Security Analysis of IEEE 802.15.4z/HRP UWB Time-of-Flight Distance Measurement

Mridula Singh*, Marc Roeschlin*, Ezzat Zalzala*, Patrick Leu, Srdjan Čapkun
Departement of Computer Science
ETH Zurich Switzerland

***Abstract*—IEEE 802.15.4z, a standard for Ultra-Wide Band (UWB) secure distance measurement, was adopted in 2020 and the chips that implement this standard are already deployed in mobile phones and in the automotive industry (for Passive Keyless Entry and Start). The standard specifies two different modes—LRP and HRP. Whereas the security of LRP mode has been analyzed, there is no publicly available security analysis of the HRP mode, which is used in different chips like NXP Trimension SR150/SR040, Samsung smartphones, and U1 chip deployed in Apple iPhones.**

In this work, we perform the first open analysis of the 802.15.4z HRP mode. Our analysis reviews possible attacks on HRP and assesses strategies that an HRP receiver could implement. We show that in realistic deployments, despite countermeasures, HRP is hard to configure to be both performant and secure. If a distance missdetection rate is set to less than 10% (in benign scenarios), the probability of a successful distance shortening attacks ranges from 7% to over 90%.

I. Introduction

In recent years we have witnessed the widespread deployment of Ultra-Wide Band ranging systems. UWB chips are now embedded in smartphones—Apple iPhones are using UWB for spatial awareness [1], Samsung's newest phone aims to use UWB ranging as a *digital key* to unlock your front door of the house [7], several car manufacturers including Volkswagen and Mercedes are using UWB chips to protect their Passive Entry and Start Systems (PKES) against relay attacks [10], and many companies have announced the use of UWB ranging for contact tracing [8], [9]. The use of UWB ranging systems in different industrial and home applications is only expected to grow.

Most of the recent UWB deployment follows the recent IEEE 802.15.4z UWB ranging standard [11], which has been in development for several years and has been finalized in 2020. This standard enhanced the existing IEEE 802.15.4a standard with new integrity features, allowing more precise and secure ranging.

802.15.4z standardizes two modes of operation—Low Rate Pulse (LRP) and High Rate Pulse (HRP). The names of these modes might indicate only small differences in the operation of the communication link. This is, however, incorrect. Packet formats, implementation and security of HRP and LRP differ significantly. The major differences are primarily due to UWB being a wide band technology. To limit interference, regulators restrict the output power of UWB devices in proportion to their communication rate: the higher the rate, the lower the transmission power per pulse.

LRP pulses are therefore transmitted at a higher power, and in many scenarios individual pulses can be detected and decoded by the receiver. The security of the LRP ranging has been studied in [27], [11] and this mode is currently deployed in automotive for Passive Keyless Entry and Start Systems [4], and available in Microchip ATA8352/8350 chips [5].

Unlike in LRP, due to the low power per pulse, in most application scenarios, individual HRP pulses cannot be detected by the receivers. HRP mode thus requires that the energy is split up into many pulses in order to transmit information successfully. The security concept of HRP reflects this shortcoming and relies on the up to 4096 pulse long random Secure Training Sequences (STS) for time-of-flight measurement. The STS is transmitted by the sender and then detected through auto-correlation. Typically, one of the correlation peaks will determine the time of arrival of the packet. Contrary to LRP where the polarity of each pulse is detected, HRP receivers calculate some aggregate statistic over the received pulses in order to determine the exact time of arrival. Unfortunately, the transmitted pulses can be severely affected by noise and channel artefacts lead to inter-pulse interference (due to the higher repetition frequency and lower power). Despite this challenging problem, HRP chips are already deployed in Apple iPhones (U1 chips) and available in NXP Trimension SR150/SR040 chips [6]. The standard does not specify how the time of arrival is calculated in HRP and how secure such a method is. Until now, companies have not released their time of arrival techniques or their security analysis.

In this paper we aim to fill this gap. We present the first open analysis of the security of the 802.15.4z HRP mode. The history of 802.15.4a development and the documents available from the IEEE 802.15.4z task group [2] allow us to reconstruct the most likely ways that STS is used and time of arrival is calculated at the receivers. We then review possible attacks on HRP and analyze different strategies that an HRP receiver could practically implement. We evaluate a wide range of thresholds that offer different performance-security trade-offs. Our results show that HRP systems are hard to secure if performance in benign scenarios is equally important. To evaluate this we analyze how the probability of the successful distance shortening attack changes with the distance missdetection rate (the fraction of distance measurements

*Authors contributed equally to this research.

for which an incorrect distance was estimated). Our results show that if a distance missdetection rate is set to less than 10% (in benign scenarios), the probability of a successful distance shortening attacks ranges from 7% to over 90%. Our evaluation includes some existing (e.g., Ciccada) and some novel attack strategies.

The rest of the paper is organized as follows. In Section II we review the most relevant concepts behind UWB Impulse Radio and the IEEE 802.15.4a and IEEE 802.15.4z standards. In Section III we discuss possible HRP receiver designs and the assumptions that we make. In Section IV we review existing and propose new attack new attack strategies specifically designed against HRP. We evaluate the security and performance of HRP in Section V. We review related work in Section VI and conclude the paper in Section VII.

II. Background

Estimating physical distance between devices using the wireless signal is becoming a crucial component for a number of security and safety-critical applications. Some of these applications include Passive Keyless Entry and Start Systems (PKES) and contactless payments. The devices can measure physical distance by observing changes in the properties of the signal, such as received signal strength [13], multicarrier phase ranging [20], frequency modulated continuous wave radars [21], or by measuring the time the signal takes to travel between the devices [29], [17].

A. UWB-IR

The time-of-flight (ToF) measurement using UWB-IR has emerged as a prominent technique for precise distance measurements. UWB-IR, standardized within 802.15.4a/f, specifies using a bandwidth upwards of $500\ MHz$, which translates to nanoseconds time resolution, satisfying requirements for centimeter-level precision. Because UWB systems operate over wide segments of a licensed spectrum, they have to be compliant with stringent regulatory constraints to prevent interference with existing wireless systems in the given band. First, the power spectral density cannot exceed $-41.3\ dBm/MHz$ averaged over a time interval of $1\ ms$. Second, the power measured in a $50\ MHz$ bandwidth around the peak frequency is limited to $0\ dBm$. These constraints limit the transmit power per pulse, and therefore, using a single pulse for ranging is inadequate for the non-line-of-sight (NLoS) and long-range measurement. To operate under such conditions, information collected over multiple pulses is aggregated for time-of-arrival (ToA) estimation and data decoding.

B. Distance shortening attacks on UWB-IR ranging

Physical distance is measured using the properties of the wireless signal and/or its arrival time. Therefore, an external attacker can control distance estimation by manipulating the signal exchanged between two legitimate entities. ToF based ranging systems are inherently secure against simple relay attacks, as a relay by definition increases the measured distance. However, an adversary can manipulate the signal to trick the receiver into measuring a different, earlier, time of arrival.

Cicada Attack Time-of-flight (ToF)-based ranging systems rely on leading edge[1] detection mechanisms to achieve accurate distance estimate. In most implementations, the search algorithm performs correlation between the received and expected signal. Because the signal arriving through the direct path is not always the strongest, the receiver has to search for the leading edge after finding the highest correlation peak, *i.e.,* the receiver will try to identify a signal above a certain noise threshold during a back-search starting from highest peak [26], [18]. Cicada attacks exploit the fundamental difficulty of distinguishing the signal arriving through the direct path from interference. Poturalski *et al.* introduced cicada attacks against ultra wide-band impulse radio IEEE 802.15.4a ranging systems [24]. In their attack, an adversary transmits uniformly-spaced ultrawideband pulses during the transmission of the legitimate preamble. The presence of the attack signal degrades the performance of the receivers by undermining leading edge detection, resulting in the distance reduction.

