A Novel Model to Quantify the Impact of Transmission Parameters on the Coexistence between Bluetooth Low Energy Pairs

Bozheng Pang, *Student Member, IEEE,* Tim Claeys, *Member, IEEE,* Jens Vankeirsbilck, *Member, IEEE,*
Kristof T'Jonck, *Student Member, IEEE,* Hans Hallez, *Member, IEEE,* and Jeroen Boydens, *Member, IEEE*

***Abstract*—We noted that communication performance of a Bluetooth Low Energy connection is heavily affected by the radio interference from other connections or networks. Reliability is becoming a key requirement in Bluetooth Low Energy for its use in various Internet of Things applications. Hence, there is a widely recognized need for an in-depth study to reveal the parameters impacting Bluetooth Low Energy reliability under such radio interference. In this paper, we investigate how transmission parameters, e.g. number of packets and packet transmission time, influence reliability of the Bluetooth Low Energy protocol. Specifically, a mathematical model is presented to explore the impact of the transmission parameters on the reliability of a Bluetooth Low Energy pair under interference caused by other pairs. This mathematical model is able to show the reliability issues from both the side of the Bluetooth Low Energy connection under interference and the side of the interference itself. The model is validated and novel insights on common usage of Bluetooth Low Energy parameters by a wide range of experimental evaluations are provided. Experimental results highlight the correctness of the mathematical model, thus quantify the interplay between transmission parameters and coexistence, also the influence of other related parameters. This research provides a design-level or system-level insight in Bluetooth Low Energy usage and deployment.**

***Index Terms*—Bluetooth Low Energy (BLE), mathematical model, transmission parameters, BLE interference, reliability.**

I. Introduction

The Internet of Things (IoT) is a concept describing a network of physical objects [1]. This concept is widely employed in all aspects of human life, such as healthcare and industry [2, 3, 4]. A crucial element in IoT systems is wireless communication [5]. Various wireless communication protocols exist, aiming at different IoT applications. Bluetooth Low Energy (BLE) is one of the most used building blocks of many low range and energy efficient IoT systems [6]. As a popular wireless protocol, BLE works in the 2.4 GHz frequency band, i.e. the worldwide industrial, scientific and medical (ISM) band. Inside this frequency band, BLE faces interference challenges due to other wireless protocols, known as external interference, and other neighboring BLE connections, known as internal interference [7]. Furthermore, research has shown that interference can induce transmission failure, compromising the reliability of BLE communications [8, 9].

Both internal and external interference occur due to the heavy occupation of the 2.4 GHz frequency band [10]. To counter the transmission failure caused by external interference, BLE divides the 2.4 GHz band into different channels and uses adaptive frequency hopping (AFH) [11]. This technology applies channel selection algorithms (CSAs) to hop pseudo-randomly among the different BLE channels during communication [12, 13]. New CSAs are being developed to further decrease the transmission failures under external interference, such as Wi-Fi [14]. In previous work, we have shown the significant impact of Wi-Fi interference, i.e. external interference, on a BLE connection [14]. Furthermore, we also provided a link layer solution to provide reliability in the BLE communication under both static and dynamic external interference.

External interference can be mostly avoided by the AFH technology and the improvements proposed for it [14, 15]. However, when it comes to internal interference, the AFH is not effective anymore [16]. With the nature of being a pseudo-random number generator, hopping pseudo-randomly in the 2.4 GHz frequency band does not help BLE devices avoid other neighboring BLE connections, since all the BLE devices apply the same AFH scheme [11, 17]. According to [16], when the number of BLE connections is over 20, no matter which channel a BLE connection hops to, it always encounters other BLE connections on it. Although the study is based on simulation, it encourages further investigations into the internal interference between BLE connections. The impact of internal interference on the BLE energy consumption and latency has been reported in [18]. It is also confirmed in some realistic scenarios, such as hospital [19]. According to [19], the internal interference between BLE connections impacts the reliability of BLE medical devices. The impact factors include but are not limited to BLE parameters, distance and on-body or off-body deployment, which emphasizes the importance of the design and deployment of BLE connections. To better design and develop BLE networks, it is essential to understand and model the transmission failure on a channel-level taking into account the many parameter settings of BLE.

Hence, in this paper, the impact of the transmission parameters, i.e. the number of packets and the packet transmission time, on the transmission failure and coexistence between two BLE pairs is modelled and experimentally validated.

The authors are with the Department of Computer Science and the Department of Electrical Engineering, Faculty of Engineering Technology, KU Leuven, Belgium, e-mail: bozheng.pang@kuleuven.be

Manuscript received MM DD, 2022; revised MM DD, YYYY.

This can be linked to a common use case, such as one BLE pair as a laptop with a wireless mouse or keyboard and the other as a smartphone with a smart watch. The use case is not reliability-critical but occurs everywhere, and such interference does impact multiple performance aspects of BLE communications [20, 21, 9]. It is worth mentioning that, to the best of our knowledge, this paper is the first one thoroughly quantifying the relationship between BLE connection parameters and its connection reliability. There are no existing approaches that can accurately explain the interference between multiple BLE pairs yet. Also note that this paper only discusses the interference between BLE pairs instead of other interference on BLE. While less realistic, it serves as a good starting point for further study or development of BLE. The significance of the developed model is to explain the BLE connection reliability challenge on frequency- and time domain through numbers and formulas. Rather than just providing a rough trend, the impact of various parameters is accurately calculated. This novel model can be useful in multiple cases. For example, researchers and engineers, such as BLE special interest group who writes the BLE standard, may use it for further improvement for BLE communications. It can also be further valorized into a more user-friendly version for BLE users to better deploy their BLE devices. Clear insights of the interference between BLE pairs are given so that a clear path of analyzing the BLE interference is provided for academic and industry, which may save time and effort for related investigations. **The contributions provided in this paper are summarized as follows:**

1) A mathematical model of a single BLE pair under the interference of another BLE pair is derived. The model provides a useful tool at the design and development stage to evaluate the impact of various parameters on transmission failure. It enables the prediction of how the packet transmission time and the number of packets affect the transmission failure probability between the two neighboring BLE pairs, which does not take environmental noise into account.
2) The mathematical model is validated using different BLE parameters through extensive experiments. Many other and more complicated scenarios, such as dynamic strength of the interference, can be employed to further validate the model. However, this is beyond the scope of this paper and is regarded as future work.
3) The impact of every parameter in the mathematical model is illustrated and explained in detail to have a clear look on how they affect the reliability between two BLE pairs. It is worth noting that the objective of the model is to reveal the influence of all frequency and time parameters on the reliability between two BLE pairs, which can be considered as a starting point for more reliable connections. To increase BLE reliability, the model can help fine-tune BLE transmission parameters. However, expecting fine-tuning to completely address all reliability issues, e.g. external interference, is impossible. We consider this research can serve as a cornerstone for internal interference control and large-scale BLE network management, also an inspiration for the modeling of BLE under external interference.

The paper is organized as follows. In Section II, the relationship between this paper and some state-of-the-art scientific literature is discussed. In Section III, the mathematical model is introduced and an analysis to study the impact of transmission parameters and other related parameters is performed. In Section IV, a description of the experimental setup that is used to prove the mathematical model is shown. The results of the experiments and a comparison between the mathematical model and the experiments are provided in Section V. In Section VI, we conclude this paper with some final remarks and our possible future work.

II. Related Work

In the following, to the best of our knowledge, the most meaningful studies related to this paper in scientific literature are mentioned and analyzed.

Karvonen et al. presented a performance evaluation of the BLE technology under ZigBee interference [22]. They introduced an analytical model to compute the packet error rate of BLE communication under ZigBee interference. Additionally, they proved the validity of their model by practical experiments under ZigBee interference. In this paper, focus is on neighboring BLE connections, which was not included in the work of Karvonen et al..

Hajizadeh et al. analyzed the coexistence between BLE and IEEE 802.15.4 TSCH in the 2.4 GHz frequency band in [23]. In their work, a probabilistic analysis of collision-free communications in the MAC layer for coexisting BLE and TSCH is presented. They also set up simulation models and provided an experimental evaluation to verify the analytical results. Again, the analysis was only conducted between different wireless protocols and not between neighbouring BLE connections as is the focus of this paper.

Spörk et al. investigated experimentally the performance of BLE under Wi-Fi interference and proposed mechanisms to sustain a high link-layer reliability while minimizing power consumption. The idea was to promptly blacklist poor channels and select another physical mode. The mechanisms have been tested through experiments and proved to increase the reliability of BLE connections by up to 22%. However, their mechanisms focus on the external interference, i.e. Wi-Fi, instead of the internal interference.

The performance of BLE was evaluated under different scenarios and interference environments such as inter-vehicular communication, mutual interference, and realistic wireless environments in [24, 25], and [26]. However, these works are all based on an experimental evaluation only, instead of a theoretical analysis, and are therefore unable to provide deep insights of the BLE performance under interference.

