백서

저전력 Bluetooth® 기술, IoT 에 활력을 불어넣다

서문

Renesas Electronics 에서는 전력 소모가 적은 무선 통신이 가능한 저전력 블루투스 MCU 제품들을 제공하고 있다. 오늘날 IoT 시대에는 컴퓨터와 마이크로 컴퓨터 기반 장치뿐만 아니라 전세계에서 사용되는 거의 모든 장치들 간의 정보 공유를 위해 인터넷 연결이 필요하며 저전력 블루투스 기술은 이러한 환경에서 꼭 필요한 무선 통신 방식이다. 여기서는 이를 더 자세히 알아보기 위해 저전력 블루투스 기술 메커니즘에 대해 살펴보고자 한다.

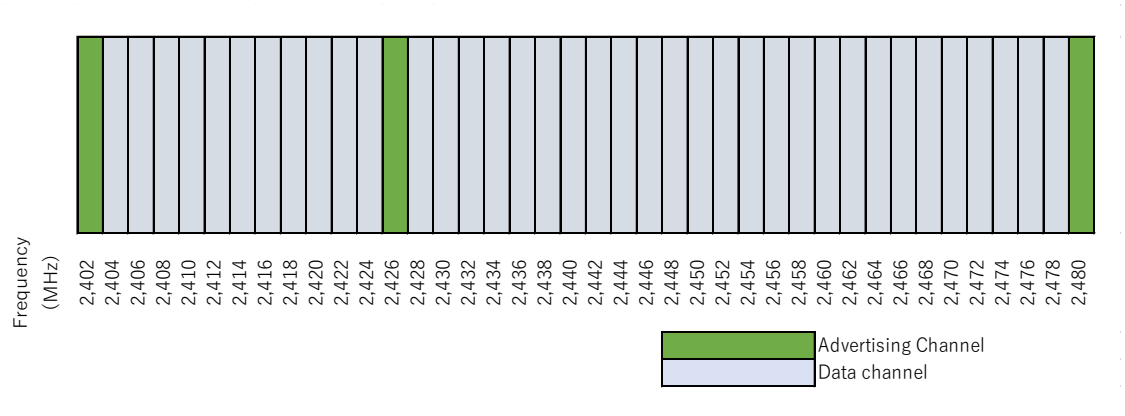
소개

저전력 블루투스 즉, BLE(Bluetooth Low Energy)는 근거리 무선 네트워크인 WPAN(wireless personal area network)을 사용한다. WPAN 은 다른 무선 연결 방식보다 훨씬 적은 전력 소모를 자랑하며 약 10 미터 내에서 데이터 통신이 가능하다. 표준화되지 않은 독립

통신 프로토콜과 같이 다양한 유형의 WPAN 이 존재하지만 표준화된 주요 무선 네트워크로는 지그비(Zigbee)와 블루투스를 들 수 있다. 특히 다수의 스마트폰 응용프로그램에서 사용하는 BLE 는 시장에서 가장 널리 사용되는 방식이다.

BLE 통신 기술에서 말하는 블루투스는 기존의 음성 통신에서의 블루투스 규격과 다르다는 점을 주지해야 한다. BLE 기술은 2.400GHz ~ 2.480GHz 범위에서 80MHz 대역으로 동작하며 2MHz 간격으로 40 개의 채널로 분류된다. 이들 채널은 다음과 같이 두 가지 유형으로 나뉜다.

