Bluetooth Reading

Technology Overview

Bluetooth Technology

Bluetooth technology is a wireless communications system intended to replace the cables connecting portable and/or fixed electronic devices. Key features of Bluetooth technology are robustness, low power, and low cost. Many features of the Bluetooth Core Specification are optional, allowing product differentiation.

Bluetooth Classic is the original version of the technology using the Basic Rate and/or Enhanced Data Rate transport. The low energy feature was introduced in version 4 of Bluetooth technology. A product implementing only this feature is known as a single mode device. A product implementing both Classic and low energy features is known as a dual mode device.

Bluetooth Core Specification

The Bluetooth Core System consists of an RF transceiver, baseband, and protocol stack. The system offers services that enable the connection of devices and the exchange of a variety of classes of data between these devices. Many features of the core specification are optional, allowing product differentiation.

Overview of Operations

This section offers an overview of the Bluetooth Radio and Link and Channel Management Protocols.

Core System Architecture

The Bluetooth core system covers the four lowest layers and associated protocols defined by the Bluetooth specification as well as one common service layer protocol.

Profiles Overview

Bluetooth profiles are definitions of possible applications and specify general behaviors that Bluetooth enabled devices use to communicate with other Bluetooth devices.

Security

Today's wireless world means that data is being sent invisibly from device to device and person to person. This data, in the form of emails, photos, contacts, addresses and more needs to be sent securely.

Bluetooth wireless technology has, from its inception, put an emphasis on security while making connections among devices.

- Classic Bluetooth Technology Security
- Bluetooth Smart Security

Profiles Overview

To use *Bluetooth*® wireless technology, a device must be able to interpret certain Bluetooth profiles. Bluetooth profiles are definitions of possible applications and specify general behaviors that Bluetooth enabled devices use to communicate with other Bluetooth devices. There is a wide range of Bluetooth profiles describing many different types of applications or use cases for devices. By following the guidance provided by the Bluetooth specification, developers can create applications to work with other Bluetooth devices.

At a minimum, each Bluetooth profile contains information on the following topics:

- Dependencies on other profiles
- Suggested user interface formats

- Specific parts of the Bluetooth protocol stack used by the profile. To perform its task, each profile uses particular options and parameters at each layer of the stack and this may include, if appropriate, an outline of the required service record

Adopted Bluetooth Profiles, Services and Protocols

- GATT based
- BR/EDR Profiles
- BR/EDR Protocols

GATT Based	Description	
ANP	Alert Notification Profile	enables a client device to receive different types of alerts and event information, as well as information on the count of new alerts and unread items, which exist in the server device.
ANS	Alert Notification Service	exposes different types of alerts.
BAS	Battery Service	exposes the state of a battery within a device.
BLP	Blood Pressure Profile	enables a device to connect and interact with a Blood Pressure Sensor device for use in consumer and professional health care applications.
BLS	Blood Pressure Service	exposes blood pressure and other data from a blood pressure monitor for use in consumer and professional healthcare applications.
CTS	Current Time Service	defines how the current time can be exposed using the Generic Attribute Profile (GATT).
DIS	Device Information Service	exposes manufacturer information about a device.
FMP	Find Me Profile	defines the behavior when a button is pressed on one device to cause an alerting signal on a peer device.
HTP	Health Thermometer Profile	enables a Collector device to connect and interact with a Thermometer sensor for use in healthcare applications.
HRP	Heart Rate Profile	enables a Collector device to connect and interact with a Heart Rate Sensor for use in fitness applications.
HRS	Heart Rate Service	exposes heart rate and other data from a Heart Rate Sensor intended for fitness applications.
HIDS	HID Service	exposes HID reports and other HID data intended for HID Hosts and HID Devices.