ED/LC Attack In a system that uses distance bounding at the logical layer to achieve secure distance measurement, the estimated distance is determined by the arrival time of a packet that contains a cryptographically generated challenge or nonce. Depending on the data encoding and the signal modulation, an adversary can launch an ED/LC attack to perform distance reduction. The attack works by exploiting the predictability of the (inner) signal structure of a symbol where the adversary learns the packet/symbol values early and commits them late in order to fool receivers about the signal arrival time. In the early detection phase, the adversary detects the entire symbol of length T_{sym} using the initial part only, i.e., within $T_{ED} < T_{sym}$. In the late-commit phase, the adversary forges the symbol such that the small initial part of the symbol is noncommittal, whereas the last part of the symbol (of duration $T_{LC} < T_{sym}$) is sufficient to generate correct data during demodulation at the receiver. This way, the attacker can start sending a symbol before knowing what data the symbol encapsulates and advance the measured arrival time of the symbol by time α. The maximum distance reduction is bounded by the symbol length (*i.e.,* $\alpha < T_{sym}$). Flury *et al.* [16] showed that ED/LC attack is possible against IEEE 802.15.4a UWB-IR, allowing distance reduction of up to $140m$.

C. The IEEE 802.15.4z standard

IEEE 802.15.4z standard, completed recently in 2020, aims to address such attacks, and introduces enhancements to improve the ranging capabilities of the UWB-IR, including precision, security, and MAC layer support. The standard

[1]The earliest occurrence of the signal.

specifies two modes of operation: Low Pulse Rate (LRP) and High Pulse Rate (HRP).

HRP vs LRP: As their names suggest, the modes have different pulse repetition frequency (PRF), which determines the spacing between pulses. In the HRP mode, there is a smaller spacing between pulses but, as a consequence, also lower power per pulse compared to the LRP mode, in order to satisfy the power spectral density of $-41.3\ dBm/MHz$. While the channel noise affects both modes, pulses sent with the HRP mode suffer from inter-pulse interference, as the spacing between consecutive pulses is smaller than the delay spread of the channel.

A single LPR pulse modulated with On-Off-Keying (OOK) or Binary Frequency Shift Keying (BFSK) can be used to represent one bit of information. In such a configuration, and when combined with distance commitment and distance bounding, LRP mode can support a secure ranging systems [14], [28]. The proposals to secure LRP for longer distances and severe NLOS have been proposed in [27], [22]. Unlike LRP, HRP, on the other hand, has lower power per pulse; as a result, the receiver cannot detect individual pulses for ToA estimation and data detection. Instead, security hinges on a cryptographically generated Secure Training Sequence (STS). The security of HRP ranging has so far not been studied in the open literature.

Secure Training Sequence is a Binary Phase Shift Keying (BPSK) modulated sequence of pulses, generated from a pseudorandom bit generator. A bit of value zero produces a positive polarity pulse, and a bit of value one produces a negative polarity pulse. These pulses are sent with the PRF of $124.8\ MHz$. As shown in Figure 1, a ranging packet can

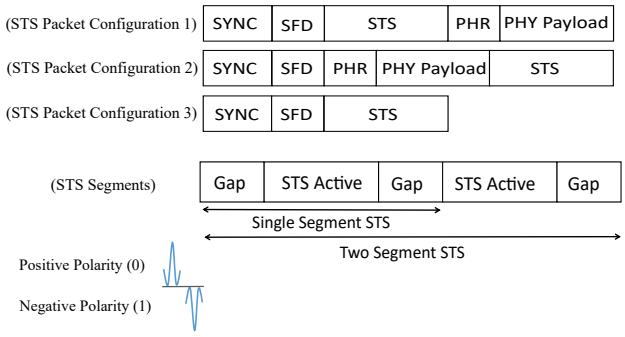

Fig. 1. Packet structure[11]. STS sequences can be transmitted in different configurations. The sequence itself consists of either one or two segments of BPSK-modulated pulses with polarity 0 or 1.

have up to two STS sequences, and each STS sequence can be divided into two segments of at least 4096 pulses each. The segments are encapsulated by silent intervals/gaps, of 512 chip ($\approx 1\mu s$) duration. The receiver calculates the ToA by correlating the received signal with a local template of the STS that has been generated using the same seed as the sender's STS. The receiver can use each STS segment to estimate and validate the integrity of the arrival time. However, the standard does not specify how this should be done.

Along with the STS sequence, the ranging packets can also accommodate a preamble and payload, as shown in Figure 1. The standard does not define the use of preamble and payload for ToA estimation. Using those parts of the packet for distance estimation would not increase the security of distance estimation. The preamble is predictable, and thus an adversary can send it in advance. The payload is BPM+BPSK modulated, as in the IEEE 802.15.4a, allowing ED/LC attack as discussed in Section II-B.

III. UWB HRP Receiver Design

The design of an HRP-capable receiver that can perform secure ranging needs to support accurate detection of the first occurence of the secure training sequence (STS). There are several aspects and implementation choices that determine whether the ranging operation is resilient to external interference, e.g., caused by an attacker who attempts to alter the time at which the receiver detects the STS. On the other hand, physical phenomena, such as multi-path fading require a robust and fault-tolerant time-of-flight estimation technique in order to not render system useless (e.g., at longer distances). The receiver design mentioned by the standard [11], [3] suggests to compute the channel impulse response (CIR) for the transmission of the STS, that is, the receiver correlates the incoming signal with a locally stored template. Based on the CIR, the receiver can determine the exact time of arrival of the STS, which in turn is reported to the higher layers for distance estimation, i.e., after having received $\mathrm{RX}(t) = \mathrm{STS}(t) * \mathrm{CIR}(t)$, the receiver computes

$$\widehat{\mathrm{CIR}}(t) = \mathrm{RX}(t) *^{-1} \mathrm{STS}_{\mathrm{local}}(t)$$

Regardless of how the receiver proceeds in determining the arrival time, it has to implement certain key components. After the correlation operation, the receiver needs to decide if $\widehat{\mathrm{CIR}}$ contains a peak that indicates the presence of STS, see, e.g., Figure 2. Further steps must then follow, such as the determination if the transmitter is in line-of-sight (LOS) or non-line-of-sight (NLOS) and the exact point in time when the STS arrived (*leading edge detection*). We identify three main aspects that govern STS detection and leading edge detection. We describe how they affect the performance and security of HRP-based receivers.

