Modeling the Trade-off between Throughput and Reliability in a Bluetooth Low Energy Connection

Bozheng Pang[1], Tim Claeys[2], Hans Hallez[1], Jeroen Boydens[1]
[1]Department of Computer Science, KU Leuven, [2]Department of Electrical Engineering, KU Leuven
{bozheng.pang, tim.claeys, hans.hallez, jeroen.boydens}@kuleuven.be

Abstract

The use of Bluetooth Low Energy in wireless systems is growing exponentially. There is a need for both theoretical and practical studies capable of quantifying the BLE communication performance, e.g. throughput and reliability, subject to interference. In this paper, a mathematical model to predict throughput of a BLE connection under interference is derived first, and linked to the reliability model developed in [8]. After that, extensive practical experiments are performed in various scenarios to sufficiently validate the theoretical results from both models. Finally, the trade-off between throughput and reliability is investigated through the validated models to give some inside properties of BLE communications. The similarity between the theoretical results and the experimental ones highlights the accuracy of the proposed throughput and reliability models. Hence, the two models can be used to explore the performance of various BLE designs or deployments from diverse perspectives.

Categories and Subject Descriptors

C.2.2 [**Computer-Communication Networks**]: Network Protocols—*Wireless Communication*

General Terms

Performance, Modeling, Experiment

Keywords

Bluetooth Low Energy (BLE), Interference, Throughput, Reliability, Trade-off

1 Introduction

Bluetooth Low Energy (BLE) is one of the most popular wireless protocols, aiming at low range and energy efficient wireless systems [15]. It works in the 2.4 GHz frequency band. There are diverse wireless technologies existing in this frequency band, e.g. Wi-Fi, Bluetooth, and BLE itself [4]. As a result, BLE always faces interference challenges, for instance, due to other neighboring BLE communications [6]. The impact of interference on BLE communications has been shown in research, such as causing transmission failure and thereby degrading throughput and reliability [9].

Some practical studies on BLE throughput have been conducted in [12, 11]. The authors of [12] published their studies on the BLE latency in [12, 11]. In [12], they introduced their analytical model of the delay performance of BLE for connection-oriented applications under different bit error rate conditions. The analytical model is based on Markov chain, and the results highlighted the impact of the device's processing speed and the timing configuration of the connection on the final measured latency. However, the model is only validated by simulation results. Based on the analytical model published in [12], the authors of [11] further evaluated BLE suitability for time-critical industrial applications [11]. Three retransmission schemes on the reliability and timeliness performance are thoroughly studied in their work, but are only evaluated by simulation results. They conclude that by optimally modifying the BLE retransmission model, a maximum delay below 46 ms and a packet loss rate in the order of 10^{-5} can be obtained. It is evident that their work concentrates on BLE latency instead of throughput, but the research idea of this paper is partially inspired by them, thus their work is discussed here.

Apart from throughput, reliability is also of interest in BLE communications. Hence, researchers conducted and proposed some research and improvements. First of all, adaptive frequency hopping (AFH) is a scheme implemented by BLE to avoid interference [15]. Inside the AFH, two channel selection algorithms (CSAs) are defined to help a BLE connection stay connected while hopping pseudo-randomly within the 2.4 GHz frequency band [15]. Both CSAs have been proved lack of efficiency or effectiveness under the environment with interference [6]. Hence, some improvements for BLE reliability were proposed [9]. More importantly, the first BLE reliability model under the interference from other BLE connections has been developed in [8]. The mathematical model for BLE reliability developed in [8] clearly demonstrates and quantifies the impact of various BLE transmission parameters on the BLE reliability. Furthermore, the reliability model has been proved by extensive practical experiments, instead of just theory or simulation.

According to all the literature discussed above, the throughput and reliability of BLE have been investigated from different perspectives. However, there is no deeper research showing the relation or the trade-off between these two communication performance metrics. Hence, in this paper, the trade-off between throughput and reliability is thoroughly investigated, i.e. modeled and experimentally validated. In order to provide a thorough understanding of the relationship between the communication performance and its various connection parameters, multiple BLE communication parameters are involved, such as packet length and number of packets. In other words, this paper can serve as a design-level guideline for BLE usage or deployment.

It is worth mentioning that, to the best of our knowledge, this paper is the first one that describes a thorough model of the trade-off between BLE throughput and reliability, and validates all the results by practical experiments. There are no existing approaches that can accurately quantify the trade-off or relationship yet. The impact of each connection parameter on the throughput and reliability can be clearly illustrated by the model introduced in this paper. The significance of the suggested model is to explain the trade-off within BLE communications simply through numbers and formulas. The contributions of this paper are summarized as follows:

1. A mathematical model to quantify the throughput of a BLE connection under interference is derived and optimized. The derived throughput model is linked to the reliability model that was developed in [8].
2. All the theoretical results from both the throughput model and the reliability model are validated by extensive practical experiments.
3. The trade-off between throughput and reliability within BLE communications is investigated through the two validated models.

The remainder of the paper is organized as follows. In Section 2, the background of BLE communications is first introduced briefly, to help the readers get a better understanding of the rest of the paper. After that, two mathematical models and the link between them are introduced. In Section 3, a description of the experimental setup used to prove the theoretical results is shown. The comparison between the models and the experiments, and a discussion on the trade-off between throughput and reliability are provided in Section 4. In Section 5, this paper is concluded with some final remarks and possible future work.

