Bluetooth Low Energy Reliability and Throughput under Wi-Fi Interference

Bozheng Pang[1], Tim Claeys[2], Kristof T'Jonck[1], Hans Hallez[1] and Jeroen Boydens[1]
[1]Department of Computer Science, M-Group, KU Leuven Bruges Campus
[2]Department of Electrical Engineering, M-Group, KU Leuven Bruges Campus
Spoorwegstraat 12, 8200 Bruges, Belgium
{bozheng.pang | tim.claeys | kristof.tjonck | hans.hallez | jeroen.boydens}@kuleuven.be

Abstract – **In this paper, the performance of Bluetooth Low Energy is studied under different Wi-Fi interference. Two aspects of BLE performance are investigated, namely reliability and throughput. According to the practical experiment results, both the reliability as well as the throughput are highly impacted by Wi-Fi interference. Besides, a new discovery is that the impacts of interference on the two performance aspects are not proportional to one another. This research can be utilized by other studies as a proof or cornerstone.**

Keywords – **Bluetooth Low Energy (BLE); reliability; throughput; interference; practical study.**

I. INTRODUCTION

Internet of Things (IoT) has been a trending concept for years. It refers to the technology which allows diverse devices and systems to communicate and exchange data [1]. Within IoT systems, wireless connectivity is an inevitable research topic. According to different requirements of IoT applications, various wireless communication protocols are introduced, such as Wi-Fi and Bluetooth Low Energy (BLE) [2].

As a prominent wireless technology, BLE is a typical communication protocol utilized by IoT applications [3]. It works in the 2.4 GHz frequency band, which suggests that a challenge for BLE is to maintain its performance under interference from other wireless technologies in the same frequency band [4]. Similarly, Wi-Fi is another popular wireless technology operating in the 2.4 GHz frequency band. Naturally, Wi-Fi becomes a noticeable interference source for BLE [4]. A salient difference between Wi-Fi and BLE is that a Wi-Fi (IEEE 802.11) channel consumes more bandwidth than a BLE (IEEE 802.15.1) channel. Depending on the version, Wi-Fi can have varying features, however, a Wi-Fi channel normally fills approximately 10 BLE channels or more. As a result, the performance of BLE is possibly highly impacted by Wi-Fi signals.

To cope with Wi-Fi interference, BLE applies an adaptive frequency hopping (AFH) scheme to ensure communication performance, such as reliability and throughput [3]. The AFH allows BLE devices to hop within the 2.4 GHz frequency band, trying to avoid the spectrum occupied by Wi-Fi [5]. It is based on channel selection algorithms (CSAs), which synchronize the hopping process for BLE devices within the same BLE connection [6]. It has been proved that, with some improvements, the CSAs are able to detect and avoid Wi-Fi interference [7], [8]. However, the current BLE specification does not provide any standard methodology for interference detection and avoidance [5]. This leads to random frequency hopping even under some interference, such as Wi-Fi. As a result, the performance of BLE is highly impacted.

Among different performance aspects of BLE communication, reliability and throughput are two of the major focuses [7], [9]. Reliability is a term widely used in wireless communication to describe the data delivery status [10]. Wireless communication technologies are mostly requested to achieve high reliability, which means the data should be delivered as much and correct as possible. Throughput is a parameter measuring the amount of successful data delivered over a certain period [11]. The limit of it might vary greatly depending on the characteristics of various wireless communication protocols. In practice, real throughput often differs from theoretical throughput due to factors such as hardware limitations and interference [12]. In this paper, the reliability and throughput of BLE under Wi-Fi interference are explored. It can be viewed as a preliminary study for additional research into this topic, such as modeling BLE communications under interference.

The remainder of this paper is arranged in the following manner. The communication principle and performance are briefly explained in Section II. The experimental setup used to test the reliability and the throughput is presented in Section III. The results are discussed in Section IV. Conclusion and future work are mentioned in Section V.

