Secure, Accurate, and Practical Narrow-Band Ranging System

Aysajan Abidin[1], Mohieddine El Soussi[2], Jac Romme[2], Pepijn Boer[2], Dave Singelée[1] and Christian Bachmann[2]

[1] KU Leuven, imec-COSIC, Belgium, firstname.lastname@esat.kuleuven.be
[2] imec, The Netherlands, firstname.lastname@imec.nl

Abstract. Relay attacks pose a serious security threat to wireless systems, such as, contactless payment systems, keyless entry systems, or smart access control systems. Distance bounding protocols, which allow an entity to not only authenticate another entity but also determine whether it is physically close by, effectively mitigate relay attacks. However, secure implementation of distance bounding protocols, especially of the time critical challenge-response phase, has been a challenging task. In this paper, we design and implement a secure and accurate distance bounding protocol based on Narrow-Band signals, such as Bluetooth Low Energy (BLE), to particularly mitigate relay attacks. Narrow-Band ranging, specifically, phase-based ranging, enables accurate distance measurement, but it is vulnerable to phase rollover attacks. In our solution, we mitigate phase rollover attacks by also measuring time-of-flight (ToF) to detect the delay introduced by such attacks. Therefore, our protocol effectively combines the best of both worlds: phase-based ranging for accuracy and time-of-flight (ToF) measurement for security. To demonstrate the feasibility and practicality of our solution, we prototype it on NXP KW36 BLE chips and evaluate its performance and relay attack resistance. The obtained precision and accuracy of the presented ranging solution are 2.5 cm and 30 cm, respectively, in wireless measurements.

Keywords: Distance Bounding; Relay Attacks; Narrow-Band Ranging; Phase-based Ranging; Time of Flight.

1 Introduction

The proliferation of internet connected devices, such as, Internet of Things, has made accurate ranging become increasingly popular and important in many real-life applications. Accurate ranging, or rather determining accurately an upper-bound on the physical distance between devices, is important in applications, such as, keyless entry systems, contactless payment systems, and smart access control systems, to name just a few. However, relay attacks against these applications have been successfully demonstrated to bypass ranging solutions [Han06, DM07, FHMM10, FDC11]. Indeed, relay attacks pose a serious security threat, and protection against them is critical.

Distance bounding (DB) protocols offer an effective countermeasure against relay attacks. Ever since Brands and Chaum introduced a DB protocol in [BC93] to counter relay attacks on Automatic Teller Machines systems, many other DB protocols have been proposed and implemented [HK05, Tv09, Rv10, SP07, RTŠ+12, RCHBC09, RDC15]. DB protocols allow to establish an upper-bound on the physical distance between two parties which are typically denoted as verifier and prover, by combining physical layer measurements and cryptography.

There are two main families of DB protocols in the literature: those that are derived from the first protocol proposed by Brands and Chaum [BC93] and the ones that are based on the protocol proposed by Hancke and Kuhn [HK05]. All DB protocols have a *setup* and a *rapid-bit exchange stage*. In the setup stage, the verifier and the prover agree or commit to some information that will be used in the next protocol stage(s). In the rapid-bit exchange stage, which is the most difficult stage to implement securely due to severe timing constraints, the verifier sends a series of single-bit challenges to which the prover replies with single-bit responses. The verifier can then calculate its distance to the prover by measuring the Round-Trip Time (RTT) between sending its challenge and receiving the response from the prover. In some DB protocols, specially those derived from Brands and Chaum's DB protocol, there is also a *verification stage* for checking that all protocol steps were performed using the parameters previously agreed upon.

Secure implementation of DB protocols that provides accurate distance measurement is a big challenge. One simple approach to distance measurement is the use of received signal strength. But signal strength based solutions are vulnerable to manipulation, by simply amplifying the signal as shown in [DM07, FHMM10, FDC11]. Therefore, DB implementations to date rely on Time of Flight (ToF) measurement of challenge and response bits exchanged between a verifier and a prover [HK05, Tv09, Rv10, TLKC15], mostly using UWB 802.15.4 radios. UWB, however, is not the only technology which is capable of delivering secure high-accuracy distance measurements. Accurate distance measurement can also be achieved using Narrow-Band radio technology, such as, Bluetooth Low Energy (BLE) using signals' phase information [ZRG+19, BRGD20]. However, phase-based ranging solutions are also vulnerable to manipulation, such as, phase slope rollover attacks, as pointed out by Ólafsdóttir, Ranganathan, and Capkun in [ORC17]. It is worth mentioning, though, that phase manipulation attacks are more difficult to execute in practice, due to the typical wide radiation-pattern of antennae and reflections in the propagation path of radio signals (multipath). The authors of [ORC17] briefly suggest ToF measurements as a mitigation to phase manipulation attacks without further details. Here, we design a complete secure ranging system combining ToF and phase-based ranging, thoroughly analyse the security, and implement the whole system. To the best of our knowledge, there has not been any Narrow-Band based accurate DB implementation that is secure against both logical- and physical-layer attacks.

There is a big demand for secure Narrow-Band ranging, specifically on secure BLE based ranging, since BLE is widely available in consumer devices. The choice for BLE is also prompted by the fact that wireless applications, such as, passive keyless entry systems, contactless payment systems, and smart access control, etc., often need to be ultra-low power and low-cost.

Therefore, the main focus of this paper is on practical relay attack mitigation with an accurate and secure BLE compatible ranging.

1.1 Our Contributions

In this paper, we design and implement a BLE compatible secure and accurate distance bounding protocol based on Narrow-Band signals. Our specific contributions are as follows.

- We design a secure ranging solution for Narrow-Band systems by using ToF as a coarse secure distance measurement that acts as a confidence interval for the accurate insecure phase-based distance measurement. We use the ToF measurements in combination with the phase measurements to detect phase manipulation attacks, such as, phase slope rollover attacks.

- We provide a detailed analysis of security of our solution against impersonation and relay attacks on the protocol, as well as the state-of-the-art physical-layer attacks.

- We implement the designed Narrow-Band secure ranging solution on NXP KW36 BLE chips and evaluate its performance. The obtained precision of the phase-based ranging and ToF solution is 2.5 cm and 1.6 m, respectively, while the accuracy is 30 cm and 2 m, respectively.

We stress that although Ólafsdóttir, Ranganathan, and Capkun in [ORC17] briefly suggest to use ToF measurements to mitigate phase manipulation attacks without further details, our protocol is the first concrete secure Narrow-Band ranging protocol combining ToF and phase-based ranging, with a full prototype implementation demonstrating high accuracy and relay attack resilience.

1.2 Overview of our protocol

The designed solution estimates the distance combining two methods: ToF that gives coarse distance estimation, and phase information that gives precise distance estimation. ToF is estimated by measuring the time-of-arrival and time-of-departure of exchanged packets containing pseudorandom bits. Phase information is obtained by measuring the in-phase and quadrature (I/Q) components of continuous Constant Tone (CT) signals. While ToF provides security against physical-layer attacks, phase-based ranging provides high accuracy. Hence, we combine the best of two worlds.

At a high level, our secure distance bounding (SDB) protocol comprises three stages: (1) authenticated key exchange (AKE), (2) distance bounding (DB), and (3) authentication and authorisation.

In the first stage, the communicating parties, namely, a verifier and a prover, employ an AKE protocol, for which we use the SIGMA-protocol by Krawczyk [Kra03], to establish a shared secret session key.

In the second stage, a phase-based narrow-band ranging solution, in combination with time-of-flight solution, is employed to securely estimate the accurate distance between the prover and the verifier. In particular, the verifier and prover engage in low-level challenge and response exchanges. The following steps are repeated N times using N different channels (Cf. Section 3 and 4.2 for details).

- The verifier sends to the prover a challenge packet, comprising preamble, Frame delimiter (FD), Protocol Data Unit (PDU) and Cyclic Redundancy Check (CRC), and a CT signal, and records a time of departure (ToD_V) for the packet. FD in the challenge packet is a pseudorandom sequence generated using the session key and is unique for each challenge.

- Upon receiving the challenge, the prover correlates the received FD with the expected FD to synchronize (using the resulting peak in the correlation) and to estimate the time of arrival (ToA_P), and then after synchronization all the bits in FD are checked to see if they are correct. If FD is correct, the prover records 1; otherwise, it records 0. In addition, the prover measures I/Q of CT signal. Now the prover sends to the verifier a response packet, which in this case comprises a CT signal followed by preamble, FD, PDU and CRC, and records a time of departure (ToD_P) for the response. FD in the response packet is also a pseudorandom sequence generated using the session key and is unique for each response.

- Upon receiving the response, the verifier measures I/Q of CT signal, correlates the received FD with the expected FD to synchronise (again using the resulting peak) and to estimate the ToA_V, and after synchronisation all bits of FD are checked for correctness. If the received FD is correct, verifier records 1; otherwise, it records 0.

In the last stage, the protocol continues as follows.

- The prover sends all estimated ToA_P and ToD_P values, bits indicating whether the received FDs in the challenge packets are correct, and the measured I/Q values to the verifier encrypted using the session key.

- Upon receiving the prover's message, the verifier decrypts it and proceeds as follows:

  - For each of the N rounds, it first calculates $\text{ToF} = \frac{1}{2}(\text{ToA}_V - \text{ToD}_V - \text{ToD}_P + \text{ToA}_P)$.
  - It then eliminates the challenge-response rounds in which any one of the following is true: (1) the received challenge FD is incorrect (according to the prover's message), (2) received response FD is incorrect (according to its own local records), and (3) the calculated ToFs are less than a predefined security threshold, needed to prevent phase slope rollover attacks on the I/Q measurements.
  - If the number N' of remaining rounds is below a threshold τ_{rounds}, it aborts. Otherwise, it calculates the average $\overline{\text{ToF}}$ for the N' rounds.
  - If $\overline{\text{ToF}}$ is less than yet another security threshold, needed for assurance that phase-based distance estimation can be trusted, then the verifier calculates the accurate distance $d_{\text{I/Q}}$ using the measured I/Q values. Otherwise, it aborts.
  - Finally, the verifier authorises the prover if $d_{\text{I/Q}} \leq d_{\text{access}}$, where d_{access} is the upper-bound for the distance within which the prover can access the verifier.