2 Mathematical Models

This section first presents some necessary background knowledge of BLE communications. Then the two mathematical models, namely the throughput model and the reliability model, are derived. The throughput model is derived in detail due to its novelty, while the reliability model is only introduced briefly since it has been derived and validated in detail in the work [8]. Finally, the link of the two models is described briefly.

2.1 Background

BLE is a wireless personal area network technology designed for novel applications, such as healthcare, fitness, smart home, and industries [10]. It supports different communication modes, e.g. connectionless and connection-oriented. The connection-oriented mode is the focus of this paper since it is designed more for data exchange comparing with the connectionless mode. In the connection-oriented mode, at least two BLE devices are used to create a BLE connection. One of the devices is defined as a central, and the other one as a peripheral [15].

As mentioned before, BLE is widely used in the 2.4 GHz frequency band. The spectrum usage of BLE is managed by the two CSAs defined in the BLE specification. The 2.4 GHz frequency band is divided into 37 data channels and the CSAs are used to calculate a pseudo-random channel for the BLE connection [15].

Each time a BLE connection hops to a channel, it stays there for a certain amount of time. This is called a connection interval [15]. The value of the connection interval is negotiated between the central and the peripheral at the beginning of the connection. The data exchange of the central and peripheral occurs at the start of each connection interval. It is always initialized by a packet sent by the central, and followed by a packet from the peripheral. This data transaction can be repeated numerous times during a single connection interval, depending on the amount of data to be sent. A connection event is made up of all the transactions that occur inside the same connection interval.

2.2 Throughput Model

Under interference, the packets exchanged between the central and the peripheral might experience situations like packet corruption and packet loss [16, 3]. When invalid packets occur, a retransmission is necessary. According to the BLE specification, the number of retransmissions for a packet is unlimited [15]. It suggests that an invalid packet is retransmitted until it is correctly received and acknowledged. However, that may lead to an infinite number of attempts, thus there are some basic rules defined in the BLE specification to limit some aspects of the retransmission:

1. A successful transaction counts when both packets from the central and the peripheral are valid, suggesting no bit errors. In this case, the transaction state is *success*.
2. If bit errors appear in a packet but not in the access address, i.e. invalid cyclic redundancy check (CRC), a transmission failure is counted, and a retransmission is required. The connection event remains open, and the retransmission is immediately performed at the next transaction. In this case, the transaction state is defined as *fail (open)*.
3. If the bit errors appear in the access address of a packet, a transmission failure is counted, and a retransmission is required. However, the connection event is immediately terminated, thus the required retransmission could only occur in the next connection interval. In such a case, the transaction state is called *fail (close)*.
4. Two consecutive packets received with an invalid CRC

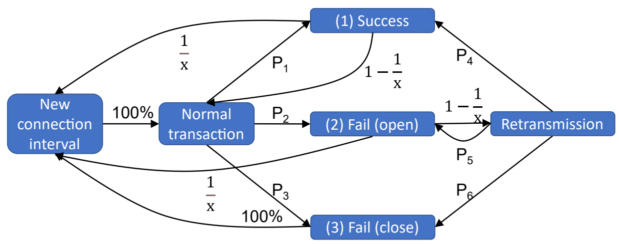

Figure 1. Graphical representation of possible status of transactions in BLE communications, in the form of a Markov chain.

match within a single connection event shall close the event. And they will be retransmitted in the next connection interval. In this situation, the transaction state is also *fail (close)*.

With all the retransmission rules introduced, the throughput model is derived. It is based on the Markov chain. The goal of this mathematical model is to predict the BLE throughput under various conditions. For instance, different interference strengths and diverse combinations of BLE connection parameters.

First of all, a graphical representation of the BLE communication details is shown in Fig. 1 through the form of a Markov chain. It summarizes all the possible events for a BLE transaction and represents the BLE communication in reality. Roughly speaking, a BLE transaction is sent at the beginning of a connection interval as a *normal transaction*. So the probability from the event *new connection interval* to *normal transaction* is always 100%. Then there are three possible states for the transaction, which are *success*, *fail (open)*, and *fail (close)*.

The *success* state represents that a transaction is without any bit errors, corresponding to the basic rule 1 of the retransmission scheme. The probability of a successful transmission is indicated as P_1. After a *success*, there are two options for the BLE connection: (1) starting another *new connection interval*, and (2) continuing with another *normal transaction* in the same connection interval. It depends on the number of transactions (x) arranged/allowed in the connection interval. For instance, when only one transaction is allowed in the connection interval, the BLE connection must start a *new connection interval* to send the next transaction. The $\frac{1}{x}$ on the left top of Fig. 1 represents the probability from the *success* status to the *new connection interval*. Consequently, another *normal transaction* in the same connection interval is not continued since the probability of that process is 0% ($x = 1 \rightarrow 1 - \frac{1}{x} = 0\%$).

The *fail (open)* status suggests that there are bit errors in the transaction but not in the access address, corresponding to the basic rule 2 of the retransmission scheme. The BLE transaction goes into *fail (open)* with a probability defined as P_2. In this case, the *retransmission* has a probability of $1 - \frac{1}{x}$. Similar to the situation discussed above, it depends on the number of transactions arranged in the same connection interval. The *fail (open)* status is the only chance for the BLE transaction to go into the *retransmission* status. Similar to the *normal transaction*, there are three possible status for a *retransmission* transaction, i.e. *success*, *fail (open)*, and *fail (close)*, with P_4, P_5, and P_6 as their probabilities respectively.