HOGP	HID Over GATT Profile	defines how a device with *Bluetooth* low energy wireless communications can support HID services over the*Bluetooth* low energy protocol stack using the Generic Attribute Profile.
IAS	Immediate Alert Service	exposes a control point to allow a peer device to cause the device to immediately alert.
LLS	Link Loss Service	defines behavior when a link is lost between two devices.
NDCS	Next DST Change Service	defines how the information about an upcoming DST change can be exposed using the Generic Attribute Profile (GATT).
PASP	Phone Alert Status Profile	enables a PUID device to alert its user about the alert status of a phone connected to the PUID device.
PASS	Phone Alert Status Service	exposes the phone alert status when in a connection.
PXP	Proximity Profile	enables proximity monitoring between two devices.
RTUS	Reference Time Update Service	defines how a client can request an update from a reference time source from a time server using the Generic Attribute Profile (GATT).
ScPP	Scan Parameters Profile	defines how a Scan Client device with *Bluetooth* low energy wireless communications can write its scanning behavior to a Scan Server, and how a Scan Server can request updates of a Scan Client scanning behavior.
ScPS	Scan Parameters Service	enables a GATT Client to store the LE scan parameters it is using on a GATT Server device so that the GATT Server can utilize the information to adjust behavior to optimize power consumption and/or reconnection latency.
TIP	Time Profile	enables the device to get the date, time, time zone, and DST information and control the functions related the time.
TPS	Tx Power Service	exposes a device's current transmit power level when in a connection.
		Back to Top

BR/EDR Profiles	Description	
A2DP	Advanced Audio Distribution Profile	describes how stereo quality audio can be streamed from a media source to a sink.

AVRCP	Audio/Video Remote Control Profile	is designed to provide a standard interface to control TVs, stereo audio equipment, or other A/V devices. This profile allows a single remote control (or other device) to control all A/V equipment to which a user has access.
BIP	Basic Imaging Profile	defines how an imaging device can be remotely controlled, how an imaging device may print, and how an imaging device can transfer images to a storage device.
BPP	Basic Printing Profile	allows devices to send text, e-mails, v-cards, images or other information to printers based on print jobs.
DI	Device ID Profile	provides additional information above and beyond the *Bluetooth* Class of Device and to incorporate the information into both the Service Discovery Profile (SDP) record and the EIR response.
DUN	Dial-Up Network Profile	provides a standard to access the Internet and other dial-up services via *Bluetooth* technology.
FTP	File Transfer Profile	defines how folders and files on a server device can be browsed by a client device.
GAVDP	Generic Audio/Video Distribution Profile	provides the basis for A2DP and VDP, which are the basis of the systems designed for distributing video and audio streams using *Bluetooth* technology.
GOEP	Generic Object Profile	is used to transfer an object from one device to another.
HFP	Hands-Free Profile	HFP describes how a gateway device can be used to place and receive calls for a hand-free device.
HCRP	Hard Copy Cable Replacement Profile	defines how driver-based printing is accomplished over a *Bluetooth* wireless link.
HDP	Health Device Profile	enables Healthcare and Fitness device usage models.
HSP	Headset Profile	describes how a *Bluetooth* enabled headset should communicate with a *Bluetooth* enabled device.
HID	Human Interface Device Profile	defines the protocols, procedures and features to be used by *Bluetooth* keyboards, mice, pointing and gaming devices and remote monitoring devices.
MAP	Message Access Profile	defines a set of features and procedures to exchange messages between devices.
MPS	Multi Profile	defines a set of features and procedures between Multiple Profiles Single Device and Multiple Profiles Multiple Devices

OPP	Object Push Profile	defines the roles of push server and push client.
PBAP	Phone Book Access Profile	defines the procedures and protocols to exchange Phone Book objects between devices.
PAN	Personal Area Networking Profile	describes how two or more *Bluetooth* enabled devices can form an ad-hoc network and how the same mechanism can be used to access a remote network through a network access point.
SAP	SIM Access Profile	defines the protocols and procedures that shall be used to access a GSM SIM card, a UICC card or an R-UIM card via a Bluetooth link.
SDAP	Service Discovery Application Profile	describes how an application should use SDP to discover services on a remote device.
SPP	Serial Port Profile	defines how to set-up virtual serial ports and connect two Bluetooth enabled devices.
SYNC	Synchronization Profile	used in conjunction with GOEP to enable synchronization of calendar and address information (personal information manager (PIM) items) between Bluetooth enabled devices.
VDP	Video Distribution Profile	defines how a Bluetooth enabled device streams video over Bluetooth wireless technology.
		Back to Top

