# Towards Secure **and** Scalable UWB-based Positioning Systems

Michael Stocker, Bernhard Großwindhager, Carlo Alberto Boano, and Kay Römer
Institute of Technical Informatics, Graz University of Technology, Austria
{michael.stocker,grosswindhager,cboano,roemer}@tugraz.at

***Abstract*—Positioning systems based on ultra-wideband (UWB) technology are becoming ubiquitous and enable a plethora of attractive Internet of Things applications, ranging from smart access and asset tracking to the navigation of autonomous vehicles. As these positioning systems are often deployed over large areas, the focus of UWB-based research has recently shifted to the development of *scalable* solutions that can offer a high positioning accuracy for countless tags while maximizing energy-efficiency. At the same time, as positioning systems are increasingly used in safety-critical settings, several academic efforts and the standardization activities of the IEEE 802.15.4*z* working group have laid the foundations for a *secure* distance estimation using UWB technology. Unfortunately, these two endeavours have followed independent tracks that do *not* blend together. In this paper, we highlight this issue and describe the challenge of securing modern UWB-based positioning systems that are designed with scalability in mind. We first illustrate how the use of unidirectional communications, the need for synchronized anchors, and the use of quasi-simultaneous responses, which are common features of recent scalable UWB systems based on time-difference-of-arrival, make these solutions vulnerable to several attacks, despite the use of IEEE 802.15.4*z*. After carrying out a security analysis and describing how scalable UWB systems are exposed to several attacks, we devise a number of design concepts to counteract the identified attacks and secure these systems.**

## I. Introduction

Ultra-wideband (UWB) technology has recently emerged as one of the most promising RF technologies for indoor positioning and tracking [1]. Thanks to its outstanding time resolution and multipath resilience, indeed, UWB radios enable the creation of real-time location systems (RTLS) that can achieve centimetre-level positioning accuracy while still being highly energy-efficient. These systems allow to support, for example, drone and robot navigation [2], asset tracking [3], [4], smart manufacturing [5], and several other Internet of Things (IoT) applications [6]. In such RTLS, the position (i.e., the 2D or 3D coordinates) of mobile devices (*tags*) is commonly derived by communicating with multiple stationary reference nodes (*anchors*). The latter form a location infrastructure supporting the collection of position-related information, such as the coordinates of the anchors, the geometry of the environment (e.g., the floor plan [7]), as well as the distance between the various devices.

The growing demand for RTLS and their potential market size have drastically increased the ubiquity and commercial penetration of UWB systems: the latest-generation of smartphones and vehicles are now equipped with UWB transceivers [8], [9], and a plethora of companies as well as spin-offs [10], [11] have started to offer a large amount of UWB-based location services to their users.

**Need for secure UWB-based positioning systems.** As these location services often target safety-critical settings (e.g., production floors [3], [4]) and applications (e.g., smart access [12]), it becomes important to design *secure* UWB-based positioning systems that provide trustable distance and position information. Such secure positioning systems should essentially satisfy four key properties:

- Position-related information shall only come from legitimate anchors belonging to the location infrastructure and/or from authenticated tags (*authenticity*).
- Such information, which will be used to compute the position of a device, shall not be manipulated neither on a data content level nor on a signal level (*integrity*) [13].
- The computed position of a device shall be kept secret to unauthorized entities (*confidentiality*).
- The presence and identity of a device shall not be detectable by undesired nearby devices (*privacy*).

Recent standardization efforts, such as the ones of the IEEE 802.15.4*z* task group [14], have focused on increasing the security of UWB-based systems, proposing, for example, physical-layer enhancements and changes to the medium access control layer allowing for an improved authentication of ranging measurements. Recent academic works have also analyzed how to detect attacks on integrity (which would result in an enlargement or reduction of the estimated distances [15]), and proposed possible mitigations [16], [17]; mostly in the context of location systems based on two-way ranging (TWR).

**Need for scalable UWB-based positioning systems.** As RTLS are expected to be deployed over large areas and to support a large number of tags with minimal delays, there is also an increasing demand for *scalable* UWB-based positioning systems. To this end, the community has relentlessly worked on solutions supporting high tag densities [18] and update rates [19], [20], on reducing the number of exchanged messages [21], [22], as well as on minimizing deployment efforts and costs [7] – all while preserving an adequate positioning accuracy and precision. A clear trend in this regard is the growing adoption of solutions based on time-difference-of-arrival (TDoA), i.e., exploiting the difference in the arrival time of a signal at two reference points [19], [20], [23]–[26]. These approaches allow to address the scalability and energy issues of classical RTLS based on TWR [18]. Another noticeable trend is the increasing popularity of quasi-simultaneous responses [19]–[22], which allow to receive position-related information from multiple devices within a single message, hence minimizing both delays and energy consumption.

**The gap to fill.** So far, research on secure UWB-based positioning systems and the standardization activities of the IEEE 802.15.4*z* working group have mostly focused on TWR, i.e., on the *bidirectional* distance estimation between a pair of devices. Unfortunately, this clashes with the increasing number of UWB-based positioning systems moving away from TWR in favour of more *scalable* approaches based on TDoA and quasi-simultaneous responses. Securing such scalable RTLS entails *a different set of challenges* compared to securing the ranging between two nodes. Scalable UWB-based systems are often characterized by the communication to *multiple devices at once*: in order to do this, several devices share the same secret, which is a potential attack vector Similarly, in TDoA systems, communication is often *unidirectional*, as opposed to the bidirectional data exchange in TWR systems: this has important implications on the ability to detect and prevent replay attacks. Moreover, a *tight synchronization among anchors* is required such that TDoA systems operate correctly, which makes these systems vulnerable to attacks on the synchronization process. On top of this, an attacker can leverage a naïve implementation of the *quasi-simultaneous responses* principle to alter the TDoA estimates.

This state of affairs represents a significant problem, and calls for a detailed analysis of the possible attacks on scalable RTLS based on UWB technology, as well as concepts enabling the design of *both secure and scalable* positioning systems.

**Contributions.** In this paper, we address this gap by first analysing in depth the characteristics of scalable UWB-based positioning systems, highlighting specific properties that set them apart from classical RTLS based on TWR and that affect their security. These properties include: (i) the unidirectionality of communications, (ii) the need of synchronization between anchors, (iii) the presence of multiple receivers for the same message, and (iv) the transmission of quasi-simultaneous responses. We then illustrate how these specific properties can expose scalable RTLS based on UWB technology to a number of attacks such as replay and wormhole attacks, as well as attacks targeting the synchronization phase and the use of quasi-simultaneous responses. Based on this analysis, we devise design guidelines to counteract the identified attacks: these include, among others, the use of timeslots instead of challenge/response schemes, the adoption of standard-compliant features to secure the principle of quasi-simultaneous responses, as well as the application of temporal leashes to bound the maximum distance between two devices [27].

