Wireless Communication: BLE

e-Yantra Team

Embedded Real-Time Systems (ERTS) Lab
Indian Institute of Technology, Bombay

IIT Bombay
March 20, 2021

Agenda for Discussion

1. Bluetooth Low Energy
2. Generic Access Profile
3. Advertising
4. Generic Attribute Profile
5. What we haven't told you?
6. References

Bluetooth Low Energy (BLE)

Bluetooth Low Energy

- Low cost, low power but also low bandwidth and low complexity.
- Introduced in 2010 with Bluetooth 4.0.
- Different from Bluetooth Classic (ER/BDR/HS).
- Bluetooth LE is used for periodic transfer of data while Bluetooth Classic is used for streaming (file sharing, music, voice).
- Can run for extended period of time off a coin cell.

Bluetooth Low Energy

- Rapid growth of BLE is due to smartphones, tablets and mobile computing.
- Early adoption by mobile industry heavyweights like Apple and Samsung.
- BLE is desgined to be extensible framework for exchanging data.

Bluetooth Device Configurations

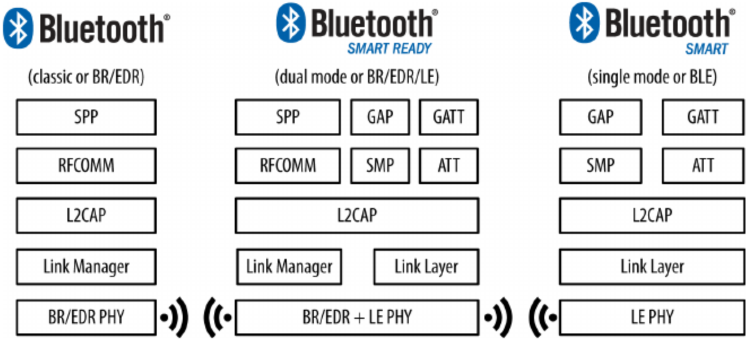


Figure 1: Bluetooth device configurations and compatibility

Limitations

- Potential maximum throughput of 5-10 KB/s.
- Can reliably trasmit upto 30 meters but typical range is clocked at 2-5 meters to save power.

Protocols and Profiles

- **Protocols** are building blocks used by all devices conformant with the spec.
- **Profiles** are features/functionalities either covering basic modes of operation or specific use-cases. Profiles define how protocols should be use.

Broadcasting and Connections

- Broadcasting allows pushing small amount of data on a fixed schedule to multiple devices. No security.
- Connections allow transmitting a lot more data between two devices in both directions. Security included.

Generic Access Profile

- **Generic Access Profile** provides a framework that all BLE implementations must follow to discover each other, broadcast data and form connections.
- GAP defines roles and modes.

GAP Roles

- Broadcaster
- Observer
- Central
- Peripheral

Broadcaster

- Optimized for transmit-only applications.
- Broadcast role periodically sends out advertising packets with data.
- A way to transmit data to more than one peer at a time.
- 31 bytes payload. Can be increased to 62 bytes with **scan response**.

Observer

- Optimized for receive-only applications that want to collect data from broadcasting devices.
- The observer role listens for data embedded in advertising packets from broadcasting peers.

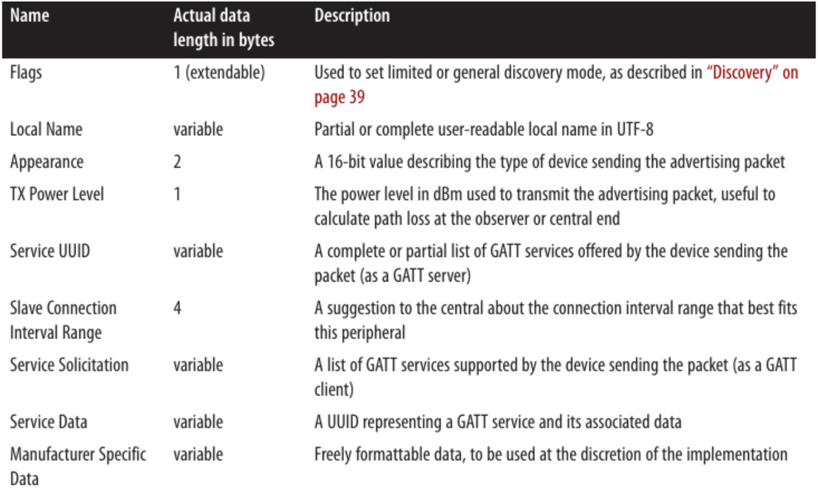
Central and Peripheral

- Central role is capable of establishing multiple connections to peers and is always the initiator of connections.
- Peripheral role uses advertising packets to allow centrals to find it and, subsequently, to establish a connection with it.

