Volume 3, Issue 9, September 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

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

Surthineni. Ashok*
M. Tech(CS), DRKIST, JNTU-Hyd
India

Dr. R.V.Krishnaiah
PG-COORDINATOR, DRKGI
India

Abstract: -- 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. This paper describes the main features of BLE, explores its potential applications, and investigates the impact of various critical parameters on its performance. BLE represents a trade-off between energy consumption, latency, piconet size, and throughput that mainly depends on parameters such as connInterval and connSlaveLatency. According to theoretical results, the lifetime of a BLE device powered by a coin cell battery ranges between 2.0 days and 14.1 years. The number of simultaneous slaves per master ranges between 2 and 5,917. The minimum latency for a master to obtain a sensor reading is 676 µs, although simulation results show that, under high bit error rate, average latency increases by up to three orders of magnitude. The paper provides experimental results that complement the theoretical and simulation findings, and indicates implementation constraints that may reduce BLE performance.

Keywords: Bluetooth Low Energy, Sensor Networks, Internet of Things

I. INTRODUCTION

Bluetooth Low Energy (BLE) is an emerging wireless technology developed by the Bluetooth Special Interest Group (SIG) for short-range communication. In contrast with previous Bluetooth flavors, BLE has been designed as a low-power solution for control and monitoring applications. BLE is the distinctive feature of the Bluetooth 4.0 specification [1]. The advent of BLE has occurred while other low-power wireless solutions, such as ZigBee, 6LoWPAN or Z-Wave, have been steadily gaining momentum in application domains that require multihop networking [2, 3]. However, BLE constitutes a single-hop solution applicable to a different space of use cases in areas such as healthcare, consumer electronics, smart energy and security. The widespread use of Bluetooth technology (e.g., in mobile phones, laptops, automobiles, etc.) may fuel adoption of BLE, since implementation of the latter can leverage similarities with classic Bluetooth. According to published forecasts [4], BLE is expected to be used in billions of devices in the near future. In fact, the IETF 6LoWPAN Working Group (WG) [5] has already recognized the importance of BLE for the Internet of Things. As of the writing of this article, the 6LoWPAN WG is developing a specification for the transmission of IPv6 packets over BLE [6]. This paper describes the main features of BLE, investigates the impact of critical parameters on its performance, and explores its potential applications. The rest of the paper is organized as follows: Section 2 overviews the BLE protocol stack and describes the operation and main characteristics of each layer; Section 3 evaluates the energy consumption, latency and network size of BLE and discusses application layer BLE throughput; Section 4 explores the application and market adoption possibilities for BLE, and provides a comparison with other wireless low-power technologies. Finally Section 5 concludes the paper with the main remarks.

II. BLUETOOTH LOW ENERGY PROTOCOL STACK

This section presents the BLE protocol stack, and describes the main mechanisms and features of each layer.

A. BLE PROTOCOL STACK OVERVIEW

Like in classic Bluetooth [7], the BLE protocol stack is composed of two main parts: the Controller and the Host. The Controller comprises the Physical Layer and the Link Layer, and is typically implemented as a small System-on-Chip (SOC) with an integrated radio. The Host runs on an application processor and includes upper layer functionality, i.e., the Logical Link Control and Adaptation Protocol (L2CAP), the Attribute Protocol (ATT), the Generic Attribute Profile (GATT), the Security Manager Protocol (SMP) and the Generic Access Profile (GAP). Communication between the Host and the Controller is standardized as the Host Controller Interface (HCI). Finally, non-core profiles (i.e., application layer functionality not defined by the Bluetooth specification) can be used on top of the Host. Figure 1(a) illustrates the BLE protocol stack. Figure 1(b) depicts the structure and size of the different fields contributed by each layer to a Physical Layer data unit when application data are transmitted. Subsections 2.2 to 2.8 focus on each layer of the BLE protocol stack. Although some of the BLE Controller features are inherited from the classic Bluetooth Controller, both types of Controller

are currently incompatible. Hence, a device that only implements BLE (which is referred to as a single-mode device) cannot communicate with a device that only implements classic Bluetooth. It is expected that many devices will implement both the classic Bluetooth and the BLE protocol stacks. These devices are called dual-mode devices.