Specifically, this paper proceeds as follows:

- We highlight how work on secure distance estimation in UWB systems has mostly focused on secure TWR (§ II).
- We analyse the properties of scalable RTLS and highlight how they have a major impact on their security (§ III).
- We carry out a security analysis of UWB-based scalable RTLS and show their vulnerability to many attacks (§ IV).
- We present concepts to counteract these attacks (§ V).
- We conclude the paper along with a summary of our contributions and planned future work (§ VI).

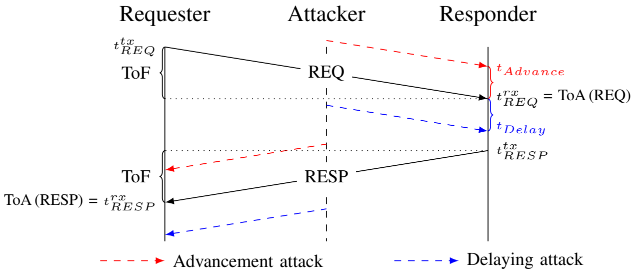

Fig. 1: Traditional TWR scheme between a requester and a responder in absence (black) and in presence of advance (red) and delay (blue) attacks on the ToA estimate. These attacks result in a reduced and enlarged estimated distance.

## II. Work on Secure Distance Estimation

UWB-based RTLS are traditionally based on Time-of-Flight (ToF) measurements of packets sent between a tag and a set of static anchors, which are then converted into distance estimates by multiplying the ToF by the speed of light $c$. The distance estimates are then used in a set of non-linear equations to unambiguously determine the position of a tag. To calculate the ToF, one can subtract the time at which a packet is transmitted by a requester node ($t^{tx}_{REQ}$) from the Time-of-Arrival (ToA), i.e., the instant $t^{rx}_{REQ}$ at which the packet is received at a given responder. However, this only works if both clocks are perfectly synchronized, as tiny differences in the relative clock speed may lead to large inaccuracies.

**Distance estimation using TWR.** To estimate the distance between unsynchronized nodes, one typically makes use of two-way ranging (TWR) schemes. In the latter, a requester sends a request message (REQ) to a responder, who answers with a RESP message, as shown in Fig. 1. By precisely estimating the ToA and the transmission time of *both* packets, one can eliminate the offset between the two clocks and estimate the correct distance. Variants of this scheme have been the gold standard to estimate distances using UWB systems for years.

TWR schemes make use of the traditional physical layers (PHYs) designed for UWB systems, which are defined by the IEEE 802.15.4 standard. The latter defines two UWB PHYs: the high-pulse repetition frequency PHY (HRP), based on the IEEE 802.15.4*a* amendment [28], as well as the low-pulse repetition frequency PHY (LRP), based on the IEEE 802.15.4*f* amendment [29]; both making use of sequences of short pulses of roughly 2 ns length each. These pulse sequences are used for data transmission and for ToA estimation by exchanging packets between nodes. A packet consists of two main blocks: a synchronization header (SHR) and a data portion. The SHR is composed of a preamble and a start-of-frame delimiter (SFD); the data portion consists of a physical layer header (PHR) and a payload [30]. The preamble is employed for frame detection and synchronization; the SFD marks the end of the preamble and allows to derive a coarse ToA estimate [31], [32].

When using HRP PHYs, the receiver builds up a channel impulse response (CIR) estimate from the preamble by constantly correlating the received signal with a template version of the preamble signal. The CIR estimate characterizes the channel and captures the first path as well as multipath components [7]. The HRP PHY supports coherent receivers, which estimate and use the phase information of the received signals to build a CIR. Instead, the LRP PHY suggests to use non-coherent receivers that are agnostic to the phase of the received signal and hence do not use any phase information. Although the use of both HRP and LRP PHY allows for accurate distance estimations, neither the IEEE 802.15.4*a* nor the IEEE 802.15.4*f* standard specifies how to carry out a *secure* distance estimation satisfying the properties discussed next.

**Properties of secure distance estimation.** On a wireless channel, any third party can easily inject signals in an effort to manipulate the data decoding and ToA estimation process. While attacks on data decoding can be reliably detected at higher layers of the network stack by employing message authentication codes (e.g., HMAC), the same does not apply to attacks on the ToA estimation process. As illustrated in Fig. 1, an attacker may indeed inject signals into the wireless channel to advance the estimated ToA ($t_{REQ}^{rx}$) at a responder by a time $t_{Advance}$ (red dashed arrows). Similarly, an attacker may manipulate the signals in the wireless channel and trick the responder to estimate a ToA delayed by a time $t_{Delay}$ (blue dashed arrows). In both cases, by manipulating the estimated ToA (and, consequently, the measured ToF), an attacker can shorten or enlarge the estimated distance, resulting in a wrong position computation. Hence, it is important to protect and secure the ToA estimation process to ensure a correct distance estimation. On a signal level, a secure distance estimation procedure should satisfy three key properties:

- *Entity Authentication.* Solely signals from legitimate nodes shall contribute to a valid distance estimate.
- *Signal Integrity.* Any attempt to manipulate signal properties shall be detected.
- *Freshness.* It must be ensured that a received signal is fresh and not a replica (replay) of a previous version.

**Standardization efforts.** To provide secure distance estimates, a new task group was formed to draft the IEEE 802.15.4*z* amendment [33], which extends the packet format of IEEE 802.15.4*a* / *f* to enhance the security of ToA estimates. Although the standard is still in approved draft status, many of its parts are becoming consolidated. IEEE 802.15.4*z* aims to provide packet and PHY structures as well as concepts to prevent distance fraud attacks, in which an attacker influences the ToA estimate during the distance estimation process between two devices. The standard introduces two new concepts to secure the ToA estimation: the *scrambled timestamp sequence* (STS) and the *ciphered sequence* (CS).

The STS method, typically coupled with an HRP PHY, uses the same correlation principle performed on the preamble. A transmitter sends out sequences of pseudo-randomized pulses generated from `AES-128` using a shared secret between requester and responder. On the receiver side, the received signal $r(t)$ is correlated with the secret sequence as shown in Fig. 2, i.e., each received symbol is multiplied by a value contained in the expected secret sequence and is summed up to build a CIR estimate. Consequently, the latter results in strong peaks if the sequences correlate (i.e., have the same or inverted polarity): this is the case for the legitimate (black) pulses shown in Fig. 2. In case malicious (red) pulses are sent before the legitimate ones by erroneously guessing the secret sequence, the correlation process yields weak or no peaks in the resulting CIR. To accept a ToA estimate as authentic, the correlation value must be above a certain threshold. The latter must be chosen such that uncorrelated sequences are not accepted as valid ones. Note that, if an attacker is able to generate a (blue) pulse with the same polarity of the legitimate one, the injected pulse will result in a peak in the resulting CIR, which may be used in the context of cancellation or over-shading attacks, as discussed in § IV-A.