1.3 Related work

The first countermeasure against relay attacks (a.k.a., mafia fraud) was suggested in [BD90, BBD+91], where the authors introduced the concept of distance bounding (DB) based on the measurement of the round trip time (RTT) of exchanged messages. In 1993, Brands and Chaum [BC93] proposed the first distance bounding protocol based on the ideas presented in [BD90, BBD+91] in order to mitigate relay attacks. Since then, numerous DB protocols have been proposed in the literature [HK05, Tv09, Rv10, SP07, RTŠ+12, RCHBC09, RDC15, BMV14, BMV15, KAK+08, MP08, DM07]; see the recent survey [ABB+19], and the references therein, for more information on DB protocols.

There has also been efforts to implement DB solutions, but to date, all known implementations rely on ToF measurement of challenge and response between a verifier and a prover [HK05, Tv09, Rv10, TLKC15], mostly using UWB 802.15.4 radios. Since most wireless applications require ultra-low power and low-cost radios, Narrow-Band (or Bluetooth Low Energy) based solutions would be a good practical choice. To the best of our knowledge, there exists only [ORC17] in the literature discussing the security of carrier phase-based Narrow-Band ranging. As such, Narrow-Band based secure ranging has remained a challenge. In this paper we fill this gap, and design and implement the first Bluetooth DB protocol secure against relay attacks.

1.4 Outline

The rest of the paper is organised as follows. After introducing background materials on distance bounding protocols and various attacks on them in Section 2, we present our system model, where we describe the structure of frame formats for challenge and response packets, and attacker model in Section 3. Next, we present our protocol in Section 4 and its security analysis in Section 5. Section 6 presents the performance analysis of our solution in terms of false acceptance and false rejection rates. In Section 7, results from the evaluation of the designed solution are presented. Finally, we conclude the paper in Section 8.

2 Background

This section introduces different ranging techniques, DB protocols and various attacks on them.

2.1 Radio-based Ranging Techniques

There are various radio-based ranging principles that have been studied in the literature. These include:

- Time-of-flight (ToF): The most direct approach to Radio Frequency (RF)-based ranging estimates ToF [GTG+05], i.e., propagation time, and multiplies it by the speed of light to obtain the distance. Such systems often use ultra-wideband radios since time resolution is inversely proportional to the radio bandwidth, and hence the ToF can be measured at a fine-grained resolution with sub-nanosecond accuracy.

- Received Signal Strength (RSS): Another approach to estimate the distance between two entities is to use the RSS [Mau12]. This is a very simple and popular approach due to its low complexity and ready availability. However, it has a low accuracy in non-line-of-sight and multipath environment, and it has a low security since it can easily be spoofed.

- Phase difference: Phase difference measurement is a new approach that was recently introduced to estimate the distance between two nodes in Bluetooth Low Energy (BLE) [ZRG+19] and ZigBee networks [RS15, Rap15]. The phase shift of the reflected signal from the target node due to the time delay between the target and transmitter is used to measure the distance between them. In pure Line-of-Sight (LoS) conditions, the phase shift introduced by the radio channel is a linear function of both frequency and distance. Hence, by measuring the phase, one can estimate the distance between two entities.

The above described ranging techniques are vulnerable to relay attacks, which can be effectively mitigated by using DB protocols.

2.2 Distance bounding protocols

DB is essentially adding authentication to ranging, and was initially proposed as an effective countermeasure against relay attacks. Here we look at the first distance bounding protocol proposed by Brands and Chaum in [BC93]. It comprises three stages: an initialization stage, a DB stage and a verification stage. The verifier V and the prover P share a secret key K. In the *initialisation stage*, the prover selects uniformly at random a nonce N_P composed of n bits and sends a commitment $\gamma_p \leftarrow \mathsf{commit}(N_p)$ to the verifier V. In each of the rounds of the DB stage (composed of n rounds), the verifier V starts the clock and sends random challenges $c_i \in \{0,1\}$ to the prover P, while P responds by $r_i = c_i \oplus (N_P)_i$. As soon as V receives the response r_i he stops the clock. In the *verification stage*, the prover P sends the verifier V the opened commitment, $\mathsf{open}(\gamma_p)$, along with message authentication code $\mathsf{MAC}_K(m)$ of a message m composed of the concatenated values c_i and r_i exchanged during the DB stage (i.e. $m \leftarrow c_1||r_1||\ldots||c_n||r_n$). Then, V verifies all the received information. If the verification succeeds, V computes an upper bound on the distance of P based on the clock difference obtained during each of the rounds of the DB stage.

2.3 Attacks on Distance Bounding Protocols

Attacks on DB protocols can be categorised as generic attacks such as, impersonation attack, distance fraud, relay attack, and terrorist fraud; and physical-layer attacks. Since our primary goal is to mitigate relay attacks, we focus on the most relevant logical- and physical-layer attacks, and exclude attacks, such as, distance fraud and terrorist fraud, by a dishonest prover. We refer to Section 4 and 5 for more details on the protocol and security analysis.

- *Impersonation attack:* In this attack, an adversary purports to be a legitimate prover.
- *Relay attack:* This attack involves an honest prover, a verifier and a Man-In-The-Middle (MITM) adversary. More specifically, the adversary uses a proxy-prover close to the verifier and a proxy-verifier close to the legitimate prover to relay over a long distance the messages exchanged between both parties [Des88].
- *Early-Detect Late-Commit attack:* This attack targets the ToF estimation [HK08]. In this attack, the adversary learns the symbol polarity early and commits to the polarity late in order to cause an early signal time of arrival at the receivers. The maximum distance that the adversary can decrease with this attack depends on, among others, the Signal-to-Noise Ratio (SNR), the pulse shaping filter, the processing time at the adversary and the decoding method.
- *Phase manipulation attack [ORC17]:* This can be any attack that manipulates the phase of the signal to reduce the estimated distance, e.g., phase slope rollover attack, on-the-fly phase manipulation attack and tone generation attack. These attacks only affect the phase and not the time.
  - In *phase slope rollover attack*, the adversary delays the signals with a fixed time delay such that the measured phase difference between the signals reaches its maximum value of 2π and rollover.
  - In *on-the-fly phase manipulation attack*, the adversary manipulates in real time the phase of the signals by mixing them with a special signal which results in an appropriate phase difference at the verifier/prover and, hence decreasing the estimated distance. In order to successfully manipulate the phase, the adversary must have a priori knowledge of the initial phase of the verifier/prover and the distance between the adversary and the nodes.
  - In *tone generation attack*, the adversary generates and then transmits his own strong signals to both the verifier and the prover. Also, in this attack in order to successfully decrease the estimated distance, the adversary must have a priori knowledge of the initial phase of the verifier/prover and the distance between the adversary and the nodes.

3 System and Attacker Model

In this section, we describe the system model and the packet format that is proposed for securely estimating the range between two nodes, and also the attacker model.

3.1 System Model

The system under consideration consists of two nodes, verifier and prover, communicating with each other. The communication can be done using any narrow-band system, e.g., Bluetooth, BLE, IEEE 802.15.4, and wide-band system, e.g., IEEE 802.11. The system is half-duplex and independent of the modulation scheme. In this paper, we focus on

narrow-band system, especially Bluetooth since this technology enables ultra-low power (ULP) and low-cost wireless functionality, and provides a vast commercial ecosystem including broad availability in smart devices. Hence, it is a key technology for future secure proximity solutions.

In order to estimate the range, Two-Way Ranging (TWR) [LZP11] is considered. The proposed frame format for secure ranging, shown in Fig. 1, is composed of a typical BLE packet that consists of preamble, FD or access address, PDU and CRC, and a CT signal, which can be attached at the beginning or at the end of the packet (the location of the CT signal depends on the transmission direction, i.e., from verifier to prover or from prover to verifier). We should note that the latest BLE release already includes a constant tone extension added to the end of packet and is used for direction finding [Woo19].

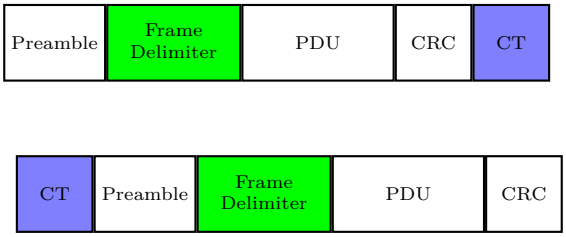

Figure 1: Frame format description. Top: from verifier to prover. Below: from prover to verifier.

The Preamble is used to detect the signal, to set the automatic gain control value and to estimate the carrier frequency offset. The FD contains a pseudo-random sequence that is only known by the verifier and the prover and is used for three purposes: 1) to synchronize, 2) to estimate the Time of Arrival (ToA), and 3) to authenticate the packet. The PDU can contain some data and the CT signal is used to estimate the accurate distance by measuring its phase. In the 2.4 GHz ISM band, the total bandwidth is 80 MHz, which can be divided into 40/80/160 channels with channel spacing of 2 MHz/1 MHz/0.5 MHz, respectively. In order to estimate the distance between the two nodes, N frames will be exchanged between the two nodes using N channels, where $N \in \{40, 80, 160\}$ is the number of channels depending on the used bandwidth. This improves the range accuracy and mitigates the effect of multi-path especially in an indoor environment. It gives the illusion of a wide-band radio using a narrow-band radio. A typical BLE packet uses Gaussian Frequency Shift Key (GFSK) modulation with bandwidth-bit period product $BT = 0.5$ (where B is the -3 dB (half-power) bandwidth of the pulse/filter and T is the symbol duration) and a modulation index (instantaneous frequency deviation from the carrier divided by one half the symbol rate) between 0.45 and 0.55. This applies to the preamble, FD, PDU and CRC part of the proposed frame. The CT is an unmodulated carrier.

3.2 Attacker Model

Here we present our assumptions regarding the three entities involved, namely, a verifier, a prover, and an attacker.

The verifier is always assumed to be trusted and not compromised during a relay attack. The prover is *honest* and far away from the verifier. The adversary comprises two devices: one located close to the verifier, one located far away from the verifier but close to the prover. We assume that the attacker controls the communication channel between the verifier and the prover. In addition, no restriction is imposed on the attacker's ability to perform physical-layer attacks to reduce the distance, except that it cannot transmit any information faster than the speed of light. We note that we only consider attacks

on the RF channel. Side-channel attacks utilising, e.g., side-channel emissions from the transmitter, are beyond the scope of this paper.