Freschi and Lattanzi investigated the role of the packet length on the reliability and energy efficiency of low-power medium access protocols [27]. They assessed the performance of Contiki's default medium access control protocol, which is called ContikiMAC, in terms of packet loss rate and energy efficiency for varying payload lengths. A mathematical model

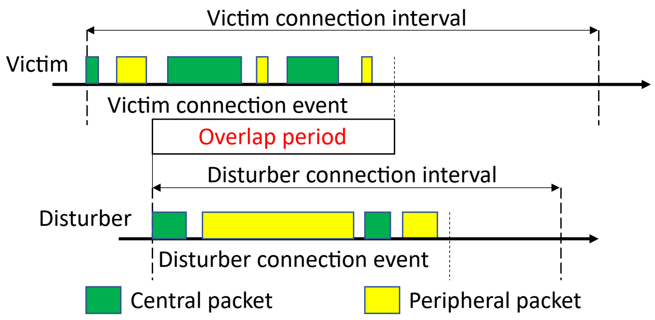

Fig. 1. Interference principle between the victim BLE pair and the disturber BLE pair.

was built and extensive experiments were performed to study the correlation between packet size and interference. They finally confirmed the impact of packet lengths on reliability under interference for ContikiMAC protocol. However, the research object of this paper, the BLE protocol, is much different from the ContikiMAC. Hence, it is impossible to adopt their model and results directly to the BLE protocol. An extra limitation of the investigation performed by Freschi and Lattanzi is that they only studied the impact of one parameter, i.e. the packet length, while in reality multiple parameters have an impact on the reliability.

III. Mathematical Model and Analysis

This section first presents definitions used for the system setup and for the interference model. Next, the mathematical model for BLE transmission failure is derived. Finally, an analytical study of BLE communication reliability is performed by using the mathematical model.

A. System Model and Interference Definition

In order to evaluate various aspects of the BLE transmission, e.g. reliability, a minimal system model (see Fig. 1) is presented. It is composed of two pairs of BLE devices, one as an interference victim connection (*victim*), the other one as an interference generator connection (*disturber*). Each of them executes as a normal BLE pair/connection containing a central (master) and a peripheral (slave). The victim is a central-peripheral BLE connection that senses the interference. Its normal function can be disrupted by interference. The disturber is also a central-peripheral BLE connection, however, it generates strong communication signals as interference, and it tries to disrupt the normal function of the victim. In the minimal system model, the desired signal of the BLE victim pair is the packets from its own connection, while all the packets from the BLE disturber connection are considered as the interference signal.

The received signal at the receiver is the sum of the desired signal itself and all other disturbances [28]. That is why, when two or more packets are transmitted on the same frequency at the same time between two or more BLE connections, a transmission failure can occur.

In BLE communication process, every packet sent from the central to the peripheral is followed by a packet from the peripheral to the central (see Fig. 1) [29]. All the packets are aligned on a timeline according to a connection interval (CI) negotiated by the BLE pair, i.e. the central and the peripheral. A connection event (CE), the effective part of a connection interval, starts with a packet from the central and ends with a packet from the peripheral, alternating between them [30]. Many previously developed communication and interference models focus on other protocols, which renders them unsuitable for BLE.

The interference principle between BLE pairs is depicted in Fig. 1. When two or more BLE pairs in a same region are on the same channel and their connection events overlap, there is a high chance of packet collisions. Except CSAs for interference avoidance in the whole spectrum, the BLE protocol has no methods for collision or interference avoidance when BLE connections are on the same channel. Only the BLE data channels are discussed in this paper. Setting up a connection between the central and the peripheral is done using the advertisement channels and is not considered in this paper. According to the transmission parameters, which is the packet transmission time and the number of packets, the interference probability differs. The interference is simplified by defining it as any collision of packets, no matter if they originate from the central or the peripheral. Note that all the signals are represented in a binary form (on and off).

B. Mathematical Model

From the system model and the interference principle in Fig. 1, a mathematical model can be described providing insights on the BLE interference and transmission failure. The goal of this mathematical study is to have an equation that describes the relations between various BLE connection parameters and the transmission failure probability.

If the same channel is used, Fig. 1 shows that interference can only occur when (I) the connection events overlap and (II) the packets collide. Hence, there are two probabilities defining interference that need to be derived, the probability of the connection event overlap and the probability of a packet collision within that connection event. After that, using another probability related to bit error rate (BER), the two probabilities can be converted to the transmission failure probability in reality [31].

Note that the mathematical model is first developed on a single data channel, which means the victim and the disturber are occupying the same channel. It is for the simplicity of mathematical derivation. Then the model is further developed on the full spectrum in the analytical study by dividing it by the number of data channels in BLE, namely 37. Besides, relevant experiments are also undertaken and displayed afterwards to prove that the model complies with the BLE standard. Note that in the development of the model, it is assumed that no matter how large the signal to noise ratio at the victim is, it can always hear the disturber. The signal to noise ratio and its consequences are introduced in the model starting from equation (13).

In one connection interval of the BLE victim (CI_V), there is only one connection event (CE_V), the remaining time of the

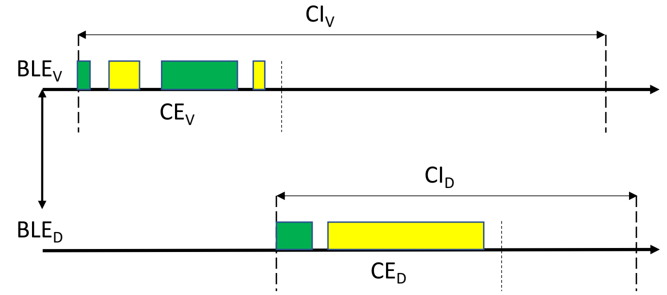

Fig. 2. Connection event overlap principle between the BLE victim and the BLE disturber. A BLE victim connection interval is considered, to illustrate the overlap probability inside the connection interval. Note that the situation when the CE_D starts before CE_V is also considered but not drawn in the figure.

CI_V, no packets are sent (see Fig. 2). To avoid an overlap, the connection event of the disturber (CE_D) should stay in the contention-free period of the CI_V. Thus, the range within which the CE_D can shift and not interfere with the CE_V is:

$$\mathrm{Range} = \mathrm{CI_V} - \mathrm{CE_V} - \mathrm{CE_D} \tag{1}$$

Assuming that a CE_D may emerge anywhere inside a CI_V and the probability of its location in time is the same everywhere in that one CI_V, the probability of not having an overlap between CE_V and CE_D can be derived as:

$$\mathrm{P}^{\mathrm{CI_V}}_{\text{no overlap}} = \frac{\mathrm{Range}}{\mathrm{CI_V}} = \frac{\mathrm{CI_V} - \mathrm{CE_V} - \mathrm{CE_D}}{\mathrm{CI_V}} \tag{2}$$

In a CI_V, the probability of overlap between its CE_V and a CE_D is then:

$$\mathrm{P}^{\mathrm{CI_V}}_{\text{overlap}} = 1 - \mathrm{P}^{\mathrm{CI_V}}_{\text{no overlap}} = \frac{\mathrm{CE_V} + \mathrm{CE_D}}{\mathrm{CI_V}} \tag{3}$$

Equations (2) and (3) are only defined for one CI_V and CI_D, and do not take into consideration the relation between multiple CI_Vs and CI_Ds. Since a pair of BLE devices hardly changes the connection interval during their connection, it can be considered a constant. This results in a fixed rate of overlap between the BLE victim and the disturber over a time period equal to t. For instance, when the CI_V equals 20 ms and the CI_D equals 10 ms, the result is 2. It suggests that each CI_V overlaps with, or covers 2 full CI_Ds. By involving this rate of overlapping, the relation between a single CI_V and CI_D are further developed into the relation between multiple CI_Vs and CI_Ds. The rate can represented by:

$$\mathrm{Rate} = \left(\frac{\mathrm{t}}{\mathrm{CI_D}}\right)/\left(\frac{\mathrm{t}}{\mathrm{CI_V}}\right) = \frac{\mathrm{CI_V}}{\mathrm{CI_D}} \tag{4}$$

and $\frac{t}{CI_D}$ and $\frac{t}{CI_V}$ as the number of connection intervals in a period t. Taking this into account, equation (3) is further developed into:

$$\frac{\mathrm{CE_V} + \mathrm{CE_D}}{\mathrm{CI_V}} \cdot \mathrm{Rate} = \frac{\mathrm{CE_V} + \mathrm{CE_D}}{\mathrm{CI_D}} \tag{5}$$

providing the total probability of connection event overlap between the victim and the disturber over multiple CI_Vs.