Back-search time window. The maximum correlation peak does not always represent the direct path between the two ranging devices. This can be due to the fact that (1) the devices are not within line-of-sight of each other, or (2) an indirect path experiences constructive interference leading to a higher peak than the direct path. Therefore, receivers must consider any peak above the noise floor as a possible candidate for distance estimation. Once the receiver detects a peak of a certain magnitude it thus needs to perform a comparison with any other peaks in the vicinity that originate from a different, but shorter path. The time window that specifies the search

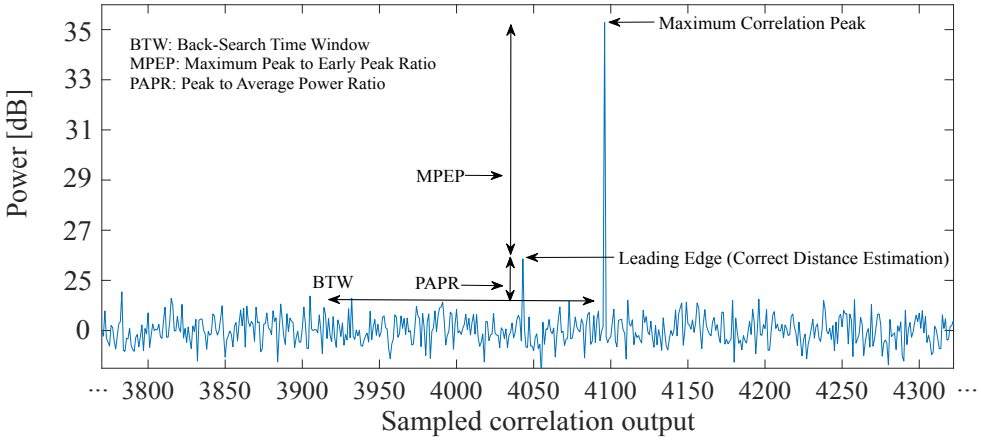

Fig. 2. Power profile of the estimated channel impulse response $\widehat{\mathrm{CIR}}$ at the receiver when correlating the incoming signal with the local STS template. We show the parameters used in the leading edge detection process. y-axis has linear scaling for clarity.

region is referred to as *back-seach time window*. Since the channel delay spread in UWB is between $100ns$ (indoors) and $300ns$ (outdoors) [23], the receiver can assume that, as soon as a peak is detected, any other peaks of interest (with lower magnitude) must have arrived in a window of 100ns to 300ns before the strongest peak.

Noise Floor Estimation. The receiver needs an accurate estimate of the noise floor on the communication channel in order to determine if a correlation peak stems from the transmitted STS or is an artifact of the channel. Ideally, the receiver can acquire a statistic on the magnitude of the noise when the channel is unoccupied. If the noise floor estimate is too high, the receiver might misclassify lower-amplitude peaks generated by an indirect path as noise. However, a low estimate leads to recognizing noise as legitimate peaks and can subvert the time-of-arrival measurement [19].

Peak Detection Thresholds. Regardless of which algorithm is used to perform peak detection, the receiver needs to have a measure of how far the peaks stand out from the noise floor. Due to multi-path, the correlation of the incoming signal with the STS can produce many correlation peaks at different points in time and with varying amplitude [30]. We compute the peak-power for all the correlation peaks the receiver observes during the back-search time window.

STS Peak Candidates Having computed correlation between incoming signal and STS template, the receiver ends up with a set of (arrival-time, power) pairs. We define this set in correlation-space as

$$\mathsf{S} = \{\ (\mathrm{toA}_0, \mathrm{P}_0), \cdots, (\mathrm{toA}_n, \mathrm{P}_n)\ \}$$

where $\forall i < j : \mathrm{toA}_i < \mathrm{toA}_j$. In order to identify the true STS correlation peak among all other peaks that are generated by noise or "side-lobes" of the correlation operation, the receiver can compute statistics across set S as well as compare arrival time and peak-power values against predefined thresholds.

Leading Edge Detection. The receiver design we assume in this work follows the standard [11] and is in line with the documents released by the task-group [2]. It identifies the earliest peak $(\mathrm{toA}_x, \mathrm{P}_x) \in \mathsf{S}$ as the true STS peak if it meets certain requirements. Mainly, the difference between peaks does not exceed the MPEP (maximal peak to earlier peak ratio) threshold, i.e., $\frac{\mathrm{P_x}}{\mathrm{P}_h} < \mathrm{MPEP},\ \forall\ (\mathrm{toA}_h, \mathrm{P}_h) \in \mathsf{S}$ and $x \neq h$. Figure 2 illustrates this requirement. In the figure, the correlation output exhibits two peaks within the back-search window. The earlier peak is 20db below the highest correlation peak and the algorithm therefore classifies it as the first path/incidence of the STS. The second requirement is given by the PAPR (peak to average power ratio). The chosen correlation peak $(\mathrm{ToA}_x, \mathrm{P}_x)$ has to attain a certain peak to average ratio to stand out from the noise, i.e., $\frac{\mathrm{P_x}}{\mathrm{P_{rms}}} \geq \mathrm{PAPR}$ where $\mathrm{P_{rms}}$ is the average power.

In the remainder of this paper we assume PAPR, MPEP and the length of the back-search window to be the main parameters for leading edge detection. The algorithm can be tuned for different thresholds, back-search window and precision and we explore performance impact of the parameters in Section V.

Ranging Error. If the receiver chooses the wrong peak from the candidate set, a ranging error occurs. The receiver might estimate a physical distance that is either too far or too close, depending on whether a peak before or after the earliest STS peak was chosen. Measured across different channel conditions (LoS, NLoS), the ranging error serves as the primary metric to assess the performance of a HRP receiver. We show performance numbers for different implementations in Section V-B. In order to cope with a variety of channel conditions, leading edge detection has to be robust and resilient to channel artefacts. We describe in Section V-C how this requirement poses a trade-off between performance and ranging security.

IV. Distance Reduction Attack

As described in the previous sections, the BPSK modulated STS sequence is used for enabling secure ranging in HRP mode of IEEE 802.15.4. In absence of multi-path and receiver noise, HRP with STS can be used to implement a secure ranging system. In such a scenario the receiver might be able to decode most of the individual pulses of the STS sequence and can require high correlation of the received and template STS. Since an adversary is unable to predict the pseudo-randomly generated sequence it will not be able to generate a high enough correlation peak that satisfies the checks applied at the receiver. However, this scenario is unlikely and in the presence of multi-path, the highest correlation peak is not always caused by the signal that arrived along the direct path, and therefore, the receiver needs to search for the peak corresponding to the direct path in the back-search window. An important observation is that, in order to manipulate the arrival time estimation, an adversary does not need to inject or manipulate the highest correlation peak. Even assuming a very conservative receiver, which prioritizes security over reliability, a correlation peak with a substantial amount of energy injected by the attacker in the back-search window will lead to a shorter than true distance being estimated. We will show in Section V that a peak with $30dB$ or more below the highest peak and only $5dB$ above the noise can successfully undermine leading edge detection, even when choosing very conservative values for the PAPR check performed at the receiver. In the following, we propose two attack strategies that manipulate/insert an early correlation peak and thus affect estimation of STS arrival time. The first strategy is an adaptation of the well-known cicada attack; the second one is a novel injection attack allowing the adversary to place the injected peak at a more precise location.

