2022 Workshop on Benchmarking Cyber-Physical Systems and Internet of Things (CPS-IoTBench) | 978-1-6654-7038-4/22/$31.00 ©2022 IEEE | DOI: 10.1109/CPS-IoTBench56135.2022.00012

On the Performance of IEEE 802.15.4z-Compliant Ultra-Wideband Devices

Michael Stocker, Hannah Brunner, Maximilian Schuh, Carlo Alberto Boano, and Kay Römer
Institute of Technical Informatics, Graz University of Technology, Austria
E-Mail: {michael.stocker, hannah.brunner, schuh, cboano, roemer}@tugraz.at

***Abstract*—Since the introduction of the IEEE 802.15.4z standard, several new-generation ultra-wideband platforms have been marketed, such as the Apple U1, the NXP Trimension, and the Qorvo DW3000. However, in the last decade, most of the experimental research focusing on communication performance has been carried out on the old Decawave DW1000 platform, which follows the IEEE 802.15.4a specifications and does not offer the security enhancements introduced by the latest standard. In this paper, we perform the first in-depth experimental study on the communication performance of an IEEE 802.15.4z-compliant platform based on the Qorvo DW3000. Among others, we explore the impact of various physical layer settings and security features, and further analyze the reliability of packet transmissions as well as the success probability of secure ToA estimations in absence and in presence of Wi-Fi 6E traffic.**

***Index Terms*—IEEE 802.15.4z, Interference, IoT, Performance evaluation, Qorvo DW3000, Reliability, UWB, ToA estimation, Wi-Fi 6E.**

I. Introduction

Ultra-wideband (UWB) technology offers outstanding time resolution and multi-path resilience compared to traditional narrow-band IoT technologies, and has thus emerged as one of the most popular choices for indoor positioning and tracking. The ability to achieve centimetre-level localization accuracy allows to support a wide range of different applications (e.g., asset tracking, robot navigation, or assisted living), and has encouraged big players such as Apple, Samsung, BMW, and VW to integrate UWB transceivers into their newest smartphones [1] and vehicles [2], respectively.

Given the increasing ubiquity of UWB-based systems and their use in safety-critical application domains such as secure access and smart manufacturing, there is an increasing need for both secure and robust solutions. In fact, several of the UWB prototypes developed in the past decade suffer from poor performance in the presence of NLOS conditions [3], [4] and are vulnerable to attacks causing an artificial distance reduction or enlargement [5], [6]: this is a major problem for UWB-based systems relying on correct distance estimates.

IEEE 802.15.4z for secure and robust UWB systems. To address these concerns and meet the requirements of safety-critical applications, several enhancements have been incorporated into the existing UWB standard and recently published as IEEE 802.15.4z amendment [7]–[9]. This new standard includes improvements in the medium access control (MAC) layer, the support of new physical layer (PHY) settings to decrease time-on-air, as well as the optional insertion of a cryptographically-generated *scrambled timestamp sequence* (STS) into the UWB frame [10]. The latter can be used to generate a channel impulse response (CIR) estimate by correlating known pulse patterns. The CIR estimate is crucial for the ranging performance, as it is required to precisely determine the arrival time of a packet. Thanks to its pseudo-random properties, the STS can only be processed by trusted receivers and transmitters (i.e., those knowing a shared secret) and can thus help to secure the reception timestamp against both accidental or intentional (malicious) interference.

Performance of new-generation UWB platforms still unexplored. The introduction of IEEE 802.15.4z has led to the emergence of a large number of new-generation UWB platforms, including Apple's U1, NXP's Trimension, and Qorvo's DW3000 [11]. These platforms offer enhanced PHY settings compared to previous UWB radios, as well as improved transceiver designs to ensure robust and low-power operation. So far, experimental research on UWB has mainly been performed on older platforms based on the IEEE 802.15.4a standard, such as the Decawave DW1000 [12], and it is not known whether new-generation devices adhere to the same trends.

Understanding IEEE 802.15.4z enhancements. Platforms compliant to the IEEE 802.15.4z standard offer several new PHY settings, e.g., additional pulse repetition frequencies, security configurations, as well as different frame formats. For example, the STS can be inserted in different frame positions [7], [8], and its length can be varied between 32 and 2048 symbols on Qorvo's DW3000 chip. Previous work focusing on IEEE 802.15.4a-compliant platforms has shown that PHY settings have a strong impact on communication performance [13], [14]. However, whether and how IEEE 802.15.4z-specific PHY settings affect UWB communications has not been characterized yet, and is hence an important gap to be filled.

Understanding the impact of Wi-Fi 6E interference. The recent opening of the 6 GHz band has raised major concerns in the UWB community, as Wi-Fi 6E is now allowed to operate in the same spectrum [15]. First studies investigating the impact of Wi-Fi 6E interference on UWB systems based on Decawave's DW1000 chip could indeed confirm that both communication and ranging performance can be degraded severely [16]. Several IEEE 802.15.4z features, including the introduction of the STS, are intended to increase the robustness and security of UWB communications, but whether they are effective in the presence of Wi-Fi 6E traffic has not been investigated yet. It is hence of interest to fill this gap and investigate the performance of IEEE 802.15.4z platforms under cross-technology interference.