II. COMMUNICATION AND PERFORMANCE

BLE is a widely used wireless technology that operates in the 2.4 GHz frequency band. To reduce interference, the BLE specification employs AFH, which divides the spectrum into 37 data channels and allows BLE to hop pseudo-randomly among them. The CSAs are considered the foundation of AFH, which are used to calculate the pseudo-random channel from the 37 channels defined [5]. Each time a BLE connection hops to a channel, it stays there for a certain amount of time, which is called a connection interval. At the start of a connection, the devices in the BLE connection, central and peripheral, negotiate the connection interval. The central and the peripheral start to exchange data packets at the beginning of each connection interval.

By hopping pseudo-randomly in the 2.4 GHz frequency band, some random interference might be avoided. Hence, BLE communication reliability is mostly guaranteed by the AFH scheme. To quantify the reliability of the BLE connection, the packet delivery ratio (PDR) is commonly used [7]. It defines the ratio of packets that are successfully acknowledged to a destination compared to the number of packets

2022 XXXI International Scientific Conference Electronics (ET) | 978-1-6654-9878-4/22/$31.00 ©2022 IEEE | DOI: 10.1109/ET55967.2022.9920206

that have been sent out by the sender. To measure the PDR, the work in [13] is adapted to be used in BLE connections. The PDR can be measured on both sides of the BLE connection, however, it is only recorded on the central device in this paper. It is calculated by dividing the number of valid acknowledgments received on the central device, i.e. *ack(c)*, by the number of packets sent from the central device, i.e. *tx(c)*. The mathematical expression is shown as Equation (1).

$$Reliability = PDR = \frac{ack(c)}{tx(c)} \quad (1)$$

As for the throughput, it can be calculated by involving the connection interval, since the BLE connection exchanges data according to the connection interval. The throughput describes the data rate of the BLE connection and is usually expressed in bits per second (bps). To keep the consistency with the reliability measurement, the throughput is also measured on the central side. Hence, by dividing the data received on the central device, i.e. *data(c)*, by the product of the connection interval value and the number of connection intervals passed, i.e. CI×num_CI, the throughput can be calculated. The mathematical expression is Equation (2). Note that the throughput in this paper is single-direction throughput.

$$Throughput = \frac{data(c)}{CI \times num\_CI} \quad (2)$$

III. Experimental Setup

The experimental setup described in this section is designed to test the reliability and throughput of a BLE connection when it is subjected to Wi-Fi interference. Fig. 1 depicts the arrangement schematically for simplicity of comprehension.

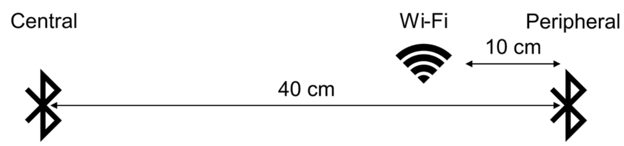

Fig. 1. Schematic of the experimental setup

As shown in Fig. 1, the experimental setup consists of a BLE connection with two BLE devices involved, and a Wi-Fi device as the interference source. Two BLE development boards, nRF52840 DK, are deployed in an office environment, with a distance of around 40 cm between one another [14]. The Wi-Fi interference is generated by a Raspberry Pi, which is located between the two BLE devices and 10 cm away from the peripheral one [15].

To build a BLE connection between the two nRF boards, Zephyr RTOS is employed, which is a fully open-source real-time operating system for BLE [16]. It allows the developers to have more control over the BLE connection, such as link-layer parameters [7]. Through Zephyr RTOS, we build up the BLE connection with the parameters needed. The transmission power of both the central and the peripheral is set to 0 dBm. LE 1M PHY is the physical mode used in the experiments, which refers to the bit rate of the physical layer. The connection interval is set to 7.5 ms, which is the minimum value allowed by the BLE specification. Each connection interval is manipulated to exchange only one pair of packets, while the payload sizes of both packets vary between 100, 150, and 200 bytes, to simulate different BLE communication scenarios.