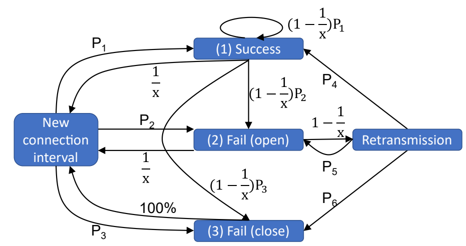

Figure 2. One step of Markov chain simplification by eliminating the status normal transaction in Fig. 1.

The *fail (close)* means that bit errors occur to the transaction and lead to the connection event to be closed, corresponding to the basic rules 3 and 4 of the retransmission scheme. A *normal transaction* ends up with this status with a probability of P_3. While a *retransmission* transaction has a probability of P_6 to close the current connection event. When the transaction is in the *fail (close)* stage, it results in a *new connection interval* with a 100% probability.

To model the throughput under interference, we are mostly interested in the three transaction states, namely *success*, *fail (open)*, and *fail (close)*. Hence, the Markov chain needs to be optimized or simplified. The purpose of the optimization and simplification is to reduce the amount of information in the Markov chain, leaving only the necessary information. In general, three states can be simplified from the Markov chain, i.e. *new connection interval*, *normal transaction*, and *retransmission*. As an example, the principle and steps to simplify the *normal transaction* status are shown in Fig. 2 and explained in detail below.

As mentioned in Fig. 1, the *new connection interval* leads to a *normal transaction* with a probability of 100%. A *normal transaction* has a probability of P_1 to be successfully transmitted. Hence, the probability between the *new connection interval* and the *success* stage is $100\% \times P_1$ (see Fig. 2). Similar results of the probabilities between the *new connection interval* and the *fail (open)* and the *fail (close)* can be calculated as P_2 and P_3 respectively (see Fig. 2). By checking Fig. 1, from the *success* status, a chance exists to go back to the *normal transaction*. Therefore, another three probabilities need to be calculated. These are the probabilities between *success* and *success*, *success* and *fail (open)*, and *success* and *fail (close)*. Similarly, according to Fig. 1, the *success* goes to the *normal transaction* with a probability of $1 - \frac{1}{x}$, while the *normal transaction* goes back to the *success* stage with a probability of P_1. As a result, the probability of *success* turning into itself is $(1 - \frac{1}{x}) \times P_1$. Under the same logic, the probability results between *success* and *fail (open)*, and *success* and *fail (close)*, are calculated as $(1 - \frac{1}{x}) \times P_2$, and $(1 - \frac{1}{x}) \times P_3$ respectively.

Following the same principle and steps explained above, the Markov chain is finally simplified into Fig. 3. Where only three stages are left, i.e. *success*, *fail (open)*, and *fail (close)*, and the transition probabilities among them are listed in the graph. With this simplified Markov chain of BLE communi-

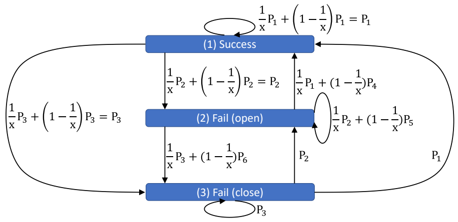

Figure 3. Final simplified version of the Markov chain to represent the three possible outcomes of a single transaction. The three possible outcomes are (1) Success, (2) Fail (open), and (3) Fail (close).

cation, the transition matrix (A) can be written as follows:

$$A = \begin{array}{c} \\ (1) \\ (2) \\ (3) \end{array} \begin{array}{c} \begin{array}{ccc} (1) & (2) & (3) \end{array} \\ \begin{bmatrix} P_1 & P_2 & P_3 \\ \frac{1}{x}P_1 + (1-\frac{1}{x})P_4 & \frac{1}{x}P_2 + (1-\frac{1}{x})P_5 & \frac{1}{x}P_3 + (1-\frac{1}{x})P_6 \\ P_1 & P_2 & P_3 \end{bmatrix} \end{array}$$

The transition matrix A is a 3×3 matrix that illustrates the transition probabilities between either two status in the Markov chain of Fig. 3 [18]. For example, $A_{(2)(3)}$ represents the transition probability from status (2) *fail (open)* to status (3) *fail (close)*, which equals $\frac{1}{x}P_3 + (1 - \frac{1}{x})P_6$.

According to the property of a Markov chain, given an initial distribution (π_0), after a sufficiently long time, e.g. n generations/iterations, the generation n (π_n) does not change any longer, which is called a stationary distribution [13]. According to the accuracy requirement of the applications, it can be decided when the iterations should stop, e.g., when the third decimal place stays stationary. The mathematical representation of this property is:

$$\begin{aligned} \pi_n &= \pi_{n-1} \times A = \pi_0 \times A^n \\ &= \begin{bmatrix} Num_{Success} & Num_{Fail\ (open)} & Num_{Fail\ (close)} \end{bmatrix} \end{aligned} \tag{1}$$