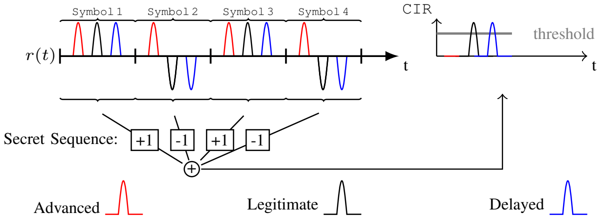

Fig. 2: Sketch of the STS method proposed in IEEE 802.15.4*z*.

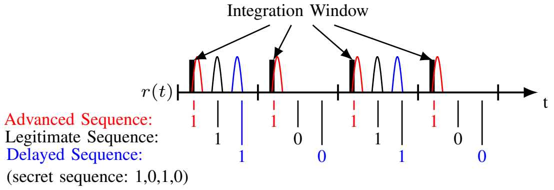

Fig. 3: Sketch of the CS method proposed in IEEE 802.15.4*z*.

The CS method – typically coupled with the use of an LRP PHY – instead, directly decodes the presence or absence of pulses into a binary sequence, and checks afterwards whether the latter matches a known secret sequence, as illustrated in Fig. 3. To this end, the decoding process is adjusted such that the receiver sets the integration window (during which energy is accumulated to decode a symbol) around the estimated ToA of each pulse (black rectangle). Therefore, an attacker trying to shift the ToA estimate ahead in time (red pulse) will fail if it cannot correctly predict the secret sequence. Hence, differently from STS (where an advancement attack results in a low correlation), when using CS an advancement attack results in a mismatch between the decoded and the secret sequence.

Besides the STS/CS methods proposed in IEEE 802.15.4*z*, several academic efforts have presented methods to secure ToA estimations using UWB PHYs [13], [15], [16], [34], [35]. This is done by either (i) adjusting symbol encoding such that attackers cannot easily manipulate physical properties, and/or (ii) by introducing techniques to check the integrity of the received signals, e.g., detecting manipulation attempts by analysing the strength and the variance of a received signal.

**Distance bounding protocols.** Methods securing the ToA estimation, such as the STS and CS, are typically coupled with the use of *distance bounding* protocols [36], [37] to prevent replay and wormhole attacks [38]. While there are a variety of implementations, the underlying concept behind distance bounding protocols is the use of *challenge/response schemes*. In a first step, two nodes (verifier and prover) agree on a common secret. Subsequently, the verifier sends a challenge to the prover, who uses the challenge and the secret to produce a response. In a last step, the prover signs the response, such that the verifier can authenticate it. These protocols prevent replay attacks, since each new challenge makes use of a new fresh value. Furthermore, these protocols prevent attacks in which an attacker tricks the verifier to think that a prover is closer than it actually is. Indeed, an attacker cannot create the correct response by itself and cannot relay messages faster than light. Distance bounding protocols also prevent attacks in which an attacker relays messages between two nodes that are not within their communication range, arbitrarily delaying them. Indeed, one can set a maximum value for the distance measurement, such that any malicious activity is detected.

Such distance bounding protocols are often integrated into TWR schemes, as they anyway foresee the bidirectional exchange of REQ/RESP messages, as shown in Fig. 1. However, in order to privilege scalability, modern positioning systems based on UWB technology tend to move away from TWR schemes, and hence do not make use of distance bounding protocols. Furthermore, modern scalable UWB systems have distinctive characteristics, as we detail in the next section, which can result in a number of potential attack vectors.

## III. Scalable Positioning

The use of TWR and distance bounding schemes in UWB-based positioning systems has several drawbacks. First, the need for a bidirectional data exchange between each tag and each anchor results in a *large message overhead* and requires the use of scheduling techniques for collision avoidance, which limits the system's responsiveness and the achievable update rate [18]. Second, the large message overhead of TWR results in an increased energy consumption and limits the number of supported tags, which lowers the scalability and applicability of such systems. Third, due to the nature of TWR and distance bounding schemes, the privacy of tags is not preserved, as they actively exchange messages, thus revealing their presence.

Because of this, modern RTLS based on UWB technology are moving away from TWR-based approaches, towards more scalable design principles [19], [20]. The latter allow to minimize the number of exchanged packets (which enhances responsiveness while reducing energy consumption) and to enable a fully-passive (i.e., privacy-preserving) localization for countless tags. These scalable RTLS are based on two key principles: TDoA-based positioning (illustrated in § III-A), and the use of quasi-simultaneous responses (described in § III-B).

### A. TDoA-based Positioning

Compared to TWR-based systems, TDoA approaches do not need to derive the ToF of a packet, but exploit instead the difference in the arrival time of signals from two reference points [23]. Fig. 4 shows an exemplary setup of a TDoA-based RTLS with four anchors (A1–A4), and one tag T (note that, in principle, an arbitrary number of tags can be supported). To derive the tags' position, the following steps are performed:

*I* ) *Synchronization of anchors.* A reference anchor (in this case $A1$) broadcasts a `SYNC` message to all anchors. Based on this message, the anchors precisely synchronize their clocks in the sub-ns range. This is crucial to precisely determine the transmission time of the `RESP` messages at each anchor in a later step.

*II* ) *TDoA estimation.* The anchors broadcast a `RESP` message that is received by any tag in the surroundings. Tags can hence passively estimate the ToA of each received `RESP` message using the synchronization header. By subtracting the estimated ToA of two `RESP` messages, the tags derive the estimated TDoA. In the example of Fig. 4, the TDoA between A1 and A2 ($\Delta\tau_{1,2}$) is derived by subtracting the ToA of `RESP 2` from that of `RESP 1`.

*III* ) *Position computation.* The position of a tag is then calculated by solving a set of non-linear equations based on the estimated TDoA values. Note that, at this stage, deviations in the ToA estimates (and, consequently, in the TDoA estimates) from their true values result in large discrepancies of the estimated position.