Contributions. In this paper, we perform an empirical study on the communication performance of an IEEE 802.15.4z-compliant UWB radio, namely the Qorvo DW3000. First, we explore the impact of different PHY settings on link reliability, confirming the trends observed on IEEE 802.15.4a hardware [13]. We then investigate whether and how IEEE 802.15.4z-specific PHY settings, such as the STS configuration, affect the reliability with which UWB packets are received as well as the success probability of secure ToA estimations. Finally, we evaluate the performance of the DW3000 in the presence of Wi-Fi 6E interference as a function of different PHY settings and STS configurations. Among others, our experiments show that: (i) fine-tuning PHY settings such as the preamble acquisition chunk size has a significant impact on the receiver sensitivity; (ii) secure ToA estimations can fail even in absence of cross-technology interference; (iii) Wi-Fi 6E interference has a detrimental effect on UWB performance; (iv) longer scrambled time sequences and specific frame configurations negatively affect both packet reception and secure ToA estimation in the presence of Wi-Fi 6E traffic.

Paper outline. This paper proceeds as follows. Sec. II gives a background on the IEEE 802.15.4a standard and its latest amendment, IEEE 802.15.4z. Sec. III describes the employed UWB chip, the Qorvo DW3000, as well as the experimental setup used in our study. Sec. IV presents a detailed analysis of our experimental results. Sec. V concludes the paper along with a discussion on future work.

978-1-6654-7038-4/22/$31.00 ©2022 IEEE
DOI 10.1109/CPS-IoTBench56135.2022.00012

II. UWB Technology: From IEEE 802.15.4a to 802.15.4z

Impulse Radio Ultra-Wideband (IR-UWB) technology utilizes a large bandwidth ($\geq$ 500 MHz) allowing for ns-scale pulses. Thanks to this large bandwidth, UWB offers a high resilience to multipath fading and an outstanding time resolution that allows to precisely estimate a signal's time-of-arrival (ToA): this makes UWB especially popular for the development of location-based systems.

A. Ultra-Wideband (IEEE 802.15.4a – HRP)

In 2007, the IEEE 802.15.4a task group [17] finalized a first standard for UWB systems based on the HRP (high rate pulse) PHY.

Frame structure and PHY settings. An IEEE 802.15.4a-compliant UWB frame is split into a *synchronization header* (SHR) and a *data portion (DP)*, as shown in Fig. 1. The SHR is sent using single pulse modulation, i.e., it consists of single 2-ns long pulses representing +1, 0, or -1. These pulses are combined according to pre-defined *preamble codes* and form roughly 1µs-long preamble symbols. The length of the preamble code determines the rate at which pulses are sent, typically referred to as *pulse repetition frequency* (PRF). The IEEE 802.15.4a standard defines PRF values of 16 and 64 MHz. The preamble symbols are repeatedly sent to constitute the preamble field in the SHR. Its length is determined by the number of *preamble symbol repetitions* (PSR), which can amount to 16, 64, 1024, or 4096. The end of the SHR is marked by the *start of frame delimiter* (SFD). The SFD also consists of preamble symbols, but breaks the symbol pattern to indicate the start of the data portion. The latter is sent using burst position modulation and binary phase-shift keying (BPM/BPSK), and makes use of error correction codes to enhance reliability. The *physical header* (PHR) contains information about the data rate (DR) and length of the *payload* field, which can be sent using a DR of either 110 kbps, 850 kbps, 6.8 Mbps, or 27.2 Mbps.

ToA estimation. The SHR is not only used for signal detection and synchronization, but also to derive a channel impulse response (CIR) using cross-correlation of the received signal with a known preamble sequence. The CIR allows to precisely estimate the ToA by identifying the first path component and is thus crucial for achieving an accurate ranging [18]. Previous work has shown that the CIR is prone to accidental or malicious manipulation [5], [6], [14]. In fact, the injection of signals within the SHR can lead to an altered ToA and, consequently, to a (largely) inaccurate distance estimation.

B. Enhanced Ultra-Wideband (IEEE 802.15.4z – HRP)

In order to tackle the security concerns in IEEE 802.15.4a systems, several improvements have been developed to enhance the standard. These have been released as IEEE 802.15.4z amendment in 2020 and include, among others, the introduction of higher pulse repetition frequencies (HPRF) to decrease time-on-air and energy consumption, as well as new MAC layer options [19]. Furthermore, the IEEE 802.15.4z amendment foresees a base pulse repetition frequency (BPRF) mode operating at a PRF of 64 MHz.

The most noteworthy novel feature w.r.t. to security is the introduction of the *scrambled timestamp sequence* (STS), which enables a *secure* ToA estimation. Similar to the symbols in the preamble field and as shown in Fig. 2, the STS segment contains several STS symbols. While the sequence of pulses in the preamble is predefined and static, it is pseudo-random in the STS, based on a shared secret between sender and receiver. This enables the receiver to create a CIR estimate by cross-correlating the received STS signal with a local template version, and allows to determine the authenticity of ToA estimates: a CIR estimate is only considered legitimate, if the correlation value is above a certain threshold, i.e., if sender and receiver use the same valid sequence [20].

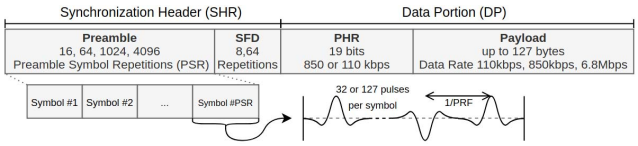

Fig. 1: **Frame structure of an IEEE 802.15.4a-compliant packet.** An UWB frame consists of a synchronization header (SHR), used for packet detection, and a data portion, containing the payload.

