A Comprehensive Study of Bluetooth Low Energy

Chendong Liu1,†, Yilin Zhang2,† and Huanyu Zhou3,*,†

1Electronic Information Engineering, Nanjing Tech University, Nanjing, Jiangsu, 210000, China
2Electrical Engineering, Xi’an Jiaotong University, Xi’an, Shaanxi, 710049, China
3Electronic Information Engineering, Nanjing Tech University, Nanjing, Jiangsu, 210000, China
*Corresponding author’s e-mail: 201821139038@njtech.edu.cn
†These authors contributed equally.

Abstract: Bluetooth Low Energy (BLE) is an innovative technique that was firstly employed in Bluetooth 4.0 and is being applied in the Bluetooth 5.0 and 5.2 technologies. Bluetooth 5.0 and 5.2 technologies are now widely used in all kinds of electronic communication equipment (e.g., PCs, tablets, smartphones, wearable devices). BLE has the capacity to minimize the power consumption and equipment cost in the low-power devices, which becomes a competitive scheme among the huge number of standard wireless transmission techniques already existing in everyday life for a large number of applications. As one of the available solutions in wireless transmission, Bluetooth technology equipped with the BLE module is very suitable for developing internet of things (IoTs) technology, which is gaining more and more interest. This paper briefly introduces the modulation and encoding of the BLE standard in the physical layer (PHY). The applications of cyclic redundancy check (CRC) in BLE are then presented. Moreover, the main characteristics, including the maximum reachable range, transmission latency, and power consumption of BLE, are also introduced.

1. Introduction

The concept of the internet of things (IoTs) was firstly presented by the International Telecommunication Union (ITU) in 2005 [1], and a conventional and universally recognized concept of IoTs was established until 2009. In the past decade, great progress has been made on IoTs. The new technology of connecting sensors with the existing Internet is rapidly spreading. The intelligent recognition and management of industry are gradually realizing, and the real-world objects are transformed into intelligent virtual objects. The goal of IoTs is to unify everything connected with the Internet (e.g., intelligent furniture, intelligent traffic network, intelligent medical, intelligent grid, intelligent logistics, intelligent car, and intelligent agriculture). Under a common infrastructure through the small, compact, and embedded sensors, wireless transmission between these sensors and the base stations (BSs) plays an important role. There are many wireless transmission solutions, such as IEEE 802.11 (WiFi) technology, ZigBee, Bluetooth Classic, and Bluetooth Low Energy (BLE). Though the WiFi technology can achieve high data rate transmission, it brings great power consumption. Moreover, compared with the BLE technology, WiFi is inconvenient from the perspective of device connection. BLE merging together low-energy consumption and widespread diffusion is developed by the Bluetooth Special Interest Group (SIG) as an innovative technology. It has become one of the main technologies to promote the
development of the IoT [2,3].

The Bluetooth was first named by Jim Kardach, which aimed to become a unified and universal transmission standard and connect all disparate devices and content. The real development of Bluetooth started in World War II. The core of Bluetooth is short-range radio communication. Its foundation comes from the frequency hopping spread spectrum (FHSS) technology that was not recognized until the end of the last century. In 1999, Bluetooth 1.0 was published by the Bluetooth Special Interest Group (SIG), which was an early exploration achievement of short-range communication. However, Bluetooth 1.0 was buried due to some unsolved problems, e.g., it was difficult to be compatible with some products, and anonymity could not be achieved at the protocol level, which caused the risk of data leakage [4]. In 2004, Bluetooth 2.0 added Enhanced Data Rate (EDR) technology enhanced the ability of multi-tasking and supported multiple Bluetooth devices running simultaneously, and the transmission rate was up to 3Mbps. Moreover, the Bluetooth 2.0 could support the duplex mode, which could transmit documents or high-quality pictures simultaneously for voice communication. In 2009, the core of Bluetooth 3.0 used the new alternating radiofrequency technology Alternate MAC/PHY (AMP). The AMP technology allowed the Bluetooth protocol stack to select the correct radio frequency for any task dynamically.

Bluetooth 4.1 and 4.2 integrated three modes, i.e., low-power Bluetooth, traditional Bluetooth, and high-speed Bluetooth, was successfully equipped with BLE [5]. Compared with 4.0, Bluetooth 5.0 greatly improved power consumption, capacity, transmission speed, and coverage [6]. A brief history of Bluetooth is shown in Figure 1.