B. PHYSICAL LAYER

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 used in several countries. An adaptive frequency hopping mechanism is used on top of the data channels in order to face interference and wireless propagation issues, such as fading and multipath. This mechanism selects one of the 37 available data channels for communication during a given time interval. All physical channels use a Gaussian Frequency Shift Keying (GFSK) modulation, which is simple to implement. The modulation index is in the range between 0.45 and 0.55, which allows reduced peak power consumption. The physical layer data rate is 1 Mbps. The receiver sensitivity is defined in BLE as the signal level at the receiver for which a Bit Error Rate (BER) of 10−3 is achieved. The BLE specification mandates a sensitivity better than or equal to −70 dBm. The coverage range is typically over various tens of meters.

C. LINK LAYER

In BLE, when a device only needs to broadcast data, it transmits the data in advertising packets through the advertising channels. Any device that transmits advertising packets is called an advertiser. The transmission of packets through the advertising channels takes place in intervals of time called advertising events. Within an advertising event, the advertiser sequentially uses each advertising channel for packet transmission. Devices that only aim at receiving data through the advertising channels are called scanners. Bidirectional data communication between two devices requires them to connect to each other. The creation of a connection between two devices is an asymmetric procedure by which an advertiser announces through the advertising channels that it is a connectable device, while the other device (referred to as an initiator) listens for such advertisements. When an initiator finds an advertiser, it may transmit a Connection Request message to the advertiser, which creates a point-to-point connection between the two devices. Both devices can then communicate by using the physical data channels. The packets for this connection will be identified by a randomly generated 32-bit access code. 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.

D. L2CAP

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 signaling, on top of a Link Layer connection. The data of these services are handled by L2CAP in a best-effort approach and without the use of retransmission and flow control mechanisms, which are available in other Bluetooth versions. Segmentation and reassembly capabilities are not used, since upper layer protocols provide data units that fit into the maximum L2CAP payload size, which is equal to 23 bytes in BLE.

E. ATT

The ATT defines the communication between two devices playing the roles of server and client, respectively, on top of a dedicated L2CAP channel. The server maintains a set of attributes. An attribute is a data structure that stores the information managed by the GATT, the protocol that operates on top of the ATT. The client or server role is determined by the GATT, and is independent of the slave or master role. The client can access the server's attributes by sending requests, which trigger response messages from the server. For greater efficiency, a server can also send to a client two types of unsolicited messages that contain attributes: (i) notifications, which are unconfirmed; and (ii) indications, which require the client to send a confirmation. A client may also send commands to the server in order to write attribute values. Request/response and indication/confirmation transactions follow a stop-and-wait scheme.

F. GATT

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. The data related to services and characteristics are stored in attributes. For example, a server that runs a "temperature sensor" service may account with a "temperature" characteristic that uses an attribute for describing the sensor, another attribute for storing temperature measurement values and a further attribute for specifying the measurement units.

G. SECURITY

BLE offers various security services for protecting the information exchange between two connected devices. Most of the supported security services can be expressed in terms of two mutually-exclusive 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 BLE Link Layer supports encryption and authentication by using the Cipher Block Chaining-Message Authentication Code (CCM) algorithm [8] and a 128-bit AES block cipher. When encryption and authentication are used in a connection, a 4-byte Message Integrity Check (MIC) is appended to the payload of the data channel PDU (see Figure 1(b)).

Encryption is then applied to the PDU payload and MIC fields. It is also possible to transmit authenticated a over an unencrypted Link Layer connection. In this case, a 12-byte signature is placed after the data payload at the ATT layer. The signature is computed by applying an algorithm that uses 128-bit AES as the block cipher [1]. One input to the algorithm is a counter, which is used in order to provide protection against replay attacks. If the receiver verifies the signature, it assumes that the data have been sent by the trusted source. In addition to the described services, BLE supports a mechanism called privacy feature, which allows a device to use private addresses and frequently change them. The privacy feature mitigates the threat by which an adversary can track a BLE device.