- 애드버타이즈 채널: 3 개
- 데이터 채널: 37 개



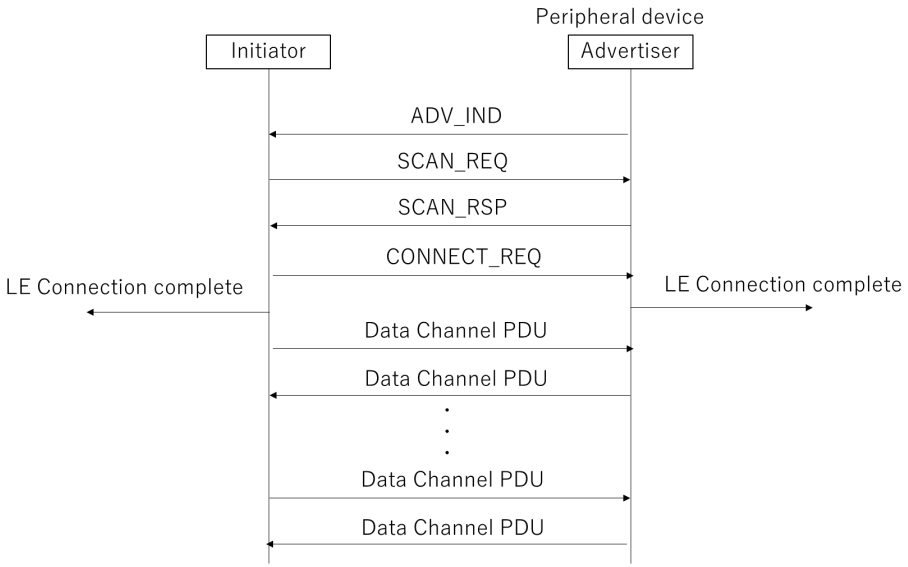
<BLE 통신 주파수 채널>

이 두 유형의 채널은 다음과 같은 방식으로 사용된다:

주변 장치가 애드버타이즈 채널에서 애드버타이즈 패킷을 전송하면 애드버타이즈 패킷은 3 개의 다른 채널을 통해 장치의 위치를 해당 범위에 있는 다른 장치로

전송하고 다른 BLE 장치를 감지하여 무선으로 연결한다. 애드버타이즈 간격은 블루투스 규격에서 정한 20ms 에서 10.24s 로 이 간격은 연결의 용이성과 소비 전력에 영향을 준다.

데이터 채널은 연결이 완료된 후 장치들 간 통신에 사용되며 BLE 에서 데이터 채널은 안정적인 통신을 위해 AFH(Adaptive Frequency Hopping)를 사용하고 연결 간격에 따라 채널들 간에 전송이 전환된다. 여기서 "adaptive"라는 용어는 주파수 간섭을 막기 위한 채널 전환 방식을 의미한다. BLE 는 시간 초과 대기 방식(time out wait)를 적용하여 예를 들어 다중 전송으로 인해 통신이 중단되는 경우에도 통신을 지속시킬 수 있도록 호핑(hopping)을 구현한다. BLE 통신은 일부 채널이 간섭을 받더라도 통신이 중단되지 않도록 구축되어 있다. 블루투스 규격에서 연결 간격은 7.5ms 에서 4s 사이로 정의되어 있고 이 간격은 처리량과 소비 전력에 영향을 준다.



<BLE 동작 흐름 예시>

그럼 이제 블루투스 보안에 대하여 살펴보자.

블루투스 전송 데이터는 암호화가 가능하며 이를 위해 먼저 두 장치 간 고유 정보를 교환하는 “페어링(pairing)”이라는 과정을 거친다. 그 다음 고유한 보안 및 식별 정보를 교환 및 저장하는 "본딩(bonding)" 절차로 이어진다. 즉, 장치들은 보안 기능을 서로 교환하여 페어링되고 교환한 장치 및 페어링 정보를 저장함으로써 본딩된다.

BLE 보안 요구 사항에서는 "보안 모드(Security Mode)"와 "보안 수준(Security Level)"이라는 용어를 사용한다. 각 보안 요구 사항을 충족하려면 페어링이 필요한데 페어링에는 MITM (man-in-the-middle) 공격으로부터 보호하는 인증된 페어링과 보호가 되지 않는 인증되지 않은 페어링으로 구분된다.

BLE 는 다음과 같이 네 가지 유형의 페어링을 사용한다.

- Just Works: 다른 확인 과정 없이 단순히 장치를 선택하는 페어링 방식이다. LE Security Mode 1 Level 2 으로 인증과 MITM 에 대한 보호 기능을 제공하지 않는다.
- Passkey Entry: 6 자리의 인증코드 입력 후 페어링되는 방식이다. LE Security Mode 1 Level 3 으로 인증과 MITM 에 대한 보호 기능을 제공한다.
- Out of Band (OOB): 블루투스 이외의 통신 방식(유선, NFC 등)으로 페어링되며 LE Security Mode 1 Level 3 으로 인증과 MITM 에 대한 보호 기능을 제공한다.
- Numeric Comparison: Just Works 와 동일한 방식으로 페어링되지만 각 장치에서

6 자리 코드를 생성 및 표시하여 일치 여부를 확인하는 추가 과정을 거친다. 이 방식은 블루투스 4.2 에 추가된 LE Secure Connection 에서만 지원된다.