Equation (5) shows that the probability of overlap relates to both connection events and one of the connection intervals (CI_D). According to the BLE specification, a connection interval can range from 7.5 ms to 4 s [17]. The maximum length of the connection event is only 150 μs less than the connection interval, thus occupying nearly the entire connection interval. In addition, the CE_V is independent of CI_D and can therefore be much larger than CI_D. This fact may lead to a probability higher than 1 in equation (5), while the probability of an event should always be a number between 0 and 1 [32]. In fact, a larger probability than 1 means that there is always overlap, as the connection free periods on the CI_Ds are too small. As a realistic instance, imagine there are two connections with each a different connection interval of 1 s and 1.5 s. If these connection intervals need to be scheduled within a period of 2 s, they definitely overlap with one another, which leads to an overlap probability of 100%, instead of $\frac{1+1.5}{2} = 125\%$. Therefore the probability of overlap between CE_V and CE_D is finally written as:

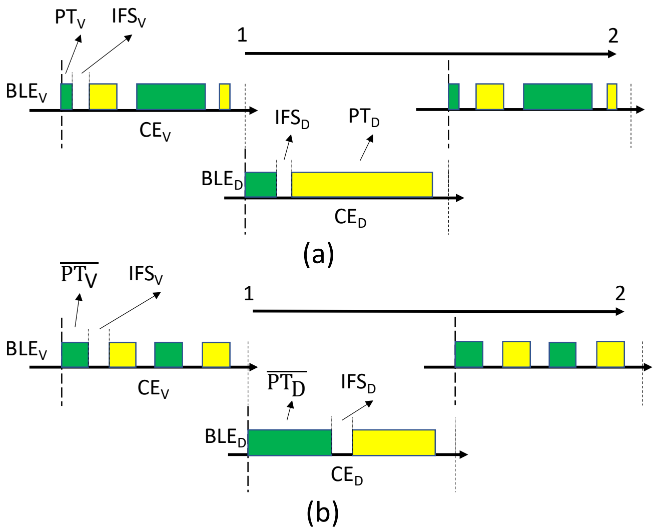

Fig. 3. Packet collision principle between the BLE victim and the BLE disturber. (a) shows a realistic packet arrangement in BLE connections (Packets may have different transmission time.) while (b) shows a simplified packet arrangement (Packets have the same transmission time.).

$$\mathrm{P_{overlap}} = \min\left(1, \frac{\mathrm{CE_V} + \mathrm{CE_D}}{\mathrm{CI_D}}\right) \tag{6}$$

When two connection events overlap, there is a possibility that a packet collision may happen. Packets in a connection event may differ in transmission time as shown in Fig. 3 (a), while the inter frame space (IFS) between every two packets has a fixed length of 150 μs. Accordingly, to avoid packet collision, the BLE victim packets must either be sent outside of the BLE disturber connection event as defined by $1-P_{overlap}$, or be sent within the disturber IFS, which means that the packets have to be smaller than 150 μs. As a result, the probability of no packet collision when connection events overlap is equal to the probability of each BLE victim packet set within all of the disturber IFSs.

To have an accurate result, the probability for all the BLE victim packets has to be calculated separately due to the possible difference of the victim packet transmission time (PT_V). The reasoning behind this calculation is similar to $P_{overlap}$ with the difference that there may be multiple IFSs since there can be multiple packets in a connection event. Here, we first calculate the probability of no packet collision between one victim packet and multiple IFSs, i.e. the whole victim packet stays within the IFSs, and it is derived as:

$$\mathrm{P^{n}_{no\ collision}} = \sum_{i=1}^{n} \frac{\mathrm{IFS^{i}_{D} - PT_{V}}}{\mathrm{CE_{D}}} = \mathrm{n} \cdot \frac{\mathrm{IFS_{D} - PT_{V}}}{\mathrm{CE_{D}}} \quad (7)$$

in which n is the number of packets in the CE_D and is always even. Since all the IFS^i_D are equal to 150 μs, equation (7) is further simplified.

The packet transmission time PT_V ranges from 80 μs to 2120 μs for the LE 1M PHY data rate which is one of the most commonly used data rates in BLE. This results in a value lower than 0 when $PT_V > IFS_D$. When the PT_V is larger than the IFS_D, the victim packet either collides with the disturber packet in front of or the one behind it. Similar to the explanation of Equation (6), a probability should stay within 0 and 1. Hence, when $PT_V > IFS_D$, which leads to $IFS_D - PT_V < 0$, the probability should be considered 0 instead of a negative value. Thus the probability of having no collisions for one BLE victim packet should be written as:

$$\mathrm{P^{n}_{no\ collision}} = \max(0, \mathrm{n} \cdot \frac{\mathrm{IFS_{D} - PT_{V}}}{\mathrm{CE_{D}}}) \quad (8)$$

The equation above only calculates the probability of having no collision for one BLE victim packet. To know the probability of no collision for multiple BLE victim packets, equation (8) must be used multiple times. Considering an even number m packets inside the BLE victim connection event, the probability of having no collisions between m BLE victim packets and n BLE disturber packets is written as:

$$\mathrm{P^{mn}_{no\ collision}} = \prod_{i=1}^{m} \max(0, \mathrm{n} \cdot \frac{\mathrm{IFS_{D} - PT^{i}_{V}}}{\mathrm{CE_{D}}}) \quad (9)$$

As we can see, equation (9) can be difficult to use when there is a lot of variability of the packet transmission time. To further simplify equation (9), Fig. 3 (b) is introduced. The difference between Fig. 3 (a) and Fig. 3 (b) is the packet transmission time of both the BLE victim and the BLE disturber. In Fig. 3 (b), we simplify the connection events by changing all the packet transmission time into the average packet transmission time. Since all the BLE victim packets are now considered to have the equal transmission time, equation (9) can be simplified to:

$$\mathrm{P^{mn}_{no\ collision}} = \max(0, \mathrm{n} \cdot \frac{\mathrm{IFS_{D}} - \overline{\mathrm{PT_{V}}}}{\mathrm{CE_{D}}})^{\mathrm{m}} \quad (10)$$

where $\overline{PT_V}$ is the average packet transmission time in a connection interval of the BLE victim. Note that there are some errors introduced due to the simplification. According to our theoretical study, errors are either zero or minor even when individual packet transmission times fluctuate significantly from the average, thus they are not shown or evaluated experimentally in this paper. As a detailed example, given $m = n = 8$, $IFS_D = 150$, $CE_D = 6832$, and $PT_V = 80, 512, 912, 1312$ to Equations (9) and (10), both of them calculate the $P^{mn}_{no\ collision}$ as 0.

The collision probability can now be calculated as:

$$\begin{aligned}\mathrm{P^{mn}_{collision}} &= 1 - \mathrm{P^{mn}_{no\ collision}} \\ &= 1 - \max(0, \mathrm{n} \cdot \frac{\mathrm{IFS_{D}} - \overline{\mathrm{PT_{V}}}}{\mathrm{CE_{D}}})^{\mathrm{m}}\end{aligned} \quad (11)$$

Finally, the total interference probability on a connection-interval level $P_{interference}$ is the combination of the probability of having a connection event overlap ($P_{overlap}$) and the probability of having a packet collision ($P^{mn}_{collision}$). The total interference probability can be defined as:

$$\begin{aligned}\mathrm{P_{interference}} &= \mathrm{P_{overlap}} \cdot \mathrm{P^{mn}_{collision}} \\ &= \min(1, \frac{\mathrm{CE_{V} + CE_{D}}}{\mathrm{CI_{D}}}) \\ &\cdot (1 - \max(0, \mathrm{n} \cdot \frac{\mathrm{IFS_{D}} - \overline{\mathrm{PT_{V}}}}{\mathrm{CE_{D}}})^{\mathrm{m}})\end{aligned} \quad (12)$$

When interference occurs, it does not necessarily mean that the transmission would fail. Only when the interference causes some errors in the packets, one can assume the packet is lost [27]. The probability of at least one bit error during transmission, i.e. P_{error}, is defined by equation (13), where BER_V indicates the BER at the BLE victim side and L_V represents the number of bits in a PT_V [22, 33]. In this paper, the BLE disturber is considered the interference source, therefore, the BER_V is mostly produced by the interference from disturber pair. Note that the BLE physical mode used in this paper is LE 1M PHY, thus there is no error correction code introduced. However, when an error correction technology is used (like the LE Coded S2/S8 in BLE 5), the BER_V from that coded channel should be used. Indeed, the BER will be lower for a coded channel compared with an uncoded channel in an equal scenario.

$$\mathrm{P_{error}} = 1 - (1 - \mathrm{BER_{V}})^{2 \cdot \mathrm{L_{V}}} \quad (13)$$

The BER_V is a metric that defines the average BER of a victim packet in a specific interference situation [34]. It depends on the percentage-wise overlap between a BLE victim packet and a BLE disturber packet as well as the signal to noise ratio, etc. In this paper, we assume the BER_V is known. Modeling the BER_V in accordance with the BLE disturber's parameters is planned as future work. Also note that this equation is calculating the probability of two packets ($2 \cdot L_V$), since in BLE communications, to avoid transmission failure, both packets from the central and the peripheral have to be successfully transmitted.

Considering the probabilities defined in equations (12) and (13), the probability of a transmission failure (P_{TF}) is finally written as:

$$\begin{aligned}\mathrm{P_{TF}} &= \mathrm{P_{error}} \cdot \mathrm{P_{interference}} \\ &= (1 - (1 - \mathrm{BER_{V}})^{2 \cdot \mathrm{L_{V}}}) \\ &\cdot \min(1, \frac{\mathrm{CE_{V} + CE_{D}}}{\mathrm{CI_{D}}}) \\ &\cdot (1 - \max(0, \mathrm{n} \cdot \frac{\mathrm{IFS_{D}} - \overline{\mathrm{PT_{V}}}}{\mathrm{CE_{D}}})^{\mathrm{m}})\end{aligned} \quad (14)$$

The logic to calculate P_{TF} like this can be concluded into two points. The first condition for the transmission failure to occur is that the BLE victim connection is under interference. The second condition is that there are errors within the packets exchanged between the victim central and peripheral. These two conditions occur with probabilities of $P_{interference}$ and P_{error} respectively. A reasonable assumption of this paper is that the packet errors only occur when the BLE connection is under interference. Hence, the transmission failure probability P_{TF} is calculated as the product of $P_{interference}$ and P_{error}, as shown in equation (14).

C. Analytical Study

In this section, some analytical study about the mathematical model is conducted theoretically. Equation (14) gives a thorough look at the transmission failure probability between the BLE victim and the disturber. To do a deep analytical study in BLE communication using this equation, more BLE details must be included.