π_n is comprised of three terms, which are $Num_{Success}$, $Num_{Fail\ (open)}$, and $Num_{Fail\ (close)}$. As the stationary distribution vector, the first element of π_n, which is $\pi_n[0]$ and equals to $Num_{Success}$, represents how many transactions or packets are finally successfully transmitted. The sum of all the elements in the π_n is the total number of transmitted transactions or packets. With these two numbers, a ratio called transmission success ratio (TSR) can be defined as:

$$\mathrm{TSR} = \frac{\pi_n[0]}{sum(\pi_n)} \tag{2}$$

The TSR defined above describes the ratio between the successful transactions/packets and the total transactions/packets. The ideal throughput is defined in Equation (3), where the PL represents the BLE packet length in the unit of bytes, the x is the number of transactions/packets in each connection interval, and the CI represents the connection interval length in the unit of seconds. As we want to express the throughput in bits instead of bytes, a multiplication factor of 8 is added to the numerator. This idea throughput represents the throughput when all the transactions/packets are successfully transmitted, such as under an environment with no noise.

$$\mathrm{Throughput}_i = \frac{PL \times 8 \times x}{CI} \tag{3}$$

The real throughput under interference can be calculated as the product of the TSR and ideal throughput, which is shown in Equation (4). Both throughputs are calculated into the unit of bits per second (bps).

$$\mathrm{Throughput}_r = \mathrm{TSR} \times \mathrm{Throughput}_i \tag{4}$$

Till now, the throughput calculation framework has been set up. With the transition matrix A, the stationary distribution π_n can be found easily, thus the TSR is solved. However, currently the distribution matrix A is composed of six unknown probabilities, namely P_1 to P_6. They are discussed in the following paragraphs and equations.

According to Fig. 1, P_1 to P_6 describe the probabilities of the *normal transaction* or the *retransmission* going into the three possible states, i.e. *success*, *fail (open)*, and *fail (close)*. Based on literature [2, 8], the successful probability of transferring a series of data bits depends on the bit error rate (BER) and bit length of the data. To describe the dependency, Equation (5) is introduced.

$$\rho = (1 - BER)^l \tag{5}$$

Equation (5) defines the successful probability ρ of transferring l data bits under a BER defined by a specific interference condition. With this initial equation, six basic equations are defined as follows.

$$\begin{aligned} \rho_{AA} &= (1 - BER)^{l_{AA}} \\ \rho_{CP} &= (1 - BER)^{l_{CP} - l_{AA}} \\ \rho_{PC} &= (1 - BER)^{l_{PC} - l_{AA}} \\ q_{AA} &= 1 - \rho_{AA} \\ q_{CP} &= 1 - \rho_{CP} \\ q_{PC} &= 1 - \rho_{PC} \end{aligned} \tag{6}$$

Based on the four basic rules of BLE communication, six basic equations are defined in (6). AA is the abbreviation of access address. CP and PC represent the directions of the packets: from central to peripheral and peripheral to central respectively. l_{AA} is the bit length of the access address, which is 32 bits in BLE. l_{CP} and l_{PC} are the number of bits of the packets from different directions. $l_{CP} - l_{AA}$ and $l_{PC} - l_{AA}$ are the numbers of bits in the packets except the access address. As mentioned before, ρ represents the probability of a successful transmission of a certain amount of data bits, while q represents the probability if the transmission of at least one bit in the packet is unsuccessful. Thus ρ_{AA} refers to the success probability of the access address within a BLE packet. ρ_{CP} and ρ_{PC} denote the success probability of the other data bits within the BLE packet except the access address. On the contrary, q_{AA}, q_{CP}, and q_{PC} are the failure probabilities respectively.

With all the probabilities defined for different parts of the BLE packet, the probabilities in the Markov chain of Fig. 1, i.e. P_1 to P_6, can be derived. First of all, P_1 is the success probability of a *normal transaction*. To successfully transfer the *normal transaction*, both packets from the central and the peripheral should be without bit errors to both the access address in the packets and all the other data bits. Note that $\rho_{AA}\rho_{CP}$ is the multiplication of ρ_{AA} and ρ_{CP}, and represents the successful transmission probability of the central packet.

It is written without $\times$ between ρ_{AA} and ρ_{CP} to illustrate that they both belong to a same packet. The $\times$ between $\rho_{AA}\rho_{CP}$ and $\rho_{AA}\rho_{PC}$ means that the combination of both of them results in a transaction. Hence, P_1 is calculated as the product of:

$$P_1 = \rho_{AA}\rho_{CP} \times \rho_{AA}\rho_{PC} \tag{7}$$

P_2 is the probability of the *normal transaction* going into the *fail (open)* status. The calculation idea is similar to P_1. Considering the four communication rules defined in BLE specification, P_2 can be calculated by:

$$\begin{aligned} P_2 = &\rho_{AA}q_{CP} \times \rho_{AA}\rho_{PC} \\ &+\rho_{AA}\rho_{CP} \times \rho_{AA}q_{PC} \\ &+\rho_{AA}q_{CP} \times \rho_{AA}q_{PC} \end{aligned} \tag{8}$$

There are three terms in Equation (8), which represent three possible cases between the *normal transaction* and the *fail (open)* status. The first term suggests the case that at least one bit error occurs only in the packet sent from the central, and not in the access address domain. The second term gives the probability that at least one bit error occurs only in the packet sent from peripheral, and not in the access address domain. While the last term means that some bit errors are in the packets from both the central and the peripheral, and not in the access address domains. Following the same principle and based on the BLE communication rules, P_3 is the probability of bit errors occurring in the access address domains of either packet or both. The mathematical representation is:

$$P_3 = q_{AA} + \rho_{AA}q_{AA} \tag{9}$$

Apart from P_{1-3}, P_{4-6} are originated from the *retransmission* state. The *retransmission* status can only be from the *fail (open)* status. Therefore, the calculation for P_4 to P_6 is based on P_2. However, to calculate the marginal probability from the *retransmission* to the *success*, the probability between the *normal transaction* and the *fail (open)*, i.e. P_2, must be eliminated from P_4. As a result, P_2 is shown as the denominator of P_4, P_4 is calculated as below.

