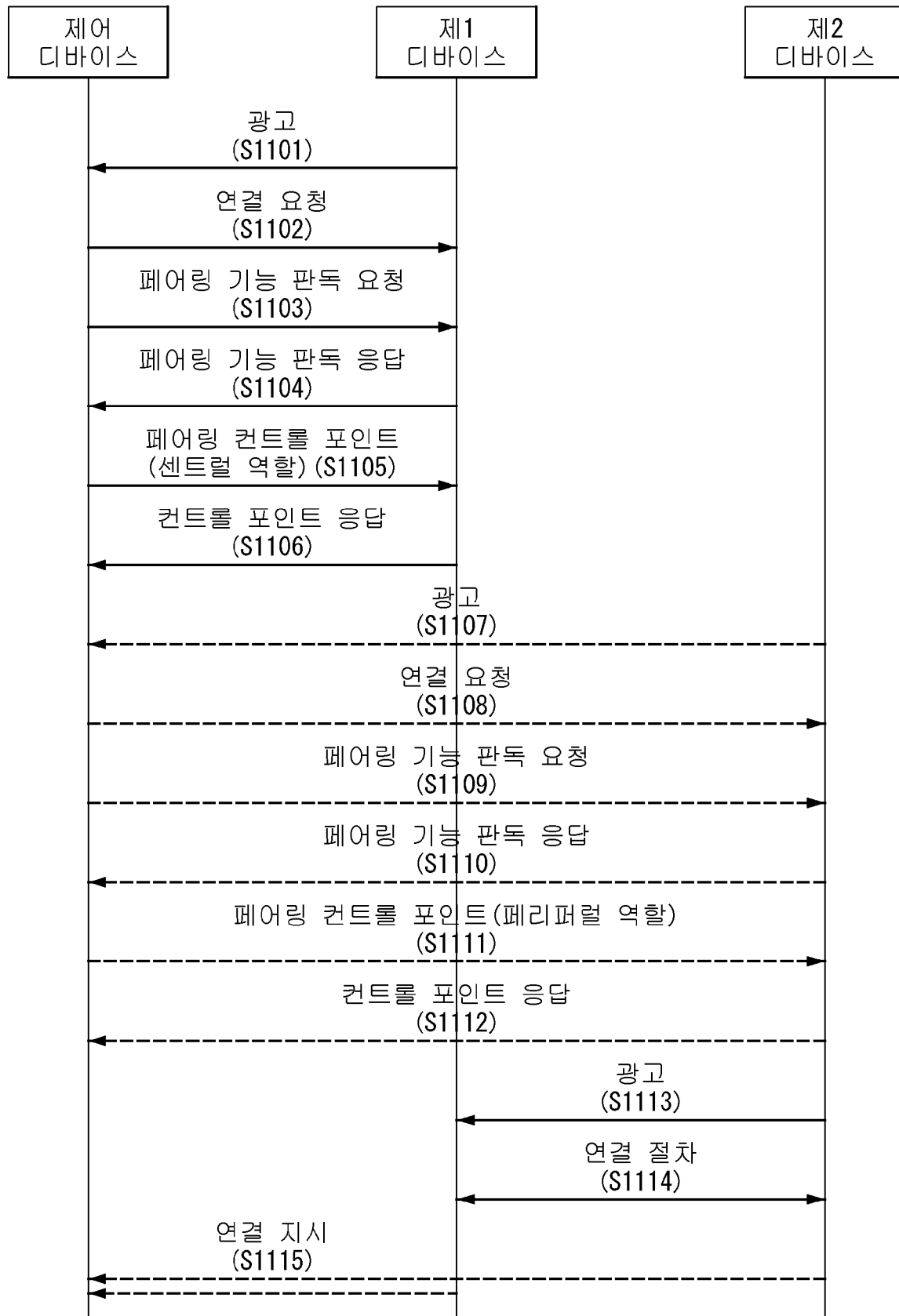
[도9]



[도10]



[도11]



[도12]