1) Impacting Parameters: In BLE communication, a connection interval contains only one connection event [17]. The connection event is composed of packets from both the central and the peripheral separated by an IFS in between every two packets. By replacing the connection event variables (CE_V, CE_D) with PT and IFS, equation (14) can be written as:

$$\begin{aligned} \mathrm{P_{TF}} &= (1-(1-\mathrm{BER_V})^{2\cdot \mathrm{L_V}}) \\ &\cdot \min(1, \frac{\mathrm{m}\cdot(\overline{\mathrm{PT_V}}+\mathrm{IFS})+\mathrm{n}\cdot(\overline{\mathrm{PT_D}}+\mathrm{IFS})}{\mathrm{CI_D}}) \\ &\cdot (1-\max(0, \cdot\frac{\mathrm{IFS}-\overline{\mathrm{PT_V}}}{\overline{\mathrm{PT_D}}+\mathrm{IFS}})^{\mathrm{m}}) \end{aligned} \tag{15}$$

where the CE is represented by $x\cdot(\overline{PT}+IFS)$ with x the number of packets in the connection event. All the IFS_V and IFS_D are represented by IFS, since all the IFSs have a fixed length of 150 μs.

Equation (15) shows that the probability of a transmission failure is determined by these parameters:

(a) The number of packets m in a CE_V
(b) The number of packets n in a CE_D
(c) The average packet transmission time of the BLE victim $\overline{PT_V}$ and the average number of bits inside that packet $\overline{L_V}$
(d) The average packet transmission time of the BLE disturber $\overline{PT_D}$
(e) The connection interval of the BLE disturber CI_D
(f) The inter frame space of the victim and the disturber IFS
(g) The BER at the BLE victim BER_V

2) Real Scenario: The BLE specification stipulates all BLE devices should use AFH to avoid interference. It defines 37 channels for data exchange between the BLE devices. According to literature, the probability of each channel to be used is approximately uniformly distributed [11, 12]. Although the mathematical model is derived for the probability of transmission failure on a single channel, it is directly applicable to the whole spectrum. The explanation is that the measurement of BER_V decides the scope of the application of equation (15). When the BER_V is measured on a single channel, the equation should be used to calculate the transmission failure probability for that channel. While if the BER_V is measured for the whole spectrum, the equation can be directly applied to all the 37 data channels. To distinguish with P_{TF}, the transmission failure probability over all the 37 channels is written as P_{TF_37} and introduced in equation (16).

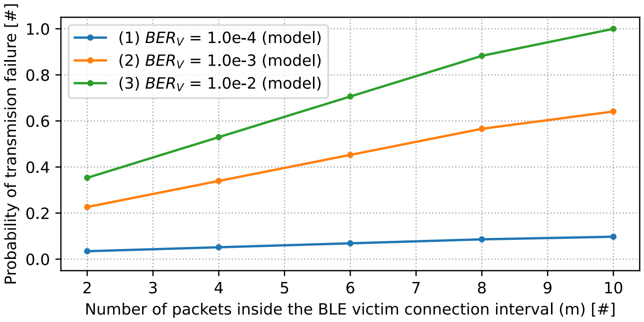

Fig. 4. Expected probability of transmission failure (P_{TF}) as a function of number of packets inside the BLE victim connection interval (m). Parameters: m = 2 - 10, n = 2, $\overline{PT_V}$ = 512 μs (payload: 50 bytes), L_V = 512 bits, $\overline{PT_D}$ = 512 μs (payload: 50 bytes), CI_V = 7.5 ms, CI_D = 7.5 ms, IFS = 150 μs.

$$\mathrm{P_{TF\_37}} = \mathrm{P_{TF}} \tag{16}$$

3) Reliability: The transmission failure probability closely relates to the reliability of the BLE communication. Normally the reliability of a wireless protocol is represented by the packet loss rate (PLR). Equation (15) calculates the probability of a transmission failure on the connection interval level. Hence, it is supposed that the PLR of the BLE communication should be close to the outcome of the equation, since a packet loss normally means a transmission failure. Therefore, the total probability of transmission failure P_{TF_37} might be used to quantify the reliability of the BLE connection. So the reliability can be estimated as the following:

$$\mathrm{Reliability} \approx 1 - \mathrm{P_{TF\_37}} \tag{17}$$

4) Case Study: Using equations (14) and (15), it is convenient to study the impact of the transmission parameters, the number of packets and the packet transmission time, on the transmission failure and the coexistence between the BLE pairs. In what follows, some examples are given from the presented mathematical model.

The probability of a transmission failure (P_{TF}) as a function of the number of packets inside the BLE victim connection interval (m) and the (average) BLE victim packet transmission time ($\overline{PT_V}$) are plotted in Fig. 4 and Fig. 5, respectively.

Fig. 4 is shown under an assumption of a number of fixed parameters, including the number of packets inside the BLE disturber connection interval (n = 2), both the average BLE victim packet transmission time ($\overline{PT_V}$) and the average BLE disturber packet transmission time ($\overline{PT_D}$) as 512 μs, both the BLE victim connection interval (CI_V) and the BLE disturber connection interval (CI_D) as 7.5 ms, and the IFS as 150 μs. Also the assumption is made that the BER on the BLE victim side, i.e. BER_V, is a constant value of 1e-4, 1e-3 or 1e-2. This assumption replicates environments with different levels of interference, and the constant values indicate that BLE parameters such as transmission power and distance do not change. The number of packets inside the BLE victim

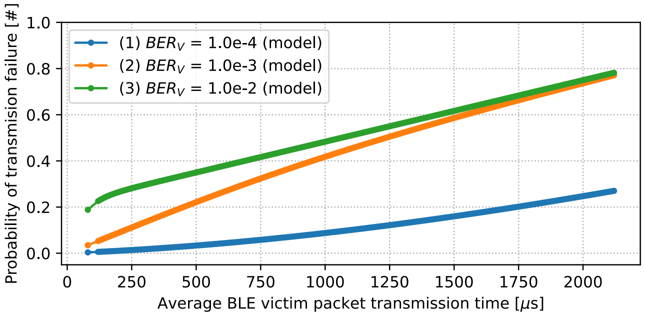

Fig. 5. Expected probability of transmission failure (P_{TF}) as a function of average BLE victim packet transmission time ($\overline{PT_V}$). Parameters: m = 2, n = 2, $\overline{PT_V}$ = 80 μs - 2120 μs (payload: 0 - 251 bytes), L_V = 80 bits - 2120 bits, $\overline{PT_D}$ = 512 μs (payload: 50 bytes), CI_V = 7.5 ms, CI_D = 7.5 ms, IFS = 150 μs.

connection interval (m) is the independent variable ranging from 2 to 10 since 10 is the maximum number of packets, with packet transmission time of 512 μs, that can be accommodated within 7.5 ms.

Fig. 5 is generated under a similar assumption as Fig. 4. Yet, m is now fixed to 2, while $\overline{PT_V}$ ranges from 80 μs to 2120 μs (corresponding to BLE packets from 10 bytes to 265 bytes). This range limits the (average) transmission time of a BLE victim packet, which is mentioned in BLE specifications since version 4.2 [17].

Analyzing the two figures reveals that, first of all, there is a linear trend of both curves from Figs. 4 and 5. With a certain set of parameters for the BLE disturber, the probability of the transmission failure increases linearly with the increment of the number of the BLE victim packets inside its connection interval or BLE victim packet transmission time.

Secondly, the large difference between the curves in both Figs. 4 and 5 illustrates the influence of the BER_V (environment). The larger the BER_V, the higher the probability of transmission failure. According to literature, the BER_V relates to various factors that are mainly dependent on the environment of the practical setup itself, for example, noise, interference, distortion, attenuation, transmission power, relative position and location [35]. Hence, it is important but at the same time almost impossible to control the BER_V at a specific low level. Note that the convergence of curves (2) and (3) in Fig. 5 is due to the large BER_V and L_V since large BER_V and L_V make the P_{error} close to one.

From Figs. 4 and 5, it is interesting to point out that, to send and receive a larger amount of data under a low-BER_V environment, using multiple small packets is a more reliable strategy than using fewer big packets. As an example, when a 500-byte payload has to be exchanged in a 1e-4 BER_V environment, using 10 smaller packets with 50-byte payload in each, results in a P_{TF} of 10% shown in Fig. 4. It is more reliable than using 2 bigger packtes with 250-byte payload in each, resulting in a P_{TF} of more than 20% shown in Fig. 5. Big packets obviously result in a higher probability of transmission failure, which is about two to three times that of small packets when exchanging the same amount of payload such as 500 bytes. Nevertheless, under a higher-BER_V environment (1e-3 or 1e-2), the mathematical model gives different results. For instance, when the BER_V is 1e-2, a smaller transmission failure probability is achieved by using 2 bigger packets instead of 10 smaller packets. The contradictory conclusions are drawn mainly due to the large difference of P_{error} under varied BER_V values.

In the transmission parameters, there are still the other two parameters, i.e. $\overline{PT_D}$ and n, impacting the transmission failure probability. Note that changing these two parameters actually means differing the environment.

