Bluetooth Smart

Rui Yang

Student number: 467656

rui.yang@aalto.fi

Abstract

Bluetooth 4.x is the latest version of Bluetooth. It embraces the feature of BLE (Bluetooth Low Energy), which is one of the reasons contributing to BLE being considered an ideal platform for Internet of Things (IoT). Compared to its previous version, BLE provides improvement of power saving, lower deployment cost and enhanced radio range, etc[3]. This article will focus on the evolutions of BLE from Bluetooth 4.0 to Bluetooth 4.2, the reasons behind these changes and an analysis of a special use case.

KEYWORDS: Bluetooth Low Energy, BLE, Bluetooth Smart

1 Introduction

Bluetooth is a wireless communication technology for short range communications especially dedicated in personal area networks (PAN). Launched to this world about 21 years ago, it has been widely implemented in our societies and provided great conveniences to our daily life. For instance, more than 2.5 billion Bluetooth products were shipped in 2013[2]. Benefiting from the low energy consumption of BLE, a button sized cell can provide a Bluetooth instance running with singular module for more than 3 years depending on different use cases[3], which enlightens the way for a huge number of possible applications.

Since Bluetooth belongs to one kind of PANs, which means it is more connected to our body area, in addition to the significant importance and privacy of transmitted data, its protection of users' privacy and security issues naturally become the main focus of its users. Thus this article introduces the potential challenges regarding the concerns of privacy and security issues, and possible solutions.

2 Background

BLE is currently hosted by Bluetooth Special Interest Group (SIG), the design goals of which are lowest cost and easy to deploy. Since the classic Bluetooth is connection oriented, designed

Bluetooth Version	Speed
v 1.1	1Mbps
v 2.0	3Mbps
v 3.0	54Mbps
v 4.0	0.3Mbps

Table 1: Transmission Speed Over Different Bluetooth Version

for data streaming in the past, it means the Bluetooth instances have to keep the connection alive even there is no data needed to be transmitted. Without the integration of sleeping mode in classic Bluetooth, this mechanism has caused it huge amount of energy consumptions. This is not good for some devices which only have a button cell battery. In order to overcome this shortcoming of classic Bluetooth, SIG introduces Wibree of Nokia to be part of Bluetooth standard and this standard evolved to BLE later on. It mainly focuses on keeping the energy consumption as low as possible. To achieve this goal, classic Bluetooth is redesigned (not optimized from the classic Bluetooth) in BLE from radio, protocol stack, profile architecture and qualification regime[5].

We may benefit a lot from the BLE. However, in some use cases, the role of classical Bluetooth cannot be replaced by BLE. For instance, as table 1 shows, being limited by the transmission speed of BLE (mainly in Basic Rate, optional in Extend Data Rate), it would no longer be suitable for some applications which require huge amount of data transmission, such as data streaming for music from a mobile phone to a headset. In order to be compatible with classical Bluetooth, BLE instance can run in either single-mode or dual-mode. The instance running in the single-mode cannot communicate with classical Bluetooth while the instance running in the dual-mode is capable of.

Moreover, the BLE has the Client/Server structure in its attribute protocol. This can allow BLE connect to the wide area network while only a gateway is needed, such as a PC or mobile devices. With the expansion of the concept of IoT, in addition to the ongoing integration of IPv6 in Bluetooth 4.2, it has been estimated that more than 2 billion units of BLE will be deployed around the globe[6]. The increasing popularity and huge amount of deployment[2] requires thorough and careful analysis of potential issues behind BLE. This is one of the reason why this article is written.

One of the major competitors of BLE is IEEE 802.15.4 known as ZigBee, which uses the same radio frequency as BLE. But the shipments of ZigBee instances are not comparable with BLE[1]. It mainly because ZigBee is not embedded in commonly used PCs and mobile phones whereas BLE is. With the rapid development of IoT, the shipment of BLE instances will even be bigger. From the perspective of techniques, although ZigBee is low power and its stack is quite light, BLE has even lower power and lighter stack[5].

This article is organized as follows. Section 3 introduces the evolution of BLE essential features. Section 4 demonstrates one scenario of use cases. Section 5 presents the security

features of BLE. Section 6 concludes the article.