Hence, RTLS based on TDoA-based positioning performing these three steps are characterized by the following properties:

- *Unidirectional communications*. The transmission of both the `SYNC` message in step $I$ and of the `RESP` messages between anchors and tags in step $II$ is unidirectional. While the use of unidirectional communications minimizes the number of exchanged packets and maximizes both scalability and update rate, it exposes these systems to several attacks, as discussed in § IV-C.
- *Multi-cast communication.* The exchanged messages are broadcasted to all surrounding anchors (step $I$) and tags (step $II$), which means that the same message has multiple recipients. As discussed in § IV-B, this implies that a secret needs to be shared across multiple receivers, which makes these systems vulnerable to malicious tags.
- *Need for tight synchronization across anchors.* In order for a tag to correctly compute its position, the responses of the anchors need to be precisely timed. This is a fundamental requirement of any TDoA-based system. As we show in § IV-D, however, this also means that an attacker can explicitly aim to break the synchronization process in step $I$ to affect the computed position at all tags.

The exemplary system shown in Fig. 4 is often referred to as *downstream-TDoA*, as the anchors sequentially broadcast messages to the tags. In these RTLS, the position is then estimated directly on each tag (e.g., for indoor-navigation applications [24], [39]). Differently, in *upstream-TDoA* systems such as [2], the positioning process is initiated by tags, which broadcast an initial message to the anchors, which then compute their position. Consequently, *upstream-TDoA* systems still suffer from the need to coordinate and schedule the transmissions of multiple tags, which results in a lower scalability and achievable tag density. Moreover, *upstream-TDoA* systems do not allow a passive (and hence privacy-

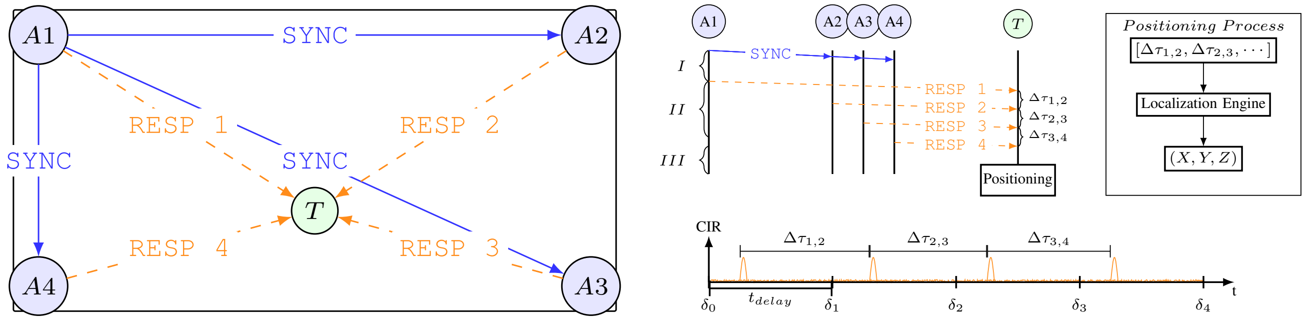

Fig. 4: Illustration of a typical *downstream-TDoA* system setup with a single cell (left) and of the three steps of a TDoA-based localization process (right), namely $(I)$ synchronization of anchors, $(II)$ TDoA estimation, and $(III)$ position computation. The right-bottom of the figure illustrates an exemplary CIR obtained using quasi-simultaneous responses.

preserving) localization. Therefore, we focus only on scalable *downstream-TDoA* systems in this work.

### *B. Quasi-simultaneous Responses*

Recently, the concept of concurrent transmissions [40] was introduced also in the context of UWB systems. Specifically, this concept was applied to TDoA-based RTLS by enabling the quasi-simultaneous transmission of `RESP` messages [19], [20]. In contrast to classical TDoA systems such as ATLAS [23], where the `RESP` messages are individual responses sent sequentially from every anchor, in recent RTLS such as SnapLoc [20] and Chorus [19], the anchors respond almost at the same time, such that a tag can receive all anchors' responses within a *single* `RESP` message.

The working principle can be explained as follows. After the reception of the `SYNC` message, each anchor $A_i$ is triggered to transmit the `RESP` message after a pre-defined delay $\delta_i = t_{delay} \cdot i$, where $i = 1, \ldots, \mathrm{N}$ (with N being the number of anchors) and $t_{delay} \approx 200\,\mathrm{ns}$: this divides the CIR into slots. By doing so, one is able to extract the quasi-simultaneous responses from multiple anchors using the estimated CIR received as a *single* packet. The estimated CIR will indeed contain multiple peaks (one for each quasi-simultaneous `RESP` message, as shown in Fig. 4). This minimizes the time during which tags turn on their radio (resulting in a higher energy efficiency) and enables a higher update rate.

The concept of quasi-simultaneous transmissions has recently been demonstrated on off-the-shelf devices by several researchers [20]–[22]. However, existing works have mostly focused on developing prototypical implementations, without discussing how to make this principle secure and investigating potential attacks. As we discuss in § IV-E, when applying IEEE 802.15.4$z$ security principles to quasi-simultaneous responses, one faces the fact that all anchors need to transmit the same secret in order for a message to be correctly demodulated, which opens the door to many attacks.

## IV. Security Analysis of TDoA-based positioning

The scalable systems we just described in § III have distinctive characteristics that set them apart from TWR-based RTLS and to all other approaches on which the existing literature on secure UWB positioning has focused. Therefore, we carry out next a detailed security analysis of TDoA-based positioning systems and highlight the vulnerabilities deriving from the use of multi-cast communication (§ IV-B) and unidirectional communications (§ IV-C), from the need of tight synchronization across anchors (§ IV-D), as well as from the adoption of the quasi-simultaneous responses principle (§ IV-E).

As in other secure UWB works, in our analysis we consider the Dolev-Yao model [41], where an attacker can receive and inject pulses from/into a wireless channel, but cannot block pulses. We do not consider attacks aiming to physically damage or manipulate a tag. We start our analysis in § IV-A by examining common attacks on ToA estimation, as this is a prerequisite for a correct TDoA estimation (see § III). Note that all attacks on ToA estimation presented in § IV-A also apply to positioning systems based on TWR.

### *A. General Attacks on ToA Estimation*

A large body of literature describes attacks on ToA estimation in pulse-based UWB systems [35]. Attacks can be coarsely classified as ToA-*advancement* and ToA-*delaying* attacks, which aim to shift the estimated ToA ahead or to a later point in time, respectively.

*1) Cicada attack (ToA-advancement):* Advancement attacks in which an attacker sends pulses in order to cause artefacts in the CIR estimate and thus influence the ToA estimation are often referred to as *cicada attacks* [35], [42]. In the examples shown in Figs. 2 and 3, this corresponds to the case in which an attacker blindly injects the red pulses. As discussed in § II, both the STS and the CS methods allow to prevent this kind of attacks, as they result in a low correlation (STS) or in a mismatch between the decoded binary sequence and the secret sequence (CS). Similar to the STS method, other schemes propose the use of random preamble sequences which sum up to zero, so that wrong pulses cancel out [35]: these schemes also allow to prevent this attack.