The impact of the number of packets inside the BLE disturber connection interval, i.e. n, is discussed mathematically. By analysing equations (12) and (15), the parameter n could have a similar influence on the interference probability ($P_{interference}$) as the parameter m. By looking into the overlap part of equation (15), the parameters n and m have a similar effect on the connection event overlap probability since they have similar positions in the equation, while the collision part of the equation shows the difference, which is only m appears. As a result, theoretically the two parameters should affect the result differently, but actually they do not. In the BLE specification [17], the IFS is fixed to a length of 150 μs, while a packet ranges from 80 μs to 2120 μs, using LE 1M PHY. This provides a tiny probability for the packet being accommodated in the IFS. Hence, in most cases, as long as the $\overline{PT_V}$ is larger than the IFS, the collision part of equation (15) is equal to one no matter the values of n and m. With this point in mind, the parameter n provides a similar or even equal influence on the interference probability $P_{interference}$ as the parameter m.

However, changing the parameter n may change the environment itself, which, as mentioned before, changes the BER_V, hence the value of the equation (13) changes. Assuming that the BER_V increases, the value of the equation (13) also increases. With all these analytical results in hand, we could draw a temporary conclusion that the parameter n affects the transmission failure probability similarly as the parameter m, but should give a higher transmission failure probability.

The analysis of the impact of the BLE disturber packet transmission time $\overline{PT_D}$ is similar to the analysis for the parameter n. The conclusion is similar as well. With an increase of the parameter $\overline{PT_D}$, the transmission failure probability also increases. Although the transmission failure also increases with an increase of $\overline{PT_V}$, the rise due to an increase of $\overline{PT_D}$ is larger, under the assumption of a larger BER_V.

IV. Experimental Setup

The experimental setup introduced in this section aims at validating the introduced mathematical model and investigating, in detail, the impact of transmission parameters and other parameters on transmission failure and coexistence between BLE pairs.

The experimental setup follows the minimal system model by placing two pairs of BLE development boards (nRF52840 DK [36]) in an office environment close to one another. Six scenarios are defined by varying parameters like distances and transmission powers. Each scenario represents a different

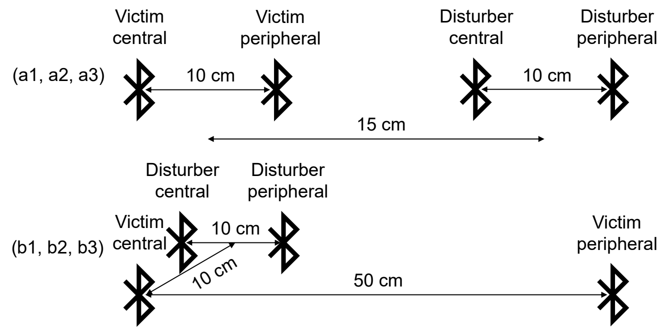

Fig. 6. Schematic of the three designed scenarios.

electromagnetic environment. To exhaustively validate and evaluate the proposed model, the six scenarios are designed as in Fig. 6 and described as follows:

(a1) 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 is also easier for readers to have a first understanding on how the model works since it is derived on a single channel till equation (15). The distance between the victim/disturber central and peripheral is within 10 cm, while the distance between the BLE victim and the disturber is around 15 cm. The transmission power of the BLE victim devices in our experiment is -4 dBm while the BLE disturber is programmed to communicate using an output power of 8 dBm. This scenario is considered as a preliminary validation of the model.

(a2) The CSAs are still disabled in this scenario. All the parameters of this scenarios are the same as the ones of scenario (a1). However, the transmission power of both the victim and the disturber devices is adjusted to a same level, i.e. 0 dBm. This scenario simulates an environment full of BLE connections and none of them uses a biased transmission power, such as -4 dBm and 8 dBm.

(a3) The CSAs are enabled in this scenario, and CSA #2 is used. Except that, all the other parameters of this scenarios are the same as the ones of scenario (a2). This scenario simulates a realistic environment with only two BLE pairs inside. With the CSAs enabled and unbiased transmission power, the proposed model is validated in this realistic environment.

(b1) Similar to scenario (a1), the CSAs are disabled in this scenario as well. The distance between the victim central and peripheral is changed to approximately 50 cm, whereas still around 10 cm between the disturber central and peripheral. Furthermore, the disturber pair is positioned around 10 cm away from the victim central. The transmission power of the BLE victim devices is -4 dBm while the BLE disturber is 8 dBm. This scenario is considered as a further validation of the model.

(b2) The CSAs are still disabled in this scenario. The parameters of this scenarios follow the ones of scenario (b1). But the transmission power of both the victim and the disturber devices is adjusted to 0 dBm. Similar to scenario (a2), this scenario simulates an environment full of BLE connections and all of them use an unbiased transmission power.

(b3) All the parameters of scenario (b3) are the same as the ones of scenario (b2), except the use of the CSAs. In this scenario, the CSA #2 is enabled for both the victim and the disturber. Hence, scenario (b3) can be considered a real-world use case, with one BLE pair acting as a laptop with a wireless mouse or keyboard and the other acting as a smartphone with a smart watch. This scenario is the final validation and evaluation of the model.

In the experiment, there are different experiment sets. Each contains multiple experiment runs, which are used to find a stable outcome. Every experiment run is a communication session, which includes many connection intervals. Hence, the time of each experiment set differs due to various parameters, such as the BLE connection interval and the number of runs of that experiment set. For example, if the connection interval is set to 7.5 ms, the number of connection intervals will reach 500 in 3.75 s, and if 500 runs are needed to find a stable outcome, it will cost around 32 minutes. Assuming that the connection interval equals 4 s, the total experiment time takes up to 278 hours.

As assumed in the mathematical model, till equation (15), only one channel is considered. Hence, the effect of the CSAs is eliminated by enforcing both the BLE victim and the disturber to work only on the same BLE channel, which refers to scenarios (a) and (b). Channel 35 is chosen in this experiment because it is far away from popular Wi-Fi channels 1, 6, and 11 which are the major source of external interference in an office environment. To achieve this, the Zephyr RTOS is deployed, a fully open-source real-time operation system for BLE, on the development boards so that full control of the channel is available during the connection by modifying its link layer code [37]. For scenario (c), the CSAs are enabled, so a real-world standard-compliant use case is studied. By changing the link layer code, it also enables one to control the number of packets and the packet transmission time inside each connection interval. In the experiment, the packet transmission time is changed randomly within the range of the aimed payload size ± 10 bytes. Note that the change of packet transmission time can only happen on the BLE victim, since changing the BLE disturber packet transmission time results in a change of the environment (BER_V).

The practical arrangement of both the victim and disturber determines the BER_V. In order to correctly compare the experiment with the model, the model is provided with the BER_V calculated in a similar way as in [27, 38, 39]. To be more specific, the BER_V is determined by dividing the packet corruption rate by the bit length of the payload. The BER_V changes over multiple measurements (500 in this paper), therefore, the average of the measurements is used. For scenario (a1), the average value of 1.43e-4 is used as BER_V for all the data points. The BER_V of scenario (b1) is

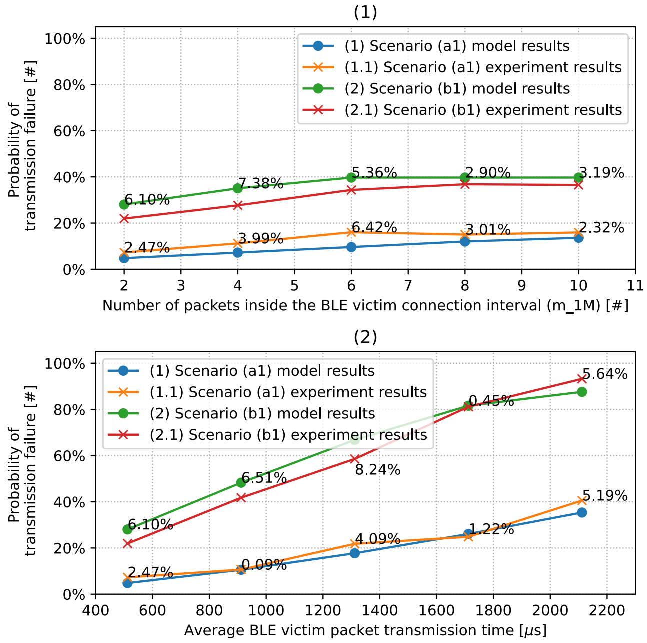

Fig. 7. Detailed comparison of experimental result with the model one under scenarios (a1) and (b1). The deviations are displayed in percentage next to the curves. CSAs are disabled, and biased transmission powers are used for the victim (-4 dBm) and the disturber (+8 dBm). Parameters in (1): m = 2 - 10, n = 2 in scenario (a1) while 6 in scenarios (b1), $\overline{PT_V}$ = 512 μs (payload: 50 bytes), L_V = 512 bits, PT_D = 512 μs (payload: 50 bytes), CI_V = 7.5 ms, CI_D = 7.5 ms, IFS = 150 μs, BER_V = 1.43e-4 in scenario (a1) while 4.94e-4 in scenario (b1). Parameters in (2): m = 2, n = 2 in scenario (a1) while 6 in scenarios (b1), $\overline{PT_V}$ = 512 μs - 2112 μs (payload: 50 bytes - 250 bytes), L_V = 512 bits - 2112 bits, PT_D = 512 μs (payload: 50 bytes), CI_V = 7.5 ms, CI_D = 7.5 ms, IFS = 150 μs, BER_V = 1.43e-4 in scenario (a1) while 4.94e-4 in scenario (b1).