Cicada++ Attack. This attack is inspired by the cicada attack [24]. An adversary injects pulses at a fraction of the repetition frequency of 124.8 MHz, i.e., the adversarial PRF is $\frac{1}{R} \cdot 124.8\ MHz$ where $R \in \mathbb{N}$ is a parameter. In addition, each pulse is K times stronger than the legitimate pulse, i.e., the adversarial pulses have a peak-amplitude K times as high as the pulses part of the legitimate STS. Furthermore, the

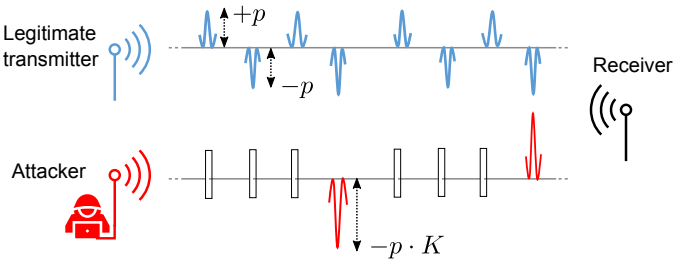

Fig. 3. Example of *Cicada++ Attack*. The adversary sends (random) pulses at one fourth of the PRF of the legitimate STS. The adversarial pulses are K times stronger.

adversary needs to perform the following steps: First, if the overall power of the legitimate signal is low, the attacker needs to amplify the legitimate signal, such that it arrives at the receiver, which will then estimate it as the highest correlation peak. Second, the adversary needs to synchronize with the legitimate transmission and transmit its pulses such that they coincide with the legitimate STS at the receiver. Third, the adversary needs a rough estimate of the legitimate pulses' received signal strength (at the legitimate receiver) to estimate at which power to transmit the attack pulses. The polarity of the attack pulses is not relevant and can be chosen randomly or fixed to a predefined value. An overview of the *Cicada++ Attack*is given in Figure 3.

The result of this attack is that the receiver receives the superposition of legitimate signal and the attacker's signal. Since large parts of the legitimate STS arrive at the receiver unmodified (i.e., whenever legitimate transmission does not coincide with an attack pulse), the receiver can still successfully correlate the transmission with the local template of the STS and observe a high correlation peak. The attacker's signal, on the other hand, leads to an increase in the power of the side peaks. It is harder for the receiver to differentiate if such earlier peaks created by the attacker's signal (satisfying PAPR and MPEP thresholds) are generated in a non-adversarial (e.g., NLOS) setting or caused by a superimposed attack signal.

The adversary succeeds if it can add a peak to the receivers candidate set $\mathsf{S}' = \mathsf{S} \cup (\mathrm{ToA}_A, \mathrm{PAPR}_A)$ such that $\mathrm{ToA}_A < \mathrm{ToA}_x$ where $(\mathrm{ToA}_x, \mathrm{PAPR}_x)$ is the true STS correlation peak. In addition, the inserted correlation peak needs to meet the MPEP and PAPR requirements described in Section V, as otherwise the receiver does not consider $(\mathrm{ToA}_A, \mathrm{PAPR}_A)$ as the true STS correlation peak.

The experimental evaluation in Section V-C provides success probabilities of *Cicada++ Attack*when operating under different thresholds for leading edge detection. Even when $(PAPR, MPEP) = (16, 20)$, a very conservative setting, that is willing to sacrifice reliability for security, i.e., where the receiver a priori discards most first paths, *Cicada++ Attack*still shows a likelihood of success of over 10%. We show detailed attack success numbers in Section V.

Adaptive Injection Attack This attack introduces a fine-grained control over the position of the injected peak.

The adversary's goal in this attack is to inject a peak exactly $\alpha \pm e\ ns$ earlier than the legitimate signal's arrival time. α denotes the time advancement the adversary aims for and e is the imprecision. We assume that the attacker can relay or block transmission of the legitimate signal. For example, if legitimate devices are 20m apart in an NLoS scenario, they cannot communicate directly, but they can communicate through a relay. Therefore, the adversary can selectively choose the part of the signal he wants to relay or block. We also assume that an attacker can determine or control the channel impulse response that the receiver observes by, e.g., placing an adversarial transceiver close to the receiver.

Like in the *Cicada++ Attack*, the attacker also transmits pulses at the repetition frequency of $\frac{1}{R} \cdot 124.8\ MHz$ with

the transmit power K times higher than the legitimate pulses. However, after the adversary has relayed N pulses (of the legitimate STS) and has injected N/R attack pulses, the adversary correlates its attack pulse-train superimposed on the part of STS it has received so far with the actual legitimate signal. The adversary then determines if it will succeed in injecting the peak at the intended position during the back-search window. The attacker stops relaying the legitimate signal and transmitting the attack signal when the correlation output is in favor of the attacker.

Such an attack is more likely to succeed in injecting the peak at the intended position, as the attacker has access to the partial STS sequence (*i.e.,* the part transmitted by the legitimate device), and the signal committed to the legitimate receiver (*i.e.,* the combination of the legitimate and attack signal). Therefore, attackers can decide to allow or block the legitimate signal transmission and inject more attack pulses into the channel.

V. Experimental Evaluation

We use MATLAB simulations to analyze the performance and security of the ToA estimation using STS segments. The STS is modeled as a sequence of 4096 BPSK-modulated pulses, where the polarity of the pulses is chosen at random and the repetition frequency of the pulses is 124.8 MHz, as specified in the 802.15.4z standard [11].

A. Channel Models and Assumptions

We use IEEE 802.15.4a channel models that are provided for UWB and represent different LoS and NLoS conditions, including residential, office, outdoors, and industrial [23]. These models generate the pulse and multi-path profile that resembles the real-world effect of those channels. They also feature random phase noise that is added on top of the entire fading profile. We do not add additional noise or extra path-loss to the channel. The effect of path-loss and distance is captured by varying transmit power. We explicitly do not introduce noise since it proportionally affects both missdetection and attack success rates.

We use the receiver design specified in Section III, the parameters this receiver requires for ToA estimation is the duration of the backsearch time window and ToA detection thresholds (*i.e.,* MPEP and PAPR). In order to apply the thresholds and determine ToA, the receiver estimates the channel impulse response $\widehat{\mathrm{CIR}}$ as described in Section III, i.e., it correlates the incoming signal with a locally stored template of the STS (segment). We compute the received signal RX by convolving the transmitted STS with the channel impulse response obtained from the model. In the benign scenario, the simulation can thus be summarized as follows:

$$\widehat{\mathrm{CIR}}(t) = \mathrm{abs}[\ \underbrace{\mathrm{STS}(t) * \mathrm{CIR}(t)}_{\mathrm{RX}(t)} *^{-1} \mathrm{STS}_{\mathrm{local}}(t)\ ]$$

Since the IEEE 802.15.4a channels introduce random phase noise to the transmitted STS[2], the CIR returned by the model is a complex-valued array. After performing convolution/correlation in the complex domain, we take the absolute value to arrive at the power profile of $\widehat{\mathrm{CIR}}$, which serves as the basis for ToA estimation.

Adversarial interference. When the receiver is under attack, we assume that the adversarial signal is superimposed on the legitimate STS sequence. Moreover, we make the assumption that the adversary manages to obtain a channel similar to the one between legitimate sender and receiver. Especially if the adversary is located in the vicinity of the sender, the adversarial transmission is subject to very similar channel effects. However, in a realistic setting, the adversary's location differs (at least slightly) from the legitimate sender and therefore the channel is only similar, but not identical. We model this fact by generating two channel impulse responses CIR and $\mathrm{CIR}_{\mathrm{adv}}$, one for the legitimate transmission and a second one for adversarial interference. Both are of the same type, e.g., indoor office, but different instances (with different random seed). Finally, we can model the received signal as

$$\mathrm{RX}'(t) = \mathrm{STS}(t) * \mathrm{CIR}(t) \ + \ s_{\mathrm{adv}}(t) * \mathrm{CIR}_{\mathrm{adv}}(t)$$

where s_{adv} is the pulse train introduced by the adversary.