![Figure 1. A brief history of Bluetooth.](image-url)

Bluetooth 5.2, joined with the latest Low Complexity Communication Codec (LC3), improving the processing speed [7]. However, some problems are still unsolved, such as short coverage and transmission distance, occasional connection failure. Although the data transmission speed of Bluetooth 5.0 has doubled compared with Bluetooth 4.0, the transmission efficiency has not doubled. The limitation of Bluetooth will also become the limitation of the development of the IoT, thus solving the defects of Bluetooth technology will be a key to the technological breakthrough of IoT. BLE enhances the transmission distance as a module used after Bluetooth 4.0 and reduces the long response delay. Meanwhile, it also further reduces the energy consumption based on Bluetooth, thus allowing a button battery to support the operation of the device for several months or even years.

BLE mainly uses the CRC check codes. As a widely used check code, CRC is often used in the data link layer to check whether the network packet is wrong or not. If the test result is wrong, the data will be retransmitted. This leads to a waste of time for retransmission once an error occurs. If the check function based on the CRC check code can be optimized, the transmission time will be greatly shortened. This work is organized as follows:

Firstly, the modulation and coding performance of BLE at the physical layer (PHY) are discussed, which includes the BLE core and its protocol layer, the BLE work field, the GFSK technology used in PHY, and the new 2M PHY.

Then, the main characteristics, e.g., the maximum reachable range, transmission latency, and power consumption of BLE, are presented.

Finally, the application principle of CRC check in BLE is presented, and we also give the use area and significance of CRC.
2. Physical layer modulation

2.1. PHY structure of BLE
The Bluetooth protocol consists of two levels of protocols, i.e., Bluetooth core and Bluetooth application. The Bluetooth core protocol contains two parts, the BLE controller and the BLE host. The physical layer is the lowest layer protocol of the BLE core protocol layer. Its function is to specify the wireless frequency band, modulation, and demodulation methods used by BLE.

2.2. The role and modulation method of PHY
BLE transmits on the 2.4GHz band, also known as the industrial, scientific, and medical (ISM) band. Since 2.4GHz is an unlicensed frequency band, it can be used for free in short-distance transmission, which is very suitable for Bluetooth transmission. However, the data transmission at 2.4 GHz often becomes congested. In BLE, information at PHY is transmitted by using a scheme called Gaussian Frequency Shift Keying (GFSK). This is an improvement of the frequency shift keying (FSK) in which digital information is transmitted through discrete frequency changes of a carrier signal [8], and two different frequency oscillations are used to represent two different signals, 1 and 0 at FSK.

Based on the modulation scheme, multiple symbols may be used to represent a single bit, or a single symbol can potentially represent multiple bits. GFSK modulation is a digital modulation method in which the input data is pre-modulated and filtered by a Gaussian low-pass filter, and then FSK modulation is performed. GFSK has the potential to remove Gaussian noise from the input signal. With the BLE modulation specifically, the zero is coded to a negative frequency deviation of at least 185kHz. The one is coded to a positive frequency deviation of at least the same amount.

2.3. New PHY configuration
The 2Mbit PHY is a new PHY configuration introduced in BLE 5.0. This new configuration has the capacity to increase the symbol rate at PHY, which can achieve a symbol rate of 2M symbols per second, and each symbol corresponds to a bit. Compared with 1Mbit, the new configuration can halve the transmission data time of the signal, thus reducing the energy consumption. A 2Mbit PHY requires a frequency deviation of at least 370 kHz instead of 185 kHz for 1M bit. It is noticed that although the
transmission data has doubled, the transmission efficiency has not doubled. One reason is that the inter-frame interval remains the same, which results in an increase of time used for the inter-frame interval. The other reason is that the numbers of TX-RX exchanges have increased during data transmission.

3. The fundamental of BLE
In this section, the main characteristics, including the maximum reachable range, transmission latency, and power consumption of BLE, are introduced.

3.1. Range
In the BLE radio frequency (RF) module, the type of antenna and path loss strongly influence the maximum reachable range of the radio signal. The type of antenna used in the BLE RF module includes printed circuit board (PCB), chip, and whip. While the path-loss, defined as the signal strength difference between the transmitter and receiver, represents the reduction of a radio signal. Moreover, the formulation between the path-loss and the distance ($d$) is given in [9] as

$$\text{pathloss} = 40 + 25 \times \log(d)$$  

(1)

Figure 3 is the relationship between path loss and the range ignoring the noise or loss in the condition.