Advertising

- Broadcasting or advertising allows sending 31 bytes or 62 bytes of data.
- **But what is the format?**
- The data is collection of structures each of which contain length (1 byte), advertising data type (AD type, 1 byte), and actual data.
- Each structure is a separate item of user data.

Advertising



Name	Actual data length in bytes	Description
Flags	1 (extendable)	Used to set limited or general discovery mode, as described in "Discovery" on page 39
Local Name	variable	Partial or complete user-readable local name in UTF-8
Appearance	2	A 16-bit value describing the type of device sending the advertising packet
TX Power Level	1	The power level in dBm used to transmit the advertising packet, useful to calculate path loss at the observer or central end
Service UUID	variable	A complete or partial list of GATT services offered by the device sending the packet (as a GATT server)
Slave Connection Interval Range	4	A suggestion to the central about the connection interval range that best fits this peripheral
Service Solicitation	variable	A list of GATT services supported by the device sending the packet (as a GATT client)
Service Data	variable	A UUID representing a GATT service and its associated data
Manufacturer Specific Data	variable	Freely formattable data, to be used at the discretion of the implementation

Generic Attribute Profile (GATT)

- Whereas GAP defines low-level interactions, GATT serves as the data model.
- Data is organized hierarchically in services, characteristics and descriptors.
- GATT also defines roles different from GAP.
- GATT is usable after central establishes a connection with a peripheral.

GATT Roles

- **Client** sends requests to server and receives responses from it. It can also request server-initiates updates.
- **Server** sends responses for client requests. It also sends server-initiated updates when configured by the client.

UUIDs

- UUIDs are 128 bit numbers guaranteed to be globally unique with a high probability.
- UUIDs are used throughout Bluetooth specification for identifying profiles, services, characteristics, etc.
- A UUID is written in 8-4-4-4-12 form
  xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
- Alternatively, 16 and 32 bit UUIDs are used to save space and bandwidth.

Attribute Hierarchy

- An attribute is smallest data entity defined by GATT.
- Attributes are used to compose Services, characteristics and descriptors.
- A service is a feature. For example, battery level service, heart rate measurement service.
- A service contains many characteristics which store value. For example, battery level service may have a read only characteristic called battery level.
- Descriptors provide more information about the characteristic.
- Services, characteristic and descriptors are identified by UUIDs.

Characteristic Properties

- A characteristic may have associated properties such as None, read, write, read and write, notify and indicate.
- Notify and indicate enable server-initiated updates for reading characteristic value.
- For notify and indicate, a special descriptor called Client Characteristic Configuration Descriptor (CCCD) is mandatory.
- **Aside** You can think of the Hierarchy being stored on BLE device as a table where each row is an attribute identified by a handle (row number).

What we haven't told you?

- Bluetooth radio uses 2.4 GHz ISM band and divides this band in 40 channels from 2.4Ghz to 2.4835Ghz.
- 3 channels for advertising and 37 for connections.
- Bluetooth device stack is divided into Host, Controller and Application.
- Host contains GAP, GATT, **Attribute Protocol, L2CAP and Security Manager**.
- Scan interval, scan window, advertising interval.
- Advertising packet types such as connectable, non-scannable, directed.

What we haven't told you?

- Connections consist of connection intervals and connection events.
- GAP modes such as non-discoverable, limited discoverable and peer procedures such as limited discovery and name discovery.
- Attribute caching and Service/Characteristic Discovery.
- Mandatory GAP service (0x1800) and GATT service (0x1801).

References

- Townsend, Kevin, et al. *Getting Started With Bluetooth Low Energy*, O'Reilly Media, 2014.
- *Make: Bluetooth*, Make: Community, 2015.

Thank You!

Post your queries on: helpdesk@e-yantra.org