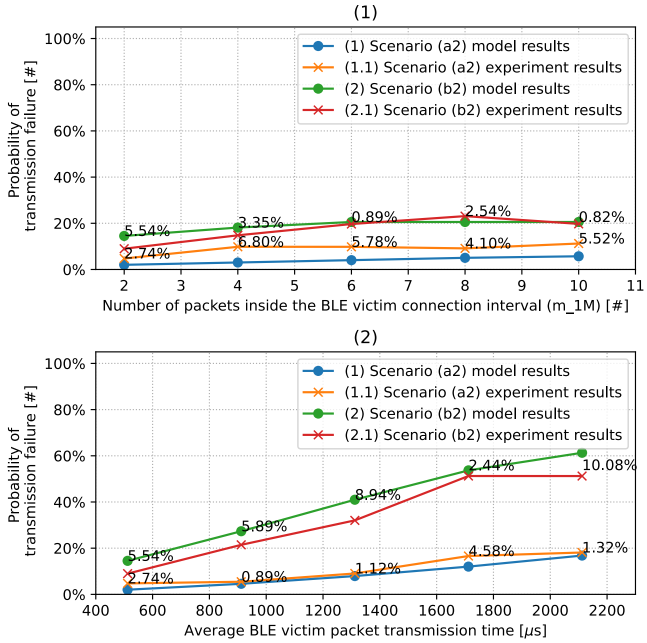

Fig. 8. Detailed comparison of experimental result with the model one under scenarios (a2) and (b2). The deviations are displayed in percentage next to the curves. CSAs are disabled, and unbiased transmission power is used for the victim (0 dBm) and the disturber (0 dBm). All the other parameters are the same as Fig. 7, thus not repeated here, except BER_V. BER_V = 5.75e-5 in scenario (a2) while 2.25e-4 in scenario (b2).

measured as 4.94e-4. Regarding scenarios (a2) and (b2), the average BER_V is measured as 5.75e-5 and 2.25e-4 respectively. While scenarios (a3) and (b3) use the BER_V measured when the CSAs are enabled, which are 3.91e-6 and 8.38e-6.

V. Experimental Validation of the Model

In this section, a set of results from our experiments are described and discussed, aiming at validating the introduced mathematical model and our analytical study. As it will be shown, the results highlight a rather accurate prediction regarding the transmission failure and the reliability under different scenarios. Consistently, the model might be used for the coexistence exploration of BLE devices or networks, and can thus be applied in the design and the deployment of such networks.

A. Validation

The results in Figs. 7, 8, and 9 show a clear correspondence between the experiment and mathematical model. Of course, the results are not exactly the same due to many factors like the property from the mathematical model and the average BER. Remember that the mathematical model only calculates the transmission failure probability on the connection interval level. Yet, the experiment clearly indicates the same trends as the mathematical model, confirming the mathematical model in different scenarios.

Fig. 7 describes the consistency between the model and the experiment results under scenarios (a1) and (b1). The CSAs are disabled to simulate a rather harsh electromagnetic environment, and biased transmission powers are used to have a preliminary validation of the model. The independent variables are the packet number inside the BLE victim connection interval (m) in Fig. 7 (1), and the victim packet transmission time (PT_V) in Fig. 7 (2). All the necessary parameters are listed in the caption of Fig. 7. Under both scenarios (a1) and (b1), the experiment results follow the trend calculated by the model, and the deviations between the experiment and the model are shown as percentages next to the curves. It is worth mentioning that the errors between the model and the experiment results are 8.24% maximum and 4.16% on average.

Fig. 8 gives the model and the experiment results under scenarios (a2) and (b2). In these two scenarios, the CSAs are still disabled to simulate a harsh environment, while an unbiased transmission power is used to have a further evaluation on the model. The variables are the same as the ones in Fig. 7, which are m and PT_V respectively in Fig. 8 (1) and (2). All the communication parameters used in Fig. 8 are the same as in Fig. 7, thus not repeated in the caption. In Fig. 8 (1), the results when m varies are illustrated. The experiment results show a similar trend as predicted by the model. The largest and average errors in Fig. 8 (1) between the model and the experiments are 6.80% and 3.81%, respectively. Fig. 8 (2) is the results of scenarios (a2) and (b2) when the PT_V is the

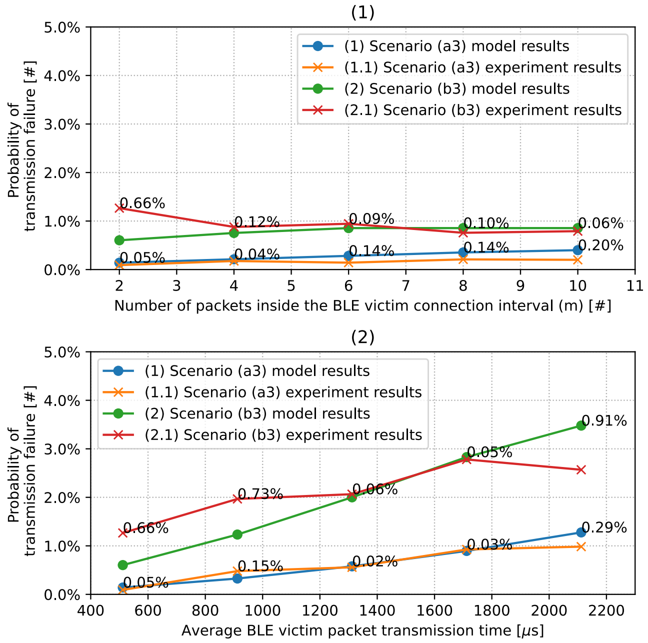

Fig. 9. Detailed comparison of experimental result with the model one under scenarios (a2) and (b2). The deviations are displayed in percentage next to the curves. CSAs are enabled, and unbiased transmission power is used for the victim (0 dBm) and the disturber (0 dBm). All the other parameters are the same as Fig. 7, thus not repeated here, except BER_V. BER_V = 3.91e-6 in scenario (a2) while 8.38e-6 in scenario (b2).

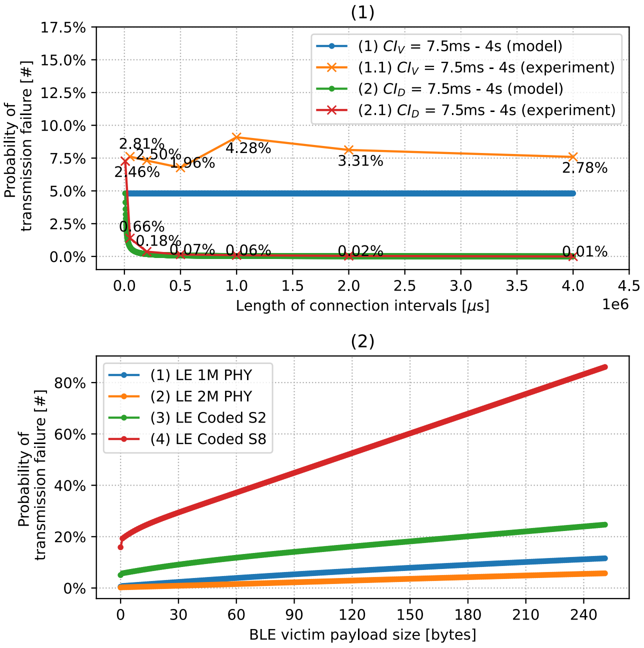

Fig. 10. Instance of using the reliability model to study the impact of connection interval and physical mode. Parameters in (1): m = 2, n = 2, $\overline{PT_V}$ = 512 μs (payload: 50 bytes), L_V = 512 bits, $\overline{PT_D}$ = 512 μs (payload: 50 bytes), CI_V = 7.5 ms (if CI_D is the independent variable), CI_D = 7.5 ms (if CI_V is the independent variable), IFS = 150 μs. All the other parameters in (2) are the same as in (1), except victim payload size = 50 bytes - 251 bytes, CI_V = 50 ms, and CI_D = 50 ms. BER_V = 1e-3 is used in this theoretical study.

independent variable. Again, the experiment results are in a good correspondence with the model ones after correction. The maximum deviation in Fig. 8 (2) is 10.08%, and the average deviation is around 4.36%.

Fig. 9 follows the same logic as Figs. 7 and 8. The main difference is that the CSAs are enabled, thus a realistic use case is simulated. Besides, the transmission power is unbiased. Same independent variables are used as discussed in Figs. 7 and 8. It is evident that the experimental results are close to the theoretical ones. The maximum difference shown in Fig. 9 is only 0.91%, and the average error is 0.23%. Comparing with Figs. 7 and 8, there is a sharp drop in the deviations. This drop can be explained as the impact of CSAs. Different from other scenarios, the CSAs are enabled in scenarios (a3) and (b3). It can be understood as the deviations from scenarios (a1), (a2), (b1) and (b2) are averaged from a single channel into 37 data channels. As a result, the deviations drop sharply. From another point of view, this phenomenon might suggest that the developed reliability model tends to give a higher error when it is applied in a harsher environment. Scenarios (a1), (a2), (b1) and (b2) simulate four harsh electromagnetic environments, i.e. full of interference in the 2.4 GHz frequency band, and the average deviation is approximately 4%. When it comes to scenarios (a3) and (b3), i.e. only one BLE connection as interference in the whole frequency band, the average error is only 0.23%.

