Bluetooth® Smart Technology

December 2015
TOPICS

- Bluetooth Smart Intro
- The Bluetooth Smart Architecture
- Radio
- Topologies
- Device Advertisement and Discovery
- Connections
- Security and Privacy
- Transferring Data - The ATT Protocol
- Exposing Data - The GATT Database
- Bluetooth versions
Benefits of *Bluetooth* Smart

- **Ultra low power** - Ability to run months on coin cell batteries
- **Lower cost** - 2 x lower cost
- Reliable and robust - AFH, retransmissions, 24-bit CRCs and FEC
- Secure - paring, privacy, MITM protection and AES-128 encryption
- Standardized profiles to cover key use cases (HR, HID, Glucose, Proximity etc.)
- **Enables profiles to be developed as Apps** - fast deployment
- **Customer specific profiles** - no need to wait OS developers
- Connectivity to Smart phones, tablets, PCs
- Supported by major platforms - iOS, Android 4.3, Windows 8, OSX and Linux
The *Bluetooth* Smart Architecture

- **GATT**: Organization of Attributes into services
- **ATT**: Data exchange protocol
- **SMP**: Bonding, privacy and encryption
- **GAP**: Advertizing, device discovery and connections
- **L2CAP**: Data multiplexing, fragmentation and reassembly
- **HCI**: Interface between controller and host
- **Link Layer**: Basic packets, state machine and radio control
- **Radio**: Receives and transmits bits
Radio

- 2.4GHz ISM Band
  - License free in most countries

- Uses Adaptive Frequency Hopping (AFH)
  - Reliable
  - Robust
  - Adapts to interference

- 40 channels
  - 3 advertisement channels
  - 37 data channels
Radio

- **1 Mbps bandwidth**
  - Typical throughput <= 100kbps due to small packets

- **TX power up to 10 dBm**
  - Limited by CE and FCC regulations

- **Range**
  - 0 - 500 meters
  - Typically 0-50 meters to a smart phone
Topologies

- **Advertizer**
  - Only sends out advertisements i.e. broadcast data
  - Can allow or disallow connections

- **Scanner**
  - Only listens for advertizements
  - Can also connect an advertizer

- **Slave**
  - Connected to one master (BT 4.0)
  - Connected to multiple masters (BT 4.1)

- **Master**
  - Connected to one or multiple slaves
Device Advertisement and Discovery

- **Discovering Devices or Broadcasting Data**
  - Devices advertise themselves
  - They broadcast advertisement packets on one, two or three ADV channels
  - Scanners listen for advertisements to discover devices

- **Benefits of Advertisements**
  - **Low power** - Radio is active <1ms during advertisement
  - **Quick** - ADV operation takes just 1.3 ms
  - **Flexible** - ADV interval range from 20ms to 10.2s
  - ADV packets can contain up to 31B of data
Connections

- Enable **reliable data transfer**

- Connections use ACKs, retransmits, 24-bit CRC to ensure **correct data delivery**

- Connections enable the use of **encryption** and protection of data **confidentiality**

10ms connection interval + ACK allow data to be sent every 20ms. At 20B payload this is about 1000B/sec.
Connections

- **Properties**
  - Connection interval from 7.5ms to 4000ms
  - Data payload between 20 to 22B

- Slave devices can use slave latency - enables them to skip N connection intervals when there is no data to transmit
• Authentication
  • Devices can be bonded to establish a trusted relationships
  • *Just Works* bonding: security keys are exchanged without user intervention
  • Man-in-the-Middle (MITM) bonding: end user needs to verify the devices either using passkey entry or passkey comparison
  • Out-of-Band bonding: security keys to be exchanged using another technology like NFC

• Authorization
  • On connection devices can be recognized, pairing verified and connection can be accepted or rejected

Learn more [here](#)
Security and Privacy

- **Encryption**
  - AES-128 encryption can be used to protect the confidentiality of the data in a connection
  - The standard does not provide methods to encrypt the broadcast data

- **Privacy**
  - Bluetooth Smart devices have a possibility to protect their identity by using a random Bluetooth address
  - Bonded devices can however resolve each others indentities and public addresses
The one and only protocol for data transfer

- Uses client–server architecture
  - Server stores the data
  - Client requests data from the server

- Data is stored in attributes
  - From 0 up to multiple kBs
  - Can be fixed or variable length

- Data can be accessed with the following operations
  - Read - reads data up to 22B
  - Read long - reads longer than 22B attributes
  - Write - writes data up to 20B
  - Write command - Just like write, but no ACK
  - Indicate - server indicates the data has changed
  - Notify - server notifies the data has changed
Transfering Data - The ATT Protocol

ACKnowledgements
- ACKs allow the application to know which data packets have been transmitted
- This can be used to design extremely reliable applications
- However one must wait for the ACK to be received before sending more data - does affect the throughput

Non-ACKed operations
- These operations can be used in "high" throughput applications, since multiple operations can be made within a connection interval
- The BLE link layer still retransmits the lost packets for reliability, but the app cannot be sure which packets have been transmitted
Data Organization with the GATT Database

Data is organized and described with the GATT database

- **Service** - Describes a set of data like Health Thermometer
  - Bluetooth SIG standardized services identified by unique 16-bit UUIDs
  - Vendor specific services identified by 128-bit UUIDs
  - Services contain one or more characteristics

- **Characteristic** - Describes data within a service
  - Describe data like Temperature Measurement
  - Standardized characteristics identified by unique 16-bit UUIDs
  - Vendor specific characteristics identified by 128-bit UUIDs

- **Characteristic properties**
  - Tell which operations can be used to access the data (Read, write, etc.)
  - Tell which security means must be used to access the data (bonding, encryption etc.)
Bluetooth Versions

- **Bluetooth 4.0**
  - Introduction of Bluetooth Smart technology

- **Bluetooth 4.1**
  - L2CAP connection oriented channels - groundwork to enable more efficient data transfer and IPv6 over BLE
  - Link layer topology - slave can have multiple masters and simultaneous master and slave operation
  - Limited discovery time - Device can be in limited discovery mode up to 180 seconds
  - LE ping - low latency ping
  - Low duty cycle directed advertising
  - Fast data advertising interval
Bluetooth Versions

- **Bluetooth 4.2**
  - LE Secure connections - Key exchange mechanism updated to ECDH for more secure bonding
  - LE privacy 1.2 - Identity resolving moved from host to controller for faster and lower power operation
  - LE data length extension - throughput increase by a factor of 2.5
  - IPv6 - Enabled the use of 6LoWPAN and IPv6 packets over BLE
  - Bluetooth Smart Internet through a Gateway - HTTP proxy and REST API whitepapers to e

- **Bluetooth 5.0**
  - 2Mbps PHY - 2Mbps physical layer for faster data transmission
  - LE long range - 250kbps and 500kbps PHYs for better sensitivity and longer range connections
  - Advertising extensions - new advertisement PDUs
  - Channel selection scheme - enhanced performance for applications requiring large amounts of data
Thank You