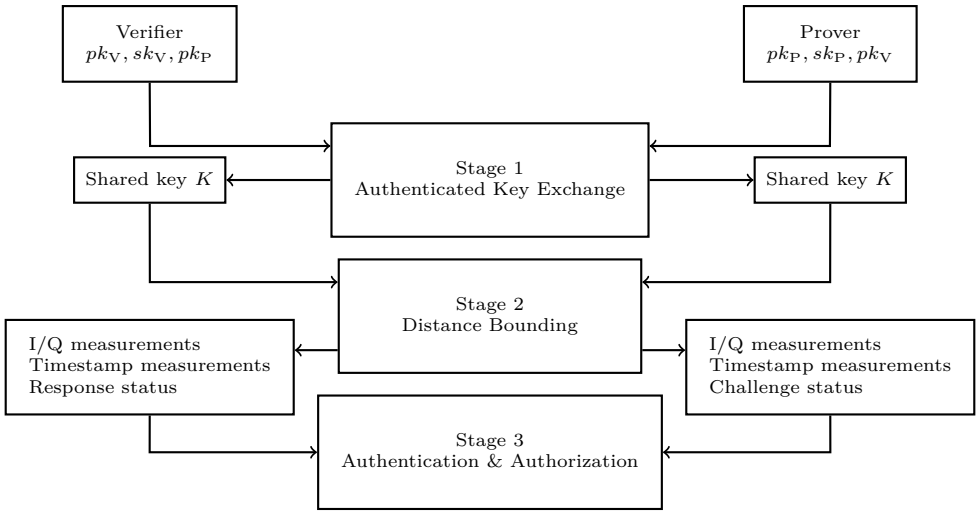

Figure 2: A high level overview of the SDB protocol proposed in this paper.

4 The protocol

Here we present our secure distance bounding (SDB) protocol. In our SDB protocol, the verifier and the prover are assumed to possess each other's public keys. That means that the verifier has its own public-private key pair and the public key of the prover, and the prover has its own public-private key pair and the public key of the verifier. We should note that the SDB protocol starts after the two nodes establish a connection and agree on performing range estimation. The SDB protocol comprises the following three stages:

- Stage 1: Authenticated key exchange (AKE) – in this stage, the verifier and the prover agree on a secret session key.
- Stage 2: Distance bounding stage – in this stage, the verifier and the prover exchange of packets and tones which are used to measure ToF and the amplitude and phase of the tone signal or I/Q components (In-phase and quadrature components). The measured ToF and I/Q values allow the verifier to calculate the distance of the prover to itself.
- Stage 3: Authentication and authorization stage – in this last stage, the prover sends its measurement results, encrypted with the shared session key, to the verifier, which then makes a decision based on the measurement results.

A high level overview of our proposed SDB protocol is summarised in Fig. 2. Next we describe the three stages in detail.

4.1 Authenticated key exchange stage

For the authenticated key exchange stage, we make use of the SIGMA protocol [Kra03], although other secure protocols for key exchange providing mutual authentication can also be chosen in practice. The SIGMA protocol is an authenticated Diffie-Hellman

key exchange providing mutual authentication. The goal of this stage is to generate a shared session key, with which the prover and verifier generate random sequences, namely, the Frame Delimiters (FDs), to be used later in the distance bounding stage. Both the verifier's and the prover's public-private key pairs are denoted by $(pk_{\mathrm{V}}, sk_{\mathrm{V}})$ and $(pk_{\mathrm{P}}, sk_{\mathrm{P}})$, respectively. So the prover has $(pk_{\mathrm{P}}, sk_{\mathrm{P}}, pk_{\mathrm{V}})$, while the verifier has $(pk_{\mathrm{V}}, sk_{\mathrm{V}}, pk_{\mathrm{P}})$. The SIGMA protocol is depicted in Fig. 3. In the figure, q is a prime and Z_q^* is the multiplicative modulo q, and $\xleftarrow{U}$ denotes a random selection. As we can see from the figure, in the SIGMA protocol, the ephemeral Diffie-Hellman keys, g^x and g^y, are combined in a Key Derivation Function (KDF) to generate the shared key $K = \mathrm{KDF}(g^{xy})$. The main goals of a KDF here are to guarantee a uniform distribution of keys, specially in the security proof, and destroy homomorphisms. The authentication of the parties follows from the signatures on the ephemeral Diffie-Hellman key shares generated using the prover's and verifier's long term private keys, sk_{P} and sk_{V}. The Message Authentication Code (MAC) on the identity (i.e., the public keys) of the parties provides mutual key confirmation.

Verifier		Prover
$pk_{\mathrm{V}}, sk_{\mathrm{V}}, pk_{\mathrm{P}}$		$pk_{\mathrm{P}}, sk_{\mathrm{P}}, pk_{\mathrm{V}}$
$y \xleftarrow{U} Z_q^*$, q is a prime	$\xleftarrow{g^x}$	$x \xleftarrow{U} Z_q^*$, q is a prime
$K = \mathrm{KDF}(g^{xy})$		
$\sigma_{\mathrm{V}} = \mathrm{sign}_{sk_{\mathrm{V}}}(g^x, g^y)$		
$t_{\mathrm{V}} = \mathrm{MAC}_K(pk_{\mathrm{V}})$	$\xrightarrow{g^y,\ \sigma_{\mathrm{V}},\ t_{\mathrm{V}}}$	Verify σ_{V}
		$K = \mathrm{KDF}(g^{xy})$
		Verify t_{V}
		$\sigma_{\mathrm{P}} = \mathrm{sign}_{sk_{\mathrm{P}}}(g^y, g^x)$
Verify σ_{P} and t_{P}	$\xleftarrow{\sigma_{\mathrm{P}},\ t_{\mathrm{P}}}$	$t_{\mathrm{P}} = \mathrm{MAC}_K(pk_{\mathrm{P}})$

Figure 3: Authenticated key exchange – the SIGMA protocol [Kra03].

For the security properties and corresponding proofs of the SIGMA protocol we refer to [CK01, CK02].

4.2 Distance bounding stage

During the DB stage, the verifier and prover exchange N frames using N channels in N consecutive rounds as shown in Fig. 4, where Ch_i and Rsp_i stand for challenge and response, respectively, for Channel $i = 1, 2, \cdots, N$. The tone signals are used to accurately estimate the distance based on the Multi-Carrier Phase Difference (MCPD) method [ZRG+19], and packets are used to securely measure and estimate the ToF. In the propose scheme, multiple channels are used in order to improve the range accuracy and mitigate the effect of multi-path especially in an indoor environment. During ranging, PDU can be empty to reduce the packet length.

MCPD method. In MCPD method, the prover measures the phase difference between its local oscillator and the received tone signal without modifying the phase and then transmits back a signal that has a phase that depends solely on its local oscillator. The verifier then measures the phase difference between its local oscillator and the received tone signal. Then, one of the nodes, typically the prover, sends his measurements (in the last stage of the proposed SDB protocol) to the other node which estimates the range using all the measurements obtained on all the channels. Hence the estimate for the range

can be written as,

$$\hat{r} = -\frac{c}{4\pi\Delta_f}\hat{\Delta}_\phi \mod \frac{c}{2\Delta_f}\,, \tag{1}$$

where c is the speed of light, Δ_f is the frequency step size which is equal to the difference between two adjacent used carrier frequencies, $\hat{\Delta}_\phi$ is the phase shift between two adjacent frequencies averaged over multiple frequencies, $c/2\Delta_f$ is the range ambiguity and mod is the modulo operation. Note that by transmitting multiple tone signals at different frequencies, the bandwidth has effectively been increased. In other words, the measurements at different frequencies are stitched together to create a wideband view on the channel. The reader can refer to Appendix A for more details about Eq. (1). We should note that the range ambiguity is inversely proportional to the frequency step size, Δ_f, hence the range ambiguity is equal to 75 m, 150 m and 300 m for a frequency step size of 2 MHz, 1 MHz and 0.5 MHz, respectively. Hence, the MCPD method can falsely estimate the range if the prover was beyond the range ambiguity. An adversary can simply use this knowledge and delay the signal to introduce an additional phase shift and hence reduce the estimated distance. In order to prevent this problem among others, ToF is implemented on top of the MCPD to detect such a simple attack.

ToF method. In order to estimate the ToF, the packets will be used as shown in Fig. 4. During the exchange of frames, each node measures the packet Time of Departure (ToD) and the packet ToA. The FD is used to estimate the ToD and ToA. We note that ToA is estimated by setting the internal clock of the nodes to where the peak of the correlation between the received FD and the expected FD occurs. Then, one of the nodes, typically the verifier, evaluates the ToF by taking the time difference between sending and receiving the packet and then subtracting it with the time spent by the other node, typically the prover, which is equal to the time difference between receiving and sending the packet. Hence, the ToF per channel can be obtained by,

$$\mathrm{ToF}_i = \frac{1}{2}(\mathrm{ToD}_{\mathrm{V}_i} - \mathrm{ToA}_{\mathrm{V}_i} - \mathrm{ToD}_{\mathrm{P}_i} + \mathrm{ToA}_{\mathrm{P}_i})\,. \tag{2}$$

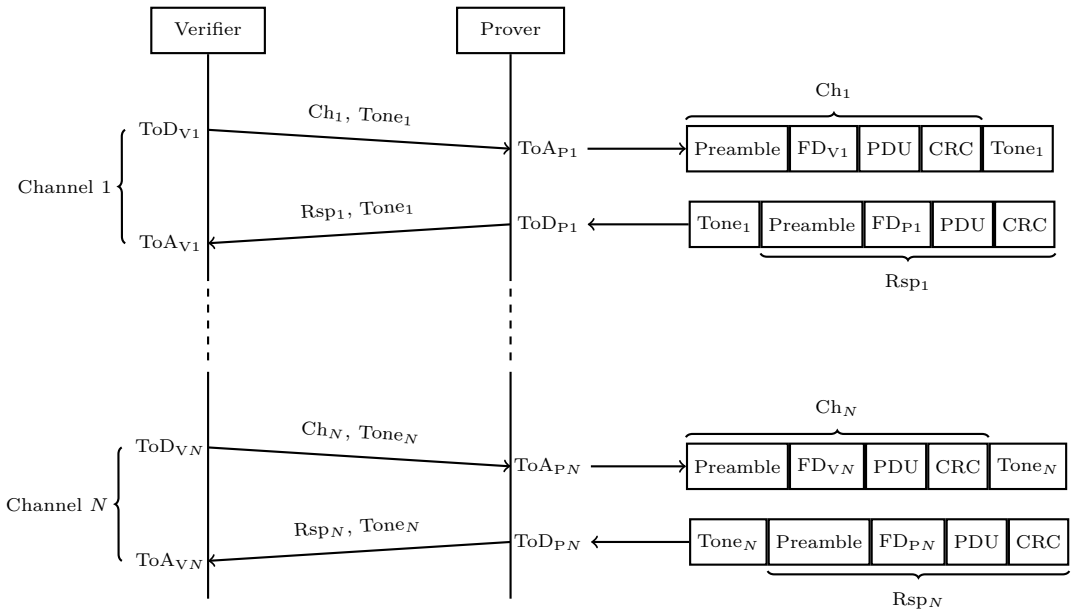

Figure 4: The distance bounding (or ranging) stage of our protocol.