BR/EDR Protocols	Description	
AVCTP	Audio/Video Control Transport Protocol	describes the transport mechanisms to exchange messages for controlling A/V devices.
AVDTP	Audio/Video Distribution Transport Protocol	defines A/V stream negotiation, establishment and transmission procedures
BNEP	Bluetooth Network Encapsulation Protocol	is used to transport common networking protocols over the Bluetooth media such as IPv4 and IPv6.
IrDA	IrDA Interoperabilit	offers the same features for applications as within the IrDA protocol hierarchy, enabling the applications to work

	y	over the Bluetooth protocol stack as well as the IrDA stack.
OBEX	Object Exchange	a transfer protocol that defines data objects and a communication protocol two devices can use to exchange those objects.
RFCOMM	RFCOMM with TS 07.10	emulates the serial cable line settings and status of an RS-232 serial port and is used for providing serial data transfer.
		Back to Top

Architecture - Overview of Operations

Radio

The Bluetooth RF (physical layer) operates in the unlicensed ISM band at 2.4GHz. The system employs a frequency hop transceiver to combat interference and fading, and provides many FHSS carriers. RF operation uses a shaped, binary frequency modulation to minimize transceiver complexity. The symbol rate is 1 Megasymbol per second (Msps) supporting the bit rate of 1 Megabit per second (Mbps) or, with Enhanced Data Rate, a gross air bit rate of 2 or 3Mb/s. These modes are known as Basic Rate (BR) and Enhanced Data Rate (EDR) respectively.

Radio Channel

During typical operation, a physical radio channel is shared by a group of devices synchronized to a common clock and frequency-hopping pattern.

Piconets—Master and Slave Devices

A piconet consists of master and slave devices. One device provides the synchronization reference, the master. All other devices are slaves. A group of devices synchronized in this fashion form a piconet. This is the fundamental form of communication for Bluetooth wireless technology.

Frequency Hopping and Adaptive Frequency Hopping (AFH)

Devices in a piconet use a specific frequency-hopping pattern algorithmically determined by certain fields in the Bluetooth specification address and clock of the master. The basic hopping pattern is a pseudo-random ordering of 79 frequencies in the ISM band. The hopping pattern may be adapted to exclude a portion of the frequencies used by interfering devices. The adaptive hopping technique improves Bluetooth technology co-existence with static (non-hopping) ISM systems.

Time Slots and Packets—Full Duplex Transmission

The physical channel is sub-divided into time units known as slots. Data is transmitted between Bluetooth enabled devices in packets positioned in these slots. When circumstances permit, a number of consecutive slots may be allocated to a single packet. Frequency hopping takes place between the transmission or reception of packets. Bluetooth technology provides the effect of full duplex transmission through the use of a time-division

duplex (TDD) scheme.

Link and Channel Management Protocols

Control Layers

Above the physical channel there is a layering of links, channels and associated control protocols. The hierarchy of channels and links from the physical channel upwards is physical channel, physical link, logical transport, logical link and L2CAP channel.

Physical Links

Within a physical channel, a physical link is formed between any two devices that transmit packets in either direction. In a piconet physical channel there are restrictions on which devices may form a physical link. There is a physical link between each slave and the master. Physical links are not formed directly between the slaves in a piconet.

Logical Links

The physical link is used as a transport for one or more logical links supporting unicast synchronous, asynchronous and isochronous traffic, and broadcast traffic. Traffic on logical links is multiplexed onto the physical link by occupying slots assigned by a scheduling function in the resource manager.

Link Manager Protocol (LMP)

A control protocol for the baseband and physical layers is carried over logical links in addition to user data. This is the link manager protocol (LMP). Devices that are active in a piconet have a default asynchronous connection-oriented logical transport used to transport the LMP protocol signaling. For historical reasons this is known as the ACL logical transport. The default ACL logical transport is created whenever a device joins a piconet. Additional logical transports may be created to transport synchronous data streams when this is required. The link manager function uses LMP to control the operation of devices in the piconet and provide services to manage the lower architectural layers (radio layer and baseband layer). The LMP protocol is only carried on the default ACL logical transport and the default broadcast logical transport.

L2CAP

Above the baseband layer, the L2CAP layer provides a channel-based abstraction to applications and services. It carries out segmentation and reassembly of application data and multiplexing and de-multiplexing of multiple channels over a shared logical link. L2CAP has a protocol control channel carried over the default ACL logical transport. Application data submitted to the L2CAP protocol may be carried on any logical link that supports the L2CAP protocol.