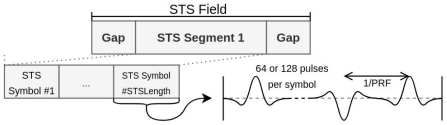

Fig. 2: **Structure of the STS field.** One STS segment is built out of many STS symbols. Each STS symbol is made from 64 or 128 pulses, with polarity determined by a deterministic random number generator.

Fig. 3: **IEEE 802.15.4z-compliant frame configurations.** SP0 does not contain an STS; SP1 and SP2 embed an STS before and after the DP, respectively; SP3 embeds an STS, but no DP.

Frame structure and STS settings. In order to integrate the STS in an UWB packet, the IEEE 802.15.4z defines different *packet configurations* (`SP0` to `SP3`), indicating the STS position within the frame. As depicted in Fig. 3, the STS can be either omitted (SP0), inserted after the SFD (SP1), or appended to the frame after the payload section (SP2). The SP3 configuration allows to reduce the airtime during ranging: it omits the data portion and the STS is sent directly after the SHR. Since our focus is on communication and not on ranging, we do not investigate the SP3 configuration in this work. Fig. 2 illustrates the STS field, consisting of an active STS segment embedded between gaps (of ≈1µs). The STS segment is built similar to the preamble and consists of ≈1µs long STS symbols that are repeatedly transmitted depending on the *STS length*. Devices compliant to IEEE 802.15.4z in base pulse repetition frequency (BPRF) mode must support an STS length of 64 symbols and have to use a PRF of 64 MHz to create STS symbols[1]. The pulse sequence of STS symbols is pseudo-randomly generated using an `AES-128` based deterministic random bit generator (DRBG). Sender and receiver have to share a 128-bit long secret *STS key* to be able to correctly generate the sequence and to create a valid ToA estimate.

Verifying the authenticity of the ToA estimate. Recently two publications hypothesized [20] and demonstrated [21] that STS-based secure ToA estimation is vulnerable to distance reduction. Specifically, malicious pulses sent within the STS segment can manifest as peaks in the CIR estimate; consequently, the ToA estimation results are incorrect. These works highlight the need for additional integrity checks on received UWB frames to ensure high-quality ToA estimates. In that regard, the standard does not specify any mandatory steps for integrity verification: thus, manufacturers are responsible for implementing sufficient ToA verification methods.

[1] IEEE 802.15.4z defines also a higher pulse repetition frequency (HPRF) mode, mandating a PRF of 128 MHz and offering the optional transmission of four consecutive STS segments. The DW3000 only supports the BPRF mode.

III. Employed Hardware and Experimental Setup

We investigate the performance of IEEE 802.15.4z-compliant devices by focusing on Qorvo's DW3000 chip, due to its off-the-shelf availability, as well as its extensive software support and documentation [22]. After highlighting the DW3000 features and available PHY settings (Sec. III-A), we describe how we have integrated this platform in our experimental testbed infrastructure so to systematically analyze its communication performance (Sec. III-B).

A. Qorvo DW3000 Transceiver

The DW3000 is Qorvo's new-generation UWB radio and implements the IEEE 802.15.4a standard along with the BPRF mode of the IEEE 802.15.z amendment. It is a fully integrated UWB solution and can operate on UWB channels 5 and 9.

PHY settings. The DW3000 supports a large number of different PHY configurations that allow to fine-tune the transceiver's performance and are summarized in Table I. As described in Sec. II, the UWB standard defines two PRFs and four data rates. While the DW3000 supports both PRFs (i.e., of 16 and 64 MHz), it offers only data rates of 850 kbps and 6.8 Mbps, respectively. In contrast, it allows to choose additional PSR values that are not mandated by the standard, ranging from 32 up to 4096 symbols. The DW3000 further allows to tune the *preamble acquisition chunk* (PAC), which specifies the number of preamble symbols (4, 8, or 16) that are combined to chunks during the cross-correlation process. A higher PAC size should result in a better performance, provided that the preamble is sufficiently long to accumulate enough chunks. The PAC configuration should thus be selected as a function of the employed PSR value [22]. Moreover, the DW3000 supports different SFD patterns and transmission power settings. We use a 8 symbol long standard SFD pattern as defined in IEEE 802.15.4z and set the `TX_POWER` control register to the recommended value of `0xfdfdfdfd`.

STS support. One of the key features of the DW3000 is its ability of secure timestamping using an STS. In compliance with the IEEE 802.15.4z standard, the DW3000 supports the four different frame configurations shown in Fig. 3 and embeds an `AES-128` DRBG unit to generate the required random keys. The STS length can be selected between 32 and 2048 symbols and is programmable in steps of power of two. When receiving a packet including an STS, the DW3000 generates two CIR and ToA estimates (one from the preamble and one from the STS), and checks their consistency using several statistical tests, so to verify the integrity of the ToA estimate. The results of these tests are available in the ToA status indicator (`TOAST`) register. In addition, the DW3000 provides a register to indicate the quality of the STS accumulation (`ACC_QUAL`). The latter contains a unit-less value summarizing the result of an algorithm assessing the STS quality, and should correlate with the number of transmitted STS symbols. Upon message reception, users need to check both registers to ensure that the ToA can be trusted. According to the DW3000 user manual [22], a ToA estimate should only be trusted if the `ACC_QUAL` exceeds at least 60% of the STS length and no flags in the `TOAST` register are triggered. The DW3000 also allows to specify the type of STS: besides the randomly-generated sequence, one can also use pre-defined sequences optimized for ToA detection. The latter are called Super Deterministic Codes (SDC) and can be used when security is no concern and a high ranging accuracy is needed.