We should note that the timestamp measurements taken at the prover should be sent to the verifier.

In order to improve the security of the measurements, a distance bounding protocol is added on top of MCPD and ToF. In the case of **MCPD**, a random phase difference (θ_i) is used per channel. This phase difference does not have to be a priori agreed between the two nodes since it will cancel out once $\phi_{2W}(f_i, r)$ is estimated. This is done so to mitigate the phase manipulation attack (Cf. Section 5.2.2). In the case of **ToF**, the FD will contain a pseudo-random sequence that is generated using the shared key established during the AKE stage as follows. Let PRF be a pseudorandom function. Then the pseudo-random sequence from the verifier to the prover is generated as $\mathrm{PRF}(K, \mathsf{MAC\text{-}Address}_{\mathrm{verifier}}, i)$, where K is the shared key established during AKE and i is the carrier number. Similarly, the sequence from the prover to the verifier is generated as $\mathrm{PRF}(K, \mathsf{MAC\text{-}Address}_{\mathrm{prover}}, i)$. Therefore, this sequence is only known to the verifier and the prover, and is also different on each transmission and on each channel. The sequence from the verifier to prover transmission acts as challenge bits and from the prover to verifier transmission acts as response bits. Thus, the FD will be used for three purposes: 1) to synchronize 2) to estimate ToA and ToD and 3) to authenticate the packet or the measurement, i.e., to mitigate the relay attack (Cf. Section 5.1.2).

After estimating the ToA of the received packets, the FD bits will be checked bit by bit and the prover node will notify the verifier whether the received challenge bits are correct or not. The notification is sent in an encrypted packet.

At this point in time, the measurements and exchange of data are finished. The verifier, as it will be described next, collects all the data and decides on the level of security and the distance estimation.

4.3 Authentication and authorization stage

In the last stage of the protocol, the prover sends its I/Q components, and timestamp measurements together with the status (indicating the correctness) of the received challenge bits in an encrypted packet to the verifier. The packet is encrypted using an authenticated encryption with the shared key generated in the AKE stage. Upon receiving the packet from the prover, the verifier makes a decision by evaluating the security and the distance based on the available measurements. The decision making procedure in illustrated in Fig. 5.

As shown in Fig. 5, the I/Q measurements, the ToF measurements, and the challenge and response status on all channels are used to securely estimate the distance. Our proposed decision making process is described as follows:

- Select the ToF measurements that have valid challenge and response and a ToF value less than the ambiguity bound threshold τ_{AB} ($\tau_{AB} = c/2\Delta_f$).
- If the remaining number of measurements N' is greater than or equal to the number of measurements threshold τ_{rounds}, then estimate

$$\overline{\mathrm{ToF}} = \frac{1}{N'} \sum_{i \in S_{N'}} \mathrm{ToF}_i,$$

  where $S_{N'}$ is the set that contains the N' valid measurements, otherwise the process is aborted and the prover will not be granted access. The value of τ_{rounds} can be the minimum threshold for measurements needed to consider the system secure and chosen by the system designer. Section 6 provides more information on how to calculate the minimum τ_{rounds}.
- If $\overline{\mathrm{ToF}}$ is less than Circle of Trust (CoT) threshold τ_{CoT} then the security level is high, and the process continues, otherwise the authorization fails and the process stops.

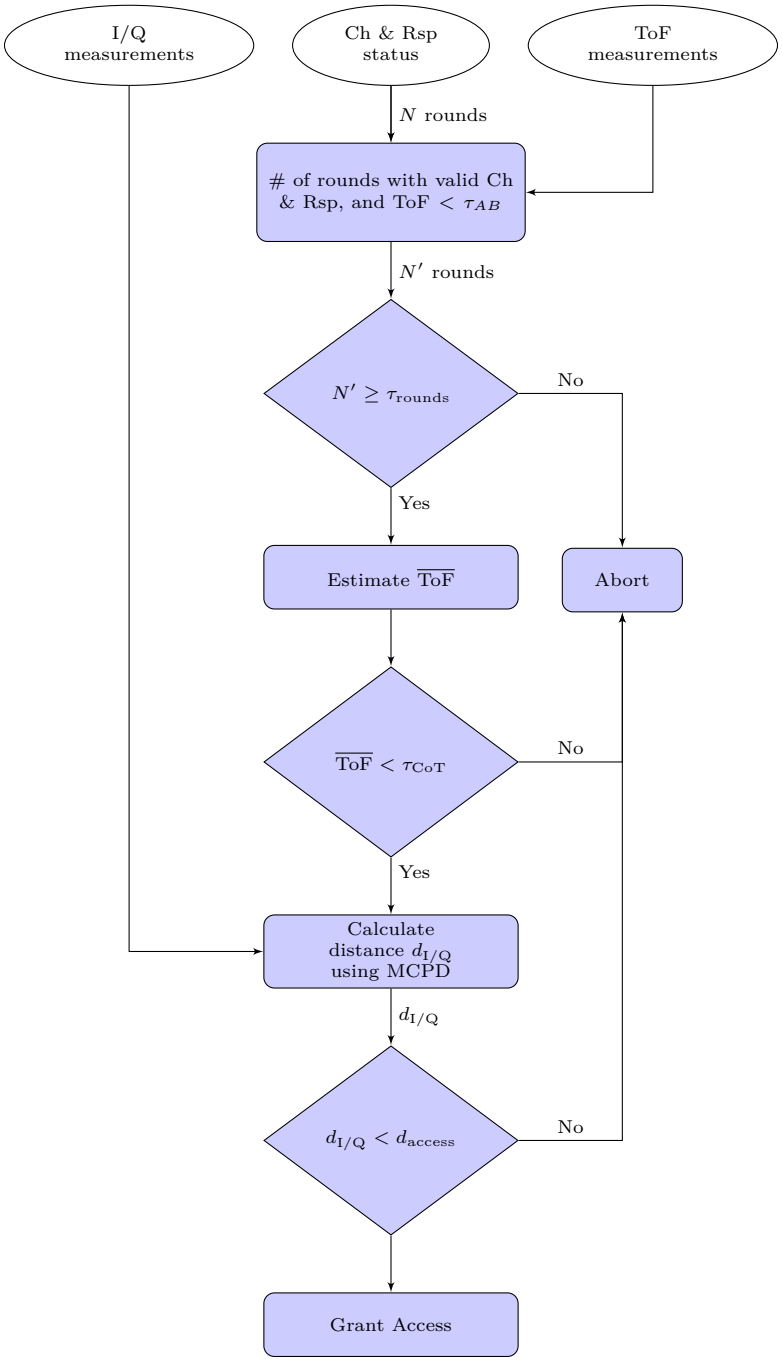

Figure 5: Schematics of our proposed decision making.

Note that the region within CoT is where the MCPD distance estimation can be trusted. Hence, the threshold τ_{CoT} can be chosen as $\tau_{\text{CoT}} \leq d_{\text{access}} + \epsilon_{\text{ToF}} + \epsilon_{\text{MCPD}}$, where d_{access} is the access distance threshold, ϵ_{ToF} and ϵ_{MCPD} are the maximum errors in ToF- and MCPD-based distance measurement, respectively.

- The accurate distance is estimated based on the I/Q measurements using the MCPD

method.

- If the estimated distance $d_{\mathrm{I/Q}}$ is less than the access distance threshold d_{access} then the prover is granted access, otherwise the process is stopped. For a car access usecase, d_{access} is typically less than 1 m.

5 Security Analysis

This section analyses the security of the proposed SDB scheme against attacks listed in Section 2.3. We first analyse generic attacks on the protocol, and then physical-layer attacks. We stress that since our main goal is to mitigate relay attacks, we exclude attacks by a dishonest prover and focus only on attacks by an external adversary.

5.1 Generic Attacks

Before we proceed, let us first present our security assumptions (or requirements) for the cryptographic building blocks of our protocol. The key cryptographic building blocks are: the SIGMA protocol used in AKE stage and PRF used for generation of FDs in the DB stage. We make the following assumptions on the security of these building blocks.

Assumption 1 (Security of SIGMA protocol [CK01])**.** *No adversary can distinguish a key established between two honest parties using the SIGMA protocol from random, except with negligible probability* negl*. Also, the SIGMA protocol is secure against impersonation and man-in-the-middle attacks.*

Definition 1. Let $\mathbb{N}$ be the set of natural numbers. Then $\mathsf{negl} : \mathbb{N} \to \{0,1\}$ is a negligible function if, for all positive polynomials poly and sufficiently large $\lambda \in \mathbb{N}$, we have $\mathsf{negl}(\lambda) < 1/\mathsf{poly}(\lambda)$.

For the validity of the Assumption 1, we refer to [CK01, CK02].

Regarding the security of PRF used for computing the Frame Delimiters, we make the following assumption.

Assumption 2 (Security of PRF)**.** *No adversary can distinguish the output of a PRF from random, except with* negl*.*

Note that this assumption follows from the formal definition of security for PRF that can be found in cryptographic literatures [KL14].

5.1.1 Impersonation attack

In this attack the adversary impersonates the legitimate prover in an attempt to get authenticated as the prover. As illustrated in Fig. 6, this happens when a single close-by adversary attempts to convince the verifier that the prover, which is not present (or simply, far away), is located close to the verifier [ABK+11]. The security against impersonation attack is guaranteed by the security of the employed SIGMA protocol in the AKE stage.

Theorem 1. *Under Assumption 1, our protocol is secure against impersonation attack.*

Proof. A successful impersonation attack on the distance bounding protocol requires that the attacker succeeds in impersonating the prover in the AKE stage. However, without a successful completion of the AKE stage, the verifier does not proceed with the latter stages of the protocol. Therefore, our protocol is secure against impersonation attack. □

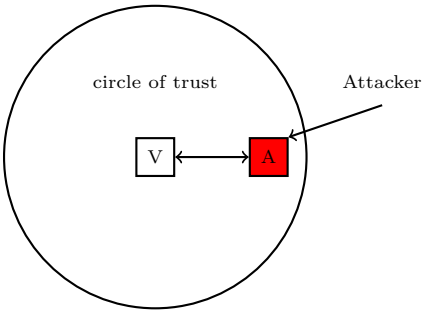

Figure 6: Impersonation attack. Note that there is no prover present in this attack, and that the attacker could also be outside the circle of trust.