The sensitivity of a BLE receiver is prescribed to be no more than -70dBm according to the BLE specification [9]. While the transmitter power is strictly limited between -20 dBm to +20 dBm. Specifically saying, the BLE IC of STMicroelectronics has a radio power form -18dBm and +8 dBm [10].

If a transmitter is with +8 dBm power and a receiver is with -70dBm power, then the path-loss is +78dB, and the communication range of BLE may reach 33m. Moreover, with the assist of the received signal strength indicator (RSSI) in the RF module, the BLE can also be used to measure the distance of different network nodes [11-15]. And the formulation between the RSSI and the distance $d$ is presented in [16] as

$$\text{RSSI} = -10 \times N \times \log(d) + a$$  

(2)

where $N$ denotes a constant assumed as one, and $a$ is the Tx transmit power at a one-meter distance.
With the continuous development of BLE technology in recent years, Bluetooth is bound to become the best choice for IoT in the future. However, the power limitation of Bluetooth's low energy makes it impossible to extend the propagation distance of Bluetooth technology indefinitely. How to increase the propagation distance as much as possible while ensuring the power loss will be a problem to be solved and the main research direction in the future.

3.2. Latency

Latency denoted as the transmission time interval of a data packet from one node to another node, plays an important role in the performance of BLE. In the BLE transmission, the latency can be modeled and measured during the connection or discovery phase. This paper will focus on the discovery latency, which represents the time interval from the transmitter transmitting the advertising information to the point when the receiver receives the information. Moreover, the discovery latency is determined by a random probability process. Since the BLE advertising device is detected through a process based on broadcast advertising messages, the process uses three separate channels to reduce interference. It sends a packet on at least one of these channels, whose repetition period is called advertising interval. And the scanner listens to the channel for a duration called the scan window, which is periodically repeated every scan interval. Therefore, the length of successful discovery latency depends on the probabilistic process, i.e., the number of attempts failed by the scanner in the discovery process. In terms of process details, it is affected by three variables, i.e., advertising interval, scan interval, and scan window.

The smaller the advertising interval that the advertiser sends and the larger the scan window and the larger the scan interval of the scanner, the easier it is to form a smaller discovery latency because, in this way, the process has higher fault tolerance and a higher probability of successful scanning [17, 18]. However, it should be noted that in the process of running the simulation, the length of the scan interval should be greater than or equal to the length of the scan window, and it is better to keep the length of the scan interval greater than the length of advertising interval. Otherwise, it will fail to model the abrupt process of discovery latency in reality.

Based on existing research, Kim and his team proposed a new discovery mechanism to reduce collision and unsuccessful discovery, which improved the BLE performance of the latency to some extent [19]. They defined two new parameters $\alpha$ and $\beta$, which are the ratios of advertising Interval and scan Interval on average discovery latency $T$, respectively. Then they obtained the average delay of the fixed value $\alpha$ and the change value $\beta$ and vice versa. They analyzed the model's data composed of average discovery latency and these two parameters, and the results also proved the relationship described above. Similarly, the correctness of Kim and his team's model analysis was confirmed in another set of model studies [20]. Furthermore, it should be noted from [19] that in the process of running the simulation, the length of scan Interval should be greater than or equal to the length of the scan window, and it is better to keep the length of scan Interval greater than the length of advertising Interval. Otherwise, it will fail to model the abrupt process of discovery latency in reality.

Nowadays, new network connection technologies for BLE are coming into being. Since the latency is closely related to other parameters such as energy consumption, these emerging technologies can reduce energy consumption or improve some other BLE performance based on a significant reduction in latency.

The continuous development of BLE technology has indeed brought a lot of convenience to our lives, but there are still some problems that need to be solved. In addition to the propagation range mentioned above, how to reduce the Bluetooth delay as much as possible and increase the system capacity as much as possible is also a problem we have to face. Latency is a common problem of every propagation method. Although Bluetooth 5.0 technology has made improvements in this regard, it is still necessary to reduce the delay as much as possible for the needs of the Internet of Things in the future. The BLE broadcast capacity is the key to the development of IoT. In the future, massive IoT devices will be deployed in a certain range with ultra-high-density, and the question of how to expand the system capacity is crucial.
3.3. Power consumption

Compared with the past Bluetooth technology, the most significant feature of BLE is the low power consumption. The main reasons why BLE can achieve low power consumption are as follows.