PHY Setting	Supported Values
RF channel	**5**, 9
Pulse repetition frequency	16 MHz, **64 MHz**
Preamble symbol repetitions	32, **64**, 128, 256, 512, 1024, 2048, 4096
Data rate	850 kbps, **6.8 Mbps**
Preamble acquisition chunk	4, 8, or **16**
STS packet configuration	SP0, **SP1**, SP2, SP3
STS length	32 to 2048 in steps of 8, default: **64**
Type of STS	SDC, **randomly-generated**

TABLE I: **Configurable PHY settings in the DW3000 radio**. The default configuration used in our experiments is highlighted in bold.

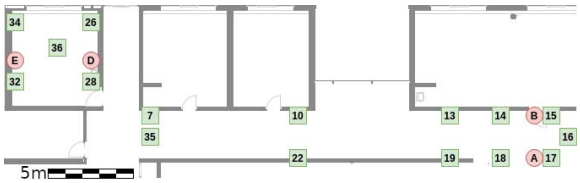

Fig. 4: **Map of devices in our testbed facility.** DW3000 nodes (green squares) and Wi-Fi 6E devices (red circles) are deployed inside an University building in an OFFICE and across an HALLWAY.

B. Testbed Facility

For all our experiments, we use a testbed facility installed at our University, which integrates 17 UWB DWM3000EVB shields based on the DW3000 radio family: these use an nRF52833-DK as a carrier board, as detailed in [23]. The UWB devices are deployed either inside a $25m^2$ office (OFFICE) or along a large corridor (HALLWAY), as illustrated in Fig. 4. The testbed further includes five Wi-Fi 6E routers that we use to generate cross-technology interference. Both Wi-Fi 6E routers and UWB nodes are connected to a dedicated infrastructure that provides power to all devices and allows remote reprogramming, collection of diagnostic data, and generation of repeatable interference patterns. Specifically, Wi-Fi 6E interference is generated by using the `iperf` tool to produce periodic UDP traffic with a fixed bitrate of 100 Mbps, resulting in an overall channel occupancy of roughly 32%. The Wi-Fi 6E routers are configured to operate on Wi-Fi 6E channel 111 (with a center frequency of 6495 MHz and 160 MHz bandwidth) at maximum transmission power. Note that this Wi-Fi channel overlaps with UWB's channel 5, which has a center frequency of 6489.6 MHz and a bandwidth of 499.2 MHz.

IV. Experimental Results

Using the testbed facility described in Sec. III-B, we investigate the communication performance of the DW3000 radio experimentally. We express the performance in terms of *header reception rate* (HRR), *packet reception rate* (PRR), and *secure ToA estimation rate* (STR). The HRR is computed as the number of packets for which the SHR was received successfully (possibly with errors in the data portion) divided by the number of transmitted packets. The PRR is the ratio between the number of successfully received and transmitted packets (i.e., no errors or corrupted bits in the data portion). The STR is computed as the number of successful ToA estimates divided by the number of transmitted packets, where a ToA estimate is deemed as successful if: (i) none of the STS integrity checks fails, i.e., the `TOAST` register is zero, and (ii) the STS quality indicator is above 90%, i.e., the `ACC_QUAL` value is higher than $0.9 \times STS\,length$.[2]

Setup validation. In a first experiment, we verify our experimental setup and let nodes 16 and 35 separately broadcast 500 messages to all other UWB nodes in the HALLWAY in absence of any Wi-Fi 6E activity. Fig. 5 confirms that all nodes can successfully communicate,

[2]While the user manual proposes a threshold of 60%, we use a more stringent value of 90% in accordance with Qorvo's default driver implementation released with SDK version 1.1.

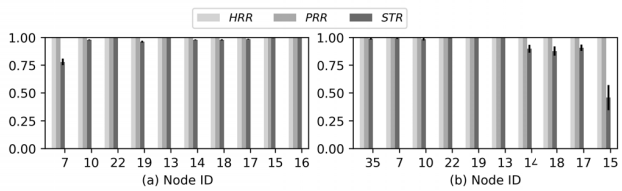

Fig. 5: **Communication performance of the DW3000 with default settings.** Performance is expressed in terms of HRR, PRR, and STR for each device in the HALLWAY when using node 35 (a) and 16 (b) as transmitter in absence of cross-technology interference.

i.e., the HRR and PRR is 100% for each node. Interestingly, however, we can observe that this is not the case for the STR: nodes in close proximity to the transmitter experience values in the order of 60–90%. We will analyze this phenomenon in more detail in Sec. IV-B.