The Wi-Fi interference is generated by the Raspberry Pi device. To do so, a tool to produce noisy radio frequency environments is implemented, called JamLab-NG [17]. It allows the user to simulate Wi-Fi communication with just one Raspberry Pi, instead of two devices. Through JamLab-NG, the Wi-Fi interference can be controlled with the selected parameters. The transmission power is set to 30 dBm so that the interference is strong enough to disturb the BLE communication. The Wi-Fi channel is also a parameter that can be changed by the users. Each Wi-Fi channel overlaps with 10 BLE channels. In all the experiments, only Wi-Fi channels 1, 6, and 11 are used, since they are the most popular channels used by Wi-Fi.

The experiments include two variables, BLE payload size, and Wi-Fi interference channel. The BLE connection varies its payload size under Wi-Fi interference. The Wi-Fi interference is changed among no interference, static interference on Wi-Fi channel 1, and dynamic interference on Wi-Fi channels 1, 6, and 11. The dynamic Wi-Fi interference alters within the three channels randomly, and the channel occupied period is also a random value from 1 s to 10 s. All the experiments focus on the reliability and throughput of the BLE connection, which can be calculated by Equations (1) and (2). Extra codes are added in Zephyr RTOS to log the inputs required for the equations, specifically in the application and link layers. To reach a stable result, each payload size under each type of Wi-Fi interference is tested for 10000 connection intervals. The reliability and throughput are calculated for the whole connection each time a packet is received on the BLE central side. With these experimental logics/ideas in mind, the experiments are conducted, and the reliability and throughput are recorded.

IV. Results and Discussion

In this section, the experimental results are shown and discussed. They are investigated in two categories, reliability and throughput.

A. Reliability

Fig. 2 shows the results of the reliability measurement with three different BLE payload sizes under three different Wi-Fi interference environments. It is reasonable that interference causes the reliability to decrease, thus the reliability under static and dynamic Wi-Fi interference is always lower than the one without Wi-Fi interference. However, the dynamic Wi-Fi interference does not necessarily lead to lower reliability than the static Wi-Fi interference. This phenomenon is noticed during our experiments but is out of the scope of this paper, thus not shown in any figures. The dynamic Wi-Fi is random on both the frequency and time domains, hence there is a chance that the BLE avoids the dynamic interference more than the static one. We suppose that the probability is influenced by many parameters, including the BLE connection interval and the Wi-Fi dynamic features.