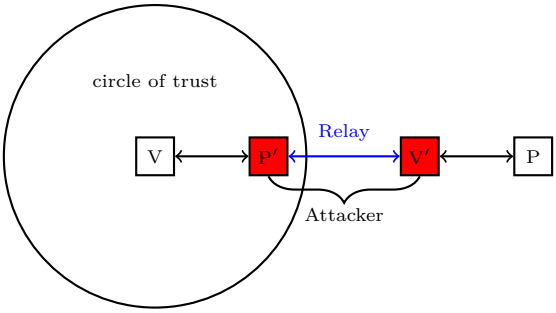

Figure 7: Relay attack on a distance bounding protocol.

5.1.2 Relay attack

In a relay attack, the attacker could employ two strategies: pre-ask strategy and post-ask strategy. In the case of pre-ask strategy, the adversary does nothing in the AKE stage other than simply relaying the AKE stage between the verifier and the prover. Then, the attacker first executes the distance-bounding stage with the prover, before the verifier starts it. Afterwards, it carries on the fast stage with the verifier. Finally, it simply relays the last stage of the protocol. In the post-ask strategy, the attacker relays the AKE stage and the last stage, as in the previous strategy. In the distance-bounding stage, however, it employs a different strategy. It first executes the fast stage with the verifier without involving the prover. It then asks the prover with the correct challenges received from the verifier. Relay attack is depicted in Fig. 7.

Theorem 2. *Let ℓ be the length of the Frame Delimiter. Then, under Assumption 1 and 2, in a single round of challenge-response in the distance-bounding stage, the attacker's success probability ϵ in a relay attack is*

$$\epsilon \leq \frac{2 \cdot 2^{\ell} - 1}{2^{2\ell}} + \mathsf{negl}\,. \tag{3}$$

Proof. Let us analyse the attacker's success probability in each of the two attack strategies. In the case of pre-ask strategy, if the attacker's challenge that is sent to the prover matches the challenge that the verifier sends, then the attacker wins by simply relaying the prover's response to its challenge. Otherwise, it has to guess the response (i.e., the Frame Delimiter) and hope for the best. This is illustrated in Fig. 8. So the attacker's success probability is

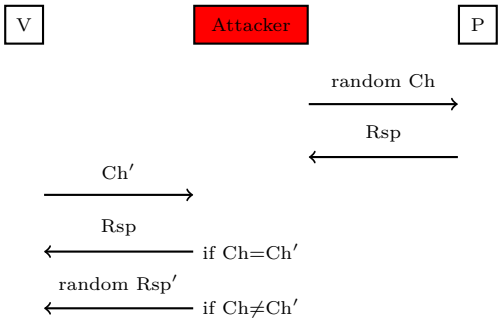

Figure 8: Pre-ask strategy in a relay attack.

$$\begin{aligned}\epsilon_{\text{pre}} &= \Pr\{\text{Ch} = \text{Ch}'\} + (1 - \Pr\{\text{Ch} = \text{Ch}'\})\Pr\{\text{Rsp}' \text{ correct}\} \\ &\leq 2^{-\ell} + (1 - 2^{-\ell})2^{-\ell} + \mathsf{negl} = \frac{2 \cdot 2^{\ell} - 1}{2^{2\ell}} + \mathsf{negl}\,.\end{aligned} \tag{4}$$

Here $\Pr\{\text{Ch} = \text{Ch}'\}$ and $\Pr\{\text{Rsp}' \text{ correct}\}$ correspond to probabilities of guessing a random bitstring of length ℓ correctly. Following Assumption 2, these probabilities are upper bounded by $2^{-\ell} + \mathsf{negl}$.

In the case of post-ask strategy, the attacker responds with a random Rsp′ to the verifier's challenge Ch directly, without any information from the prover, as illustrated in Fig. 9. Therefore, the attacker's success probability depends only on its ability to guess the response correctly, and is bounded by

$$\epsilon_{\text{post}} = \Pr\{\text{Rsp}' \text{ correct}\} \leq 2^{-\ell} + \mathsf{negl}\,. \tag{5}$$

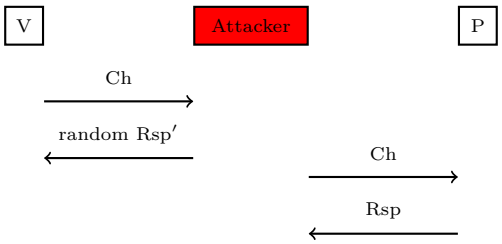

Figure 9: Post-ask strategy in a relay attack.

Hence, in a single round of challenge-response in the DB stage of our protocol, the attacker has a success probability

$$\epsilon = \max(\epsilon_{\text{pre}}, \epsilon_{\text{post}}) \leq \frac{2 \cdot 2^{\ell} - 1}{2^{2\ell}} + \mathsf{negl}\,. \tag{6}$$

□

5.2 Physical-layer attacks

Besides the generic attacks on the protocol exploiting potential weaknesses in the employed cryptographic primitives, there are physical-layer attacks that can be mounted independently of the cryptographic primitives. Below, we analyse security of the proposed ranging solution against most relevant physical-layer attacks: early-detect late-commit attack and phase manipulation attack. See Section 2.3 for details on how these attacks work.

5.2.1 Early-detect late-commit attack

In this attack, the adversary aims at decreasing the estimated ToF by detecting the FD symbols from one node earlier and then forwarding them to the other node.

In the early-detection step, the adversary attempts to detect the symbols of the FD using only the initial part of each symbol. Given that the duration of the symbol is large (500 ns for a bandwidth of 2 MHz) and the adversary can position itself close to the transmitter and get a higher SNR than the legitimate receiver, an early detection of all of the FD symbols is possible. In the late-commit step, the adversary prepares the symbol in such a way that the initial part of the symbol does not correspond to a bit, whereas the remaining part of the symbol corresponds to a bit. This means that the adversary can start sending a symbol even before knowing which symbol polarity to send. The adversary needs to perform this attack on all of the FD symbols in each challenge/response packet.

In order to successfully decrease the distance, the adversary needs to synchronize to the intercepted packets, perform ED/LC attack and minimize the delays and processing time of its radio.

In BLE, receivers rely on FD symbols to synchronize to the received packet. The adversary, however, can only rely on the preamble to synchronize to the intercepted packet since it does not know the FD symbols in advance. We should note that BLE uses two given preamble sequences of length one byte. Since the FD is of length 4-bytes and the preamble is of length 1-byte, the adversary needs $20\log_{10}(32/8) = 12\,\text{dB}$ additional SNR to be able to synchronize correctly using only the preamble. After correct synchronization, the adversary mounts ED/LC attack. As stated earlier, the maximum distance that the adversary can decrease with ED/LC attack depends on the SNR, the pulse shaping filter, the processing time at the adversary and the decoding method. In order to succeed in decreasing the distance using the ED/LC attack, the adversary must have a good SNR and minimize its processing time. However, as we shall see below, our solution obliges the adversary to use filters to be able to decode all FD symbols correctly, and the adversary's use of filters will introduce noticeable delays (i.e., increased ToF).

SNR is the key to detect the symbols earlier, because with an γ-times better SNR than the legitimate receiver, the attacker can save up to $(\gamma - 1)/\gamma$ of a symbol's transmission time *but* at the expense of decoding the symbol with error [CHKM06]. Note that in our design, all decoded symbols of FD need to be correct. To increase the SNR, the attackers (remember that in relay attack there are two attackers) need to be close to both prover and verifier and/or use directive antennae. At 2.4 GHz and in line-of-sight environment the SNR degrades by 6 dB when doubling the distance. Moreover, the attackers' transceivers must have low noise and be able to reject interference signals located not only in the band of interest but also in the neighboring bands. The filter increases SNR by rejecting all the interference signals and noise outside the band-of-interest.

In addition to a good SNR, the attackers, during reception and transmission of the signals, must not add considerable latency or delay. The added latency or processing time must be much lower than the reduced time gained with early detection, otherwise the attackers will not be able to decrease the distance. This means that the antenna and other front-end modules, e.g., low noise amplifier, variable gain amplifier, mixer, analog-to-digital converter, and filters must have very low delay.

In order to keep the added latency or processing time as low as possible, the attackers can choose to use either wide-band filters or no filters at all to avoid additional delays at the expense of having additional interference. If the interference and noise are not canceled by the adversaries during the early detection, this results in uncertainty in detecting the FD symbols. Since in the proposed algorithm the receiver accepts the estimated ToA if and only if all the decoded symbols in the received FD are correct, the attackers must early detect all the symbols in the FD correctly. Therefore, this obliges the adversary to use filters. Since the bandwidth of the filters is inversely proportional to the time delay, the

use of filter will add additional delays to the signal and hence will increase the estimated ToF at the verifier. For example, using a filter of bandwidth approximately 2 MHz (2 MHz is the bandwidth of one channel in BLE) will add a delay of approximately 500 ns to the ToF which corresponds to additional 150 m to the estimated distance. This can be easily detected by the proposed algorithm. We should note that the delays introduced by the legitimate radios are compensated before estimating the ToF.

The adversaries may succeed in an ideal scenario where there is no interference and where they have access to perfect hardwares (i.e., efficient transceiver with negligible delay). However, interference is unavoidable in practice and transceivers have non-negligible delays (typical transceiver delays are in order of microseconds). As we have seen above, interference will either cause the adversary to decode the FD symbols incorrectly or introduce additional delays due to the need for filters. In either case, this will be detected by the legitimate nodes. These constraints make the ED/LC attack hard to execute in practice.

Security against wide-band attacker. In [Li], Li presents a time-domain attack on Orthogonal Frequency Division Multiplexing (OFDM) signal. A more advanced ED/LC attack strategy against our solution perhaps would be to use wideband maximum-likelihood decoding techniques over multiple bands in parallel as described in [Li]. However, the practical feasibility evaluation of such an attack is beyond the scope of this paper and will be a topic of future research.