보안 모드	보안 수준	개요	참고
LE Security Mode 1	1	보안 없음(확인 및 암호화 없음)	
	2	인증되지 않은 페어링을 기반으로 암호화됨	Just Works 방식의 페어링
	3	인증된 페어링을 기반으로 암호화됨	Passkey 와 OOB 방식의 페어링
	4	인증된 LE 보안 연결 페어링을 기반으로 암호화됨	RL78/G1D 에서는 지원되지 않음
LE Security Mode 2	1	인증되지 않은 페어링을 기반으로 하는 데이터 서명	
	2	인증된 페어링을 기반으로 하는 데이터 서명	

<LE 보안 모드와 수준>

LE Security Mode 1 Level 3 은 LE Security Mode 2 의 보안 요구 사항을 충족한다.

LE Security Mode 2 에서의 데이터 서명(data signing)은 주로 고속 연결과 연결 해제, 전송에 사용되기 때문에 데이터가 암호화되지 않은 경우에 주로 사용된다. 데이터 서명은 암호화와 인증, 그리고 CSRK (Connection Signature Resolving Key) 방식을 사용한다.

각 페어링 방식에서 키 생성 방식은 장치 구성에 따라 다르다. OOB(Out of Band)는 OOB 를 키 교환 프로토콜로 설정한 경우 MITM 공격으로부터 보호할 수 있다.

Passkey Entry 는 6 자리 임시 키를 사용하는 또 다른 방식으로 장치 간 6 자리 수를 전송하면 MITM 공격 성공률이 1/1,000,000 로 줄어들게 된다. 즉, MITM 공격에 대한 위험이 현저하게 낮아지게 된다. 또한 BLE 통신이 근거리로 제한되기 때문에 공격자가 "수신 대기(listen in)" 상태에 매우 근접해야 한다. 또한 페어링 중 도청 가능성이 낮기 때문에 Passkey Entry 는 실내 사용 시 높은 수준의 보안을 제공한다. Passkey Entry 가 확인된 후 암호화된 연결이 이루어지므로 안심하고 사용할 수 있다.

MITM 보안에 대한 다른 제안사항: 페어링 모드에 한하여 페어링을 실행하거나 물리적으로 제한된 장소에서만 페어링을 허용하도록 시스템을 설정하면 MITM 공격을 방지할 수 있다. 모드 설정은 물리 설정이나 통신 설정으로 가능하다.

RL78/G1D 는 블루투스 4.2 에 추가된 LE Secure 연결 옵션을 지원하지 않는다. LE Secure 연결은 Numeric Comparison 방식으로만 페어링이 가능한데 이를 위해서는 두 장치 모두

디스플레이 기능이 요구된다. 제품에 따라 디스플레이 기능을 장착할 공간을 확보할 수 없는 경우도 있기 때문에 설계 진행 전 이러한 문제를 고려해야 한다.

아래 표에는 페어링 방식과 장치 구조(IO 기능)의 개요가 나타나 있다.

	전송 장치				
응답 장치	디스플레이만 있음	디스플레이 유무	키보드만 있음	입출력 장치 없음	키보드 디스플레이
디스플레이만 있음	Just Works	Just Works	Passkey Entry	Just Works	Passkey Entry
디스플레이 유무	Just Works	Just Works	Passkey Entry	Just Works	Passkey Entry:
		Numeric Comparison (LE Secure 연결)			Numeric Comparison (LE Secure 연결)
키보드만 있음	Passkey Entry	Passkey Entry	Passkey Entry	Just Works	Passkey Entry
입출력 장치 없음	Just Works	Just Works	Just Works	Just Works	Just Works
키보드 디스플레이	Passkey Entry	Passkey Entry	Passkey Entry	Just Works	Passkey Entry
		Numeric Comparison (LE Secure 연결)			Numeric Comparison (LE Secure 연결)

<장치 구조(IO 기능) 맵핑>

아래는 암호화에 사용되는 주 교환 방식을 설명하고 있으며 교환 방식은 여러 단계로 진행된다.