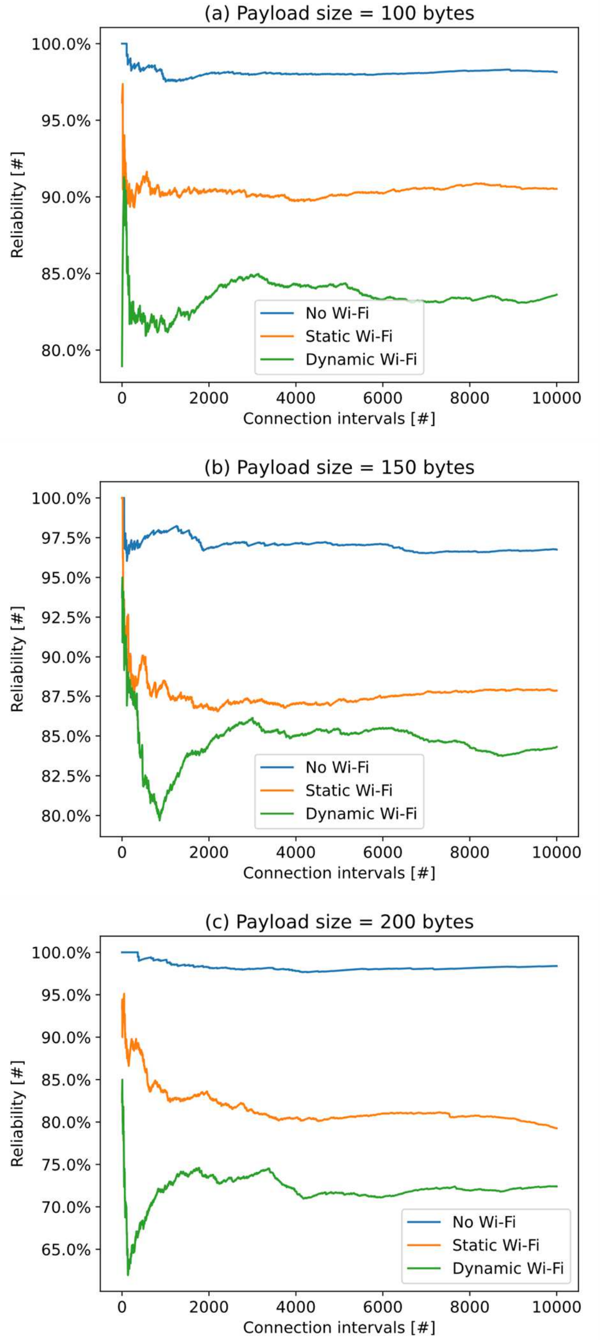

Fig. 2. Results of reliability measurement with various BLE payload sizes and Wi-Fi interference

The three curves without Wi-Fi interference in Fig. 2 demonstrate the BLE connection reliability in an office environment. They serve as a foundation for reliability measurement. As can be observed, in all the three plots, the measured reliability remains between 95% and 100%. They are not 100% constantly due to the sporadic interference in the office environment. The curves under static Wi-Fi interference show how the size of the BLE payload has an impact on BLE communication reliability. With the increment of the BLE payload size from 100 bytes to 200 bytes, the reliability decreases from 90% to 80%. Similarly, the reliability under the dynamic Wi-Fi interference decreases from around 85% to 70%. The payload size of 150 bytes does not show much difference from the 100-byte payload, which can be explained by our assumption before.