B. Setting Receiver Parameters in Non-Adversarial Conditions

Backsearch time window: To determine the duration of the backsearch window we analyzed the channel impulse response for different channels when no attacks are performed. Our results (Table I) show that in more than 50 percent of the cases, the highest correlation peak did not indicate the leading edge. Thus we conclude that the arrival time of the strongest signal highly depends on the channel conditions and is not a reliable indicator for the distance. For example, in Industrial LoS conditions, the strongest signal arrives within $12\ ns$ of the leading edge (which indicates the correct distance), whereas in the NLos outdoor setting the strongest peak can appear up to $381\ ns$ delayed. This delay estimation is important when determining the duration of the backsearch window; to detect the leading edge, the backsearch window duration should be longer than the delay of the strongest signal w.r.t. the leading edge. However, using a very long backsearch window incurs more processing at the receiver. In this analysis, we set the backsearch window duration to $128\ ns$ (which corresponds to approximately 38m in distance)—a reasonable choice for all channels, except for very few outdoor NLoS scenarios.

Setting Thresholds (MPEP, PAPR): As we already discussed in Section III, MPEP and PAPR thresholds are crucial for accurate ToA estimation. In order to set these thresholds, we simulate ranging in non-adversarial settings and show the

[2]While the modeled channels contain multi-path effects and random phase noise, they do not implement (random) frequency-dependent fading.

Channel Condition	Percentile			
	50	75	95	100
Residential Los	4	12	32	75
NLos	11	21	38	74
Office Los	4	6	17	46
NLos	11	17	27	50
Outdoor Los	6	20	53	127
NLos	24	68	157	381
Industrial Los	1	1	4	12
NLos	9	12	18	35

TABLE I
TIME DIFFERENCE (IN NS) BETWEEN THE ARRIVAL OF THE STRONGEST PEAK AND LEADING EDGE. IF THE BACK SEARCH TIME WINDOW IS SMALLER THAN THE TIME BETWEEN THE FIRST AND STRONGEST PATH, THE RECEIVER CANNOT DETECT THE DIRECT PATH.

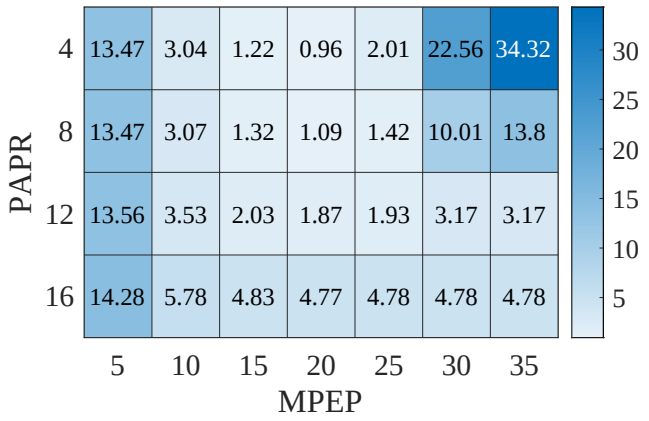

Fig. 4. Misdetection Rate (%): the estimated distance is considered incorrect if ranging error is more than $7ns$.

misdetection (error in distance estimation) rate for different combinations of thresholds. Our results are given in Figure 4 and show that the optimal choice of thresholds is (15,4), (15,8), (20,4), (20,8), or (25,8), where misdetection is lower than 1.5%. In these simulations we allowed (a generous) ranging error of up to $7ns$, *i.e.,* the measured distance is considered correct if inaccuracy in the distance measurement is less than $\pm 2.1m$. Such tolerance corresponds to, e.g., Passive Keyless Entry and Start Systems where ranging errors of this order are acceptable. Setting PAPR lower than $4\ dB$ would result in receiver detecting noise as the leading edge, and setting it higher than $8\ dB$ prevents distinguishing the direct-path signal from noise.

As shown in Figure 5, if MPEP threshold is set too low (*e.g.,* MPEP = $5\ dB$), the receiver will discard the leading edge as noise and mistake one of the stronger multipath contributions as the leading edge and select it for ToA measurement. This would result in the measured distance being longer than the actual distance. Setting such a low threshold would make the system unusable for proximity-based applications; for example, even when a car and key are close, they would fail to

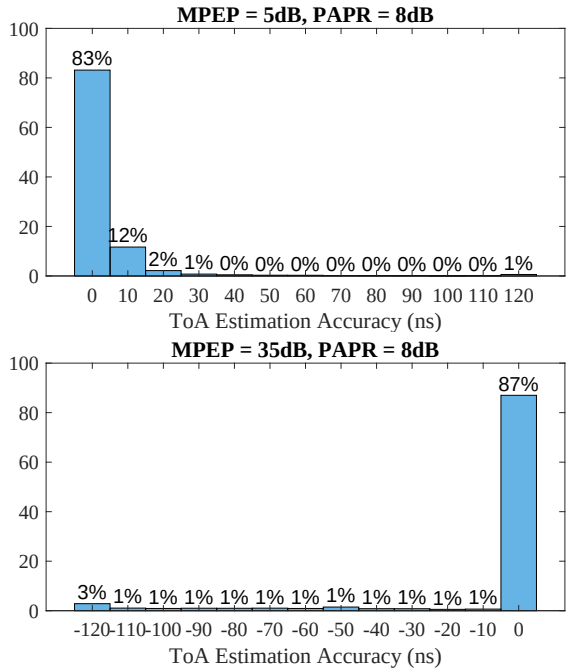

Fig. 5. Estimate ToA distribution

establish proximity for 13% of the ranging operations. On the other hand, setting it too high (*e.g.,* MPEP = $35\ dB$) would result in noise being selected as leading edge, *i.e.,* the car will perceive that the key is nearby when it is in fact far away, which of course would be a major concern.

Table II provides insight into the receiver's performance using different thresholds and under different channel conditions. Some of the threshold combinations, such as (20,4), (20,8), and (25,8), are performant under all channel conditions. In outdoor NLoS settings, our choice of the shorter backsearch time window also leads to incorrect distance measurement.

C. Security Analysis of HRP

We analyze STS and receiver design against the attacks that we describe in Section IV. We assume that the adversary can relay signals between two legitimate devices, listen to the relayed signal, and inject the signal with the different power levels. We also assume that the adversary can synchronize its transmission with the legitimate STS transmission, for example, by using the preamble of the legitimate ranging packet.

Setting attack parameters (R,K): Both attack strategies transmit attack pulses during STS transmission to inject an earlier path, *i.e.,* a peak satisfying both thresholds before the leading edge. The important parameters for injecting the attack pulses are their PRF and transmit power. An adversary does not need to adhere to the FCC and ETSI regulations, therefore, an adversary can choose an optimal value for the repetition frequency as well as transmit power.