In the remainder of this section we explore the communication performance of the DW3000 radio in different ways. First, we focus on the impact of PHY settings that were already present in IEEE 802.15.4a-compliant platforms, and verify whether the trends observed by Großwindhager et al. [13] still apply to this new-generation platform (Sec. IV-A). We then extend this analysis by studying the impact of different STS configurations (Sec. IV-B), and by investigating the performance of the DW3000 radio in the presence of Wi-Fi 6E interference using both different PHY settings and IEEE 802.15.4z-specific features (Sec. IV-C).

A. Impact of PHY Settings on Communication Performance

Großwindhager et al. [13] have shown that PHY settings largely affect the performance of IEEE 802.15.4a devices. Specifically, their experiments on the DW1000 platform have shown that especially the number of preamble symbol repetitions and the employed data rate have a profound impact on the reliability of UWB communications.

Our aim is to verify that these findings hold true for the DW3000 radio and to further investigate the impact of the PAC size on communication performance. To this end, we configure node 35 to send broadcast messages to all HALLWAY nodes. We then use the adjustable transmission power gain setting of the DW3000 [24, p. 30], [22, p. 109] to simulate attenuation within the radio channel and observe the impact of different PHY settings. Specifically, we vary the transmission power gain from -6 dB to -22 dB in 1 dB steps and send 200 packets for each configuration. Unless differently specified, we use the default settings listed in Table I. In the following, we report in the plots only the HRR and PRR of node 16 in order to keep them readable; however, please note that the very same trends were observed across all other nodes in the HALLWAY.

Impact of the PSR (preamble symbol repetition). The amount of preamble symbol repetitions affects the length of the SHR: therefore, as shown in [13], we should expect an impact on the HRR and not on the PRR. Fig. 6 shows our experimental results, which confirm our expectations: (i) the PRR is unaffected, and (ii) longer preambles result in a higher HRR at lower signal-to-noise ratios. Specifically, we observe an increase in sensitivity by roughly 4 dB when moving from a PSR of 64 to 1024, a similar delta as reported in [13]. The other nodes in our testbed exhibit a similar trend ($\approx$ 3 to 4 dB increase). Note that, although the PRR does not increase when tuning the PSR, more preamble symbols are beneficial during the ToA estimation process, as they increase the distance estimation performance [25].

Impact of the DR (data rate). The data rate affects the data portion of an UWB packet and influences the amount of transmitted pulses per symbol. As presented in [13], lower data rates help increasing

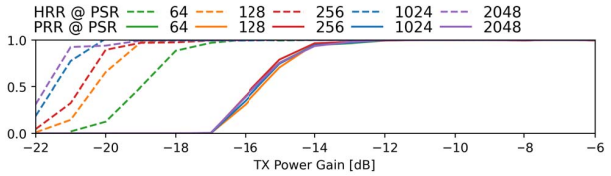

Fig. 6: **Impact of PSR on the reliability of communications.** Higher PSR values increase the reliability of the HRR, whereas the PRR is unaffected. A PAC size of 16 was used in these experiments.

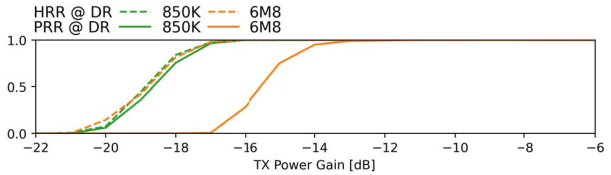

Fig. 7: **Impact of DR on the reliability of communications.** Lower data rates increase the PRR; the HRR is independent of the data rate.

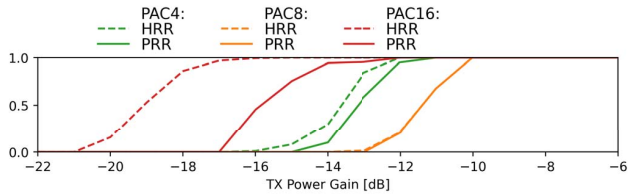

Fig. 8: **Impact of PAC size on the reliability of communications.** A PAC size of 16 leads to the highest HRR and PRR, whereas a PAC size of 8 results in the lowest receiver sensitivity.

the robustness of the data portion and, consequently, the PRR. Fig. 7 shows the communication performance as a function of different data rates in our experimental results. The latter confirms our expectations: (i) the HRR is unaffected, and (ii) when using lower data rates, there is a visible increase in the PRR also at lower signal-to-noise ratios. Specifically, we can observe an increase in the link margin by roughly 4 dB, which is in line with the observations in [13].

Impact of the PAC (preamble aqucition chunk). The size of the PAC determines the number of preamble symbols used for correlation during preamble detection: therefore, a bigger PAC should result in an increased receiver sensitivity. We analyze the HRR and PRR when using a PAC of 4, 8, and 16 symbols, respectively: Fig. 8 summarizes our experimental results. As expected, increasing the PAC size from 4 to 16 allows to increase the sensitivity of the receiver, leading to a higher HRR at lower signal-to-noise ratios (i.e., there is a difference of about 4 dB between the dashed red and dashed green lines). This increase in sensitivity results also in a better PRR when using a PAC size of 16, as the correct detection of the SHR is a prerequisite for a correct packet reception. Interestingly, we have observed that a PAC of 8 symbols leads to a lower receiver sensitivity than when using 4 symbols only: this trend – which is consistent in all our experiments – can be seen as the HRR and PRR orange curves overlap in the area between -10 and -13 dB. The overlap of the two orange lines also confirms that this PAC configuration strongly affects the preamble detection, as the PRR is limited by the HRR (indeed, a correct reception of the data portion requires a successful SHR detection).