Security, Bluetooth Smart (Low Energy)

To make sure the communication over *Bluetooth®* Smart (Low Energy, BLE, LE) is always secure and protected, the Bluetooth Core Specification provides several features to cover the encryption, trust, data integrity and privacy of the user's data. We will further explain the

technical details of those features in this article.

Pairing (also known as Association Models

The pairing mechanism is the process where the parties involved in the communication exchange their identity information to set up trust and get the encryption keys ready for the future data exchange. Depending on the user's requirement and the capability of the device, Bluetooth has several options for pairing.

In version 4.0 and 4.1 of the core specification, Bluetooth Smart uses the Secure Simple Pairing model (referred to as LE Legacy after the Bluetooth 4.2 release), in which devices choose one method from Just Works, Passkey Entry and Out Of Box (OOB) based on the input/output capability of the devices.

With the release of the Bluetooth Core Specification version 4.2, security is greatly enhanced by the new LE Secure Connections pairing model. In this new model, the numeric comparison method is added to the other three methods and the Elliptical Curve Hellman-Diffie (ECDH) algorithm is introduced for key exchange in this process.

Reference:

- *BLUETOOTH SPECIFICATION Version 4.2 [Vol 1, Part A] 5.4.2 Key Generation*
- *BLUETOOTH SPECIFICATION Version 4.2 [Vol 3, Part H] 3.6.1 Key Distribution and Generation*

If you use LE legacy pairing, each of these association models is similar to BR/EDR Secure Simple Pairing with the exceptions that Just Works and Passkey Entry do not provide any passive eavesdropping protection. In LE Secure Connections pairing, the four association models are functionally equivalent to BR/EDR Secure Connections. The use of each association model is based on the I/O capabilities of the devices. You could choose the best pairing method based on the following table.

	Initiator				
Responder	**DisplayOnly**	**Display YesNo**	**Keyboard Only**	**NoInput NoOutput**	**Keyboard Display**
Display Only	Just Works Unauthenti-cated	Just Works Unauthenti-cated	Passkey Entry: responder displays, initiator inputs Authenti-cated	Just Works Unauthenti-cated	Passkey Entry: responder displays, initiator inputs Authenti-cated
Display YesNo	Just Works Unauthenti-cated	Just Works (For LE Legacy Pairing) Unauthenti-cated	Passkey Entry: responder displays, initiator inputs Authenti-cated	Just Works Unauthenti-cated	Passkey Entry (For LE Legacy Pairing): responder displays, initiator inputs Authenti-cated
		Numeric Comparison (For LE Secure Connections) Authenti-cated			Numeric Comparison (For LE Secure Connections) Authenti-cated

	Initiator				
Responder	**DisplayOnly**	**Display YesNo**	**Keyboard Only**	**NoInput NoOutput**	**Keyboard Display**
Keyboard Only	Passkey Entry: initiator displays, responder inputs Authenticated	Passkey Entry: initiator displays, responder inputs Authenticated	Passkey Entry: initiator and responder inputs Authenticated	Just Works Unauthenticated	Passkey Entry: initiator displays, responder inputs Authenticated
NoInput NoOutput	Just Works Unauthenticated	Just Works Unauthenticated	Just Works Unauthenticated	Just Works Unauthenticated	Just Works Unauthenticated
Keyboard Display	Passkey Entry: initiator displays, responder inputs Authenticated	Passkey Entry (For LE Legacy Pairing): initiator displays, responder inputs Authenticated Numeric Comparison (For LE Secure Connections) Authenticated	Passkey Entry: responder displays, initiator inputs Authenticated	Just Works Unauthenticated	Passkey Entry (For LE Legacy Pairing): initiator displays, responder inputs Authenticated Numeric Comparison (For LE Secure Connections) Authenticated

Reference:

- *BLUETOOTH SPECIFICATION Version 4.2 [Vol 1, Part A] 5.4.1 Association Models*

Key Generation

Key generation in Bluetooth Smart is performed by the Host on each LE device independent of any other LE device. Note: Key generation in BR/EDR is performed in the Controller. By performing key generation in the Host, the key generation algorithms can be upgraded without the need to change the Controller.