$$P_4 = \frac{(\rho_{AA}q_{CP} \times \rho_{AA}q_{PC}) \times (\rho_{AA}\rho_{CP} \times \rho_{AA}\rho_{PC})}{P_2} \tag{10}$$

The calculation of Equation (10) is similar to the successful *normal transaction*. A successful *retransmission* asks for both packets to be without bit errors. Besides, only the last term of Equation (8) is shown in P_4. This is to avoid the packets from the next transaction to be involved into the current one. If they are involved, more packets are counted as successfully transmitted. This will lead to the increment of TSR, which further results in the inaccuracy of the throughput model.

P_5 is the probability of the *retransmission* turning back to the *fail (open)* stage. To achieve this, there must be some bit errors existing in the retransmission, meanwhile those bit errors do not lead to the connection interval to be terminated. It suggests that the bit errors do not exist in the access address of the retransmitted packets, or the same packet which leads the *normal transaction* into *fail (open)*, as referred to the rule 4 of BLE communication. With these limitations in mind, P_5 is defined in Equation (11). It is worth mentioning that, the packets from the next transaction mentioned in the last paragraph are classified as a part of P_5, since they can be considered neither a part of *success* nor *fail (close)*. As a result, P_5 is written as:

$$P_5 = \frac{\begin{aligned}&(\rho_{AA}q_{CP} \times \rho_{AA}\rho_{PC}) \times (\rho_{AA}\rho_{CP} \times \rho_{AA}) \\ &+ (\rho_{AA}\rho_{CP} \times \rho_{AA}q_{PC}) \times (\rho_{AA} \times \rho_{AA}\rho_{PC})\end{aligned}}{P_2} \tag{11}$$

Following the same logic, P_6 aims to fail the *retransmission* and close the current connection event with P_2 as the prerequisite. To not repeat the similar derivation process too much, P_6 is given in Equation (12) without further description. Note that P_6 can also be calculated by $1 - P_4 - P_5$, which is an easier way. But here it is derived from scratch to ensure the rigor of this paper. The easier way can be considered a check for the derivation, which has been validated during our experiments.

$$P_6 = \frac{\begin{aligned}&(\rho_{AA}q_{CP} \times \rho_{AA}\rho_{PC}) \times ((1-\rho_{AA}\rho_{CP}) + \rho_{AA}\rho_{CP} \times q_{AA}) \\ &+ (\rho_{AA}\rho_{CP} \times \rho_{AA}q_{PC}) \times (q_{AA} + \rho_{AA} \times (1-\rho_{AA}\rho_{PC})) \\ &+ (\rho_{AA}q_{CP} \times \rho_{AA}q_{PC}) \times (1-\rho_{AA}\rho_{CP} \times \rho_{AA}\rho_{PC})\end{aligned}}{P_2} \tag{12}$$

Finally, with the probabilities P_1 to P_6 (Equations (7) to (12)), the transition matrix A can be calculated. With the matrix A and a random initial distribution π_0, the stationary distribution vector π_n can be obtained. As a result, TSR and Throughput$_r$ in Equations (2) and 4 are achieved. Till now, the BLE throughput model is fully developed, and the Throughput$_r$ is the predicted value of the BLE throughput for a given BER. It is expected to be close to the measured throughput under the same condition and parameter settings, such as packet length and connection interval.

2.3 Reliability Model

After the throughput model, a BLE reliability model is introduced. The reliability model is derived and validated in detail in [8]. It has been validated by extensive practical experiments in [8], and is further confirmed by some extra experiments in this paper while being combined with the proposed throughput model. The reliability model is defined with the equations below.

$$\begin{aligned} P_{TF} = &(1-(1-BER_V)^{2L_V}) \\ &\times min(1, \frac{m(PT_V + IFS) + n(PT_D + IFS)}{CI_D}) \\ &\times (1 - max(0, \frac{IFS - PT_V}{PT_D + IFS})^m) \end{aligned} \tag{13}$$

Equation (13) calculates the probability of a transmission failure for a BLE connection (P_{TF}). As a result, the reliability of a BLE connection (victim) under interference is written as:

$$Reliability = 1 - P_{TF} \tag{14}$$

In Equation (14), *Reliability* calculates the reliability of the victim connection under the interference of the disturber connection. It is directly related to the transmission failure, which can be estimated by the packet loss rate measured in a BLE connection.

2.4 Combination and Analysis

As can be seen from both developed models, there are several common/related parameters inside, such as BER, packet/bit length, number of transactions/packets. Hence, it

Figure 4. Schematic of the deployment of two BLE connections.

is achievable to link the throughput model to the reliability model mathematically through those common parameters. For instance, by eliminating the BER in both models, we obtain a model where both throughput and reliability are present. Next to the combination, some analyses and further illustrations of the two models are mentioned below.