*2) ED/LC attack (ToA-advancement):* When using redundancy on a symbol level to enhance robustness, UWB systems may be exposed to the so-called *early-detect late-commit* (ED/LC) attack illustrated in Fig. 5 (top). Imagine, for example, that a logical '1' is sent as a sequence of consecutive pulses. An attacker could quickly detect the value of a symbol by observing the first few legitimate (black) pulses in an early detect (ED) phase, and then send the upcoming pulses in advance (red) in a late commit (LC) phase. This way, the

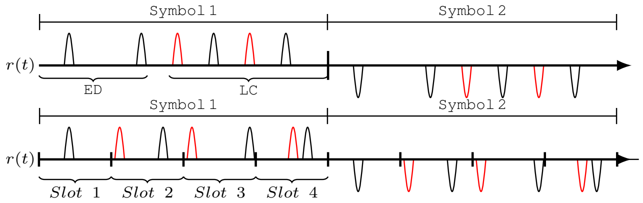

Fig. 5: Illustration of the ED/LC attack (top), and of an attack on quasi-simultaneous transmissions (bottom).

estimated CIR will contain early peaks leading to an advanced ToA estimate. The use of both STS and CS prevents this kind of attacks, as both methods use only one pulse per symbol. In general, to mitigate this attack, one can also use short symbols, such that an attacker cannot react fast enough. This, however, would have an impact on the bit error rate, which increases due to the reduced number of pulses per symbol. The authors in [16] suggest to still use multiple pulses per symbol, but to randomize the symbol-to-pulse encoding based on a shared secret, such that an attacker cannot predict the next pulses.

*3) Power increasing attack (ToA-advancement):* In UWB systems making use of symbol spreading, an attacker can steer the energy injected for each pulse to perform power increasing attacks. In the example shown in Fig. 2, the attacker needs to guess the polarity of the first symbol. If its guess is wrong, the attacker can increase (e.g., double) the energy used to inject the next guessed pulse. If the guess is correct, the use of pulses with increased power allows to cancel out the previous (erroneous) guess, which will alter the estimated ToA in the derived CIR accordingly. While the IEEE 802.15.4$z$ standard leaves the mitigation of this attack up to the radio vendor, several methods to prevent this attack on correlator-based systems are proposed; among others by limiting the received pulse energy, such that each pulse can only contribute the same amount of energy [35]. The CS method is immune to power increasing attacks, as it uses one pulse per symbol and decodes the presence or absence of pulses into a binary sequence: therefore the first erroneous guess already leads to a mismatch with the secret sequence. When using more than one pulse per symbol, one can compute the variance of the pulse energy [34], or randomize the pulse-to-symbol encoding to make it impossible to reliably inject the desired energy [15].

*4) Cancellation attack (ToA-delaying):* An attacker sending timely pulses with opposite phase can perform a signal cancellation attack [13]. In the examples shown in Fig. 2 and 3, an attacker would essentially cancel out all the black pulses and re-send them later in the form of a blue pulse to successfully delay a ToA estimate. To this end, the attacker must know the exact position of the victim's antenna, the phase offset of the sender's carrier signal, as well as the pulse sequence, which makes this attack rather unlikely. UWB systems based on the HRP standard are vulnerable to this attack, as they use well-known preambles for both packet detection and synchronization. Non-coherent (phase-agnostic) radios, instead, can mitigate this attack, as a complete pulse cancellation is infeasible when using a random sequence of [0,1] in combination with randomized carrier phase [15].

*5) Over-shading attack (ToA-delaying):* Another attack that delays the ToA estimate is over-shading, which aims to make the original signal insignificant by re-sending a delayed version that is much stronger. When performing an over-shading attack in the exemplary scenarios shown in Fig. 2 and 3, the blue pulses will be injected with a much higher energy than the original (black) ones. If this is the case, the original black pulse will no longer be recognized as a first path and the ToA estimate will be delayed accordingly. While the IEEE 802.15.4$z$ does not give guidelines on how to handle this attack, it is in principle possible to detect an unusually high energy with a high-resolution ADC [15], [31].

### *B. Attacks deriving from the use of Multi-Cast Communication*

As discussed in § III, when using downstream-TDoA systems, an anchor sends the same `RESP` message to multiple tags: this has important implications when implementing a secure communication based on IEEE 802.15.4$z$.

When using the STS method, a secret has to be known prior reception of a message to allow for an efficient correlation without the need to store the entire pulse sequence. Therefore, the secret needs to be shared in advance with *all* potential recipients of a message. In RTLS where mobile tags dynamically join the network at runtime, however, this is highly undesirable. Indeed, if an anchor provides to a tag $E$ the same secret used to communicate with the other tags, and $E$ turns out to be malicious, all tags are exposed to advancement attacks. This would not be the case when using TWR schemes, as communication only takes place between a *pair* of devices, which allows to share a secret on an individual basis.

The same problem applies to other methods such as [13], [15], [16], [34], [35]. Indeed, these methods also require knowledge of a secret prior message reception: either for secure signal authentication, or to make use of additional symbol spreading (which implies prior knowledge of the secret used to hide the symbol-to-pulse encoding).

Instead, when using the CS, a receiver directly decodes the presence or absence of pulses into a binary sequence, which is later matched with a secret sequence (see Fig. 3). This enables a transmitter to send a message and only reveal the secret afterwards (e.g., by signing the message at the end). This way, the secret does not need to be shared in advance with all potential receivers, which prevents advancement attacks.

### *C. Attacks due to the use of Unidirectional Communications*

As described in § III, modern RTLS make heavy use of *unidirectional* communication in an attempt to increase energy efficiency and the achievable update rate, while preserving the privacy of tags. When exploiting unidirectional communications, however, one is unable to reuse distance bounding and challenge/response schemes, which are a fundamental principle of secure UWB distance estimation as discussed in § II: this exposes the system to replay and wormhole attacks.

*Replay attacks.* A classical attack in computer networks is the replay attack: an attacker records a legitimate message and sends it at a later point in time. Since the recorded message is authenticated, the receiver (victim) deems the replayed version as legitimate. In the scenario shown in Fig. 4, this would result, for example, in a tag being unable to distinguish whether the received RESP message is an original or replayed version. This is a problem, as the attacker is then able to perform both advancement and delaying attacks on the ToA by replaying the message at any point in time. When using distance bounding, this situation is prevented by having the tag itself send a new challenge (nonce) for each message, which only anchors possessing a secret can convert into a valid response, and by ensuring that the response time from the anchor is bounded. Moreover, with unidirectional communications one cannot abort the distance estimation process if the first pulses of a message do not lie within an expected time window, as there is no common time-base with the transmitter [13].