B. Throughput

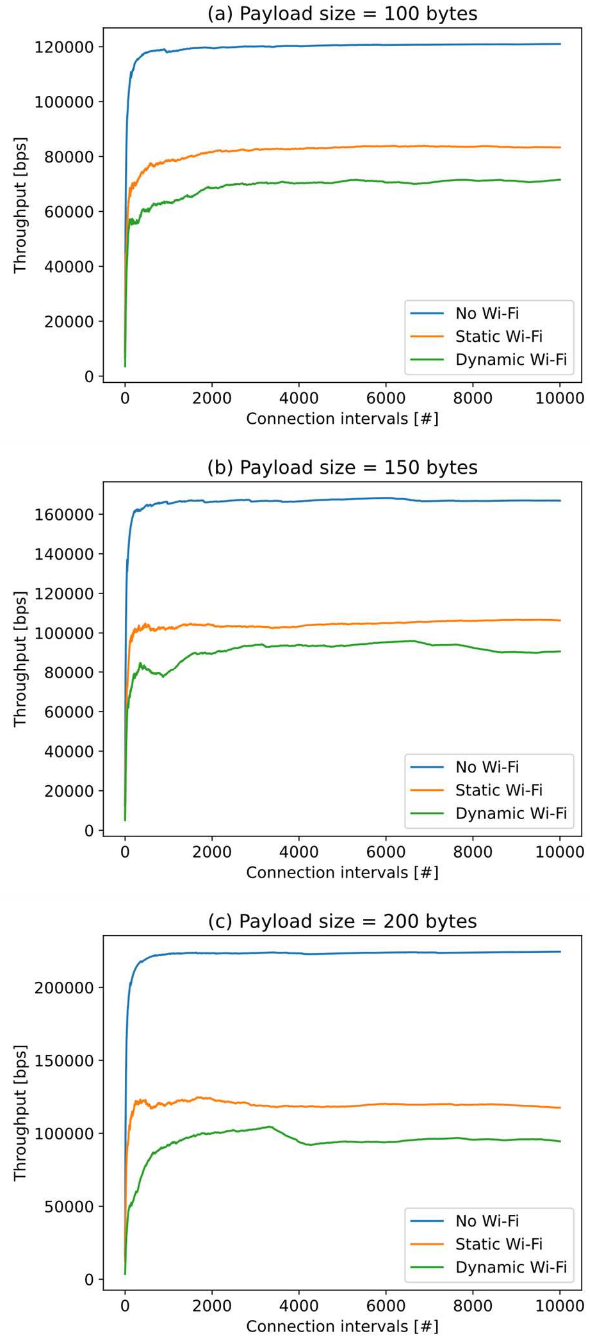

Fig. 3. Results of throughput measurement with various BLE payload sizes and Wi-Fi interference

Fig. 3 illustrates the results of the throughput measurement with three different BLE payload sizes under three different Wi-Fi interference environments. Similar to the reliability, the throughput drops when there is interference. A general trend for all the measured results is that the throughput always starts with a low value and raises to its steady value within a short period. Based on the results shown in Fig. 3, the short period is mostly within 1000 connection intervals.

As a hint to BLE developers/users, the stable throughput is recommended to be measured after a certain period.

Some details inside Fig. 3 are interesting and thus are further studied below. The theoretical throughput values with no interference calculated through Equation (2) are 121600 bps, 174933 bps, and 228266 bps respectively, while the measured values are 120967 bps, 166814 bps, and 224430 bps. The maximum difference between the theory and the practice is approximately 4.6%, which is similar to the results reported in [12]. The reasons behind this are the sporadic interference from the office environment and the hardware and BLE stack limitations.

C. Discussion

Under all interference environments, the throughput increases almost linearly as the payload size increases. Although the throughput and reliability results are measured together in the same connection, they seem to have no direct relation between them, especially under some interference. For instance, when the BLE connection is with a payload size of 100 bytes and under static interference (Fig. *2* (a) and Fig. *3* (a)), the reliability is measured as 90.5% and the throughput is 83317 bps. Compared with the results of the same payload size under no interference, 98.1% and 120967 bps, the reliability is 7.6% different, while the throughput is a difference of 31.1%. In other words, the 7.6% reduction in reliability results in a 31.1% reduction in throughput. Our explanation for this phenomenon is the retransmission mechanism applied by BLE. However, to confirm the exact relationship between BLE reliability and throughput, more research is needed.

V. Conclusion and Future Work

In conclusion, this research investigates BLE in terms of its reliability and throughput under Wi-Fi interference through a few practical experiments. The experimental results demonstrate the behavior of a BLE connection under different Wi-Fi interference. A general conclusion is that both the reliability and the throughput of the BLE connection decrease under Wi-Fi interference. However, the reliability reduction and the throughput reduction are not proportional to one another. With a small decrease in reliability, the throughput drops a large percentage, and a possible explanation is the retransmission mechanism of BLE.

Regarding future work, as mentioned in this paper, more research is necessary to confirm the exact relationship between BLE reliability and throughput. A mathematical model can be a promising solution to the challenge. Note that, some other interference sources can be considered for further tests and studies, such as BLE.

References

[1] A. Nauman, Y. A. Qadri, M. Amjad, Y. B. Zikria, M. K. Afzal, and S. W. Kim, “Multimedia Internet of Things: A Comprehensive Survey,” IEEE Access, vol. 8, pp. 8202–8250, 2020, doi: 10.1109/ACCESS.2020.2964280.

[2] F. Montori, L. Bedogni, M. Di Felice, and L. Bononi, “Machine-to-machine wireless communication technologies for the Internet of Things: Taxonomy, comparison and open issues,” Pervasive and Mobile Computing, vol. 50, pp. 56–81, Oct. 2018, doi: 10.1016/j.pmcj.2018.08.002.