Receiver Parameters	Channel Conditions: Residential		Office		Outdoor		Industrial	
(MPEP,PAPR)	LoS	NLos	LoS	NLos	LoS	NLos	LoS	NLos
(5 , 4)	7.07	18.99	3.05	21.72	11.8	32.89	0.32	11.91
(5 , 8)	7.07	18.99	3.05	21.72	11.8	32.9	0.32	11.91
(5 , 12)	7.07	19	3.05	21.74	11.82	33.58	0.32	11.91
(5 , 16)	7.13	19.4	3.08	22.69	12.51	35.86	0.32	13.27
(10 , 4)	1.23	3.63	0.46	3.31	2.04	13.4	0.04	0.23
(10 , 8)	1.23	3.63	0.46	3.31	2.04	13.65	0.04	0.23
(10 , 12)	1.24	3.69	0.46	3.62	2.16	16.79	0.04	0.27
(10 , 16)	1.44	5.31	0.66	7.46	4.01	24.47	0.04	2.84
(15 , 4)	0.23	0.64	0.06	0.31	0.21	8.28	0	0
(15 , 8)	0.23	0.66	0.06	0.35	0.25	8.99	0	0
(15 , 12)	0.24	0.94	0.07	1.03	0.54	13.35	0	0.05
(15 , 16)	0.59	3.19	0.37	5.91	2.9	23.07	0	2.64
(20 , 4)	0.01	0.05	0.01	0	0	7.62	0	0
(20 , 8)	0.02	0.13	0.01	0.06	0.04	8.49	0	0
(20 , 12)	0.04	0.58	0.04	0.82	0.36	13.06	0	0.05
(20 , 16)	0.44	3.05	0.36	5.86	2.8	23.04	0	2.64
(25 , 4)	0.92	1.08	0.88	0.85	1.09	9.6	0.39	1.25
(25 , 8)	0.63	0.49	0.41	0.18	0.52	8.79	0.35	0.02
(25 , 12)	0.2	0.58	0.04	0.82	0.37	13.06	0.31	0.05
(25 , 16)	0.44	3.05	0.36	5.86	2.8	23.04	0.02	2.64
(30 , 4)	35.42	19.77	24.85	7.68	22.46	21.23	44.85	4.24
(30 , 8)	16.74	3.13	5.04	0.46	4.22	9.14	41.32	0.03
(30 , 12)	0.53	0.58	0.07	0.82	0.39	13.06	9.86	0.05
(30 , 16)	0.44	3.05	0.36	5.86	2.8	23.04	0.02	2.64
(35 , 4)	55.88	25.79	35.16	8.44	29.97	22.25	92.78	4.25
(35 , 8)	18.43	3.19	5.19	0.46	4.31	9.14	69.64	0.03
(35 , 12)	0.53	0.58	0.07	0.82	0.39	13.06	9.86	0.05
(35 , 16)	0.44	3.05	0.36	5.86	2.8	23.04	0.02	2.64

TABLE II
INCORRECT DISTANCE ESTIMATION RATE (%) UNDER DIFFERENT CHANNEL CONDITION. NLOS CONDITIONS ARE MORE PRONE TO INCORRECT DISTANCE ESTIMATION. HOWEVER, CAREFUL SELECTION REDUCES THE ERROR.

For example, when the adversary uses a PRF of $124.8\ MHz$ (R = 1) and the same transmit power as legitimate signal (K = 1), this attack will increase the average noise but will produce a valid leading edge (i.e., a valid attack) only with a small probability. However, if the attacker injects fewer pulses but with a higher transmit power, for example, at R = 16 and K=32, the probability of injecting a leading edge that satisfies both thresholds MPEP and PAPR will increase. Given the thresholds, the length of the STS sequence and the channel, the attacker can therefore choose the PRF and pulse strength that maximizes the probability of the successful attack. In our simulations, we choose $R = 8$, $K = 32$.

Distance Reduction with *Cicada++ Attack*: Figure 6 shows that this attack is effective against the varied range of the receiver parameters. We do not consider the attack to be successful, if the inaccuracy in the measured distance is smaller than 7 ns. For the optimal receiver setting of (20,4), where misdetection is less than 0.96%, the attack success rate is 88.4%. As shown by Figure 7, for all receiver settings where misdetection is low ($< 1.5\%$), the attack success rate is at least 50%. Therefore, we can either achieve a reliable or secure system using STS and the given receiver design, but no receiver configuration can fulfill both requirements.

As shown in Table III, all channels are vulnerable to the *Cicada++ Attack*. However, attack success is comparatively higher for the Industrial LoS; the leading edge happens to be the strongest correlation peak, allowing a longer backsearch window to insert an earlier peak. A "clean" channel, where the leading edge is strongest, provides a performant system for multiple receiver configurations (MPEP, PAPR), but backsearch makes it more vulnerable to the distance reduction attack.

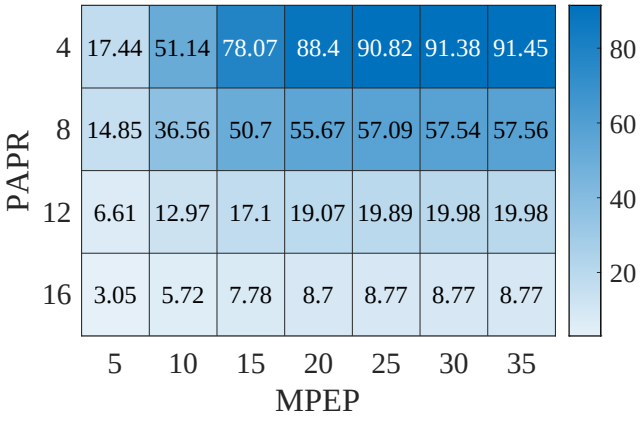

Fig. 6. Distance Reduction attack success (%) with *Cicada++ Attack*; the attack is successful if the estimated arrival time is at least $8ns$ earlier than the legitimate STS's arrival time.

Receiver Parameters	Channel Conditions: Residential		Office		Outdoor		Industrial	
(MPEP,PAPR)	LoS	NLos	LoS	NLos	LoS	NLos	LoS	NLos
(5 , 4)	16.18	17.15	16.34	17.76	15.78	16.45	19.93	19.92
(5 , 8)	16.07	16.15	15.78	13.41	14.6	12.31	19.93	10.55
(5 , 12)	11.12	5.56	7.31	1.54	5.29	1.94	19.84	0.26
(5 , 16)	2.87	0.56	1.13	0.03	0.69	0.06	19.02	0
(10 , 4)	49.31	52.13	48.23	54.56	52.06	49.71	41.75	61.37
(10 , 8)	47.54	43.11	43.32	29.98	40.66	26.46	41.75	19.69
(10 , 12)	25.43	9.93	13.32	1.98	9.05	2.35	41.44	0.27
(10 , 16)	4.89	0.62	1.29	0.03	0.8	0.06	38.05	0
(15 , 4)	79.84	80.82	78.19	82.48	82.89	71.56	63.33	85.43
(15 , 8)	73.72	59.38	63.67	35.86	56.84	31.25	63.33	21.56
(15 , 12)	32.74	11.28	15.67	2.03	10.04	2.4	62.35	0.27
(15 , 16)	5.39	0.64	1.32	0.03	0.81	0.06	53.98	0
(20 , 4)	94.11	91.86	92.67	89.66	93.8	76.68	78.78	89.66
(20 , 8)	84.02	63.18	69.74	36.46	60.04	31.63	78.69	21.63
(20 , 12)	34.47	11.46	15.9	2.03	10.07	2.4	75.99	0.27
(20 , 16)	5.42	0.64	1.32	0.03	0.81	0.06	61.31	0
(25 , 4)	96.81	93.71	95.63	90.35	95.06	77.24	87.9	89.85
(25 , 8)	85.36	63.48	70.36	36.48	60.22	31.63	87.58	21.63
(25 , 12)	34.54	11.46	15.91	2.03	10.07	2.4	82.41	0.27
(25 , 16)	5.42	0.64	1.32	0.03	0.81	0.06	61.86	0
(30 , 4)	96.99	93.83	95.79	90.4	95.15	77.27	91.78	89.85
(30 , 8)	85.42	63.48	70.36	36.48	60.22	31.63	91.07	21.63
(30 , 12)	34.54	11.46	15.91	2.03	10.07	2.4	83.15	0.27
(30 , 16)	5.42	0.64	1.32	0.03	0.81	0.06	61.86	0
(35 , 4)	97	93.83	95.79	90.4	95.15	77.27	92.31	89.85
(35 , 8)	85.42	63.48	70.36	36.48	60.22	31.63	91.29	21.63
(35 , 12)	34.54	11.46	15.91	2.03	10.07	2.4	83.15	0.27
(35 , 16)	5.42	0.64	1.32	0.03	0.81	0.06	61.86	0

TABLE III
DISTANCE REDUCTION BY *Cicada++ Attack* UNDER DIFFERENT CHANNEL CONDITIONS.