In principle, a tag can prevent a replay attack by refusing a message containing a previously-used nonce: this, however, would assume that all previous messages sent by an anchor were correctly received. If an attacker is able to prevent the reception of a legitimate message at a tag[1], then it can still perform advancement or delaying attacks on the ToA by later replaying that message at any time, without being noticed.

Note that a similar problem affects the SYNC messages sent by the reference anchor, which can results in attacks to the synchronization procedure, as described in § IV-D.

*Wormhole attacks.* The ability of a malicious entity to perform a relay attack, where messages or signals are recorded in an area of a network and tunnelled into another area (outside the communication range), is often referred to as wormhole attack. When using bidirectional schemes such as TWR and distance bounding, one can mitigate this attack by setting a maximum upper bound $d_{upper}$ on the estimated distance that is proportional to the maximum communication range. If two nodes are within $d_{upper}$, it is assumed they can hear each other directly. If they are further away and an attacker relays packets, the estimated distance $\hat{d}$ violates the $d_{upper}$ bound. When using unidirectional communications, however, nodes cannot measure the distance $\hat{d}$ to the other node and, therefore, are unable to constrain the distance.

### D. Attacks on the Synchronization Process between Anchors

As illustrated in Fig. 4, state-of-the-art TDoA-based systems make use of *one-way* SYNC messages to synchronize the clocks between anchors and to trigger the transmission of RESP messages. Thus, a malicious entity can directly attack the infrastructure by exploiting the unidirectionality of the synchronization process, which makes the system vulnerable to replay and relay attacks in the same way as highlighted in § IV-C. Attacks on the synchronization process, however, have a much more profound impact: while the attacks presented in § IV-C target specific tags, by playing havoc with the synchronization of an anchor, an attacker can affect the estimated TDoA values (and consequent distance estimates) of *all* surrounding tags. For example, an attacker can make use of directional antennas to individually control the $t_{delay}$ time of an anchor, affeting the resulting TDoA at its own will. Moreover, in this context, the position of the anchors is often static and precisely known, which makes signal cancellation attacks as described in § IV-A more likely to succeed.

### E. Attacks exploiting Quasi-Simultaneous Responses

In modern RTLS using quasi-simultaneous responses, anchors send the same packet (and hence the same preamble), only slightly delayed, to generate multiple peaks in the CIR and let surrounding tags estimate the TDoA from all anchors with a single message reception (see § III-B). This results in a potential attack to the tags, as illustrated in Fig. 5 (bottom). The attack principle is similar to that of the ED/LC, where the use of redundant pulses gives an attacker the possibility to inject the upcoming pulses once the first legitimate ones are observed. When using quasi-simultaneous transmissions on HRP radios, even though only one pulse per symbol is used (e.g., with the STS method), one ends up with multiple pulses per symbol, as the (slightly delayed) reply of each anchor will generate an individual pulse. An attacker can hence detect the pulse polarity coming from the first anchor (black) and send the pulses of the next anchors in advance (red). This allows to manipulate the TDoA estimates, since an attacker can precisely advance the ToA of all anchors except the first one.

## V. Design Guidelines

Based on the analysis in § IV, we now present several concepts to secure modern TDoA-based UWB RTLS. We start by securing the synchronization process between anchors (§ V-A). We then let each tag synchronize to the location infrastructure by carrying out a secure TWR (§ V-B). This way, the anchors' timestamps can be used to generate time-dependent secrets preventing replay attacks. Moreover, we add temporal and geographical leashes protecting against wormhole attacks (§ V-C), and adapt IEEE 802.15.4$z$ standard-compliant features to secure quasi-simultaneous responses on HRP radios (§ V-D).

### A. Secure Synchronization between Anchors

As discussed in § IV-D, the use of one-way SYNC messages to synchronize the clocks between anchors exposes the system to several attacks. For this reason, we propose to secure the synchronization process between anchors by using a three-way handshake prior each localization round, as illustrated in Fig. 6. Specifically, we assume that all nodes belonging to the location infrastructure (i.e., the reference anchor $A_1$ and all other anchors) share the same secret, which they use to perform a secure three-way handshake. We also assume that all nodes in the location infrastructure know their exact locations beforehand, e.g., this is hard-coded during deployment.

During the three-way handshake, the reference anchor $A_1$ first transmits an authenticated message $M_1$ to all other anchors using the techniques described in § II. Anchors $A_2 - A_4$

[1] An attacker has several options to impair the reception of a message. (1) It can "spam" the victim by sending a well-formatted packet, keeping the victim's radio busy decoding unwanted messages. (2) It can generate noise and "jam" the channel. (3) It can send strong signals that prevent an UWB radio from decoding a consistent CIR estimate across different parts of a SHR, which results in the corresponding message being discarded [43].

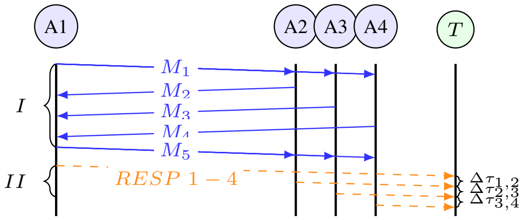

Fig. 6: Scheme securing the synchronization between anchors.

respond sequentially to $M_1$: this way, $A_1$ can estimate each distance and make sure that it matches the expected one (i.e., that no attacker has manipulated the ToA of $M_1 - M_4$). Thereafter, $A_1$ broadcasts a message $M_5$ to all anchors to trigger the transmission of the RESP messages, i.e., $M_5$ is functionally equivalent to a SYNC message in Fig. 4. Anchors $A_2 - A_4$ make use of this last message to detect any manipulation of $M_2 - M_5$: to this end, they compare the estimated distance from $A_1$ to the true one. An attacker who introduces a $\Delta\tau$ during any of the message exchanges will also introduce an error in the calculated distance estimate $\hat{d} > d$: if this is the case, the localization round is aborted. Note that all messages are exchanged among anchors, which are typically wall-powered: hence, no extra energy is consumed on the tags.

### B. Secure Synchronization between Tags and Infrastructure

We propose to synchronize all tags to the location infrastructure (anchors) in order to enable the creation of time-dependent secrets used to protect the ToA estimates. Essentially, time is split into time-slots: each tag joining the RTLS carries out a secure TWR with *one* of the anchors to synchronize its clock. Prior to this, tag and anchor should mutually verify their authenticity and exchange all necessary secrets to perform secure TWR: we assume this to be done using common public key infrastructure schemes. Depending on the PHY scheme used to secure the distance estimates, one may also need to exchange a shared secret during the TWR to be able to receive secure RESP messages during the TDoA estimation. As discussed earlier, when using the STS method, a secret has to be shared before the reception of a message to perform correlation without the need to store the received signal. Therefore, during the TWR, the anchor informs the tag about a secret seed $k_{STS}$ that is used to encode all the RESP messages. In contrast, when using the CS method, no secret needs to be shared by the anchor in advance, as discussed in § IV-B. Note that the synchronization between tags and infrastructure is, in principle, only carried out *once* when the tag joins the network, as shown in Fig. 7. Indeed, as we will see in § V-C, each tag implicitly reuses subsequent localization rounds to maintain a clock synchronization to the location infrastructure.