H. GAP AND APPLICATION PROFILES

At the highest level of the core BLE stack, the GAP specifies device roles, modes and procedures for the discovery of devices and services, the management of connection establishment and security. The BLE GAP defines four roles with specific requirements on the underlying controller: Broadcaster, Observer, Peripheral and Central. A device in the Broadcaster role only broadcasts data (via the advertising channels) and does not support connections with other devices. The Observer role is complementary for the Broadcaster, i.e., it has the purpose of receiving the data transmitted by the Broadcaster. The Central role is designed for a device that is in charge of initiating and managing multiple connections, whereas the Peripheral role is designed for simple devices which use a single connection with a device in the Central role. In consequence, the Central and Peripheral roles require that the device's controller support the master and slave roles, respectively. A device may support various roles, but only one role can be adopted at a given time. Finally, since certain types of applications may benefit from reusing common functionality, additional profiles can be built on top of the GAP. Bluetooth follows a profile hierarchy, whereby a new profile including all the requirements of an existing profile can be defined..

III. PERFORMANCE EVALUATION

This section evaluates the performance of BLE in terms of energy consumption, latency and piconet size, for various use cases and configurations, and discusses application layer BLE throughput. The size of the notification, command and response messages considered in this study is the maximum one (i.e., 37 bytes at the Physical Layer), whereas polls sent by the master and acknowledgments are assumed to be empty PDUs (i.e., PDUs without payload). Latency results have been obtained by exploiting simulation tools that we developed for this purpose (given that current simulators do not support BLE yet), and have been complemented by means of experimental measurements. The simulation tools model two connected BLE devices that communicate with each other, taking into account all the BLE stack layers and their behavior in the presence of bit errors. Piconetsize results have been obtained theoretically, whereas energy consumption has been analyzed both theoretically and empirically. Further details about the evaluation methods are provided in each corresponding subsection.

A. ENERGY CONSUMPTION

We first investigate the theoretical lifetime of a slave that is connected to a master in a data collection application. Note that a slave is typically a device with limited energy supply, whereas a master may not suffer the same energy constraints. We consider two different methods by which the master obtains sensor measurement readings (which are handled as attribute values) from the slave, which is assumed to act as the attribute server. We denote these methods by one-way ATT communication and round-trip ATT dialogue, respectively. In the one-way ATT communication, the slave sends a notification in response to a poll from the master. In the round-trip ATT dialogue, the master sends a request to the slave, which transmits a response to the master (and both the request and the response trigger Link Layer acknowledgments). For the two methods described, the first packet transmission from the master takes place at the beginning of each connection event. The evaluation is carried out theoretically by assuming current consumption values obtained from measurements for the CC2540 radio chip, for a transmit power of 0 dBm [11]. Specifically, 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 fipost-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. For the evaluation of the device lifetime, we assume an ideal battery with a capacity of 230 mAh (i.e., a common value for a coin cell battery). The study considers the impact of connInterval and connSlaveLatency parameters. The whole range of valid connInterval values (i.e., from 7.5 ms to 4000 ms) is covered. For connSlaveLatency, values in the range between 0 and 7 are considered, since these values can be used for any permitted connSupervisionTimeout setting. The study is also carried out for the maximum possible connSlaveLatency value, which is given for the maximum connSupervisionTimeout value (i.e., 32 s), and depends on the connInterval value. For this study, a BER equal to zero is assumed, which gives an upper bound on the slave lifetime under the described conditions. The maximum slave lifetime obtained is 14.1 and 12.4 years for the one-way and round-trip methods, respectively.