Our experiments show that a PAC size of 16 leads to the largest difference between the HRR and PRR curves for the same configuration ($\approx$ 4 dB): such difference is significantly lower when using a PAC

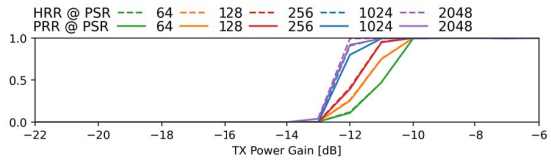

Fig. 9: **Performance as a function of the PSR on communication performance when using a PAC size of 8.** As shown in Fig. 9, a PAC size of 8 results in the lowest receiver sensitivity, and an increase in PSR does not help in increasing the reliability of communications.

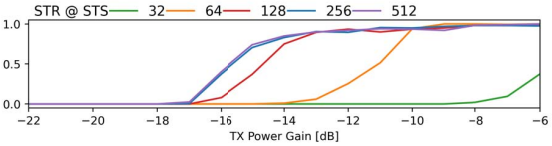

Fig. 10: **Impact of STS length on the STR.** A longer STS helps increasing the STR until the limit dictated by the PRR.

of 4 and 8 symbols ($\approx$ 1 and 0 dB, respectively). This trend can also be observed in Fig. 9, which shows the communication performance as a function of the number of PSR when using a PAC size of 8. In contrast to Fig. 6, which was obtained using a PAC size of 16, the receiver sensitivity is much lower, and the increase in HRR is not as visible. For this reason, the use of a PAC size of 16 is recommended, and we use this configuration in the remainder of Sec. IV-A.

B. Impact of the STS Configuration on Communication Performance

One of the new key features of IEEE 802.15.4z-compliant devices is secure ToA estimation. Its success rate is of great interest and requires special attention, especially since we have observed a low STR for pairs of nodes in close proximity (cf. Fig. 5). We hence investigate next the STR under low signal strength conditions and the impact of various PHY settings on its performance.

Impact of the STS length. The STS length determines the number of STS symbols sent during an STS segment. Fig. 10 shows the STR as a function of the STS length and transmission power gain between nodes 35 and 16. While increasing the STS length from 32 to 256 symbols vastly increases the STR, STS lengths beyond 256 symbols do not bring any significant benefit: this is because the STR is limited by the actual packet reception (cf. Fig. 7).

Impact of PHY settings on the STR. In Fig. 5 we have observed that the STR can decrease by up to 30% for pairs of nodes that are close to each other. This is unexpected, as close nodes experiencing high signal power should typically perform better than nodes that are far away. We observed that two bits in the `TOAST` register are causing the failure of secure TOA estimates for nodes in close proximity: the peak growth rate (PGW) check, which compares how much energy is acquired per preamble and STS symbol during accumulation, and the STS consistency check (SCC) check, checking the channel consistency during STS reception. We next analyze systematically the impact of different PHY settings on the STR for pairs of nodes that are close to each other; we summarize our results in Fig. 11, which shows the average performance of node pairs (35,7), (16,18), (16,17), and (16,15) as a function of selected PHY settings. Surprisingly, increasing the STS length does not impact the STR positively (Fig. 11 (c)) for close node pairs: we observe this negative trend also for larger STS values. The PAC size significantly impacts the STR (Fig. 11 (a)): specifically, when changing the PAC from 8 to 16 symbols, the mean STR reduces from 80% to 30%. We also observe a higher STR when increasing the PSR from 64 to 128 (Fig. 11 (b)): this

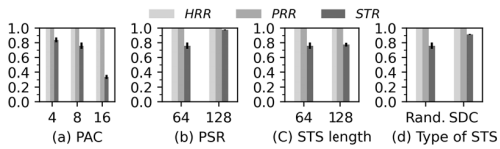

Fig. 11: **Impact of PAC, PSR, STS length, and type of STS on the STR for close node pairs.** All settings affect the STR performance.

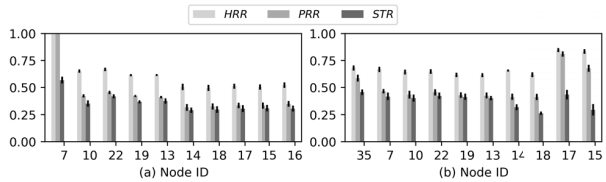

Fig. 12: **Impact of Wi-Fi 6E on communication performance.** HRR, PRR, and STR for individual nodes in the `HALLWAY` when using node 35 (a) and node 16 (b) as transmitter.

considerably helps mildening the decrease in STR at close nodes. Finally, we observe that the type of STS also has a visible impact on the STR: specifically, the use of super deterministic codes improves performance by roughly 12% (Fig. 11 (d)).

C. Impact of Wi-Fi 6E Interference on Communication Performance

The opening of the 6 GHz band to Wi-Fi 6E has raised concerns about cross-technology interference affecting UWB communication performance, which has been empirically confirmed by recent work [16] on the DW1000 platform. We investigate next whether and how Wi-Fi 6E traffic affects the HRR, PRR, and STR on the DW3000 as a function of different PHY settings and STS configurations.