### C. Secure TDoA and Position Estimation

We exploit the synchronization between tags and anchors to address the attacks deriving from the unidirectionality of RESP messages highlighted in § IV-C. To this end, all actions during a localization round occur within given timeslots of pre-defined size, as shown in Fig. 7. When an anchor receives the last message of a three-way handshake ($M_5$), it

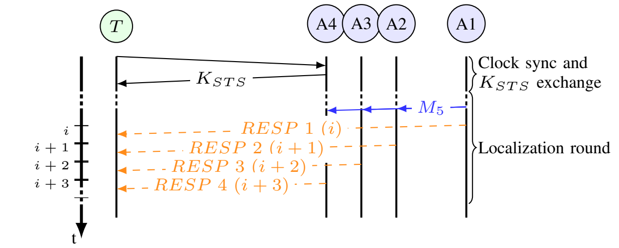

Fig. 7: Secure TDoA and position estimation by exploiting the synchronization between tags and location infrastructure.

generates a RESP message by encoding the current timeslot information $i$: this way, a tag can verify the freshness of a message and prevent replay attacks. Specifically, when using the STS method, one can generate a RESP message embedding a distinct sequence for each timeslot $STS_i = \theta(i, k_{STS})$, with $\theta$ being an AES-128 random key generator, $i$ the current timeslot, and $k_{STS}$ the secret seed shared previously. When using the CS method, instead, one can generate a RESP message embedding a distinct sequence $CS_i$ for each timeslot, which is created with a random nonce $r_i$ that is signed using a combination of the current timeslot $i$, the nonce $r_i$ itself, and the anchor's private key. A tag either pre-computes the sequence $STS_i$ and decodes the RESP message accordingly, or it first receives the message, extracts $CS_i$ as well as $r_i$, and later verifies its correctness using the current timeslot info. Note that, after receiving a message, a tag should discard every subsequent message received in the same timeslot. Tags should also actively detect attempts to impair the reception of a message (e.g., cancellation, jamming, or over-shading) and interrupt a localization round in case of a suspected attack.

The tight synchronization between tags and anchors resulting from the initial TWR can also be exploited to establish *temporal leashes* protecting against wormhole attacks. Essentially, by embedding the anchor's transmission time in the RESP message during the first localization round after the initial TWR, the tag can derive the ToF (and hence the distance to the anchor). If this distance is too large (i.e., it is beyond the communication range), the tag discards the message, as it was likely relayed by an attacker. After performing this step for all anchors, the position of the tag is calculated. A tag can then re-synchronize to the location infrastructure by deriving the ToF using the newly-computed position and the known position of the anchor; this value is then subtracted from the original transmission time of a RESP message to compute the clock offset. In any subsequent localization round, tags rely on *geographical leashes* [38] by using an approximation from the last computed position in order to exclude any message received from anchors that are too far away.

Therefore, the TWR procedure described in § V-B is only carried out *once*: this allows, among others, to maximize a tag's privacy. A tag should proactively make sure that the synchronization with the location infrastructure is maintained across multiple localization rounds. Should a tag detect an excessive drift (e.g., by means of guard times between timeslots), it should re-trigger the synchronization procedure accordingly.

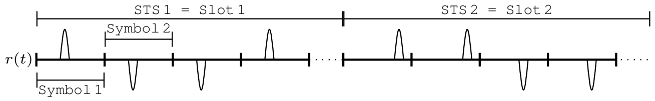

Fig. 8: Multiple STS to secure quasi-simultaneous responses.

### *D. Secure Quasi-Simultaneous Responses*

As discussed in § IV-E, RTLS making use of quasi-simultaneous responses are vulnerable when multiple anchors send the *same* STS. To prevent these attacks, we propose the use of multiple STS. Specifically, the IEEE 802.15.4$z$ standard foresees the possibility to send up to four sequential STS within the same message, as partially shown in Fig. 8 with only two anchors responding. One can reuse this feature to let each anchor respond using an individual STS within one of four available slots. To comply with the timeslots introduced in § V-C, we allow for up to four different STS in one timeslot $i$, i.e., we now have $STS_{i,n}$ where $n$ is the anchor number and $i$ is the timeslot. The generation function for the STS has to change accordingly to account for that $\theta$=($i$,$k_{STS}$,$n$). A tag that receives a packet within a given timeslot $i$ configures its correlator first to decode $STS_{i,1}$, afterwards $STS_{i,2}$, and so on. This way, the attacker cannot use the pulse emitted from the first anchor to infer the pulses of the other anchors.

## VI. Conclusions and Future Work

In this paper we have highlighted why the body of work on secure UWB positioning systems is not applicable to modern RTLS based on TDoA and quasi-simultaneous transmissions, which mainly target scalability. After breaking down the properties of such scalable systems, we have highlighted how they are vulnerable to several attacks, and proposed possible countermeasures. Our analysis and guidelines serve as an input for the next revisions of the IEEE 802.15.4$z$ draft standard, towards a generation of secure **and** scalable UWB systems.

## Acknowledgments

This work was performed within the TU Graz LEAD project "Dependable Internet of Things in Adverse Environments". This work was also supported by the SCOTT project. SCOTT (http://www.scott-project.eu) has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement no. 737422. This joint undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Spain, Finland, Ireland, Sweden, Germany, Poland, Portugal, Netherlands, Belgium, Norway. SCOTT is also funded by the Austrian Federal Ministry of Transport, Innovation and Technology under the program "ICT of the Future" (https://iktderzukunft.at/en/).

## References

[1] A. Alarifi *et al.*, "Ultra Wideband Indoor Positioning Technologies: Analysis and Recent Advances," *Sensors*, vol. 16, no. 5, 2016.

[2] A. Ledergerber *et al.*, "A Robot Self-Localization System using One-Way Ultra-Wideband Communication," in *Proc. of the IROS Conf.*, 2015.

[3] Sewio Networks, s.r.o., "UWB Real-Time Location System," https://tinyurl.com/y87bmlah, [Online] - Last access: 2020-07-15.