Distance Reduction with *Adaptive Injection Attack*: This adversary is capable of observing the channel impulse response that the legitimate receiver observes with respect to the legitimate and adversary's transmitter. The adversary has all the knowledge that the legitimate receiver has, therefore, an adversary can determine the correlation output at the legitimate receiver. If receiver parameters (MEMP, PAPR) are known, it can also check if the committed signal injects the peak at the intended position, *i.e.,* α ns earlier than the leading edge. This attack is more effective when a ranging packet uses multiple STS segments. As shown by Figure 8 and Figure 7, this attack strategy is comparable to *Cicada++ Attack*in generating an earlier peak, but it has higher chances of creating a peak at an intended position[3]. Table IV compares the success rates of the *Cicada++ Attack* and *Adaptive Injection Attack*, for the receiver threshold (20,8) and for different values of α and allowed measurement error e. *Adaptive Injection Attack*achieves a higher success rate in injecting a peak at the intended position. For example, when injecting a peak 100ns earlier than the leading edge and the required precision is 4ns, the success rate is 6.15% and 14.21% for the *Cicada++ Attack* and *Adaptive Injection Attack*, respectively.

[3]Each value is computed over 1600 different channels for the legitimate and attack signal

	Cicada++			Adaptive Injection		
	$e=4$	$e=8$	$e=12$	$e=4$	$e=8$	$e=12$
$\alpha=25\ ns$	0.54	0.95	1.49	2.65	3.03	7.07
$\alpha=50\ ns$	1.55	2.91	4.68	5.29	9.26	14.95
$\alpha=100\ ns$	**6.15**	12.66	17.34	**14.21**	24.85	29.44

TABLE IV
ATTACK SUCCESS RATE FOR INJECTING A PEAK $\alpha \pm e\ ns$ EARLIER THAN THE LEADING EDGE FOR THE RECEIVER PARAMETER (20,8).

VI. RELATED WORK

Undoubtedly, one of the main uses of UWB is secure distance bounding. An extensive survey on secure distance bounding in the wireless domain can be found in [12]. UWB is considered to be particularly useful for distance bounding due to the introduction of a distance commitment (in the form of a preamble) that determines the time-of-arrival (ToA) as well as the arrival time of the subsequent data symbols [28]. Even though it is straightforward to advance the preamble for an attacker, doing so also advances the time at which the receiver expects the data bits which are unknown to an external adversary, e.g., in a challenge-response type of distance bounding protocol.

Such mechanisms are, however, not mentioned by the standard for HRP mode of UWB and since ToA is purely based

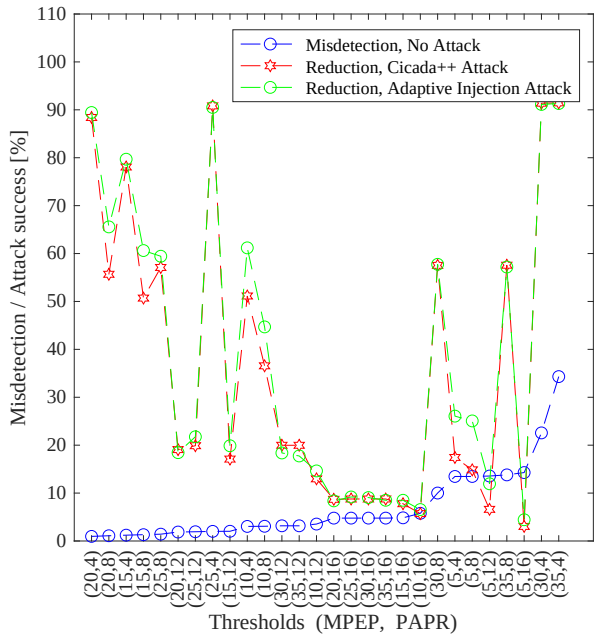

Fig. 7. The different choices of thresholds can provide either a secure or performant system. In scenarios where chances of attack success are low (*e.g.,* MPEP $= 5\ dB$), the system has a higher likelihood of providing inaccurate distance measurement. $(10, 16)$ is the optimal choice where security and performance balance out. However, misdetection and attack success are higher than 5%, which is unacceptable for many systems.

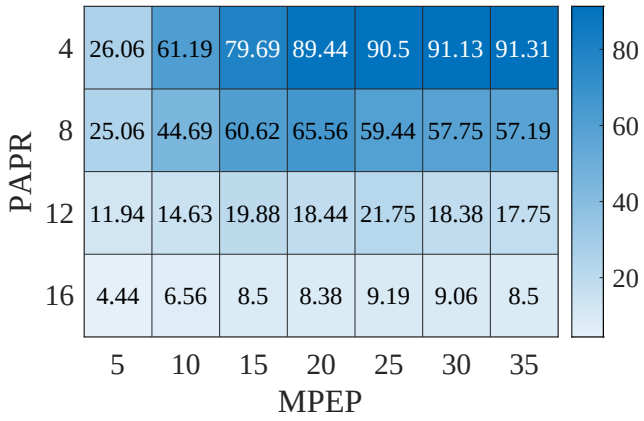

Fig. 8. Distance Reduction attack success (%) with *Adaptive Injection Attack*; the attack is successful if the estimated arrival time is at least $8ns$ earlier than the legitimate STS's arrival time.

on STS, security hinges on leading edge detection, which, if it just searches for the "first arriving path", is susceptible to cicada attacks. The original Cicada attack presented in [24] can be considered as the first systematic attack against time-of-flight (ToF) based ranging systems and, in particular, UWB-IR ranging. The cicada attack was enhanced to a "coded" version in [25] where the amplitude of pulses is adapted with a non-constant code. The simplicity and effectiveness of those attacks made it apparent that the leading edge detection is a crucial component of any ToF system, which is especially true for modulation schemes that experience inter-symbol interference, such as HRP mode of IEEE 802.15.4z. Although currently not a concern for most UWB-ranging systems, the research community has also started to focus on enlargement attacks that aim to increase the measured distance. The work in [15] assesses different ToA estimation algorithms, including back-search leading edge detection, when subjected to signal overshadowing attacks that cause distance enlargement.

Recently, the research community has suggested the term Message Time of Arrival Codes (MTAC) as a theoretical notion for secure distance estimation and ranging based on ToF measurements [22]. A ranging system is deemed secure if it can provide secure MTAC construction: physical-layer message codes that allow the receiver to verify the message time of arrival securely. If we try to understand IEEE 802.15.4z/HRP ranging from the perspective of the MTAC framework, we can consider the generation of STS as the code-generation algorithm *Mtac* and cross-correlation with leading edge detection to be the verification algorithm *Vrfy* that performs verification of the contents of the STS as well as time-selective detection.