Fig. 12 shows how all nodes in the `HALLWAY` are strongly affected by Wi-Fi 6E traffic when using the default settings listed in Table I. First, we observe that, when node 35 is used as transmitter (Fig. 12 (a)), the HRR and PRR decrease with increasing distance: this is expected, as the signal to interference ratio (SIR) is reduced. Second, nodes close to the transmitting node have a high HRR and PRR even in proximity of the Wi-Fi 6E routers (cf. nodes 15 and 17 in Fig. 12 (b)): this hints that even under interference, a correct packet reception is possible when the SIR is sufficiently high. This is in contrast to the observations made in [16], where a correct packet reception was not possible even for close nodes with the DW1000. Third, the STR remains below 50% for all nodes regardless of their distance from the Wi-Fi 6E routers. For far nodes, this is due to the low PRR, whereas for close nodes it is due to the observations made in Fig. 5 and thus the difference between PRR and STR is higher. This suggests that Wi-Fi 6E interference hinders some integrity checks to pass.

Impact of the PSR (preamble symbol repetitions). Brunner et al. [16] observe two opposing effects when using more preamble symbols. On the one hand, a higher PSR increases the chances to recover from a Wi-Fi 6E hit. At the same time, more preamble symbols raise the chances of multiple Wi-Fi 6E hits, hindering the DW1000 from receiving the rest of the packet correctly under some circumstances (e.g., by wrongly identifying a Wi-Fi 6E packet as SFD). Fig. 13 shows the average impact of Wi-Fi 6E interference on all nodes in the testbed for different transmitters. While the HRR increases when using a higher PSR value, the same does not hold true for the PRR. In fact, a PSR of 256 seems to lead to the highest PRR, confirming the trade-off observed in [16]; in addition, we note that also a PSR of 2048 leads to a higher PRR than the one obtained with a PSR of 512 and 1024. The STR follows the same trend as the PRR.

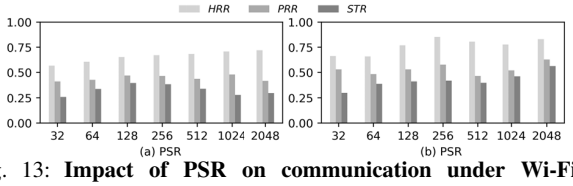

Fig. 13: **Impact of PSR on communication under Wi-Fi 6E interference.** Average HRR, PRR, and STR for HALLWAY nodes when using node 35 (a) and node 16 (b) as transmitter.

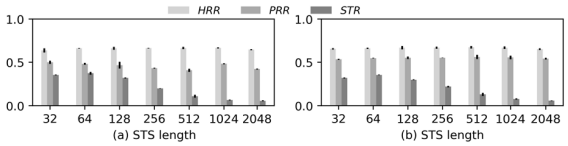

Fig. 14: **Impact of STS length and frame format on communication under Wi-Fi 6E interference in HALLWAY.** Short STS lengths increase the STR; the use of the SP2 frame format increases the PRR.

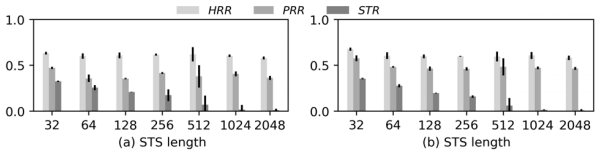

Fig. 15: **Impact of STS length and frame format on communication under Wi-Fi 6E interference in OFFICE.** Short STS lengths increase the STR; the use of the SP2 frame format increases the PRR.

Impact of STS length and frame configuration. We finally investigate whether specific STS lengths and the use of specific frame formats help mitigating the impact of Wi-Fi 6E traffic. We carry out experiments on both HALLWAY and OFFICE: the latter emulates a very harsh scenario, as the Wi-Fi devices are located inside the room where UWB nodes are deployed. Figs. 14 (HALLWAY) and 15 (OFFICE) illustrate our results by showing the average performance of all nodes. In HALLWAY, we select nodes 16 and 35 as transmitters in separate runs, whereas node 36 is the transmitter in OFFICE. First, we can observe that the HRR stays constant for different STS lengths, but that the STR drastically decreases when using a long STS. Specifically, the STR decreases by $\approx 60\%$ when increasing the STS length from 32 to 2048 symbols. This is expected, as a longer STS is more likely to be hit by a Wi-Fi 6E packet. Second, we notice that using the SP2 frame format leads to a higher PRR independently of the employed STS length. The reason for this lies in the position of the STS within the frame: by inserting the STS in between the SHR and the data portion as in the SP1 format, we increase the probability that Wi-Fi traffic will hit the UWB frame, compromising its successful reception. When using the SP2 format, instead, Wi-Fi 6E traffic hitting the end of the frame (i.e., the STS) will still lead to a successful packet reception. Third, we do not observe any relevant difference in the HRR and STR performance as a function of the frame format. Finally, when comparing the performance of the nodes deployed in HALLWAY and OFFICE, we observe identical trends, but the average HRR, PRR, and STR in OFFICE is 5.5%, 6.4%, and 5.6% lower than that in HALLWAY when using the SP2 format: this is expected, given the closer proximity of the UWB nodes to the Wi-Fi 6E devices.