3 Evolutions of BLE Essential Features

3.1 Introduction to BLE

Bluetooth Smart is described as an revolutionary technology introduced in 2010. Great conveniences have been brought to its manufacturers, developers and consumers since it emerged. According to the definition from the SIG, Bluetooth Smart is an brand name for Bluetooth version 4.0 featuring low energy consumption for the first time. So, the Bluetooth Smart is also called BLE. Compared to previous versions of Bluetooth, BLE is newly designed and has a distinct feature of low energy consumption. With the flourish of Internet of Thing (IoT) and mobile devices, it has been estimated that more 2 billion units of BLE will be deployed around the globe[6].

Normally, the design goal determines a product in respect of functionalities and performances. The goal of the classic Bluetooth is to stand by for several days or data streaming for several hours., while the BLE is designed to stand by for several years collecting or broadcasting data such as temperature and location information. In the earlier design of BLE, it is aimed to be equipped with several key features, including low cost, supporting worldwide operation, low power consumption and robustness, etc. All of these design goals determine how each sub-systems in BLE should be implemented. In order to achieve the lowest cost, the system shall be kept as small and efficient as possible and new methodologies should be adapt to boost the performance. For instance, to provide supports for new network topologies, BLE has been optimized to low the cost using research based methodology[4]. In addition, BLE uses the 2.45GHz ISM band to transfer signals to support worldwide operations. However, this radio band is unlicensed and every organization can use it for commercial purpose. As a result, it is crowded with many transmission signals such as Bluetooth and Wi-Fi. In order to co-exist in such a radio band, a mechanism called Adaptive Frequency Hopping has been introduced to help Bluetooth avoid signal conflicts. Last but not least, the low energy consumption feature has had a great impact on the design of the protocol stack of BLE. For example, the link layer has been considered as the most complicated layer in the Bluetooth protocol stacks. While in BLE, the link layer has been lightened and even provides super low energy consumption.

For a successful technology like Bluetooth, even with the revolutionary update, all the traditional features of classical Bluetooth should be included in the BLE as well. So in order to inherit all the features from previous version of Bluetooth at the same time, the BLE is designed to run in two modes: single-mode and dual-mode. In single-mode implementation, only the low energy protocol stack is implemented. In dual-mode implementation, the functionalities of BLE is integrated in classic Bluetooth controller[7]. Furthermore, one thing needed to be mentioned is

its change of transmission speed. Because of the top concerns of low energy consumption, BLE commonly adopts the Basic Rate (BR) with transmission rate about 0.3 Mbps while optional with Enhanced Data Rate (EDR)(see in table 1).

In sum, low energy, as the revolutionary feature of BLE, influenced BLE from its design to implementation. As its expanded feature, new applications shall be rising and benefits will be brought to its manufactures, developers and consumers.

3.2 Evolutions introduced in Bluetooth 4.1

3.3 Evolutions introduced in Bluetooth 4.2

4 User Case Demonstration

5 Security Features

5.1 Safe Communication

5.2 Possible Security Issues and Solutions

6 Conclusion

References

[1] Z. Alliance. Market Leadership. Technical report, ZigBee Alliance, Available on February 2014. http://old.zigbee.org/About/AboutTechnology/MarketLeadership.aspx.

[2] Bluetooth.org. History of the Bluetooth Special Interest Group. Technical report, Bluetooth Special Interest Group, Available on February 2015. http://www.bluetooth.com/Pages/History-of-Bluetooth.aspx.

[3] Bluetooth.org. The Low Energy Technology Behind Bluetooth Smart. Technical report, Bluetooth Special Interest Group, Available on February 2015. http://www.bluetooth.com/Pages/low-energy-tech-info.aspx.

[4] R. Heydon. *Bluetooth Low Energy: the developer's handbook*. 2013.

[5] S. A. Joe Decuir. Bluetooth 4.0: Low Energy. Technical report, CSR plc, Available on February 2015. http://chapters.comsoc.org/vancouver/BTLER3.pdf.

[6] A. West. Smartphone, the key for Bluetooth low energy technology. Technical report, IMS Research, Available on February 2015. http://www.bluetooth.com/Pages/Smartphones.aspx.

[7] Wikipedia. Bluetooth. Technical report, avaiable on Feb. 16th, 2015. http://en.wikipedia.org/wiki/Bluetooth.