[4] Infsoft GmbH, "Tracking of Floor Conveyors and Goods in Logistics," https://tinyurl.com/yc4h4als, [Online] - Last access: 2020-07-15.

[5] S. Huang *et al.*, "A RTLS Based on RFID and UWB for Digital Manufacturing Workshop," *Procedia CIRP*, vol. 63, no. 1, 2017.

[6] F. Zafari *et al.*, "A Survey of Indoor Localization Systems and Technologies," *IEEE Communications Surveys&Tutorials*, vol. 21, no. 3, 2019.

[7] B. Großwindhager *et al.*, "SALMA: UWB-based Single-Anchor Loc. System Using Multipath Assistance," in *Proc. of the SenSys Conf.*, 2018.

[8] EETimes, "VW and NXP Show First Car Using UWB To Combat Relay Theft," https://tinyurl.com/ybh88y5e, accessed: 2020-07-15.

[9] Wired, "The Biggest iPhone News Is a Tiny New Chip Inside It," https://www.wired.com/story/apple-u1-chip/, accessed: 2020-07-15.

[10] 3db Access AG, "Next Generation Secure Access and Positioning," https://www.3db-access.com/, [Online] - Last access: 2020-07-15.

[11] Pozyx NV, "Accurate Positioning," https://www.pozyx.io, [Online] - Last access: 2020-07-15.

[12] B. Ledvina *et al.*, "Mobile device for comm. and ranging with access control system for automatic functionality," Patent US10486646B2, 2019.

[13] N. O. Tippenhauer *et al.*, "Physical-layer Integrity for Wireless Messages," *Computer Networks*, vol. 109, 2016.

[14] IEEE 802.15 WPAN Task Group 4z, "Enhanced Impulse Radio," https://tinyurl.com/ybj6384d, [Online] - Last access: 2020-07-15.

[15] M. Singh *et al.*, "UWB-ED: Distance Enlargement Attack Detection in Ultra-Wideband," in *Proc. of the 28th USENIX Security Symp.*, 2019.

[16] ——, "UWB with Pulse Reordering: Securing Ranging against Relay and Physical-Layer Attacks," *IACR Cryptology*, 2017.

[17] N. O. Tippenhauer *et al.*, "UWB Rapid-bit-exchange System for Distance Bounding," in *Proc. of the ACM WiSec Conf.*, Jun. 2015.

[18] M. Ridolfi *et al.*, "Analysis of the Scalability of UWB Indoor Localization Solutions for High User Densities," *Sensors*, vol. 18, no. 6, 2018.

[19] P. Corbalán *et al.*, "Chorus: UWB Concurrent Transm. for GPS-like Passive Loc. of Countless Targets," in *Proc. of the IPSN Conf.*, 2019.

[20] B. Großwindhager *et al.*, "SnapLoc: An Ultra-Fast UWB-based Indoor Loc. Syst. for an unlimited No. of Tags," in *Proc. of the IPSN Conf.*, 2019.

[21] P. Corbalán *et al.*, "Concurrent Ranging in UWB Radios: Exp. Evidence, Challenges, and Opportunities," in *Proc. of the EWSN Conf.*, 2018.

[22] B. Großwindhager *et al.*, "Concurrent Ranging with UWB Radios: from Exp. Evidence to a practical Solution," in *Proc. of the ICDCS Conf.*, 2018.

[23] J. Tiemann *et al.*, "ATLAS: An Open-Source TDOA-based Ultra-Wideband Localization System," in *Proc. of the IPIN Conf.*, 2016.

[24] ——, "ATLAS FaST: Fast and Simple Scheduled TDOA for Reliable Ultra-Wideband Localization," in *Proc. of the ICRA Conf.*, 2019.

[25] D. Vecchia *et al.*, "TALLA: Large-scale TDoA Localization with Ultra-wideband Radios," in *Proc. of the IPIN Conf.*, 2019.

[26] Bitcraze, "Loco Positioning system," https://www.bitcraze.io/loco-pos-system/, [Online] - Last access: 2020-07-15.

[27] Y. C. Hu *et al.*, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks," in *Proc. of the INFOCOM Conf.*, Mar. 2003.

[28] IEEE Comp. Society, "IEEE Standard 802.15.4a-2007. Part 15.4, Amendment 1: Add Alternate PHYs," 2007.

[29] ——, "IEEE Standard 802.15.4a-2007. Part 15.4, Amendment 2: Active Radio Frequency Identification (RFID) System Physical Layer," 2012.

[30] B. Großwindhager *et al.*, "Enabling Runtime Adaptation of PHY Settings for Dependable UWB Comm." in *Proc. of the WoWMoM Symp.*, 2018.

[31] P. Perazzo *et al.*, "Secure Positioning in Wireless Sensor Networks through Enlargement Miscontrol Detection," *ACM TOSN*, vol. 12, 2016.

[32] A. Compagno *et al.*, "Modeling Enlarg. Attacks against UWB Distance Bounding Protoc." *IEEE Trans. on Inf. For. & Security*, vol. 11, 2016.

[33] IEEE Comp. Society, "IEEE Draft Standard 802.15.4z/D03. Part 15.4, Amendment: Enhanced Ultra Wide-Band (UWB) Physical Layers (PHYs) and Associated Ranging Techniques," 2019.

[34] P. Leu *et al.*, "Message Time of Arrival Codes: A Fundamental Primitive for Secure Distance Meas." *CORR – arXiv preprint 1911.11052*, 2019.

[35] M. Poturalski *et al.*, "On Secure and Precise IR-UWB Ranging," *IEEE Transactions on Wireless Communications*, vol. 11, no. 3, 2012.

[36] K. B. Rasmussen *et al.*, "Realization of RF Distance Bounding," in *Proc. of the USENIX Security Symp.*, 2010.

[37] D. Singelee and B. Preneel, "Location Verification using Secure Distance Bounding Protocols," in *Proc. of the IEEE MASS Conf.*, 2005.

[38] Y. C. Hu *et al.*, "Wormhole Attacks in Wireless Networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, 2006.

[39] P. Bihler *et al.*, "SmartGuide – A Smartphone Museum Guide with Ultrasound Control," in *Proc. of the ANT Conf.*, 2011.

[40] M. Zimmerling *et al.*, "Synchronous Transmissions in Low-Power Wireless: A Survey," *CORR – arXiv preprint 2001.08557*, 2020.

[41] D. Dolev and A. Yao, "On the Security of Public Key Protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, 1983.

[42] M. Poturalski *et al.*, "The Cicada Attack: Degradation and Denial of Service in IR Ranging," in *Proc. of the ICUWB Conf.*, vol. 2, 2010.

[43] M. McLaughlin, "Receiver for use in an Ultra-Wideband Communication System," Patent US10090879B2, 2018.