INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES TOULOUSE

January 05, 2020

Touzani Ismail

Pajanissamy Poonkuzhali

Krishna Sujan Inuganti

Introduction:

Bluetooth Low Energy (BLE) is an emerging low-power wireless technology developed for short-range control and monitoring applications that is expected to be incorporated into billions of devices in the next few years. It is part of the Bluetooth 4.0 Core specification and also a highly optimized version of the classic Bluetooth but in reality, BLE has an entirely different lineage and design goals.

It is the result of an initiative by Nokia, which was adopted by the Bluetooth Special Interest Group, and eventually included in the Bluetooth specification on June 30, 2010. Initially named as Wibree and Bluetooth ULP (Ultra Low Power) which was abandoned and the BLE name was used for a while. In late 2011, new logos "Bluetooth Smart Ready" for hosts and "Bluetooth Smart" for sensors were introduced as the general-public face of BLE.

It is attractive to consumer electronics and Internet-connected machine manufacturers because of its low cost, long battery life, and ease of deployment. From thermometers and heart rate monitors to smart watches and proximity sensors, Bluetooth LE facilitates infrequent short-range wireless data communication between devices, powered by nothing more than a dime-sized battery.

Classic Bluetooth or BLE? Classic Bluetooth works best when the throughput required is of a higher value and where power consumption, cost, connection speed and slave attachments are not important. BLE is used when these factors do matter. While Bluetooth and BLE have considerable differences, they also have a fair share of similarities:

- Both Bluetooth Classic and Bluetooth LE operate with the same pairing technology, authentication and even encryption,
- Both Bluetooth and Bluetooth Low Energy involve devices that operate in a classic master-slave model. First the Bluetooth devices need to be paired and then the data transmission can happen.
- Both Bluetooth Classic and Bluetooth LE operate in the same 2.4 GHz ISM band and have similar RF output power.

Bluetooth Low Energy essentially operates in sleep mode and awakens only when a connection is initiated. Consequently, a BLE device offers power consumption of microamperes and peak power consumption of only 15-20 mA. This translates to a power savings over Classic Bluetooth of a magnitude 1-5 percent versus Classic Bluetooth devices. Amazingly, Bluetooth Low Energy devices can be powered by a coin cell battery for one to five years. Consequently, Bluetooth Low Energy is ideally suited to connectivity in products that require only periodic transfer of data and not continuous streaming of data. This makes Bluetooth Low Energy suitable to IOT applications such as building automation and lighting.

Comparison with other wireless standards

While BLE is emerging, other low-power wireless technologies, such as ZigBee, 6LoWPAN or Z-Wave, have already achieved significant presence in several market segments. However, they do not have high deployment expectations in devices such as smartphones. BLE, on the other hand, is expected to have a strong position in these.

Table 1: Comparison of ZigBee, 6LoWPAN, Z-Wave, BLE
[Source: Link to the article to be added….]

		ZigBee	6LoWPAN (Over 802.15.4)	Z-Wave	Bluetooth Low Energy
Physical layer	**RF band (MHz)**	868/915/2400		868/908 (all chips) 2400 (400 serie chip)	2400
	Bit rate (kbps)	20/40/250		9.6/40 (from 200 series chip) 200 (only 400 series chip)	1000
	Modulation	BPSK/BPSK/O-QPSK		BFSK	GFSK
	Spreading technique	DSSS		No	FHSS (2 MHz channel width)
	Receiver sensitivity (dBm)	−85 or better(2.4 GHz band)−92 or better(868/915 MHz bands)		−101 (at 40 kbps)	−87 to −93 (typical)
	Transmit power (dBm)	−32 to 0		−20 to 0	−20 to 10
Link layer	**MAC mecha-nism**	TDMA+CSMA/CA (beacon mode) and CSMA/CA (beaconless mode)		CSMA/CA	TDMA
	Message size (bytes)	127 (maximum)		64 (max. MAC payload in 200 series chip)	8 to 47
	Error control	16-bit CRC. ACKs (optional)		8-bit checksum. ACKs (optional)	24-bit CRC. ACKs
	Latency (ms)	<5 (beaconless mode, at 250 kbps)		<39 (at 40 kbps)	<3
Identifiers		16- and 64-bit MAC addresses. 16-bit NWK identifiers	16- and 64-bit MAC addresses. 128-bit IPv6 addresses	32-bit (home ID), 8-bit (node ID)	48-bit public device Bluetooth address or random address

Table 2: Cont.

Device types or roles		Coordinator, Router and End device	Edge Router, Mesh Node (mesh under), Router (route over), Host	Controller and slave	Master and slave
Network layer	**Multi-hop solution**	Mesh routing, tree routing, and source routing	RPL (other protocols are not excluded)	Source routing	Not currently supported
	Hop limit	30/10/5 (mesh routing/tree routing/source routing)	255	4	1
Security		Integrity, confidentiality, access control (IEEE 802.15.4 security, using 128-bit AES)		128-bit AES encryption (400 series chip)	Security Modes/Levels. Pairing. Key Gener. /Distribution. Confidentiality, Authentication, and Integrity
		Key management	Key management currently out of scope		
Implementation size		45–128 kB (ROM), 2.7–12 kB (RAM)	24 kB (ROM), 3.6 kB (RAM)	32–64 kB (Flash), 2–16 kB (SRAM)	~40 kB (ROM), ~2.5 kB (RAM)

BLE Protocol Stack Architecture:

BLE Protocol Stack

Overview:

BLE protocol stack is composed of two main parts: the Controller and the Host.