[3] B.-Z. Pang, T. Claeys, D. Pissoort, H. Hallez, and J. Boydens, “Comparative Study on AFH Techniques in Different Interference Environments,” in 2019 IEEE XXVIII International Scientific Conference Electronics (ET), Sep. 2019, pp. 1–4. doi: 10.1109/ET.2019.8878594.

[4] H. Karvonen, K. Mikhaylov, D. Acharya, and Md. M. Rahman, “Performance Evaluation of Bluetooth Low Energy Technology Under Interference,” in 13th EAI International Conference on Body Area Networks, Cham, 2020, pp. 147–156. doi: 10.1007/978-3-030-29897-5_12.

[5] “Bluetooth Core Specification v5.3,” p. 3085.

[6] B. Pang, T. Claeys, D. Pissoort, H. Hallez, and J. Boydens, “A Study on the Impact of the Number of Devices on Communication Interference in Bluetooth Low Energy,” in 2020 XXIX International Scientific Conference Electronics (ET), Sep. 2020, pp. 1–4. doi: 10.1109/ET50336.2020.9238240.

[7] B. Pang, K. T’Jonck, T. Claeys, D. Pissoort, H. Hallez, and J. Boydens, “Bluetooth Low Energy Interference Awareness Scheme and Improved Channel Selection Algorithm for Connection Robustness,” Sensors, vol. 21, no. 7, Art. no. 7, Jan. 2021, doi: 10.3390/s21072257.

[8] B. Pang, T. Claeys, J. Vankeirsbilck, K. T’Jonck, H. Hallez, and J. Boydens, “A Probability-based Channel Selection Algorithm for Bluetooth Low Energy: A Preliminary Analysis,” in 2021 XXX International Scientific Conference Electronics (ET), Sep. 2021, pp. 1–4. doi: 10.1109/ET52713.2021.9579643.

[9] F. J. Dian and R. Vahidnia, “Formulation of BLE Throughput Based on Node and Link Parameters,” Canadian Journal of Electrical and Computer Engineering, vol. 43, no. 4, pp. 261–272, 2020, doi: 10.1109/CJECE.2020.2968546.

[10] V. Díez, A. Arriola, I. Val, and M. Velez, “Reliability Evaluation of Bluetooth Low Energy for Industry 4.0,” in 2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Sep. 2019, pp. 1148–1154. doi: 10.1109/ETFA.2019.8869211.

[11] F. J. Dian, A. Yousefi, and S. Lim, “A practical study on Bluetooth Low Energy (BLE) throughput,” in 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Nov. 2018, pp. 768–771. doi: 10.1109/IEMCON.2018.8614763.

[12] M. A. Ayoub and A. M. Eltawil, “Throughput Characterization for Bluetooth Low Energy with Applications in Body Area Networks,” in 2020 IEEE International Symposium on Circuits and Systems (ISCAS), Oct. 2020, pp. 1–4. doi: 10.1109/ISCAS45731.2020.9180727.

[13] R. Teles Hermeto, A. Gallais, K. V. Laerhoven, and F. Theoleyre, “Passive Link Quality Estimation for Accurate and Stable Parent Selection in Dense 6TiSCH Networks,” in EWSN 2018 - International Conference on Embedded Wireless Systems and Networks, Madrid, Spain, Feb. 2018, pp. 114–125. Accessed: May 13, 2022. [Online]. Available: https://hal.archives-ouvertes.fr/hal-01886778

[14] “nRF52840 DK.” https://www.nordicsemi.com/Products/Development-hardware/nRF52840-DK (accessed May 18, 2022).

[15] R. P. Ltd, “Buy a Raspberry Pi 3 Model B,” Raspberry Pi. https://www.raspberrypi.com/products/raspberry-pi-3-model-b/ (accessed May 18, 2022).

[16] “Zephyr Project,” Zephyr Project. https://www.zephyrproject.org/ (accessed May 18, 2022).

[17] JamLab-NG. TuGraz-ITI, 2022. Accessed: May 18, 2022. [Online]. Available: https://github.com/TuGraz-ITI/JamLab-NG