V. Conclusions and Future Work

In this work, we experimentally analyzed the communication performance of the Qorvo DW3000, one of the IEEE 802.15.4z-compliant new-generation UWB transceivers. First, we explored the impact that different PHY settings have on link reliability. We did this by first confirming the observations made using the DW1000 by Großwindhager et al. [13], and by then investigating additional PHY settings, such as the PAC and various STS configurations. Second, we investigated the success ratio of secure ToA estimates, showing that it is also strongly dependent on the employed PHY settings. Finally, we investigated the communication performance in the presence of Wi-Fi 6E interference and observed large disruptions in the connectivity, but identified the use of short STS lengths and SP2 frame formats as beneficial to mitigate the impact of Wi-Fi traffic. In the future, we aim to investigate the impact of PHY settings and Wi-Fi 6E interference also on UWB's ranging accuracy and precision.

Acknowledgements. The authors would like to thank Markus Schuß and Florian Dietrich for their support during the setup and maintenance of the testbed. This work was supported by the TU Graz LEAD project "Dependable Internet of Things in Adverse Environments".

References

[1] Wired, "The Biggest iPhone News Is a Tiny New Chip Inside It," 2019. [Online] https://bit.ly/3B9B6VK – Last access: 2022-02-10.
[2] EETimes, "VW and NXP Show First Car Using UWB To Combat Relay Theft," 2019. [Online] https://bit.ly/3oyFHfh – Last access: 2022-02-10.
[3] M. Stocker *et al.*, "Performance of Support Vector Regression in Correcting UWB Ranging Measurements under LOS/NLOS Conditions," in *Proc. of the 4th CPS-IoTBench Workshop*, 2021.
[4] S. Maranò *et al.*, "NLOS Identification and Mitigation for Localization Based on UWB Experimental Data," *J-SAC*, vol. 28, no. 7, 2010.
[5] M. Poturalski *et al.*, "The Cicada Attack: Degradation and Denial of Service in IR Ranging," in *Proc. of the ICUWB Conf.*, vol. 2, 2010.
[6] M. Singh *et al.*, "UWB-ED: Distance Enlargement Attack Detection in Ultra-Wideband," in *Proc. of the 28th USENIX Security Symp.*, 2019.
[7] IEEE 802.11 WG, "IEEE Std. for Information Technology, Part 802.11-2020: Wireless LAN MAC and PHY Specifications," 2021.
[8] D. Coppens *et al.*, "An Overview of Ultra-WideBand (UWB) Standards (IEEE 802.15.4, FiRa, Apple): Interoperability Aspects and Future Research Directions," *CORR – arXiv preprint 2202.02190*, 2022.
[9] M. Stocker *et al.*, "Towards Secure and Scalable UWB-based Positioning Systems," in *Proc. of the 17th MASS Conf.*, 2020.
[10] P. Sedlacek *et al.*, "An Overview of the IEEE 802.15.4z Standard and its Comparison to the Existing UWB Standards," in *Proc. of the 29th RadioElektronika Conf.*, 2019.
[11] Qorvo, "DW3000 Datasheet, version 1.1," 2019.
[12] Decawave, "DW1000 Datasheet, version 2.09," 2015.
[13] B. Großwindhager *et al.*, "Enabling Runtime Adaptation of Physical Layer Settings for Dependable UWB Communications," in *Proc. of the 19th WoWMoM Symp.*, 2018.
[14] D. Vecchia *et al.*, "Playing with Fire: Exploring Concurrent Transmissions in UWB Radios," in *Proc. of the 16th SECON Conf.*, 2019.
[15] UWB Alliance, "Notice of Inquiry on Expanding Flexible Use in Mid-Band Spectrum Between 3.7 and 24 GHz," Oct. 2018. [Online] https://bit.ly/3JfkgYt – Last access: 2022-02-10.
[16] H. Brunner *et al.*, "Understanding and Mitigating the Impact of Wi-Fi 6E Interference on Ultra-Wideband Communications and Ranging," in *Proc. of the IPSN Conf.*, 2022.
[17] IEEE 802.15.4 WG, "IEEE Std. for Information technology – Local and Metropolitan Area Networks, Part 802.15.4a-2007," 2007.
[18] Decawave, "APS006 – DW1000 Metrics for Estimation of Non Line Of Sight Operating Conditions, version 1.1," 2016.
[19] IEEE 802.15.4 WG, "IEEE Std. for Low-Rate Wireless Networks, Part 802.15.4z-2020: Enhanced UWB PHYs and Ranging Techniques," 2020.
[20] M. Singh *et al.*, "Security Analysis of IEEE 802.15.4z/HRP UWB Time-of-Flight Distance Measurement," in *Proc. of the 14th WiSec Conf.*, 2021.
[21] P. Leu *et al.*, "Ghost Peak: Practical Distance Reduction Attacks Against HRP UWB Ranging," in *Proc. of the IROS Conf.*, IEEE / RSJ, 2021.
[22] Qorvo, "DW3000 User Manual, version 1.1," 2019.
[23] M. Schuh *et al.*, "First Steps in Benchmarking the Performance of Heterogeneous Ultra-Wideband Platforms," in *Proc. of the 5th CPS-IoTBench Worksh.*, 2022.
[24] Qorvo, "DW3000 Device Driver Application Programming Interface Guide, version 1.4," 2019.
[25] H. Mohammadmoradi *et al.*, "UWB PHY Adaptation for Best Ranging Perform. within Appl. Constraints," in *Proc. of the ICSDE Conf.*, 2018.