The correctness of the proposed throughput model can be validated by some properties of Markov chain [18]. In Fig. 1, the sum of P_1, P_2, and P_3 should be 100%, same for the probabilities, P_4, P_5, and P_6. Similarly, in the transition matrix A, the sum of each line should be 100% as well. For example, the sum of the second line of A is $\frac{1}{x}(P_1+P_2+P_3)+(1-\frac{1}{x})(P_4+P_5+P_6)$. It can be further simplified as $\frac{1}{x}+(1-\frac{1}{x})=100\%$, as long as the six probabilities follow the Markov chain property mentioned before. Another instance is the stationary distribution vector π_n. The sum of all the three elements in π_n should equal to the sum of the initial distribution π_0. With these mentioned properties, the throughput model can be easily validated during any experiments.

The reliability model has been developed and discussed in detail in [8]. However, for the ease of understanding in this paper, some details are mentioned here. First, the reliability model is only applicable when the interference source is another BLE connection, since it aims to study the coexistence between multiple BLE pairs. As a result, the experiments in this paper also use BLE as the interference source. Second, although there are several common parameters/symbols in the two models, they should be taken care of when employing them. For instance, the PT_V in Equation (13) is the packet transmission time of a single packet from either the central or the peripheral in the victim connection. Hence, given the corresponding PL to Equation (3), the throughput is calculated as a single-direction throughput. For a bidirectional throughput, the packet transmission time from the other device also should be considered.

3 Experimental Setup

The experimental setup introduced in this section aims to validate and illustrate the accuracy of the newly introduced throughput model and the earlier developed reliability model. After the experiments, the two models are considered trustworthy with tolerable errors, and are further utilized to discuss the trade-off between throughput and reliability in a BLE connection.

The experimental setup is similar to the one designed in [8]. The object under interference is a BLE connection, and the interference source is another BLE pair. Each BLE connection is built up using two nRF52840 DK development boards, placed in a noiseless office environment [14]. Various scenarios can be achieved by differing parameters, such as transmission power and connection event structure. In this paper, three specific scenarios are tested and discussed. Since each scenario represents a different electromagnetic environment, the developed models can be considered widely examined and validated. The deployment of the two BLE connections are graphically shown in Fig. 4. It is worth noting that, although the location of the BLE devices is constant, the variation of other parameters is sufficient to simulate diverse interference environments. For example, the amount of data exchanged in the disturber connection.

Common information for the two scenarios is listed here. Both scenarios use the same spatial setup where the distance between the victim/disturber central and peripheral is around 10 cm, while the distance between the BLE victim and the disturber is around 20 cm, and no other Wi-Fi devices or BLE pairs are nearby that might interfere with the setup. The connection interval for both the victim and the disturber connections is set to 7.5 ms. The two scenarios and their difference are illustrated as follows:

(a) The CSAs are disabled in this scenario, and both the victim and the disturber connections are forced to communicate on the same BLE channel. There are two reasons behind this setting. First, it is used to simulate a rather harsh environment for the BLE communication, which implies that the whole 2.4 GHz frequency band is full of interference. Second, it provides easy-to-understand insights on the working principle of both models. The transmission power of the BLE victim devices in this scenario is 0 dBm while the BLE disturber is programmed to communicate using an output power of +8 dBm. The payload in each packet in the victim connection from both the central and the peripheral is designated to 50 bytes. The same payload size is also used for the disturber connection. The number of transactions in each connection interval of the disturber is 2, i.e. $x=2, n=4$. While the number of transactions in each victim connection interval increases from 1 to 5, i.e. $x=1\sim 5, m=2\sim 10$. This scenario is considered as a preliminary validation of the proposed models.

(b) Different from scenario (a), the CSAs are enabled in this scenario. The CSA #2 is used for both the victim and the disturber. Hence, scenario (b) can be considered a real-world use case. This scenario is considered as a realistic validation and evaluation of the accuracy of the models. In this scenario, biased transmission powers are used, i.e. 0 dBm and +8 dBm. The number of transactions in each victim connection interval is fixed to 1. While for the disturber connection, it is 3. The payload of each packet inside the disturber connection is 50 bytes ($PT_D = 512\ \mu s$), and the payload of each victim packet raises from 100 bytes to 200 bytes, with a gap of 20 bytes ($PT_V = 912\ \mu s \sim 1712\ \mu s$). Due to the enabled CSAs and the change of the disturber parameters, this scenario can be considered as a completely different electromagnetic environment from the first one. Hence, it is a further validation of the two models.

The experiments can be divided into experiment runs and sets. Each experiment run is a BLE connection with 1000 connection intervals. The throughput and the reliability are measured and calculated for the whole connection after 1000 connection intervals. In this way, these two performance metrics can reach a stable state under interference. Since it has been reported that a BLE connection requires a certain amount of time to reach a stable throughput and reliability when subjected to interference [7]. According to [7], BLE communication performance metrics converge to their stable values after around 1000 connection intervals. As a result, 1000 connection intervals are planned for each experiment run. Each experiment run is repeated 500 times and forms an experiment set. Results are averaged over all experiment runs. This is to avoid a possible outlier from a single experiment run. As explained in [8], due to the varying connection event overlap probability and packet collision probability between BLE pairs, a single experiment run may lead to an extremely high or low result. Hence, multiple experiments runs are necessary to find the stable results. With the results shown in [8], 500 is chosen. As an example, scenario (a) increases its number of transactions from 1 to 5 ($x = 1 \sim 5$), hence, there are 5 experiment sets in total within the scenario. Extensive experiments are conducted just to ensure the correctness of the measured data, and to better validate the proposed models.