1 단계: 페어링 기능의 교환 (장치 구조 (IO 기능), 인증 요구 등)

2 단계: STK (Short Term Key) 생성. STK 는 1 단계에서 교환된 정보에 기반하여 생성된다.

3 단계: 특정 키 배포(Transport Specific Key Distribution). 2 단계에서 생성된 키를 사용하여 암호화된 링크를 통해 배포가 진행된다.

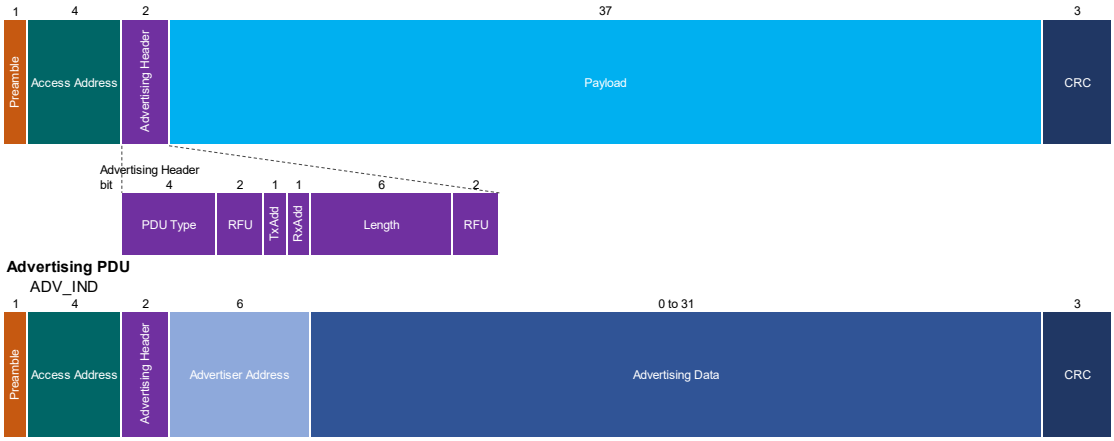
페어링과 암호화, 개인 주소 결정, 서명된 데이터 등에서 처리되는 키 목록은 다음과

같다. 이들 키는 각 단계에서 사용된다.

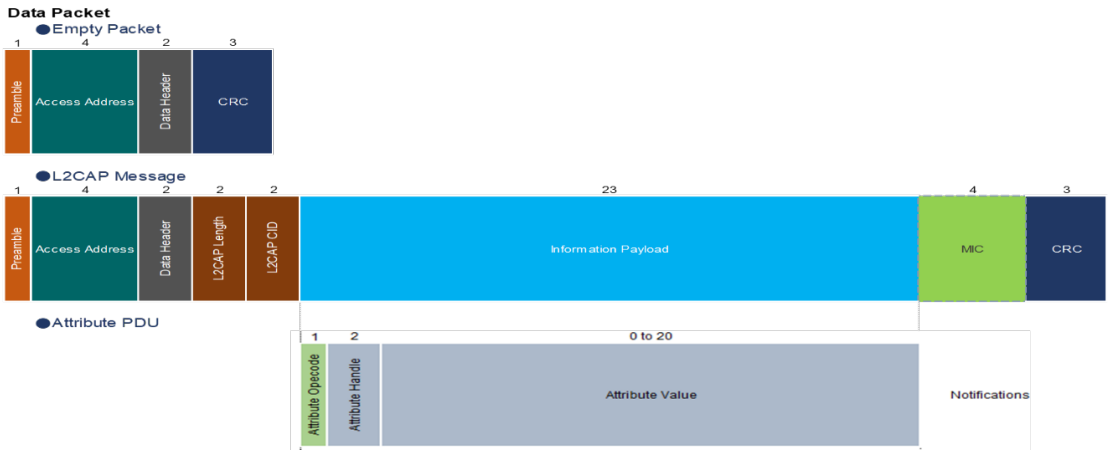
키 유형	설명	생성
TK (Temporary Key)	128 bits 페어링 2 단계에서 STK 생성에 사용됨.	애플리케이션에서 생성
STK (Short Term Key)	128 bits 페어링 2 단계에서 TK 를 사용하여 생성됨. 2 단계 이후 링크 암호화에 사용됨.	BLE 소프트웨어에서 생성
LTK (Long Term Key)	128 bits (키 크기에 대한 합의에 따라 일부 사용됨) 암호화에 필요한 세션 키 생성에 사용됨.	애플리케이션에서 생성
EDIV (Encrypted Diversifier)	16 bits LTK 식별에 사용됨. EDIV 는 LTK 가 배포될 때마다 생성됨.	애플리케이션에서 생성
RAND (Random Number)	64 bits LTK 식별에 사용됨. RAND 는 LTK 가 배포될 때마다 생성됨.	애플리케이션에서 생성
IRK (Identity Resolving Key)	128 bits 무작위 주소 생성 및 결정에 사용됨.	애플리케이션에서 생성
CSRK (Connection Signature Resolving Key)	128 bits 시그니처 생성 및 수신된 데이터의 시그니처 확인을 위해 사용됨.	애플리케이션에서 생성

<저전력 블루투스 키 유형>

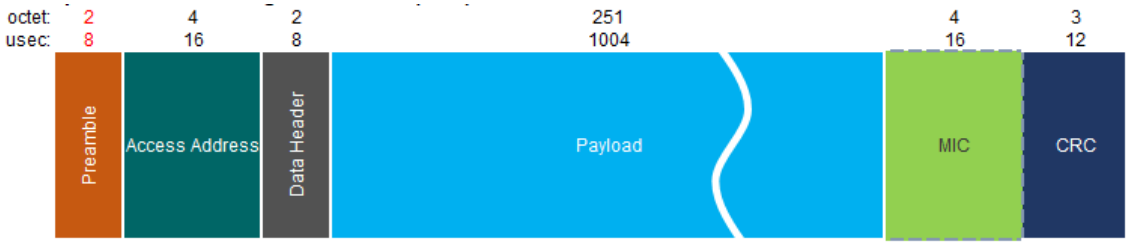
그럼 이제 전송 패킷에 대하여 살펴보기로 한다. 블루투스 4.0 규격(저전력)에서 정한 애드버타이즈 패킷은 애드버타이즈 데이터에 31 바이트를 사용한다. 새로운 블루투스 비콘(beacon)은 저전력 장치가 이 애드버타이즈 패킷을 일정 간격으로 전송하기 위해 사용하는 하드웨어로 그 신호는 비콘 형식으로 수신된다. 비콘(브로드 캐스팅) 장치의 응용예는 뒤에서 설명하기로 한다.



데이터 채널을 사용하여 장치들 간에 통신하는 데 사용되는 패킷은 아래 구성표와 같이 최대 20 바이트를 데이터 전송에 사용할 수 있다. 데이터가 20 바이트를 초과하면 20 바이트 단위로 분할된다.

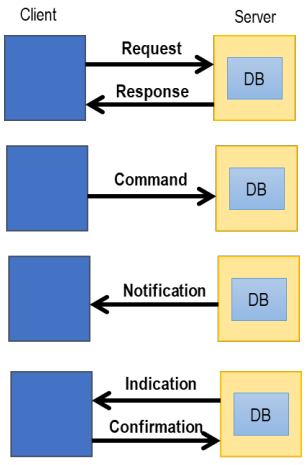


블루투스 4.2 에 추가된 LE Data Extension 을 이용하면 아래와 같이 전송 패킷을 확장할 수 있다. 이 LE Data Extension 은 선택 규격으로 RL78/G1D 에서 지원하지 않는다.



이제 통신 패킷을 처리하는 방법을 살펴보기로 한다. 패킷은 통신 확인/응답이 있는 패킷과 없는 패킷의 두 가지 종류로 구분된다. 통신 처리는 다음과 같은 조합을 가진다.

BLE 응답 통신 과정에서 응답(응답/확인)은 다음 간격의 동작에서 전송된다. 즉, 1s 간격으로 동작 시 1s 후에 응답 전송이 이루어진다. 이는 통신 전송/응답이 2 개의 간격을 두고 이루어짐을 의미한다. 고속 데이터 통신에서는 전송/확인 응답을 보내지 않는 통신 방식을 사용하여 처리 속도를 높일 수 있다. 대신 애플리케이션에서 전송을 확인하도록 설정되어야 한다.



블루투스 저전력 데이터 교환 규격에 대해서는 앞에서 자세히 살펴보았다. 이름에서도 알 수 있듯이 BLE 의 원래 개념은 저전력 동작을 구현하는 것이다. 이를 위해서는 소량의 데이터를 전송하는 것이 더 효과적이며 이를 통해 배터리의 수명을 연장시켜 수년 동안 교체없이 사용할 수 있다. 목표는 블루투스로 저전력 장치와 배터리로 동작하는 애플리케이션에 연결한 다음 인터넷 연결로 데이터를 전송하는 것이다.

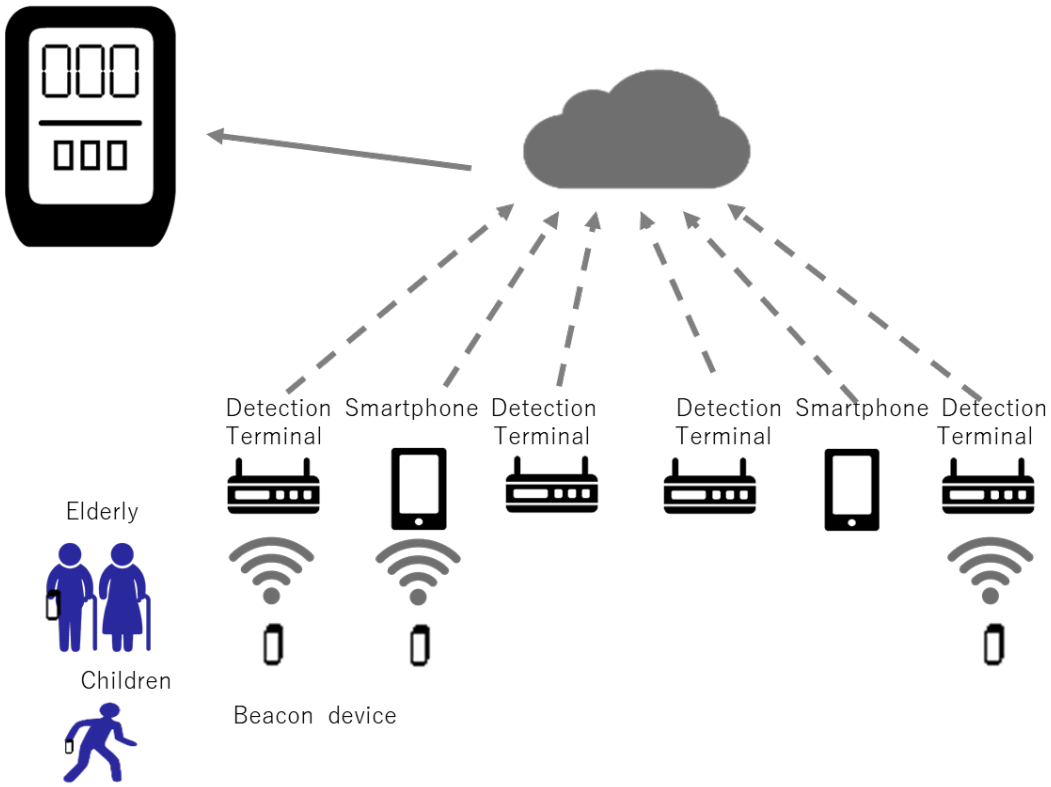
최근 블루투스 규격에서 저전력 블루투스는 블루투스 4.0 을 기반으로 수정되었다. 이 규격에는 대용량, 고속 통신과 장거리 통신이 추가되었다. 2016 년 출시된 블루투스 5 는 이러한 기능이 옵션으로 제공된다.

앞으로 (블루투스 4.0 에서 정한) 저전력 블루투스 코어 표준은 필수 기능이 되어 모든 BLE 호환 제품을 지원할 것이다. 이 BLE 코어 규격을 사용하면 안정적인 연결이 보장되어 향후 많은 장치에서 구현될 전망이다. 또한 BLE 가 연결 문제를 해결하는 데에도 도움이 될 것이다.

그럼 이제 몇 가지 예시 애플리케이션을 살펴보기로 한다. 먼저 기존의 블루투스에서 지원하지 않는 기능인 애드버타이즈 패킷을 전송하여 애플리케이션에 새로운 가능성을 제시하고 있는 비콘 장치에 대하여 알아보고자 한다.

비콘 장치는 주로 노인이나 어린 아이들이 차고 다니는 위치 탐지기로 사용되며 비콘

장치로부터 전파를 수신하기 위한 감지 단말기가 관련 시설에 설치된다. 예를 들어, 감지 단말기는 가정이나 기타 공공 장소 뿐만 아니라 노인 복지 시설이나 학교에 설치된다. 또는 자원봉사자가 비콘 장치에서 전파를 수신하는 앱이 설치된 스마트폰을 사용하기도 한다. 수신된 비콘 정보는 감지 단말기 또는 스마트폰의 위치 정보와 함께 클라우드에 저장된다. 저장된 데이터는 스마트폰에서 위치를 표시하는데 사용되고 이는 비콘 장치에 연결된 가족 구성원이나 보호자만 접근이 가능하다. 비콘 장치에서 BLE 를 사용하면 간병인이 주위에 있지 않을 때에도 환자를 돌볼 수 있다.



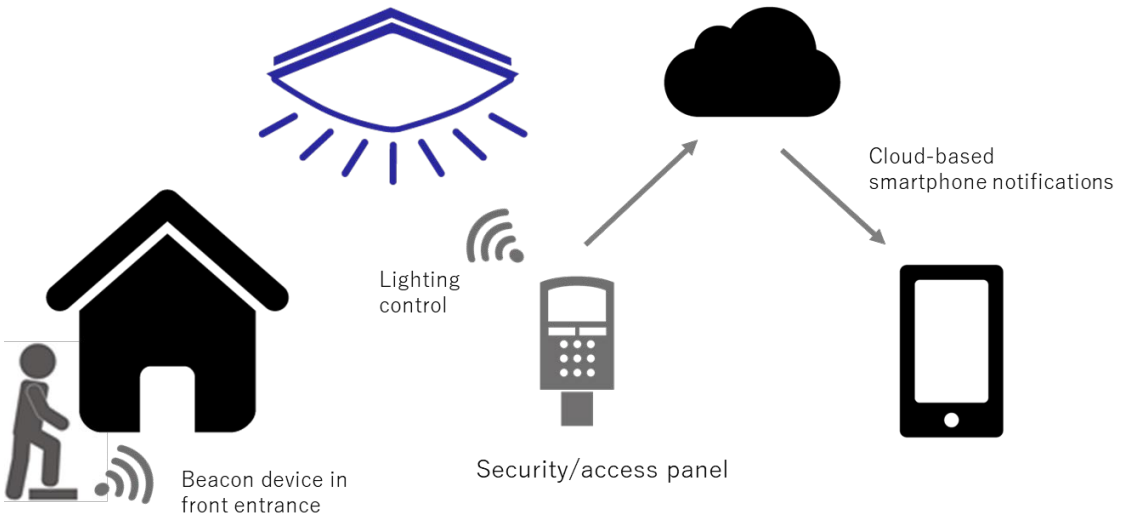
<보호용 위치감지 단말기의 예시>

이 예시는 Renesas 홈페이지에서 설명되어 있으며 아래 링크를 통해 확인이 가능하다.

IoT 기술로 보호용 위치감지 서비스 기능을 향상시켜주는 BLE 솔루션: https://www.renesas.com/promotions/cases/bluetooth-low-energy-1.html

다음은 애드버타이즈 패킷 전송 기능을 구현하는 또 다른 애플리케이션의 예시다. 이 예시에서는 감지 장치에서 BLE 를 활용하고 있는데 비콘 장치를 집 앞에 설치하여 침입을 감지하고 가전 제품을 원격으로 제어한다. 이 애플리케이션은 홈오토메이션을 구현하여 원격 제어장치나 사람이 개입할 필요가 없다.

BLE 는 저전력 소모 표준으로 BLE 장치는 에너지를 거의 사용하지 않고 애드버타이즈 패킷을 전송할 수 있다. 아래 예시에서는 특수 바닥 매트를 밟아 생성한 에너지를 사용하여 비콘(애드버타이즈 패킷)을 전송한다. 매트는 배터리 교체없이 반영구적으로 사용이 가능하며 비콘의 전파는 보안/접속 패널에 수신된다. 사용자는 클라우드를 통해 다른 가족에게 알리고 조명을 제어할 수 있다. 이 애플리케이션은 침입 방지와 노인 간병 등에 활용될 수도 있다.



<감지 장치 애플리케이션의 예시>

커스터마이즈된 비콘 스택은 이러한 방식으로 애드버타이즈 패킷 전송 기능을 이용하여 애플리케이션을 통합하는 비콘 장치에 적용할 수 있다. 이 비콘 스택은 BLE 의 모든 기능을 사용하지 않고도 비콘 장치가 사용하는 애드버타이즈 패킷을 송신하고 수신(스캔)할 수 있도록 해준다.

비콘 스택은 기능이 제한되어 있어 설정이 단순하고 크기가 작다. 사용자는 평가용 버전에서 빌드 기능을 사용하여 프로그램을 컴파일 할 수 있으며 적은 전력 소모로 구동과 작동이 모두 가능하다.

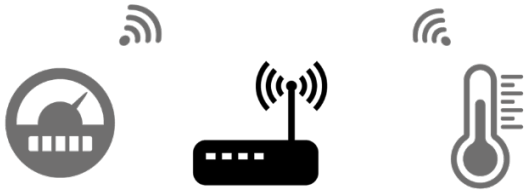
그럼 이제 BLE 장치에 연결한 후 전송된 데이터를 사용하는 애플리케이션을 살펴보자. 이 예시에서 스마트폰은 저전력 무선 인터페이스를 사용하여 손쉽게 데이터를 수집하는 BLE 규격을 지원한다. 대부분의 의료 장비는 BLE 기능을 활용하여

스마트폰에 무선으로 연결할 수 있다. 예시에서 알 수 있듯이 BLE 지원 스마트폰은 심박수 모니터, 혈압 모니터, 욕실 체중계 등 다양한 측정 및 감지 장치에 사용할 수 있다.

<스마트폰 연결 예시>

아래 예시에서처럼 BLE 장치 연결 기반 데이터 통신은 장치들 간의 데이터 전송에 활용될 수 있다.

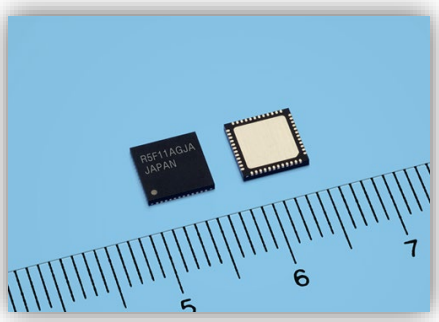
BLE 센서는 BLE 전송 시 최소량의 전력만을 사용하여 BLE 와 LTE/3G 게이트웨이(브리지)를 통해 클라우드에 데이터를 저장하는 데 사용할 수 있다. BLE 는 장거리 전송용 무선 표준을 기반으로 게이트웨이(브리지)의 반대편 장치와 센서단 장치의 데이터 전송에 사용이 가능하다.



<무선 장치 연결 예시>

이처럼 저전력 블루투스 MCU 는 애드버타이즈 패킷 전송 기능을 구현하는 애플리케이션과 BLE 장치에 연결 후 전송 데이터를 사용하는 애플리케이션의 두 가지 방식으로 사용이 가능하다. 이에 따라 Renesas 에서는 저전력 블루투스 프로토콜 스택과 비콘 스택의 두 종류의 소프트웨어 스택을 제공하며 사용자는 용도에 따라 원하는 스택을 선택할 수 있다.

Renesas 또한 블루투스 4.2 인증을 받은 IC 및 모듈 제품을 제공한다. 대량 생산이나 개발 기간, RF 기술의 유무에 상관없이 애플리케이션의 다양한 요구 사항을 충족시킬 수 있는 IC 및 모듈 제품을 보유하고 있다.



RL78/G1D (R5F11A)

RL78/G1D Module (RY0711)

Renesas Electronics 의 Bluetooth® Low Energy 솔루션 제품 링크:

https://www.renesas.com/solutions/bluetooth