Firstly, to reduce energy consumption, BLE stays in sleep mode most of the time and only wakes up the device when activity occurs. BLE has designed a deep sleep state (Duty-Cycle) to replace the idle time of traditional Bluetooth, and during the Duty-Cycle, the data transmission interval is also increased. In the sleep phase, the current consumption is approximately 1 µA. In addition, BLE has been modified compared to the traditional Bluetooth in broadcast mode and scanning mode.

Through searching for information, we know that the power consumption is proportional to the data length and the number of channels used for communication and inversely proportional to the communication interval. Meanwhile, it is noticed that in the broadcast mode, BLE only uses 3 broadcast frequency bands, while the traditional Bluetooth uses 16 to 32 frequency bands for broadcasting. Such changes greatly reduce power consumption. In scanning mode, BLE allows the broadcasting devices to connect with the scanning devices. Still, the past Bluetooth specification stipulates that if a device is broadcasting, it will not respond to the current device scanning, which will cause duplication. Connection results in unnecessary power loss. Through the improvement of the connection mechanism, the BLE connection establishment process can be controlled within 3ms. Furthermore, during the transmission of advertising and connected data packets, specific BLE IC and FW vendor implementations will slightly affect the device's power consumption.

4. CRC error correction

4.1. The working principle of CRC error correction code

This section first briefly introduces the principle of cyclic redundancy check (CRC), which uses the principle of division and remainder to detect errors. The basic idea of CRC is to add an N-bit redundancy number (i.e., the check code used for verification) after the frame to be sent, and generate a new frame and send it to the receiving terminal. This additional N-bit redundancy number is not arbitrary. It must make the generated new frame divisible by a specific number jointly selected by the sender and the receiver. After arriving at the receiving end, the received new frame is divided by the selected divisor. The result should be no remainder because the sender has already added a number to "remainder" before sending the data frame. If there is a remainder, it indicates that an error occurs during the transmission of the frame.

4.2. Application of CRC in BLE

From the BLE protocol framework, we can know that the link layer is located in the second layer of the BLE controller in the Bluetooth core protocol. The function of the data link layer is to allow the data packets received by the network layer to be reliably transmitted on the bit channel of PHY, mainly to check and deal with transmission errors. Therefore, the data link layer performs a CRC check on each frame of data to determine whether the data transmission of each frame is correct or not. The sender will add a set of results calculated based on the CRC at the end of a frame, and the receiver will perform the same CRC algorithm on the part before the end of the frame. The reason why the data link layer protocol almost always puts CRC at the end of the transmission frame is the list as follows:

Before each hop of the data frame, the source MAC, destination MAC, and other optional field items must be modified. The CRC is calculated during transmission. Once the last bit of data is sent to the outgoing line, the CRC code is immediately appended to the output stream. If it is placed in the header, the entire frame must be checked before sending to calculate the CRC so that each byte has to be processed twice. The check code is calculated in the first pass, and the sending check is done in the second pass. So, putting it at the tail can halve the time.

5. Conclusion

In this paper, we have briefly presented the evolution of BLE and introduced the modulation and coding
of the BLE standard at the physical layer (PHY). Moreover, the application of cyclic redundancy check (CRC) in BLE has been presented. The future directions of BLE have been given. The directions, including ranges, power consumption, and broadcasting capacity, have been given. We believe that this survey review can provide academic researchers and industry experts with sufficient insightful thoughts on BLE developments.

References

[1] Palattella, M.R., Dohler, M., Grieco, A., Rizzo, G., Torsner, J., Engel, T., Ladid, L. Internet of Things in the 5G. Era: Enablers, Architecture, and Business Models. *IEEE J. Sel. Areas Commun.* 2016, 34, 510–527.

[2] specifications/adopted-specifications (accessed on 15 May 2017) Pau, G.; Collotta, M.; Maniscalco, V. Bluetooth 5 Energy Management through a Fuzzy-PSO Solution for Mobile Devices of Internet of Things. Energies 2017, 10, 992.

[3] Marco, P.D.; Skillerman, P.; Larmo, A.; Arvidson, P.; Chirikov, R. Performance Evaluation of the Data Transfer Modes in Bluetooth 5. IEEE Commun. Stand. Mag. 2017, 1, 92–97.