As mentioned in scenarios (a), the CSAs are disabled, and the BLE connections are designated to communicate on a single channel (channel 35). This channel is chosen since it is far away from popular Wi-Fi channels 1, 6, and 11, which are the major source of external interference in the office environment [17]. To achieve this, Zephyr RTOS is deployed on the BLE development boards [19].

4 Results and Discussion

In this section, the results from the experiments under the two designed scenarios are described first. They are used to validate the introduced throughput model and the reliability model. As it will be shown, the results highlight the accuracy of both models. After the validation of both models, they are used to further discuss the trade-off in a BLE connection.

4.1 Validation

Most parameters can be set by the BLE connection itself, such as packet bit length (L_V) and connection interval (CI_D). However, the *BER* is a parameter which needs careful attention, as it is not an input from the BLE connection, instead, an outcome of the electromagnetic environment. Hence, it is measured in this paper similar to the method mentioned in [8, 2]. In general, packet corruption rate is first measured on the BLE victim connection. After that, the *BER* is calculated by dividing the packet corruption rate by the bit length of the packet. This *BER* is then used as an input for both models.

Fig. 5 illustrates the validation results of scenarios (a) and (b). The deviations between the theory and the practice is shown as percentages next to the curves. Both the throughput and the reliability results show a clear correspondence between the models and their related experiments.

In Fig. 5 (a), the largest difference, 9.92%, between the throughput model and its experiments appears when $x = 4$ in scenario (a). The largest difference between the reliability model and the experiments is 4.82% when $x = 4$. While the average difference from all the five data points in the throughput comparison figure is 7.60%. The average error in the reliability comparison of Fig. 5 (a) is only 3.38%.

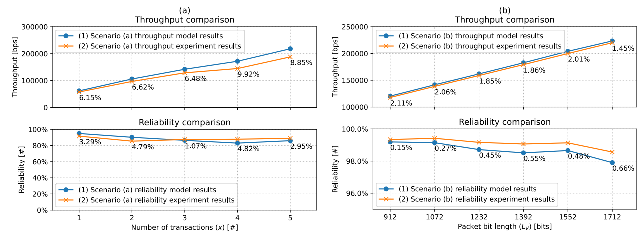

Figure 5. Comparison of experimental and model results under scenarios (a) and (b). The deviations are displayed in percentage next to the curves.

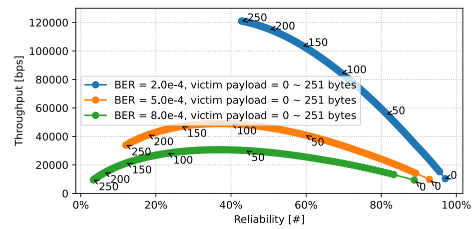

Figure 6. Pareto curve between BLE reliability and throughput when the payload in the victim connection varies. Parameters: $m = 2$ ($x = 1$), $n = 10$, $PT_V = 80\ \mu s \sim 2120\ \mu s$ (payload = 0 bytes $\sim$ 251 bytes), $L_V = 80$ bits $\sim$ 2120 bits (payload = 0 bytes $\sim$ 251 bytes), $PT_D = 512\ \mu s$ (payload = 50 bytes), $CI_V = 7.5$ ms, $CI_D = 7.5$ ms, $IFS = 150\ \mu s$, BER = 2.0e-4, 5.0e-4, 8.0e-4.

In Fig. 5 (b), the largest difference shown in the throughput comparison is 2.11% when $L_v = 912\ bits$. The largest error in the reliability comparison is only 0.66% on the point of $L_v = 1712\ bits$. The average error in the throughput comparison figure is 1.89%, and the average difference in the reliability comparison figure is only 0.43%.

The differences between the theoretical models and the practical experiments can be briefly explained from two perspectives. First, due to the nature of probability, experimental outcomes are never exactly equal to but always converge toward theoretical values. [5]. Even after 500 experiment runs in each set, mostly the average of measured results can only fluctuate around the theoretical value. Second, it has been reported in literature that there are divergences between theory and measurement due to hardware differences and BLE stack implementation. Even under an environment without interference, the divergence can be up to 3% to 6% [1].

4.2 Trade-off Discussion

The proposed models are used to analyze the trade-off between throughput and reliability of a BLE connection under interference after they have been validated under different scenarios. The trade-off is illustrated in Pareto plots by varying some common parameters in the two models. An instance is given below to better illustrate the use of the models and thus further discuss the trade-off within BLE communications.

Fig. 6 plots the trade-off while the payload size within the victim connection changes between 0 and 251 bytes, and all the other factors are fixed. This corresponds to a use case where a BLE connection adjusts its payload size frequently according to its application and need. The payload size of 0 to 251 bytes is the range defined by the BLE specification [15]. As a result, three Pareto curves are plotted by varying the BER (2.0e-4, 5.0e-4, and 8.0e-4). No linear relationship is found between reliability and throughput. But, taking the BER of 5.0e-4 as an instance, there is a throughput peak displayed. The peak point appears at the payload size of 120 bytes approximately, associated with a throughput of around 50000 bps and a reliability of 35%. It suggests that the maximum throughput does not necessarily appear at the maximum reliability point. On the contrary, according to the curve of 5.0e-4 BER, the throughput reaches its lowest value when the BLE connection is most reliable. The reason behind it is that a smaller packet has a larger chance to be transferred successfully, but meanwhile with a shorter packet length, and hence, less throughput. However, when the payload size is over 120 bytes, both the reliability and the throughput begin to decrease. This is because the transmission success rate of a packet is too low. Despite the fact that each packet contains a large amount of data, few packets can be transmitted successfully. As a result, the throughput starts to decrease together with the reliability.