When using Bluetooth LE Secure Connections, the following keys are exchanged between master and slave:

- Connection Signature Resolving Key (CSRK) for Authentication of unencrypted data
- Identity Resolving Key (IRK) for Device Identity and Privacy

In LE Secure Connections, the public/private key pair is generated in the Host and a Secure Connection Key is generated by combining contributions from each device involved in pairing.

Encryption

Encryption in Bluetooth LE uses AES-CCM cryptography. Like BR/EDR, the LE Controller will perform the encryption function. This function generates 128-bit encryptedData from a 128-bit key and 128-bit plaintextData using the AES-128-bit block cypher as defined in FIPS-1971.

Reference:

- *BLUETOOTH SPECIFICATION Version 4.2 [Vol 3, Part H] 3.6.2 Encryption Information*

Signed Data

Bluetooth Smart supports the ability to send authenticated data over an unencrypted transport between two devices with a trusted relationship. This means that in some circumstances where the communication channel is not encrypted, the device could still have a method to maintain and ensure the data authentication. This is accomplished by signing the data with a CSRK. The sending devices place a signature after the Data Protocal Data Unit (PDU). The receiving device verifies the signature and, if the signature is verified, the Data PDU is assumed to come from the trusted source. The signature is composed of a Message Authentication Code generated by the signing algorithm and a counter. The counter is used to protect against a replay attack and is incremented on each signed Data PDU sent.

Reference:

- *BLUETOOTH SPECIFICATION Version 4.2 [Vol 3, Part H] 3.6.6 Signing Information*

Privacy Feature

Since Bluetooth 4.0, Bluetooth Smart supports a feature that reduces the ability to track a LE device over a period of time by changing the Bluetooth device address on a frequent basis. The frequently changing address is called the private address and the trusted devices can resolve it.

In order to use this feature, the devices involved in the communication need to be previously paired. The private address is generated using the devices IRK exchanged during the previous pairing/bonding procedure.

There are two variants of the privacy feature. In the first variant, private addresses are resolved and generated by the Host. This is used in the pre-4.2 Bluetooth stacks. In the second variant, private addresses are resolved and generated by the Controller without involving the Host after the Host provides the Controller device identity information. Bluetooth 4.2 compliant devices use this design.

Reference:

- *BLUETOOTH SPECIFICATION Version 4.2 [Vol 6, Part B]*

How Bluetooth Utilizes these Features to Protect Your Information

The goal of the LE security mechanism is to protect communication between devices at different levels of the stack. Below are commons types of attacks against various wireless communication protocols, and how Bluetooth addresses them.

Man-in-the-Middle (MITM)

A MITM requires an attacker to have the ability to both monitor and alter or inject messages into a communication channel. One example is active eavesdropping, in which the attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all relevant messages passing between the two victims and inject new ones.
In LE Legacy pairing, MITM protection is obtained by using the passkey entry pairing method or may be obtained using the out of band pairing method. In LE Secure Connections pairing, MITM protection could be obtained by using the numeric comparison method as well as the previous two methods. To ensure that Authenticated MITM Protection (the protection through authentication) is generated, the selected Authentication Requirements option must have MITM protection specified.
Passive Eavesdropping
Passive Eavesdropping is secretly listening (by using a sniffing device) to the private communication of others without consent. LE Secure Connection uses ECDH public key cryptography as a means to thwart passive eavesdropping attacks. ECDH provides a very high degree of strength against passive eavesdropping attacks. The algorithm provides a mechanism to exchange keys over an unsecured channel.
Privacy/Identity Tracking
Since most of the Bluetooth LE advertisement and data packets have the source addresses of the devices that are sending the data, third-party devices could associate these addresses to the identity of a user and track the user by that address. This can be protected by frequently changing private addresses so only the trusted parties could resolve them.
Reference:

- *BLUETOOTH SPECIFICATION Version 4.2 [Vol 6, Part B]*

The Bluetooth Smart specification has defined powerful security features to protect the communication of a user's data and identity. Those features are either NIST compliant or FIPS approved. The Bluetooth SIG encourages and actively promotes the proper implementation of these security measures built into Bluetooth technology.