5.2.2 Phase manipulation attack

In Section 2.3, three phase manipulation attacks were introduced, the *phase slope rollover attack*, *on-the-fly phase manipulation attack* and *tone generation attack*. These attacks target the phase of the signal and manipulate the MCPD distance estimation. These attacks do not affect ToF estimation which in fact prevents *phase rollover attack*. However, ToF can not always protect the MCPD distance estimation against *on-the-fly phase manipulation* and *tone generation* attacks, e.g., in situations where the prover is close to the verifier and inside the CoT region. Hence, below we focus on *on-the-fly phase manipulation* and *tone generation attacks* in such situations.

In order to prevent these attacks, an independent random phase shift (as described in Section 4.2)–generated using the shared session key–*per channel per node* is introduced to the tone signals before being transmitted. The adversary cannot guess the introduced phase-shift and thereby cannot generate a corresponding signal to reduce the distance below d_{access}. This will result in large fluctuations in the measured phase difference across the carrier frequencies. Thus the attacker cannot successfully reduce the distance below d_{access} with *on-the-fly phase manipulation attacks* due to the random and independent phase shifts generated using the session key by the legitimate nodes for each frequency. We should note that the duration of CT signal is fixed. The CT duration must be long enough to deal with crystal-offset, time-offset, group delay of the analog front-end, but short enough to reduce power consumption and processing time. In our implementation the duration of CT signal is $\approx 35\mu$s. Given that the CT duration is fixed, the measured amplitude and phase of the CT signal should be consistent during the whole duration of CT, any discontinuity indicates that there is an attack.

Let us now analyse the *tone generation attack* in more detail. We should note that similar analysis applies to *on-the-fly phase manipulation attack*. In this attack the adversary generates its own tone signal in order to trick the verifier and decrease the MCPD estimated distance. Fig. 10 explains the MCPD method with a random phase offset at both nodes in the case of no attack. For simplicity, we focus on CT signal without including the packet.

The procedure starts whenever the verifier transmits its own tone signal that has a phase φ_{1,f_i} and a frequency f_i, where i denotes the channel number. Due to the distance between the verifier and the prover, the tone signal arrives at the antenna of the prover

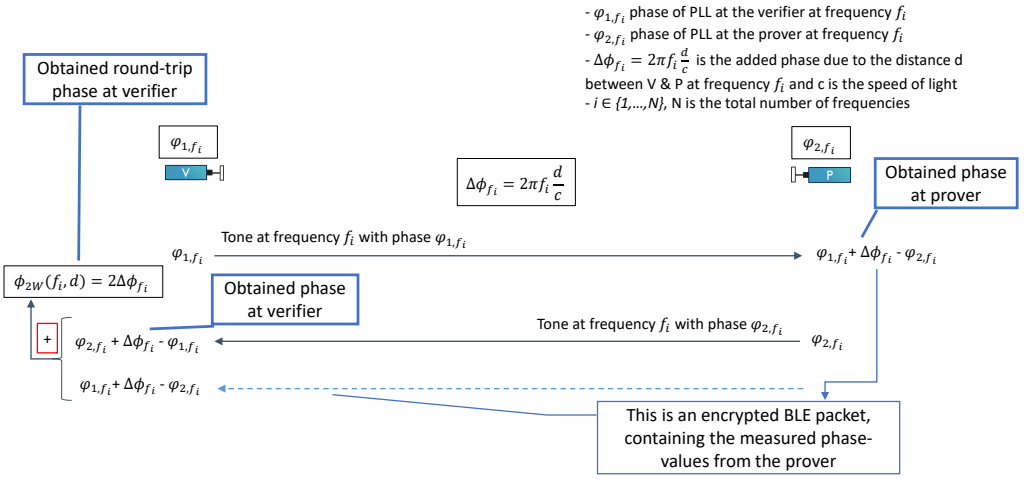

Figure 10: The MCPD method.

with a phase equal to $\varphi_{1,f_i} + \Delta\phi_{f_i}$. The prover measures the received phase with respect to its own Local Oscillator (LO) which is equal to $\varphi_{1,f_i} + \Delta\phi_{f_i} - \varphi_{2,f_i}$. The measured phase will be transmitted **encrypted** later on (together with the other measurement results) (in the last stage of the protocol) to the verifier. Then, the prover will transmit its own tone signal at the same frequency f_i that has a phase of φ_{2,f_i}. The verifier will measure the received phase with respect to its own LO. Then, the verifier combines the two measurements (the one it measured and the one it received from the prover) in order to obtain the channel induced phase shift. This process is repeated using N frequencies. To obtain the distance between the two nodes, the procedure shown in Fig. 10 needs to be executed for at least using two frequencies, f_1 and f_2, as explained in Section 4.2.

Hence, using $\phi_{2W}(f_1, d)$ and $\phi_{2W}(f_2, d)$, one way of evaluating the distance $\hat{d}$ is as follows:

$$\begin{aligned}
\hat{d} &\equiv \frac{c}{4\pi} \frac{\phi_{2W}(f_2, d) - \phi_{2W}(f_1, d)}{f_2 - f_1} \mod \frac{c}{2(f_2 - f_1)} \\
&\equiv \frac{c}{4\pi} \frac{2\Delta\phi_{f_2} - 2\Delta\phi_{f_1}}{f_2 - f_1} \mod \frac{c}{2(f_2 - f_1)} \\
&\equiv \frac{c}{4\pi} \frac{4\pi f_2 \frac{d}{c} - 4\pi f_1 \frac{d}{c}}{f_2 - f_1} \mod \frac{c}{2(f_2 - f_1)} \\
&\equiv d \mod \frac{c}{2(f_2 - f_1)},
\end{aligned} \tag{7}$$

where d is the actual distance between the two nodes. We note that the random phase shifts introduced will cancel out only when the verifier obtains the prover's phase measurements, which are sent encrypted by the prover in the last protocol stage.

We now look at the same procedure in the case of an attack by an adversary, located between the verifier and the prover, who generates its own strong tone signal. Fig. 11 depicts this attack scenario on MCPD. In this scenario, the procedure is similar to the one discussed above. For simplicity, let us assume that the prover and the verifier only receive the tone signal from the adversary. In this case, the estimated distance $\hat{d}$ is obtained as

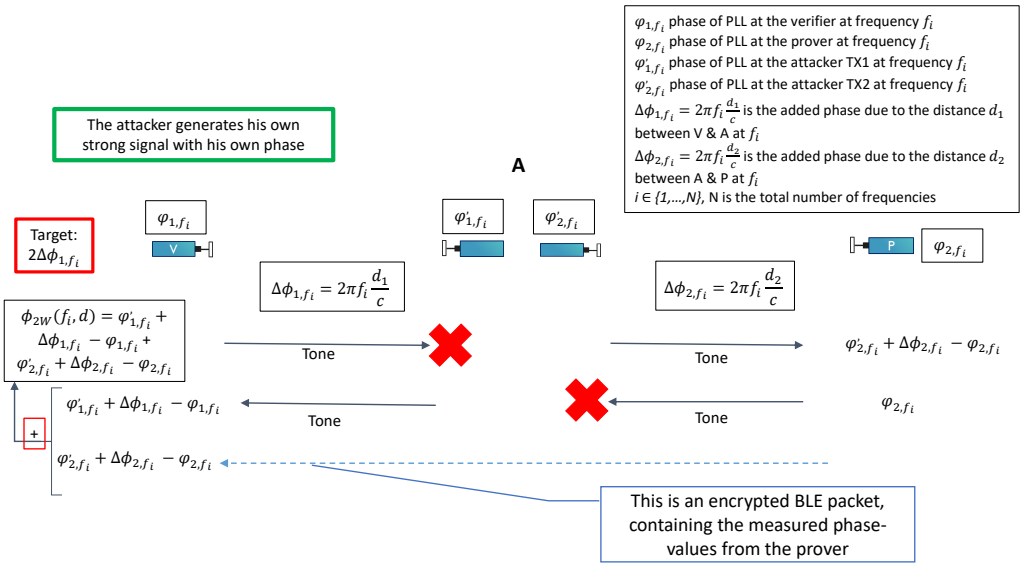

Figure 11: Phase manipulation attack on the MCPD.

follows:

$$\begin{aligned}\hat{d} &\equiv \frac{c}{4\pi}\frac{\phi_{2W}(f_2,d)-\phi_{2W}(f_1,d)}{f_2-f_1} \mod \frac{c}{2(f_2-f_1)} \\ &\equiv \frac{c}{4\pi}\left(\frac{(\varphi'_{1,f_2}+\Delta\phi_{1,f_2}-\varphi_{1,f_2}+\varphi'_{2,f_2}+\Delta\phi_{2,f_2}-\varphi_{2,f_2})}{f_2-f_1}\right. \\ &\quad \left.-\frac{(\varphi'_{1,f_1}+\Delta\phi_{1,f_1}-\varphi_{1,f_1}+\varphi'_{2,f_1}+\Delta\phi_{2,f_1}-\varphi_{2,f_1})}{f_2-f_1}\right) \mod \frac{c}{2(f_2-f_1)}\,.\end{aligned} \tag{8}$$

In order for the adversary to succeed in decreasing the distance, that is, to make $\phi_{2W}(f_2,d)-\phi_{2W}(f_1,d) = 2\Delta\phi_{1,f_2} - 2\Delta\phi_{1,f_1}$, it needs to make

$$\begin{aligned}&\varphi'_{1,f_2}+\varphi'_{2,f_2}-\varphi'_{1,f_1}-\varphi'_{2,f_1} \\ &\quad = \Delta\phi_{1,f_2}-\Delta\phi_{2,f_2}-\Delta\phi_{1,f_1}+\Delta\phi_{2,f_1} \\ &\qquad +\varphi_{1,f_2}+\varphi_{2,f_2}-\varphi_{1,f_1}-\varphi_{2,f_1}\,,\end{aligned} \tag{9}$$

and similarly, between frequencies f_2 and f_3, f_3 and f_4 and so on.

Hence, the adversary cannot predict what will happen with the distance estimation, since it does not have control over all the random phases, e.g., $\varphi_{1,f_2}+\varphi_{2,f_2}-\varphi_{1,f_1}-\varphi_{2,f_1}$ in all PLL and at each frequency. We should note that any discrepancy between the phase-based and ToF-based distance estimation will be detected by the verifier during the authorization stage of the protocol. Therefore, this attack will be detected.

6 Performance Analysis

Here we analyse the performance of our solution in terms of false acceptance rate (FAR) and false rejection rate (FRR), and present the minimum threshold for the number of valid rounds given some chosen levels of FAR and FRR. Recall that N is the number of challenge-response rounds (or, the number of carriers used) in the protocol, and that τ_{rounds} is the minimum threshold for the number of valid rounds (Cf. Section 4.3).