This graph nicely reveals the trade-off between the throughput and the reliability in BLE communications. It also emphasizes the influence of environments. With BLE communications deployed in diverse environments, the interference levels from the environments differ the trade-off of BLE communications. In a less noisy environment, corresponding to the BER of 2.0e-4, the throughput increases and the reliability decreases, with the increment of the victim payload size. It is a similar phenomenon mentioned previously, the lower the interference level, the more potential of BLE communications can be released. With the environment becoming harsher and harsher, BLE settings should be adjusted so that the BLE communication reaches the requirements of the application.

5 Conclusion

In this paper, we present three contributions: first, a mathematical model to estimate the throughput of a BLE connection subject to interference is derived and linked to the previously developed reliability model; second, extensive experiments on real-world BLE development boards are performed under different electromagnetic environments, and thus the proposed models and the combination of them are validated; third, the trade-off between BLE throughput and reliability is investigated through the validated models to illustrate some inside features of BLE communications.

Regarding future work, three future research directions can be considered. First, other types of interference, such as Wi-Fi and ZigBee, might also be interesting to investigate. Normally, different interference types may cause some variations to the proposed mathematical models, hence, further research is necessary. Second, except throughput and reliability, there are many other performance aspects in BLE communications, such as energy efficiency. It would be interesting to see that other performance metrics can be developed as models as well. Third, a smart BLE network management system can be a promising research field. The current idea is to manage BLE networks through the developed models, and gradually update or optimize the models according to the use case, application, and environment.

References

[1] 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)*, pages 1–4, Oct. 2020. ISSN: 2158-1525.

[2] V. Freschi and E. Lattanzi. A Study on the Impact of Packet Length on Communication in Low Power Wireless Sensor Networks Under Interference. *IEEE Internet of Things Journal*, 6(2):3820–3830, Apr. 2019. Conference Name: IEEE Internet of Things Journal.

[3] E. Kalinin, D. Belyakov, D. Bragin, and A. Konev. IoT Security Mechanisms in the Example of BLE. *Computers*, 10(12):162, Dec. 2021. Number: 12 Publisher: Multidisciplinary Digital Publishing Institute.

[4] Q. D. La, D. Nguyen-Nam, M. V. Ngo, H. T. Hoang, and T. Q. Quek. Dense Deployment of BLE-Based Body Area Networks: A Coexistence Study. *IEEE Transactions on Green Communications and Networking*, 2(4):972–981, Dec. 2018. Conference Name: IEEE Transactions on Green Communications and Networking.

[5] G. Pagès. *Numerical Probability: An Introduction with Applications to Finance*. Universitext. Springer International Publishing, Cham, 2018.

[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)*, pages 1–4, Sept. 2020.

[7] B. Pang, T. Claeys, K. T'Jonck, H. Hallez, and J. Boydens. Bluetooth Low Energy Reliability and Throughput under Wi-Fi Interference. In *2022 XXXI International Scientific Conference Electronics (ET)*, pages 1–4, Sept. 2022.

[8] B. Pang, T. Claeys, J. Vankeirsbilck, K. T'Jonck, H. Hallez, and J. Boydens. A Novel Model to Quantify the Impact of Transmission Parameters on the Coexistence Between Bluetooth Low Energy Pairs. *IEEE Internet of Things Journal*, 10(2):1733–1745, Jan. 2023.

[9] 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*, 21(7):2257, Jan. 2021. Number: 7 Publisher: Multidisciplinary Digital Publishing Institute.

[10] M. Porjazoski, P. Latkoski, and B. Popovski. Bluetooth Low Energy-based Smart Home Android Solution. In *IEEE EUROCON 2019 - 18th International Conference on Smart Technologies*, pages 1–5, July 2019.

[11] R. Rondón, M. Gidlund, and K. Landernäs. Evaluating Bluetooth Low Energy Suitability for Time-Critical Industrial IoT Applications. *International Journal of Wireless Information Networks*, 24(3):278–290, Sept. 2017.

[12] R. Rondón, K. Landernäs, and M. Gidlund. An analytical model of the effective delay performance for Bluetooth low energy. In *2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pages 1–6, Sept. 2016. ISSN: 2166-9589.

[13] V. Roy. Convergence diagnostics for Markov chain Monte Carlo, Oct. 2019. Number: arXiv:1909.11827 arXiv:1909.11827 [stat].

[14] N. Semiconductor. nRF52840 DK, 2022.

[15] B. SIG. Bluetooth Core Specification v5.3. *Bluetooth SIG*, page 3085, 2021.

[16] V. V. Tipparaju, K. R. Mallires, D. Wang, F. Tsow, and X. Xian. Mitigation of Data Packet Loss in Bluetooth Low Energy-Based Wearable Healthcare Ecosystem. *Biosensors*, 11(10):350, Oct. 2021. Number: 10 Publisher: Multidisciplinary Digital Publishing Institute.

[17] Wikipedia. List of WLAN channels, June 2022. Page Version ID: 1094397877.

[18] Wikipedia. Markov chain, June 2022. Page Version ID: 1094432686.

[19] Zephyr. Zephyr Project - Zephyr Project, 2022.