VII. Conclusion

To the best of our knowledge, this is the first open analysis of the security of IEEE 802.15.4z HRP. Our analysis shows that securing HRP ranging presents some hard tradeoffs between security and ranging performance. Since HRP implementations deployed by the industry are closed source, it is unclear what kind of tradeoffs those implementations made. More research into deployed HRP chips is needed to test if they deploy proper countermeasures and to assess their security level.

VIII. Acknowledgements

This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation program under grant agreement No 726227.

References

[1] Apple U1 UWBChip, howpublished="https://support.apple.com/guide/security/ultra-wideband-security-sec1e6108efd/web". [Online; Accessed 24. March 2021].
[2] IEEE Standarads Association Documents. https://https://mentor.ieee.org/802.15/documents/. [online; Accessed 18. March 2021].
[3] Introduction to Impulse Radio UWB Seamless Access Systems. https://www.firaconsortium.org/sites/default/files/2020-04/fira-introduction-impulse-radio-uwb-wp-en.pdf. [online; Accessed 22. March 2021].
[4] LRP deployment in automotive. https://www.3db-access.com/article/18. [Online; Accessed 25. March 2021].
[5] Microchip ATA8532. https://www.microchip.com/wwwproducts/en/ATA8352. [Online; Accessed 25. March 2021].
[6] NXP Trimension. https://www.nxp.com/docs/en/fact-sheet/UWB-IOT-FS.pdf. [Online; Accessed 25. March 2021].
[7] SamsungUWB. https://news.samsung.com/global/samsung-expects-uwb-to-be-one-of-the-next-big-wireless-technologies/. [Online; Accessed 24. March 2021].

[8] UWB Social Distancing. https://www.uwb-social-distancing.com/. [Online; Accessed 22. March 2021].

[9] UWB Social Distancing Meeblue. https://www.meeblue.com/blogs/UWB_For_Social_Alert/. [online; Accessed 20. March 2021].

[10] Volkswagen UWB PKES. https://www.volkswagen-newsroom.com/en/stories/realtime-safety-with-uwb-5438. [Online; Accessed 20. March 2021].

[11] Ieee standard for low-rate wireless networks–amendment 1: Enhanced ultra wideband (uwb) physical layers (phys) and associated ranging techniques. *IEEE Std 802.15.4z-2020 (Amendment to IEEE Std 802.15.4-2020)* (2020), 1–174.

[12] AVOINE, G., BINGÖL, M. A., BOUREANU, I., ČAPKUN, S., HANCKE, G., KARDAŞ, S., KIM, C. H., LAURADOUX, C., MARTIN, B., MUNILLA, J., ET AL. Security of distance-bounding: A survey. *ACM Computing Surveys (CSUR) 51*, 5 (2018), 1–33.

[13] BAHL, P., AND PADMANABHAN, V. N. Radar: An in-building rf-based user location and tracking system. In *Proceedings IEEE INFOCOM 2000. Conference on computer communications. Nineteenth annual joint conference of the IEEE computer and communications societies (Cat. No. 00CH37064)* (2000), vol. 2, Ieee, pp. 775–784.

[14] BOUREANU, I., MITROKOTSA, A., AND VAUDENAY, S. Towards secure distance bounding. In *International Workshop on Fast Software Encryption* (2013), Springer, pp. 55–67.

[15] COMPAGNO, A., CONTI, M., D'AMICO, A. A., DINI, G., PERAZZO, P., AND TAPONECCO, L. Modeling enlargement attacks against uwb distance bounding protocols. *IEEE Transactions on Information Forensics and Security 11*, 7 (2016), 1565–1577.

[16] FLURY, M., POTURALSKI, M., PAPADIMITRATOS, P., HUBAUX, J.-P., AND LE BOUDEC, J.-Y. Effectiveness of distance-decreasing attacks against impulse radio ranging. In *Proceedings of the third ACM conference on Wireless network security* (2010), pp. 117–128.

[17] GOLDEN, S. A., AND BATEMAN, S. S. Sensor measurements for wi-fi location with emphasis on time-of-arrival ranging. *IEEE Transactions on Mobile Computing 6*, 10 (2007), 1185–1198.

[18] GUVENC, I., AND SAHINOGLU, Z. Threshold-based toa estimation for impulse radio uwb systems. In *2005 IEEE International Conference on Ultra-Wideband* (2005), IEEE, pp. 420–425.

[19] GUVENC, I., AND SAHINOGLU, Z. Threshold-based toa estimation for impulse radio uwb systems. In *2005 IEEE International Conference on Ultra-Wideband* (2005), pp. 420–425.

[20] HUO, K., DENG, B., LIU, Y., JIANG, W., AND MAO, J. High resolution range profile analysis based on multicarrier phase-coded waveforms of ofdm radar. *Journal of Systems Engineering and Electronics 22*, 3 (2011), 421–427.

[21] HYMANS, A., AND LAIT, J. Analysis of a frequency-modulated continuous-wave ranging system. *Proceedings of the IEE-Part B: electronic and communication engineering 107*, 34 (1960), 365–372.

[22] LEU, P., SINGH, M., ROESCHLIN, M., PATERSON, K. G., AND ČAPKUN, S. Message time of arrival codes: A fundamental primitive for secure distance measurement. In *2020 IEEE Symposium on Security and Privacy (SP)* (2020), IEEE, pp. 500–516.

[23] MOLISCH, A. F., BALAKRISHNAN, K., CHONG, C.-C., EMAMI, S., FORT, A., KAREDAL, J., KUNISCH, J., SCHANTZ, H., SCHUSTER, U., AND SIWIAK, K. Ieee 802.15. 4a channel model-final report. *IEEE P802 15*, 04 (2004), 0662.

[24] POTURALSKI, M., FLURY, M., PAPADIMITRATOS, P., HUBAUX, J.-P., AND LE BOUDEC, J.-Y. Distance bounding with ieee 802.15. 4a: Attacks and countermeasures. *IEEE Transactions on Wireless Communications 10*, 4 (2011), 1334–1344.

[25] POTURALSKI, M., FLURY, M., PAPADIMITRATOS, P., HUBAUX, J.-P., AND LE BOUDEC, J.-Y. On secure and precise ir-uwb ranging. *IEEE transactions on wireless communications 11*, 3 (2012), 1087–1099.

[26] SHARP, I., YU, K., AND GUO, Y. J. Peak and leading edge detection for time-of-arrival estimation in band-limited positioning systems. *IET communications 3*, 10 (2009), 1616–1627.

[27] SINGH, M., LEU, P., AND CAPKUN, S. Uwb with pulse reordering: Securing ranging against relay and physical-layer attacks. In *NDSS* (2019).

[28] TIPPENHAUER, N. O., LUECKEN, H., KUHN, M., AND CAPKUN, S. Uwb rapid-bit-exchange system for distance bounding. In *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks* (2015), pp. 1–12.

[29] VASISHT, D., KUMAR, S., AND KATABI, D. Decimeter-level localization with a single wifi access point. In *13th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 16)* (2016), pp. 165–178.

[30] YU, C.-S. Factors affecting individuals to adopt mobile banking: Empirical evidence from the utaut model. *Journal of Electronic Commerce Research 13* (01 2012), 104–121.