FRR. In our solution, a round is considered valid if and only if all bits of both the challenge FD and the response FD are correctly decoded by the respective receivers. Let ξ_{noise} be the probability that a challenge and response round fails due to receiver noise, without the presence of any attacker. An honest prover is falsely rejected, if the number of valid rounds is less than τ_{rounds}. Therefore, the FRR is

$$\mathsf{FRR} = \sum_{i=0}^{\tau_{\text{rounds}}-1} \binom{N}{i} (1-\xi_{\text{noise}})^i \xi_{\text{noise}}^{N-i}.$$

FAR. Recall from Theorem 2 that in a relay attack, ϵ is the probability that an attacker succeeds in a single round of challenge-response. Taking into account the failure probability ξ_{noise} of a round due to receiver noise, the attacker's success probability becomes $\xi := \epsilon + \xi_{\text{noise}} - 2\epsilon\xi_{\text{noise}}$, since the attacker succeeds either (a) by guessing FD correctly and the legitimate receiver decodes the guessed FD correctly or (b) by guessing the FD incorrectly but the legitimate receiver decodes the attacker's FD as the expected FD due to noise. If the number of rounds in which the attacker is successful is greater than or equal to τ_{rounds}, the attacker can falsely be accepted. Therefore, the FAR is

$$\mathsf{FAR} = \sum_{i=\tau_{\text{rounds}}}^{N} \binom{N}{i} \xi^i (1-\xi)^{N-i}.$$

We can now compute the threshold τ_{rounds} for a given level of FAR and FRR, number of used carriers and the length of FD. Table 1 presents the required τ_{rounds} for different levels of FAR and FRR, in the case of 40 and 80 carriers, respectively. In all cases, the FD is of length 32-bits. We remark that in practice FAR and FRR are chosen according to security and usability requirements of the target application. The higher the security level (i.e., FAR is low), the lower the usability (i.e., FRR is high), and vice versa.

Table 1: Threshold τ_{rounds} required for different levels of FAR and FRR when using 32-bit FDs under different number of carriers.

ξ_{noise}	40 carriers		80 carriers	
	FAR, FRR $\leq 10^{-4}$	FAR, FRR $\leq 10^{-8}$	FAR, FRR $\leq 10^{-4}$	FAR, FRR $\leq 10^{-8}$
2^{-4}	11	15	16	22
2^{-5}	8	12	11	16
2^{-6}	6	9	8	12
2^{-7}	5	8	6	10
2^{-8}	4	7	5	8

7 Evaluation

In this section, we evaluate first the ranging accuracy of MCPD and ToF methods and then the relay attack on the proposed solution with a prototype implementation on NXP KW36 chips.

7.1 Evaluation of ranging accuracy

Our implementation setup is shown in Fig. 12. Two NXP KW36 (BLE) chips are used for implementing the prover and the verifier functionalities. To evaluate the ranging accuracy, we perform (wireless) outdoor measurements, and the outdoor setup is shown in Fig. 13.

The setup consists of two boards, namely a verifier and a prover, in which each board is equipped with an omnidirectional antenna. The two boards estimate the distance between

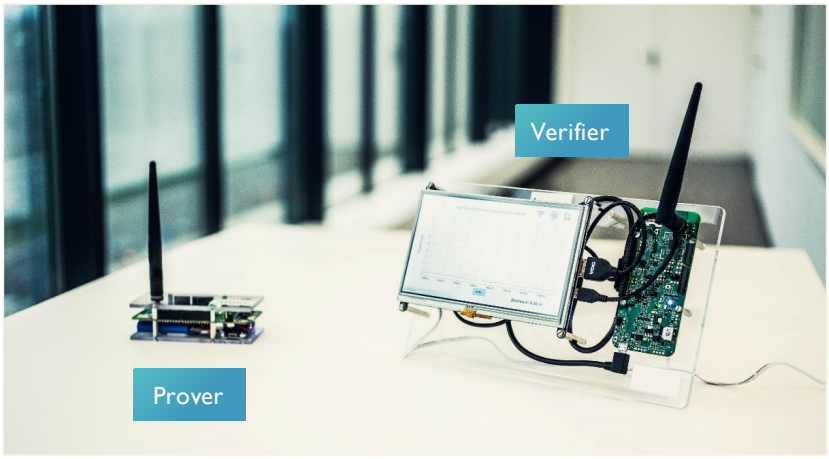

Figure 12: The proposed SDB solution is implemented on NXP KW36 chips.

them using phase (a.k.a., MCPD) and ToF when the prover and the verfier are separated by d meters, for $d = 1, 2, \cdots, 10$. The total number of measurements per position is 250 , where each one consists of measurements on 80 frequencies in the 2.4 GHz ISM band. The MCPD and ToF distance estimation is based measurements on the 80 frequencies. Recall that 80 frequencies correspond to frequency step size Δ_f =1 MHz. The obtained results are displayed in Fig. 14, where we can also observe the precision of both methods in a real practical environment. The obtained precision (i.e., the standard deviation) of the phase-based distance measurement is $\leq$ 2.5 cm and that of the ToF-based distance measurement is $\leq$ 1.6 m, as can be seen in Fig. 15 where we plot the standard deviation of both distance measurements. Fig. 16 displays the error in the distance measurements. We can see from this figure that the maximum error in phase-based distance measurement is 30 cm, while the maximum error in ToF-based distance measurement is 2 m. Therefore, our evaluation results show that the ToF-based distance measurement can offer guarantees about whether the phase-based distance measurement can be trusted.

To evaluate the time complexity of our solution, we measure the total runtime of our implementation for both MCPD and ToF measurements. As shown in Table 2, the total runtime MCPD and ToF measurements are 97.5 ms and 113 ms, respectively. The total runtime is the sum of the runtimes for setup, range measurements, data exchange, and

Figure 13: Outdoor wireless measurement setup.

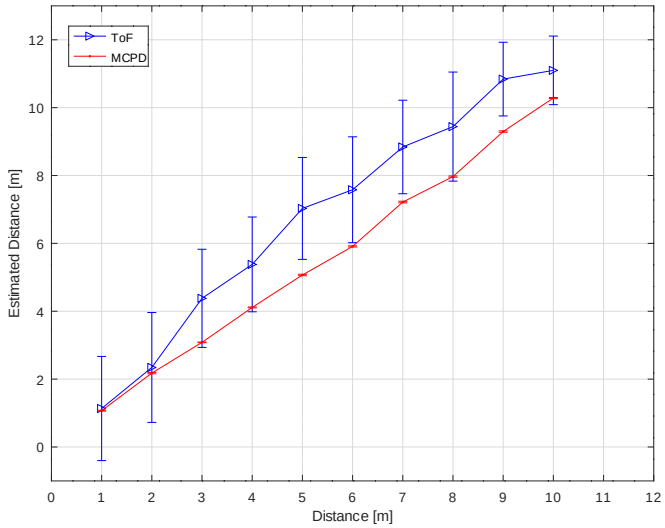

Figure 14: Outdoor distance measurement results.

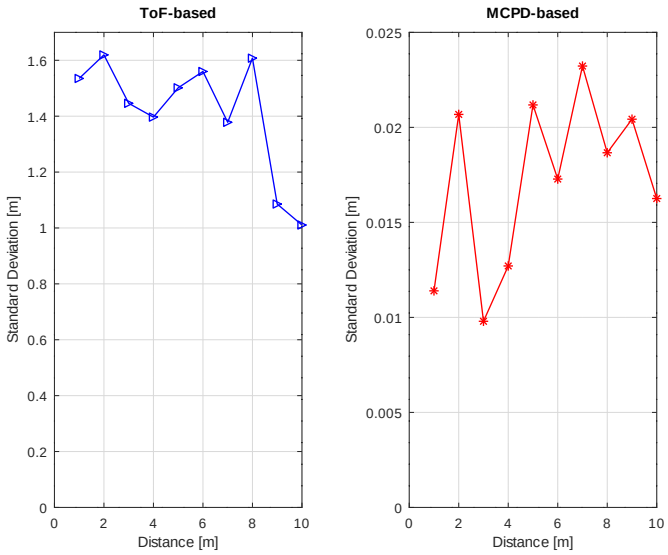

Figure 15: The standard deviation of ToF-based and MCPD-based distance measurements.

print steps. Note that the print step is the data-transfer over the UART-interface to the Host (Raspberry Pi, in our case) and it accounts for 15 ms and 11 ms of the total runtime.

Table 2: Total runtime of MCPD and ToF measurements.

	Runtime (ms)
MCPD	97.5
ToF	113
MCPD+ToF	210.5

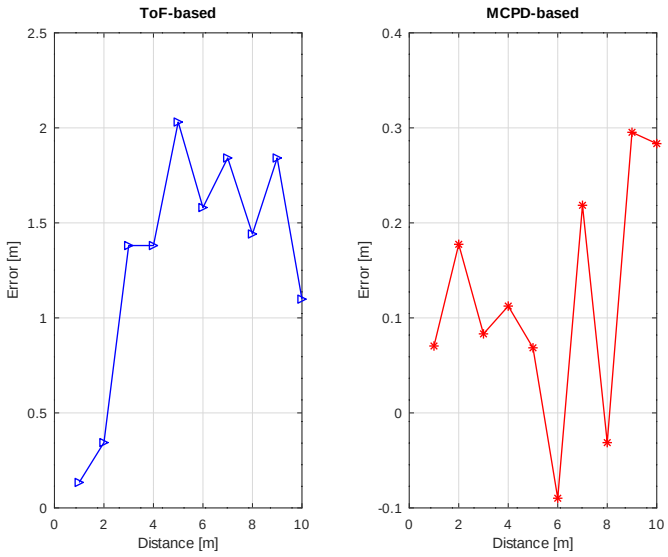

Figure 16: Error in ToF-based and MCPD-based distance measurements.