Regarding the error analysis, it is understandable that there are deviations between the theoretical results and the experimental ones. The deviations in all the validation experiments can be briefly explained in two perspectives. First, there is sporadic interference existing in the 2.4 GHz frequency spectrum, despite our best efforts to keep the office as noiseless as possible. Second, even after 500 experiment runs, the average result of them is only close to the theoretical value but not equal to it. This is due to the nature of probability and related experiments [40]. It is however clear that the model follows the same trend of the experiments.

B. Discussion

Except for the transmission parameters, there are also other parameters impacting the transmission failure probability such as the connection interval. However in our mathematical model, the only connection interval parameter is the BLE disturber connection interval, which may imply that the BLE victim connection interval has no influence at all on the probability of the transmission failure. For the parameter CI_D, we assume that if it is increased, the P_{TF} will decrease, since CI_D is inversely related to P_{TF} as shown by equation (12). But again, changing the CI_D alters the environment, thus the BER_V may also change again.

The impact of both the connection intervals CI_D and CI_V is illustrated in Fig. 10 (1). As expected, indeed the BLE victim connection interval has no impact on the transmission failure probability at all. This suggests that in a static environment, adjusting the connection interval of a BLE pair may not help with transmission failure avoidance. Instead, it introduces uncertainty for that BLE pair, as the probability of transmission failure may rise or decrease, depending on luck and the case itself. This is important for all BLE developers and users, since there is research adjusting the CI_V to improve the reliability under some other interference like Wi-Fi [41], but as shown in this paper it does not work under the BLE interference with a long-term and repeated perspective.

In contrast, the impact of the BLE disturber connection interval is high, especially at small values. When the CI_D is a relatively small value, the transmission failure probability changes dramatically with a tiny change of the parameter. After a certain value, in this measurement around 500 ms, the probability of the transmission failure stabilizes close to zero. Considering interchangeability of the BLE victim and the disturber (The BLE victim may also cause a transmission failure on the BLE disturber side.), this result may be applied in the BLE network design. For instance, setting the connection intervals of all the BLE devices in a network close to a certain value which can be obtained by the mathematical model can decrease the transmission failure occurrence among them. The considerable gap between curves (1) and (1.1) is due to the figure's scale; the difference in percentage points between the model and the experiment is only around 3-4%.

Another possible usage instance of the model is to discuss the impact of different BLE physical modes, i.e. LE 1M PHY, LE 2M PHY, LE Coded S2, and LE Coded S8. As an example, Fig. 10 (2) illustrates the theoretical investigation results using the developed reliability model. The BER_V is defined as 1e-3. Note that an equal BERv for all physical modes is a result of different SNR values at the victim. As shown, all the four physical modes give a growing trend with the increment of the victim payload size. However, they grow with different slopes. Comparing with the other three physical modes, LE Coded S8 has the highest transmission failure probability. It can be explained by the large variation of packet length under the four physical modes. For instance, with a payload size of 251 bytes, LE 2M PHY provides the shortest packet transmission time, which is 1064 μs, while the packet transmission time under LE Coded S8 is 17040 μs. This huge difference leads to the difference of the calculated transmission failure probability. This is an example of how to use the developed reliability model. Since the physical mode is out of the scope of this paper, it is not further validated or discussed, but more considered one of the future work.

VI. Conclusion

BLE is progressively considered as a primary choice for low-range IoT systems. However, to successfully deploy a BLE network in different realistic scenarios, it is crucial to grasp the transmission failure details inside the BLE network itself first. Therefore, this study is conducted to discover the essence of BLE transmission failure.

In this paper there are three contributions: first, a mathematical model of the transmission failure probability between two BLE pairs is derived; second, extensive experiments on real-world BLE devices to validate the mathematical model are performed in an office environment; and third, the impact of each parameter from the model on the BLE transmission failure is thoroughly explained.

The impact of transmission parameters, i.e. the number of packets and the packet transmission time, on the transmission failure and coexistence of BLE pairs is confirmed between the presented model and experiments. On the one hand, logically, longer and more packets can improve the throughput of the BLE connection; on the other hand, they are also exposed to higher transmission failure probabilities. Besides that, the impact of another essential parameter of BLE, connection interval, is also evaluated. The result clearly shows us the BLE victim connection interval does not vary the transmission failure probability at all, although this is often proposed as a mitigation technique against external interference [41, 15].

As for the future work, the model could be extended to non-standard BLE specifications in the future. For instance, it would be interesting to vary the parameters to values out of the BLE specification boundary and find the optimal combination of them to fight against transmission failure. As an example, another parameter shown in our mathematical model that may affect the transmission failure probability is the IFS, but according to the BLE specification, the IFS of any BLE devices should be fixed at 150 μs [17].

References

[1] S. Nižetić, P. Šolić, D. López-de-Ipiña González-de Artaza, and L. Patrono, "Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future," *Journal of Cleaner Production*, vol. 274, p. 122877, Nov. 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S095965262032922X

[2] N. Y. Philip, J. J. P. C. Rodrigues, H. Wang, S. J. Fong, and J. Chen, "Internet of Things for In-Home Health Monitoring Systems: Current Advances, Challenges and Future Directions," *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 2, pp. 300–310, Feb. 2021, conference Name: IEEE Journal on Selected Areas in Communications.

[3] F. Firouzi, B. Farahani, M. Daneshmand, K. Grise, J. Song, R. Saracco, L. L. Wang, K. Lo, P. Angelov, E. Soares, P.-S. Loh, Z. Talebpour, R. Moradi, M. Goodarzi, H. Ashraf, M. Talebpour, A. Talebpour, L. Romeo, R. Das, H. Heidari, D. Pasquale, J. Moody, C. Woods, E. S. Huang, P. Barnaghi, M. Sarrafzadeh, R. Li, K. L. Beck, O. Isayev, N. Sung, and A. Luo, "Harnessing the Power of Smart and Connected Health to Tackle COVID-19: IoT, AI, Robotics, and Blockchain for a Better World," *IEEE Internet of Things Journal*, vol. 8, no. 16, pp. 12 826–12 846, Aug. 2021, conference Name: IEEE Internet of Things Journal.

[4] D. Wu and N. Ansari, "A Trust-Evaluation-Enhanced Blockchain-Secured Industrial IoT System," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5510–5517, Apr. 2021, conference Name: IEEE Internet of Things Journal.

[5] S. Al-Sarawi, M. Anbar, K. Alieyan, and M. Alzubaidi, "Internet of Things (IoT) communication protocols: Review," in *2017 8th International Conference on Information Technology (ICIT)*, May 2017, pp. 685–690.

[6] D. Hortelano, T. Olivares, M. C. Ruiz, C. Garrido-Hidalgo, and V. López, "From Sensor Networks to Internet of Things. Bluetooth Low Energy, a Standard for This Evolution," *Sensors*, vol. 17, no. 2, p. 372, Feb. 2017, number: 2 Publisher: Multidisciplinary Digital Publishing Institute. [Online]. Available: https://www.mdpi.com/1424-8220/17/2/372

[7] 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*, vol. 2, no. 4, pp. 972–981,

Dec. 2018, conference Name: IEEE Transactions on Green Communications and Networking.

[8] 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, iSSN: 1946-0759.

[9] R. Rondón, A. Mahmood, S. Grimaldi, and M. Gidlund, "Understanding the Performance of Bluetooth Mesh: Reliability, Delay, and Scalability Analysis," *IEEE Internet of Things Journal*, vol. 7, no. 3, pp. 2089–2101, Mar. 2020, conference Name: IEEE Internet of Things Journal.

[10] L. Zhang, Y.-C. Liang, and M. Xiao, "Spectrum Sharing for Internet of Things: A Survey," *IEEE Wireless Communications*, vol. 26, no. 3, pp. 132–139, Jun. 2019, conference Name: IEEE Wireless Communications.

[11] B. 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.

[12] M. O. A. Kalaa and H. H. Refai, "Selection probability of data channels in Bluetooth Low Energy," in *2015 International Wireless Communications and Mobile Computing Conference (IWCMC)*, Aug. 2015, pp. 148–152, iSSN: 2376-6506.

[13] O. Carhacioglu, P. Zand, and M. Nabi, "Time-domain cooperative coexistence of BLE and IEEE 802.15.4 networks," in *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, Oct. 2017, pp. 1–7, iSSN: 2166-9589.

[14] 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, p. 2257, Jan. 2021, number: 7 Publisher: Multidisciplinary Digital Publishing Institute. [Online]. Available: https://www.mdpi.com/1424-8220/21/7/2257

[15] M. Spörk, J. Classen, C. A. Boano, M. Hollick, and K. Römer, "Improving the Reliability of Bluetooth Low Energy Connections," in *Proceedings of the 2020 International Conference on Embedded Wireless Systems and Networks on Proceedings of the 2020 International Conference on Embedded Wireless Systems and Networks*, ser. EWSN '20. USA: Junction Publishing, Feb. 2020, pp. 144–155.

[16] 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.

[17] "Bluetooth Core Specification v5.2," p. 3256.

[18] J. J. Treurniet, C. Sarkar, R. V. Prasad, and W. D. Boer, "Energy Consumption and Latency in BLE Devices under Mutual Interference: An Experimental Study," in *2015 3rd International Conference on Future Internet of Things and Cloud*, Aug. 2015, pp. 333–340.