Controller comprises the Physical Layer and the Link Layer with an integrated radio. The Host runs on an application processor and includes upper layer functionality. Communication between the Host and the Controller is standardized as the Host Controller Interface. non-core profiles. can be used on top of the Host.

Controller:

BLE operates in the 2.4 GHz Industrial Scientific Medical (ISM) band and defines 40 Radio Frequency (RF) channels with 2 MHz channel spacing. There are two types of BLE RF channels: advertising channels and data channels. Advertising channels are used for device discovery, connection establishment and broadcast transmission, whereas data channels are used for bidirectional communication between connected devices. Three channels are defined as advertising channels. These channels have been assigned center frequencies that minimize overlapping with IEEE 802.11 channels 1, 6 and 11, which are commonly use.

Link Layer:

BLE, transmits the data in advertising packets through the advertising channels when a device only needs to broadcast data. This takes place in intervals of time called advertising events. Further, Bidirectional data communication between two devices requires them to connect to each other.

BLE defines two device roles at the Link Layer for a created connection: the master and the slave. These are the devices that act as initiator and advertiser during the connection creation, respectively. A master can manage multiple simultaneous connections with different slaves, whereas each slave can only be connected to one master. Thus, the network composed by a master and its slaves, which is called a piconet, follows a star topology. Currently, a BLE device can only belong to one piconet.

Host:

The L2CAP used in BLE is an optimized and simplified protocol based on the classic Bluetooth L2CAP. In BLE, the main goal of L2CAP is to multiplex the data of three higher layer protocols, ATT, SMP and Link Layer control signalling, on top of a Link Layer connection.

The ATT defines the communication between two devices playing the roles of server and client, respectively, on top of a dedicated L2CAP channel.

The GATT defines a framework that uses the ATT for the discovery of services, and the exchange of characteristics from one device to another. A characteristic is a set of data which includes a value and properties.

Security:

There are two types of cyber-attacks commonly associated with hacking Bluetooth Low Energy modules: passive eavesdropping where an attack that allows an alien device to tap into data transmitted between devices on a BLE network and man-in-the-middle which involves alien device that pretends to be both central and peripheral at the same time and tricks other devices on the network into connecting to it.

The above vulnerability problems can be solved by the security modes called LE Security Mode 1 and LE Security Mode 2. These two modes provide security functionality at the Link Layer and at the ATT layer, respectively.

The link layer, supports encryption and authentication by using Cipher Block Chaining-Message Authentication Code Algorithm and a 128-bit AES block cipher. BLE also supports a mechanism called privacy feature which allows to use a dynamic private IP for communication.

Security can also been observed during the pairing of devices. After the devices register there capabilities, the devices attached generate Short term keys using which they generates three Long-term keys which is a 128 bit encrypted key called Connection Signature Resolving Key (CSRK), Identity Resolving Key (IRK) and The third key (i.e., the IRK), is used to generate a private address on the basis of a device public address

Energy consumption:

For the one-way ATT communication, the study takes into account the energy consumed during each one of the following states: device wake up, radio turn on (in order to receive the initial BLE packet from the master), request reception, radio switch to transmit mode, notification transmission and post-processing before the device returns to sleep mode.

For the round-trip ATT dialogue, the additional energy consumption due to response transmission, radio switch to receive mode, and acknowledgment reception is also considered. The energy consumption during sleep periods is considered as well for both types of ATT transactions.

Localization:

With coin-cell battery, BLE beacon can work up to years depending on the broadcasting frequency. On the other hand, GPS is traditionally thought to be power hungry. The power consumption of GPS is comparable with WiFi.

With respect to the location accuracy, GPS is born to implement the location service, whereas BLE is definitely not. BLE is mostly used to implement context-aware applications. The tricky part happens at indoor environments where GPS fails. In such situations, BLE may be used together with triangulation algorithms to locate objects.

Conclusion:

This report basically talks about BLE wireless network module, its differentiation from tradition Bluetooth. Further, the reports tries to talk about the architecture of the BLE protocol stack, security issues related to the BLE and how they are addressed. In this report, we also tried to address the energy efficiency of BLE in brief and localization.

With new enhancements, BLE is being used in health-related applications like body peripherals like smart watches, blood sugar testing machines etc. Beside this, BLE is also utilised for domestic purpose like smart houses along with WiFi.

References:

Overview and Evaluation of Bluetooth Low Energy: An Emerging Low-Power Wireless Technology

Carles Gomez 1,*, Joaquim Oller 2 and Josep Paradells 2