Next, we evaluate the proposed SDB solution, described in Fig. 2 in Section 4, under two scenarios: (1) the prover and the verifier are close to each other and (2) the prover and the verifier are far from each other, yet still within each other's communication range. For this example, we define $d_{\text{access}} = 3\,\text{m}$ and $\tau_{\text{CoT}} = 5\,\text{m} \leq d_{\text{access}} + \epsilon_{\text{ToF}} + \epsilon_{\text{MCPD}}$, since ϵ_{ToF} and ϵ_{MCPD} are 2 m and 30 cm, respectively. Fig. 17 and 18 show the estimated distances using phase and ToF measurements, and the security level versus the measurement instance (x-axis). In Fig. 17, we can see that the prover is authorised since $\overline{\text{ToF}} < \tau_{\text{CoT}}$ and $d_{\text{I/Q}} < d_{\text{access}}$. In Fig. 18, however, we can see that the security level is low and the prover is not authorised since $\overline{\text{ToF}} > \tau_{\text{CoT}}$ (and not to mention $d_{\text{I/Q}} > d_{\text{access}}$).

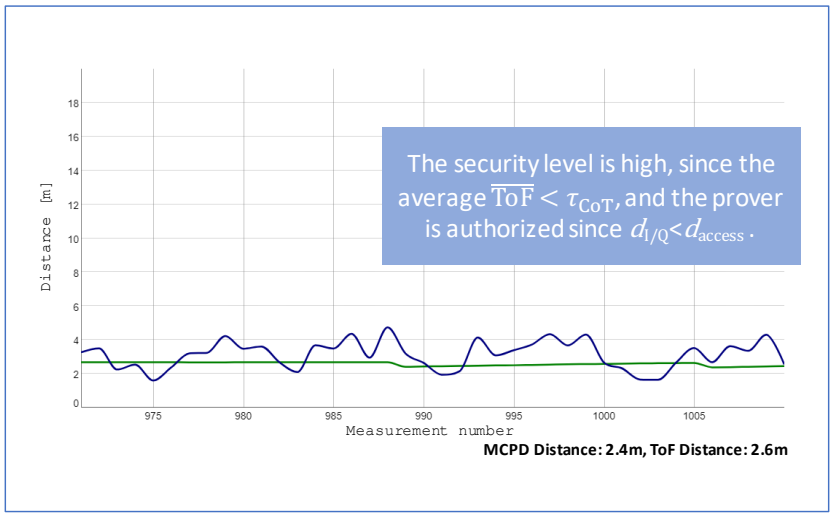

Figure 17: MCPD- and ToF-based distance measurements when the prover is close to the verifier.

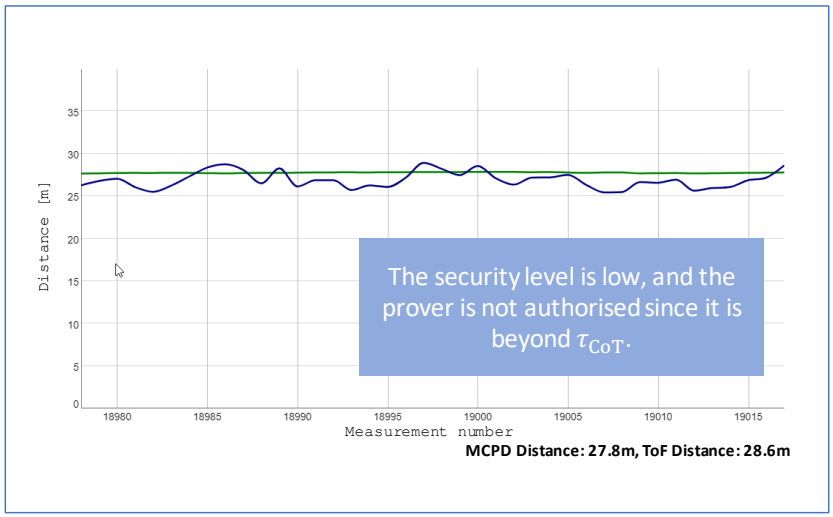

Figure 18: MCPD- and ToF-based distance measurements when the prover is far away from the verifier.

7.2 Evaluation of relay attack

Here we evaluate the relay attack, in particular, the phase rollover attack. In order to do this, a model has been built in which the verifier and the prover are not in each other's communication range (no line of sight communication) and two adversaries are in between connected via a cable, one is close to the verifier and the other to the prover, as shown Fig. 19. The adversaries consist of two antennae and a cable, meaning that they simply relay the signal between the prover and the verifier without any processing. We use Sucoflex 104PE cable that has a length of 10 m, impedance of 50 Ω, and a time delay of 4.3 ns/m. In the relay attack evaluation, we use three such Sucoflex cables which give a total time delay of 129 ns. In this setup, we choose 4 MHz frequency step size (i.e., Δ_f=4 MHz) in order to evaluate the phase manipulation attack with a short cable ($\leq$40 m) with low attenuation for connecting the adversaries. The selected frequency step size yields a $c/(2\Delta_f)$ =37.5 m distance ambiguity bound for the phase-based distance.

This means that beyond this ambiguity bound, the estimated distance will rollover due to phase rollover. The boards are equipped with directional antennae (Taoglas WDMP.2458.A) [TAO] with a gain of 5.5 dBi.

Fig. 20 shows the measured distances in the presence of a relay attack. As can be seen from this figure, the security level is low since the distance based on ToF is higher than the ambiguity bound. In this scenario, the distance estimation based on phase measurements has been compromised. Thanks to ToF-based distance estimation, the attack is detected because ToF $> \tau_{\text{AB}}$ implies that the phase-based distance measurements cannot be trusted.

8 Conclusions

Relay attacks pose serious security threats to wireless systems relying on secure proximity information, such as passive keyless entry systems, contactless payments, or smart access control. There are many distance bounding protocols proposed in the literature to mitigate relay attack, and secure implementation of distance bounding protocols to date is mostly limited to UWB radios. However, secure Narrow-Band distance bounding solution resisting physical layer attacks remained as an open challenge. As most wireless applications require

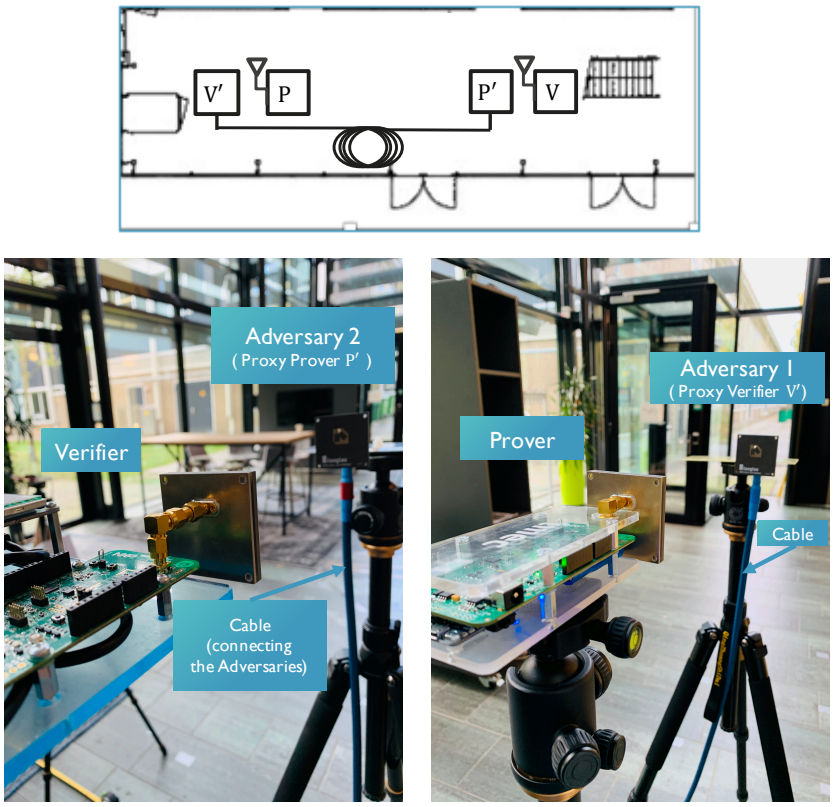

Figure 19: The relay attack model setup and the layout of the indoor environment in which the model is set up.

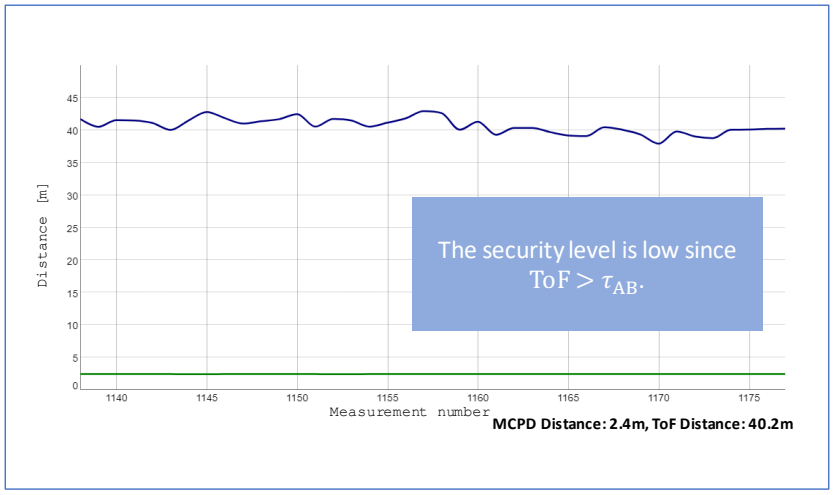

Figure 20: MCPD- and ToF-based distance measurements under relay attack.

ultra-low power and low-cost radios, Bluetooth Low Energy radio is a promising solution for secure proximity applications. In this paper, we designed and implemented the first accurate and secure distance bounding (SDB) protocol for Bluetooth Low Energy radios. The SDB protocol combines

- A multi carrier phase-based distance (MCPD) measurement that provides a high

ranging accuracy (around 30 cm) with a precision of less than 2.5 cm.

- Time-of-Flight (ToF) based distance bounding for detection of phase slope rollover attack, authentication, and security.

In addition to analysing security of our solution against generic and physical-layer attacks, we demonstrate its feasibility and practicality with an actual implementation on an NXP KW36 Bluetooth Low Energy radio platform. Our security analysis and evaluation show that the presented solution effectively mitigates relay attacks.

An extension of the presented secure Narrow-Band ranging to a group setting where multiple nodes are securely ranging each other is an interesting direction for future work.

Acknowledgments

We thank the anonymous reviewers for their valuable comments that helped improve the paper. This work is partially funded by ECSEL (Grant Agreement number: 783119) SECREDAS project and the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018.

References

[ABB+19] Gildas Avoine, Muhammed Ali Bingöl, Ioana Boureanu, Gerhard Hancke, Süleyman Kardaş, Chong Hee Kim, