3rd May 2013 [BLE] TI CC2540 Mini DK 사용하기 - Advertising Data 형식

1. 들어가기

USB 동글에서 KeyFob을 찾을 때 BTool의 로그창을 보면 아래와 같은 Rx 데이터를 발견할 수 있다.

[3] : <Rx> - 09:58:23.157
-Type : 0x04 (Event)
-EventCode : 0xFF (HCI_LE_ExtEvent)
-Data Length : 0x18 (24) bytes(s)
Event : 0x060D (GAP_DeviceInformation)
Status : 0x00 (Success)
EventType : 0x00 (Connectable Undirect Advertisement)
AddrType : 0x00 (Public)
Addr : 78:C5:E5:A0:0D:4C
Rssi : 0xDB (219)
DataLength : 0x0B (11)
Data : 02:01:05:07:02:03:18:02:18:04:18
[4] : <Rx> - 09:58:23.183
-Type : 0x04 (Event)
-EventCode : 0xFF (HCI_LE_ExtEvent)
-Data Length : 0x19 (25) bytes(s)
Event : 0x060D (GAP_DeviceInformation)
Status : 0x00 (Success)
EventType : 0x04 (Scan Response)
AddrType : 0x00 (Public)
Addr : 78:C5:E5:A0:0D:4C
Rssi : 0xDB (219)
DataLength : 0x0C (12)
Data : 0B:09:4B:65:79:66:6F:62:64:65:6D:6F

로그를 살펴 보면 여러 항목들 중에서 Data 항목에 대해서만 해석을 달지 않고 있음을 알 수 있다. KeyFob은 KeyFobDemo 애플리케이션을 실행하고 있는 중이다. 이제 Data 항목의 각 octet이 어떤 의미를 가지고 있는지 파악해 보자.

2. USB 동글에서 KeyFob 찾기

분석하고자 하는 로그를 얻기 위하여 순서대로 아래의 과정을 수행한다.

1) USB 동글을 PC에 연결한다. 장치 관리자에서 USB 동글의 포트 번호를 확인한다.
2) BTool을 실행한다. 직렬포트 설정 대화 상자에서 USB 동글의 포트 번호를 지정한다. 다른 항목은 기본으로 설정된 값을 사용한다.
3) Keyfob의 오른쪽 버튼(B3)을 눌러 Discoverable 모드로 진입한다.
4) BTool의 Discover/Connect 탭에서 'Discovery' 섹션의 'Scan' 버튼을 누른다. 잠시 후 "Devices Found"의 값이 1로 바뀌는 것을 확인한다.

BTool의 로그창에 EventType이 Connectable Undirect Advertisement와 Scan Response인 Rx 데이터가 나타날 것이다.

3. Rx 데이터의 Data 항목 해석

위에서 제시한 두 Rx 데이터의 Data 항목은 Bluetooth Core Specification 4.0의 Low Energy 부문에서 정의하고 있는 다음 두 가지 형식에 해당한다.

EventType이 Connectable Undirect Advertisement인 Rx 데이터:

PDU 유형이 ADV_IND인 패킷의 **AdvData**

EventType이 Scan Response인 Rx 데이터:

PDU 유형이 SCAN_RSP인 패킷의 **ScanRspData**

AdvData와 ScanRspData의 형식에 대한 설명은 다음 단원에서 제시하였으며 그에 대한 이해를 바탕으로 하여 Data 항목을 해석한 결과는 아래와 같다.

3번 Rx 데이터의 Data 항목 해석: AdvData

Index of octets	Value	Description	Information
0	0x02	Length of this data	
1	0x01	AD Type = Flags	
2	0x05	LE Limited Discoverable Mode, BR/EDR Not Supported	
3	0x07	Length of this data	
4	0x02	AD Type = 16-bit Service UUIDs	More 16-bit UUIDs available
5..6	0x1803	UUID for Link Loss Service	
7..8	0x1802	UUID for Immediate Alert Service	
9..10	0x1804	UUID for Tx Power Service	

[http://4.bp.blogspot.com/-UoCEDgUAbj4/UYPMI1UXFqI/AAAAAAAAAOI/afrSGnueEvc/s1600/AdvData+for+ADV_IND.png]

4번 Rx 데이터의 Data 항목 해석: ScanRspData

Index of octets	Value	Description	Information
0	0x0B	Length of this data	
1	0x09	AD Type = Local Name	Complete local name
2	0x4B	K	
3	0x65	e	
4	0x79	y	
5	0x66	f	
6	0x6F	o	
7	0x62	b	
8	0x64	d	
9	0x65	e	
10	0x6D	m	
11	0x6F	o	

[http://4.bp.blogspot.com/-G7wllaXykmY/UYPMSmMpPGI/AAAAAAAAAOQ/ebLPqsNfxxA/s1600/ScanRspData+for+SCAN_RSP.png]

AD Type의 값이 0x02인 경우는 장치가 제공하는 서비스가 더 많이 있지만 여기서는 일부 목록만 보여준다는 것을 의미한다. 이 경우에는 장치와 연결을 맺은 후 모든 서비스 찾기 기능을 실행하면 전체 목록을 알아낼 수 있다.

4. advertising 채널의 패킷 형식 이해

4.1 물리 계층

- 2.4 GHz ISM 밴드 (2400 ~ 2483.5 MHz)
- 2MHz 넓이로 40개의 RF 채널 구성
  Center frequencies
  f = 2402 + k*2 MHz, k = 0, …, 39

4.2 연결 계층

- 3개의 advertising 채널
  장치 찾기, 연결 시작하기, 데이터 방송에 사용함.
- 37개의 data 채널
  연결된 장치간 통신을 위해 사용함.

4.3 패킷 형식

- advertising 채널, data 채널 모두 아래 패킷 형식을 따른다.
  Preamble (1) + Access Address (4) + PDU (2 ~ 39) + CRC (3)

4.4 advertising 채널의 PDU 형식

- PDU size: 2 ~ 39 octets
  Header (2) + Payload (0 ~ 37)
- Header 형식
  PDU Type (4 bits) + RFU (2 bits) + TxAdd (1 bit) + RxAdd (1 bit) + Length (6 bits) + RFU (2 bits)
- PDU Type에 따른 Payload 형식
  ADV_IND : AdvA (6 octets) + AdvData (0 ~ 31 octets)

ADV_DIRECT_IND : AdvA (6 octets) + InitA (6 octets)
ADV_NONCONN_IND : AdvA (6 octets) + AdvData (0 ~ 31 octets)
SCAN_REQ : ScanA (6 octets) + AdvA (6 octets)
SCAN_RSP : AdvA (6 octets) + ScanRspData (0 ~ 31 octets)
ADV_SCAN_IND : AdvA (6 octets) + AdvData (0 ~ 31 octets)

4.5 AdvData와 ScanRspData의 형식

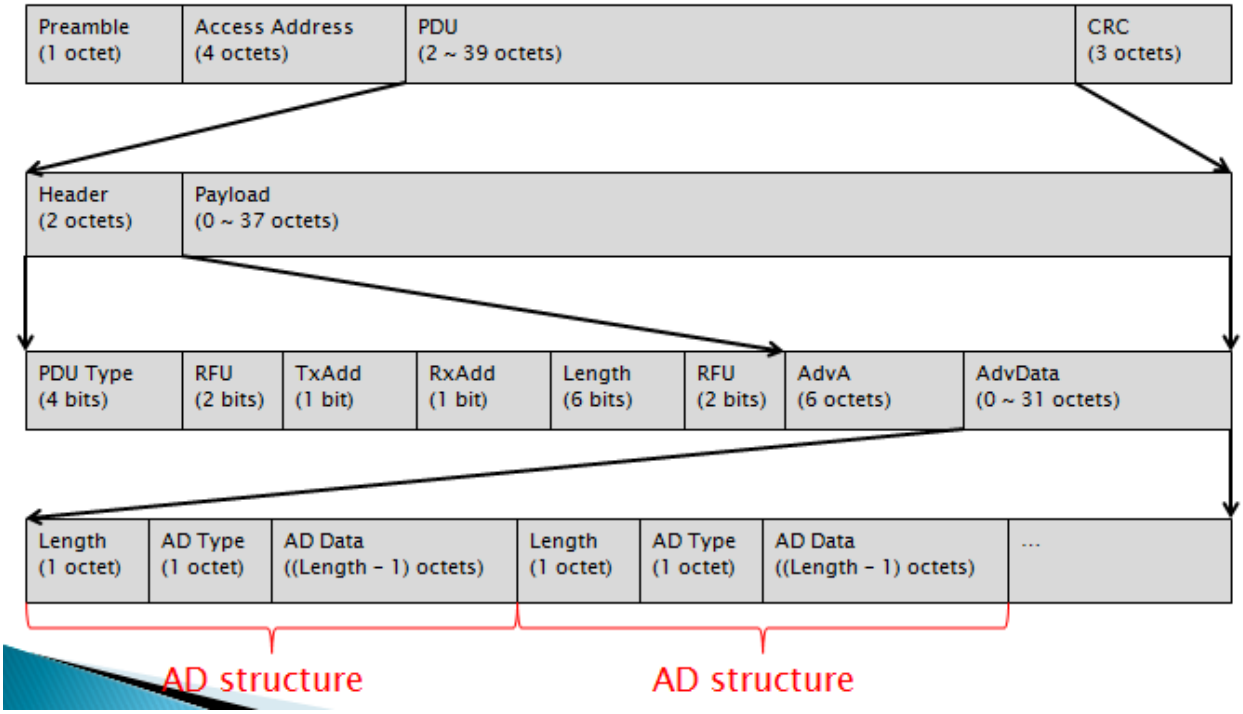
AdvData와 ScanRspData는 동일한 형식을 따르며 연속적으로 이어지는 AD structure들로 이루어진다. AD structure의 형식은 아래와 같다.

Length (1 octet) + AD Type (1 octet) + AD Data (Length - 1)

4.6 AD Type과 AD Data 형식

0x01 : Flags - **b0 LE Limited Discoverable Mode**
- b1 LE General Discoverable Mode
- **b2 BR/EDR Not Supported** (i.e. bit 37 of LMP Extended Feature bits Page 0)
- b3 Simultaneous LE and BR/EDR to Same Device Capable (Controller) (i.e. bit 49 of LMP Extended Feature bits Page 0)
- b4 Simultaneous LE and BR/EDR to Same Device Capable (Host) (i.e. bit 66 of LMP Extended Feature bits Page 1)

0x02 : 16-bit Service UUIDs - **More 16-bit UUIDs available**
0x03 : 16-bit Service UUIDs - Complete list of 16-bit UUIDs available
0x04 : 32-bit Service UUIDs - More 32-bit UUIDs available
0x05 : 32-bit Service UUIDs - Complete list of 32-bit UUIDs available
0x06 : 128-bit Service UUIDs - More 128-bit UUIDs available
0x07 : 128-bit Service UUIDs - Complete list of 128-bit UUIDs available
0x08 : Local Name - Shortened local name
0x09 : Local Name - **Complete local name**
0x0A : TX Power Level (1 byte)
....



[http://3.bp.blogspot.com/-ifQDFdEMhuI/UYPM-EDLwFI/AAAAAAAAAOY/8Fdmiwq54ng/s1600/Packet+format+for+ADV_IND.png]

부록. 참고 자료

1. 문서

가. Bluetooth Low Energy CC2540/41 Mini Development Kit User's Guide (http://www.ti.com/litv/pdf/swru270c)
4. Using BTool
Appendix

나. CC2540/41 Bluetooth Low Energy Software Developer's Guide (http://www.ti.com/lit/pdf/swru271)
4. Working with Projects using IAR Embedded Workbench 8.10.4

다. CC2540 Bluetooth Low Energy Sample Applications Guide (http://www.ti.com/litv/pdf/swru297b)
9. KeyFobDemo

라. Bluetooth Core Specifications 4.0 (https://www.bluetooth.org/docman/handlers/downloaddoc.ashx?doc_id=229737)

마. Assigned Numbers for Bluetooth GATT services (http://developer.bluetooth.org/gatt/services/Pages/ServicesHome.aspx)

2. 소프트웨어

가. Bluetooth low energy software stack and tools 1.3 (www.ti.com/blestack)
- KeyFobDemo 애플리케이션과 BTool을 포함하고 있다.

나. IAR Embedded Workbench for 8051 (http://supp.iar.com/Download/SW/?item=EW8051-EVAL)
- 30일 평가판 다운로드.

정창기님이 3rd May 2013에 게시

라벨: AdvData, BLE, Bluetooth Low Energy, Bluetooth Smart, CC2540, KeyFobDemo, ScanRspData

0 댓글 추가