B. LATENCY

We next study by simulation the average latency of one-way ATT communications and round-trip ATT dialogues between a master and a slave, as a function of the connInterval parameter, and for various BER values. Examples of the one-way ATT communications considered include the following: (i) the master polls the slave and the slave replies with a notification or a command; (ii) the master sends a notification or a command, and the slave acknowledges the master's

message at the Link Layer. The round-trip ATT dialogue considered is the same as that assumed in the energy consumption evaluation. The latency of each message exchange is measured as the difference of times between the start of the transmission of the first message and the end of the correct reception of the last message. We assume that a connection has been created between the two BLE devices before the ATT message exchange. Figure 6 illustrates the results, which are obtained as the average latency from ten million simulated message exchanges for each set of conditions. A connSlaveLatency equal to 0 is assumed. The results do not include the latency for the first packet of the connection. In fact, the master has flexibility in selecting the start time of the first packet transmission, which can occur between 1.25 ms and 11.25 + connIntervalms after the transmission of the Connection Request message. For very low BER values (e.g., 10−6), the average latency of round-trip and one-way ATT message exchanges are smaller than 2 ms and 1 ms, respectively, for any connInterval value. However, for greater BER values, the influence of connInterval becomes significant, since on average more than a single connection event is required for successful transmission of each ATT message

C. MAXIMUM PICONET SIZE

We next investigate the maximum piconet size, i.e., the maximum number of slaves that a master can handle. In BLE, each connection between a master and a slave is identified by a 32-bit access address. Beyond this fact, the Bluetooth 4.0 specification does not impose further limits on the number of slaves that can be connected to a master. However, there exist practical limits on that number, depending on the type of communication between master and slave, on the connInterval parameter setting and the BER that can be assumed. The maximum piconet size is independent of the connSlaveLatency parameter, because the inactive connection events due to slave latency cannot be used for connections with other slaves. Figure 8 depicts the theoretical maximum number of slaves that a master can handle for various configurations. This number is evaluated for the one-way and round-trip ATT interactions considered in the latency study. An upper bound on the maximum number of slaves per master is obtained by considering ideal communications (i.e., BER = 0). In addition, a safe scheduling scheme has been evaluated, whereby the communications between a master and two different slaves cannot overlap even when bit errors lead to retransmissions. Theoretical maximum number of slaves per piconet for various types of interactions between devices and scheduling schemes. The number of slaves that a master can handle varies significantly depending on the setting of the connInterval parameter..

D. THROUGHPUT

The maximum BLE application layer throughput for a connection between two devices has been obtained in prior work by simulation and mathematical analysis, as a function of connInterval and BER [13]. Whereas the physical layer data rate is 1 Mbps, the maximum application layer throughput is equal to 236.7 kbps. On the other hand, recall that if any of the two connected devices receives two consecutive packets with an invalid CRC check, the connection event ends. Thus, the transmission of data cannot be resumed until the beginning of the next connection event, whereby a new data channel (i.e., a new frequency) is used. This behavior prevents any unnecessary waste of energy while bit errors are being found in one data channel. However, this scheme degrades the effective throughput of BLE in the presence of bit errors. In such conditions, moderate to high throughput can only be achieved for very low connInterval values. Despite the theoretical or simulation-based findings, the maximum BLE throughput that can be achieved in a real scenario may be limited due to a variety of factors. These include implementation constraints such as the number of application layer messages a device can send per connection event (due to memory limitations), as well as processing delays. We have conducted experiments in order to measure the maximum achievable throughput in a BLE link composed of two connected CC2540 devices. The distance between both devices is 0.5 m and their transmit power is 0 dBm. According to our measurements, in these conditions, the BER of the BLE link is lower than 10−5. In each experiment, the slave has been programmed to send the maximum number of notifications allowed by the BLE stack currently used in the CC2540 (i.e., four notifications per connection interval). Accordingly, we have set connInterval and connSlaveLatency to the smallest possible values (i.e., 7.5 ms and 0, respectively). Each notification has the maximum size (i.e., 20 bytes of application layer payload). The experiment is carried out for 1000 connection events. In the described conditions, the maximum application layer throughput we have measured is 58.48 kbps. This low result can be explained by the following two facts: (i) whereas, in theory, up to eleven such notifications can be transmitted within a connection event of 7.5 ms, only four notifications are allowed per connection event, as aforementioned; and (ii) we have observed that less than four notifications are actually transmitted in most connection events during the experiment (however, the same phenomenon occurs less frequently for connection intervals greater than 7.5 ms). These observations show that high throughput has not been a primary goal in the design of the BLE implementation used in the evaluation.