[19] H. Karvonen, K. Mikhaylov, M. Hämäläinen, J. Iinatti, and C. Pomalaza-Ráez, "Interference of wireless technologies on BLE based WBANs in hospital scenarios," in *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, Oct. 2017, pp. 1–6, iSSN: 2166-9589.

[20] 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)*, Sep. 2016, pp. 1–6, iSSN: 2166-9589.

[21] B. Badihi, F. Ghavimi, and R. Jäntti, "On the System-level Performance Evaluation of Bluetooth 5 in IoT: Open Office Case Study," in *2019 16th International Symposium on Wireless Communication Systems (ISWCS)*, Aug. 2019, pp. 485–489, iSSN: 2154-0225.

[22] H. Karvonen, K. Mikhaylov, D. Acharya, and M. M. Rahman, "Performance Evaluation of Bluetooth Low Energy Technology Under Interference," in *13th EAI International Conference on Body Area Networks*, ser. EAI/Springer Innovations in Communication and Computing, C. Sugimoto, H. Farhadi, and M. Hämäläinen, Eds. Cham: Springer International Publishing, 2020, pp. 147–156.

[23] H. Hajizadeh, M. Nabi, M. Vermeulen, and K. Goossens, "Coexistence Analysis of Co-Located BLE and IEEE 802.15.4 TSCH Networks," *IEEE Sensors Journal*, vol. 21, no. 15, pp. 17 360–17 372, Aug. 2021, conference Name: IEEE Sensors Journal.

[24] M. O. A. Kalaa, W. Balid, N. Bitar, and H. H. Refai, "Evaluating Bluetooth Low Energy in realistic wireless environments," in *2016 IEEE Wireless Communications and Networking Conference*, Apr. 2016, pp. 1–6, iSSN: 1558-2612.

[25] Q. Duy La, D. Nguyen-Nam, M. V. Ngo, and T. Q. S. Quek, "Coexistence Evaluation of Densely Deployed BLE-Based Body Area Networks," in *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*, Dec. 2017, pp. 1–6.

[26] A. Aza, D. Melendi, R. García, X. G. Pañeda, L. Pozueco, and V. Corcoba, "Bluetooth 5 performance analysis for inter-vehicular communications," *Wireless Networks*, vol. 28, no. 1, pp. 137–159, Jan. 2022. [Online]. Available: https://doi.org/10.1007/s11276-021-02830-9

[27] 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*, vol. 6, no. 2, pp. 3820–3830, Apr. 2019, conference Name: IEEE Internet of Things Journal.

[28] J. Wildman and S. Weber, "On Protocol and Physical Interference Models in Poisson Wireless Networks," *IEEE Transactions on Wireless Communications*, vol. 17, no. 2, pp. 808–821, Feb. 2018, conference Name: IEEE Transactions on Wireless Communications.

[29] W. Ejaz and A. Anpalagan, "Communication Technologies and Protocols for Internet of Things," in *Internet of Things for Smart Cities: Technologies, Big Data and Security*, ser. SpringerBriefs in Electrical and Computer Engineering, W. Ejaz and A. Anpalagan, Eds. Cham: Springer International Publishing, 2019, pp. 17–30. [Online]. Available: https://doi.org/10.1007/978-3-319-95037-2_2

[30] J. Tosi, F. Taffoni, M. Santacatterina, R. Sannino, and D. Formica, "Performance Evaluation of Bluetooth Low Energy: A Systematic Review," *Sensors*, vol. 17, no. 12, p. 2898, Dec. 2017, number: 12 Publisher: Multidisciplinary Digital Publishing Institute. [Online]. Available: https://www.mdpi.com/1424-8220/17/12/2898

[31] "Signal-to-noise ratio," Oct. 2021, page Version ID: 1052575963. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Signal-to-noise_ratio&oldid=1052575963

[32] S. M. Ross, *Introduction to Probability Models*. Academic Press, Mar. 2019, google-Books-ID: wGOMDwAAQBAJ.

[33] "Bit error rate," Jul. 2021, page Version ID: 1035589793. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Bit_error_rate&oldid=1035589793

[34] H. Kavousi Ghafi, C. Spindelberger, and H. Arthaber, "Modeling of co-channel interference in bluetooth low energy based on measurement data," *EURASIP Journal on Wireless Communications and Networking*, vol. 2021, no. 1, p. 143, Jul. 2021. [Online]. Available: https://doi.org/10.1186/s13638-021-02005-2

[35] M. R. Manesh, Y. Arjoune, and N. Kaabouch, "A bit error rate estimation method for wireless communication systems," in *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)*, Jan. 2018, pp. 835–840.

[36] "nRF52840 DK." [Online]. Available: https://www.nordicsemi.com/Software-and-tools/Development-Kits/nRF52840-DK

[37] "Zephyr Project - Zephyr Project." [Online]. Available: https://zephyrproject.org/

[38] E. Lattanzi and V. Freschi, "In-Band Controllable Radio Interference Generation for Wireless Sensor Networks," *IEEE Access*, vol. 7, pp. 66 955–66 963, 2019, conference Name: IEEE Access.

[39] E. Lattanzi, P. Capellacci, and V. Freschi, "Experimental evaluation of the impact of packet length on wireless sensor networks subject to interference," *Computer Networks*, vol. 167, p. 106986, Feb. 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128619303755

[40] S. M. Ross, *Introduction to Probability and Statistics for Engineers and Scientists*. Academic Press, Sep. 2020, google-Books-ID: eW_hDwAAQBAJ.

[41] E. Park, M.-S. Lee, H.-S. Kim, and S. Bahk, "AdaptaBLE: Adaptive control of data rate, transmission power, and connection interval in bluetooth low energy," *Computer Networks*, vol. 181, p. 107520, Nov. 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128620311816

Bozheng Pang Bozheng Pang was born in 1995. He graduated from China University of Mining and Technology in 2017, receiving his Bachelor's degree in Mechatronics Engineering. Later, in 2018, he earned his Master's degree in Smart Product Design from Nanyang Technological University. Since his graduation, he has been pursuing a PhD at KU Leuven, Brugge Campus. His current research interests include reliable wireless communication, coexistence of wireless communications, and wireless communication modeling.

Tim Claeys Tim Claeys was born in 1990. He received the M.S. degree in industrial engineering sciences, option electronics, from the University College Katholieke Hogeschool Sint-Lieven Gent, Ghent, Belgium, in 2013, and the Ph.D. degree in electrical engineering from Katholieke Universiteit (KU) Leuven, Leuven, Belgium, in 2018. Since 2018, he has been a Postdoctoral Researcher with the M-Group Research Group (Lab FMEC), KU Leuven, Bruges, Belgium. His current research interests include near-field scanning, the development of characterization methods for shielding materials and gaskets, electromagnetic interference resilience of wireless communications, and global reliability of electronic systems. Currently he is a visiting researcher at the TELICE-IEMN group at the University of Lille. He is an IEEE member and part of the IEEE EMC Society Benelux chapter executive committee.

Jens Vankeirsbilck Jens Vankeirsbilck (Member, IEEE) was born in 1992. He received the M.S. degree in engineering technology, ICT, from Katholieke Universiteit (KU) Leuven, Technology Campus Ostend, Belgium, in 2014; and the PhD degree in engineering technology, computer science from KU Leuven, Leuven, Belgium, in January 2020. Since 2020, he has been a Postdoctoral Researcher with KU Leuven, being a part of the M-Group Research Group, which is a research group focusing on global dependability of mechatronic systems. His research interests include resilient embedded systems, soft errors, functional safety, fault injection techniques and tools, and software updates in safety-critical applications.

Kristof T'Jonck Kristof T'Jonck graduated from VIVES in 2016, receiving his Bachelor's degree in Information and Communication Technology. Later, in 2018, he also earned his Master's degree in Electronics and ICT Engineering Technology from KU Leuven. Since his graduation, he has been pursuing a PhD at KU Leuven. His main interests are sensor networks, and their applications, and his current research specifically focuses on the integration of Bluetooth Low Energy sensors in healthcare environments, such as hospitals and care homes.

Hans Hallez Hans Hallez (Member, IEEE) obtained his master's degree in Computer Science at Ghent University in 2003. He then became a PhD student at the Faculty of Engineering and Architecture at the Ghent University and obtained his PhD in Engineering Science in 2008. From 2008 to 2011, he was a Postdoctoral Fellow at the Ghent University. Since 2011 he is active at the Bruges campus at KU Leuven as a lecturer and in 2014 he became a staff member of the faculty of Engineering Technology within the KU Leuven department of Computer Science. In 2020 he became Associate Professor at the Bruges Campus of KU Leuven. Hans Hallez is a member of the M-Group research group and the imec.Distrinet research group and focusses on edge computing of machine learning within the application of sensors and sensor networks for industrial manufacturing machines and healthcare. He is also principal instructor of several bachelor's and master's courses at the faculty of Engineering Technology.

Jeroen Boydens Jeroen Boydens (Member, IEEE) received his first M.Sc. in 1988 from KIHWV - now part of KU Leuven(BE), and his second M.Sc. in computer science in 1989 from VUB(BE), and a Ph.D. in Engineering Science from KU Leuven in 2008 in the DistriNet research group. He is currently an Associate Professor KU Leuven(BE), and a visiting Professor at UNILIM(FR). In 2007, he started his research group on embedded software engineering in close cooperation with industry. Embedded software and techniques to recover from bitflips are his active research fields. He leads a team of doctoral researchers in his spearhead domains: software resilience in embedded software, functional safety and software engineering.