[4] C. J. Mathias, “Bluetooth is dead,” EETimes, October 2003.

[5] Bluetooth Special Interest Group, “Bluetooth Core Specification Version: 4.0; 4.1; 4.2,” 2010; 2013; 2014.

[6] Bluetooth Special Interest Group, “Bluetooth Core Specification Version: 5.0,” 2016.

[7] Bluetooth SIG. Adopted Specifications in Bluetooth 5. Available online: https://www.bluetooth.com/

[8] Kennedy, G.; Davis, B. (1992). Electronic Communication Systems (4th ed.). McGraw-Hill International. ISBN 978-0-07-112672-4., p 509. Heydon, K. The Physical Layer. In Bluetooth Low Energy--The Developer’s Handbook; Goodwin, B., Ed.; Prantice Hall-Pearson Education, Inc.: Upper Saddle River, NJ, USA, 2012; pp. 59–69.

[9] BluetoothSIG. Vol 6: Core System Package [Low Energy Specification], Part A: Physical Layer Specification. In Specification of the Bluetooth® System, Covered Core Package Version: 5.0; The Bluetooth Special Interest Group: Kirkland, WA, USA, 2016; pp. 2532–2546.

[10] STMicroelectronics. Upgradable Bluetooth® Low Energy Network Processor. In Datasheet-Production Data BlueNRG-MS 2016; STMicroelectronics: Ginevra, Svizzera, 2016.

[11] Koodtalang, W.; Sangsuwan, T. Improving motorcycle anti-theft system with the use of Bluetooth Low Energy 4.0. In Proceedings of the 2016 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS), Phuket, Thailand, 24–27 October 2016; pp. 1–5.

[12] Ozer, A.; John, E. Improving the Accuracy of Bluetooth Low Energy Indoor Positioning System Using Kalman Filtering. In Proceedings of the 2016 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 15–17 December 2016; pp. 180–185.

[13] Peng, Y.; Fan, W.; Dong, X.; Zhang, X. An Iterative Weighted KNN (IW-KNN) Based Indoor Localization Method in Bluetooth Low Energy (BLE) Environment. In Proceedings of the 2016 International IEEE Conferences on Ubiquitous Intelligence Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld), Toulouse, France, 18–21 July 2016; pp. 794–800.

[14] Bae, H.; Oh, J.; Lee, K.; Oh, J.H. Low-cost indoor positioning system using BLE (bluetooth low energy) based sensor fusion with constrained extended Kalman Filter. In Proceedings of the 2016 IEEE International Conference on Robotics and Biomimetics (ROBIO), Qingdao, China, 3–7 December 2016; pp. 939–945.

[15] Bae, H.; Oh, J.; Lee, K.; Oh, J.H. Low-cost indoor positioning system using BLE (bluetooth low energy) based sensor fusion with constrained extended Kalman Filter. In Proceedings of the
2016 IEEE International Conference on Robotics and Biomimetics (ROBIO), Qingdao, China, 3–7 December 2016; pp. 939–945.

[16] Karani, R.; Dhote, S.; Khanduri, N.; Srinivasan, A.; Sawant, R.; Gore, G.; Joshi, J. Implementation and design issues for using Bluetooth low energy in passive keyless entry systems. In Proceedings of the 2016 IEEE Annual India Conference (INDICON), Bangalore, India, 16–18 December 2016; pp. 1–6.

[17] Cho, K.; Park, W.; Hong, M.; Park, G.; Cho, W.; Seo, J.; Han, K. Analysis of Latency Performance of Bluetooth Low Energy (BLE) Networks. Sensors 2014, 15, 59–78.

[18] Cho, K.; Jung, C.; Kim, J.; Yoon, Y.; Han, K. Modeling and analysis of performance based on Bluetooth Low Energy. In Proceedings of the 2015 7th IEEE Latin-American Conference on Communications (LATINCOM), Arequipa, Peru, 4–6 November 2015; pp. 1–6.

[19] Liu, J.; Chen, C.; Ma, Y. Modeling Neighbor Discovery in Bluetooth Low Energy Networks. IEEE Commun. Lett. 2012, 16, 1439–1441.

[20] Jeon, W.S.; Dwijaksara, M.H.; Jeong, D.G. Performance Analysis of Neighbor Discovery Process in Bluetooth Low-Energy Networks. IEEE Trans. Veh. Technol. 2017, 66, 1865–1871.