IV. APPLICATIONS AND MARKET ADOPTION

BLE may benefit from the widespread use of Bluetooth technology, since BLE easily integrates into classic Bluetooth circuitry, and hence it is likely that future Bluetooth devices will be dual-mode devices. According to published forecasts, BLE is expected to be used in billions of devices in the near future [4]. In view of the important role that BLE may play in the Internet of Things, the IETF 6LoWPAN WG is developing a specification in order to enable end-to-end IP communications for BLE devices [6]. For example, BLE-equipped smart phones can act as IP routers for BLE-enabled sensors and actuators. IP connectivity may dramatically increase the potential space of services and added value for BLE devices. 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 smart phones. BLE, on the other hand, is expected to have a strong position in these. Table 2 shows the main characteristics of BLE and the aforementioned technologies (classic Bluetooth has been included for comparison purposes).

V. CONCLUSIONS

This paper describes the BLE protocol stack, provides a performance evaluation of this technology and explores its potential applications. In BLE, there exists a trade-off between energy consumption, latency, piconet size, and throughput that mainly depends on the connInterval and connSlaveLatency parameters. Evaluation results show how these parameters can be tuned wisely in order to meet application requirements. On the other hand, the paper points out several implementation constraints that may reduce BLE performance in a real scenario, in comparison with the theoretically expected one. BLE emerges as a strong low-power wireless technology for single-hop communication use cases which may contribute to connecting a dramatically large amount of new devices to the Internet of Things.

REFERENCES

1. Specification of the Bluetooth System, Covered Core Package, Version: 4.0; The Bluetooth Special Interest Group: Kirkland, WA, USA, 2010.
2. Gomez, C.; Paradells, J. Wireless home automation networks: A survey of architectures and technologies. IEEE Commun. Mag. 2010, 48, 92–101.
3. Ludovici, A.; Calveras, A.; Casademont, J. Forwarding techniques for IP fragmented packets in a real 6LoWPAN network. Sensors 2011, 11, 992–1008.
4. West, A. Smartphone, the key for Bluetooth low energy technology. Available online: http://www.bluetooth.com/Pages/Smartphones.aspx (accessed on 24 June 2012).
5. Hui, J.W.; Culler, D.E. Extending IP to low-power, wireless personal area networks. IEEE Internet Comput. 2008, 12, 37–45.
6. Nieminen, J.; Patil, B.; Savolainen, T.; Isomaki, M.; Shelby, Z.; Gomez, C. Transmission of IPv6 packets over Bluetooth low energy draft-ietf-6lowpan-btle-08. 2012, in preparation.
7. Haartsen, J.C. The Bluetooth radio system. IEEE Pers. Commun. 2000, 7, 28–36.
8. Zheng, J.; Lee, M.J.; Anshel, M. Towards secure low rate wireless personal area networks. IEEE Trans. Mob.Comput. 2006, 5, 1361–1373.
9. Echevarraí, J.J.; Ruiz-de-Garibay, J.; Legarda, J.; Álvarez, M.; Ayerbe, A.; Vázaquez, J.I. WebTag: Web browsing into sensor tags over NFC. Sensors 2012, 12, 8675–8690.
10. Callegati, F.; Cerroni, W.; Ramili, M. Man-in-the-Middle attack to the HTTPS protocol. IEEE Secur. Priv. 2009, 7, 78–81.
11. Kamath, S. Measuring Bluetooth Low Energy Power Consumption; Application Note AN092; Texas Instruments: Dallas, TX, USA, 2010.
12. Ko, J.; Terzis, A.; Dawson-Haggerty, S.; Culler, D.E.; Hui, J.W.; Levis, P. Connecting low-power and lossy networks to the internet. IEEE Commun. Mag. 2011, 49, 96–101.

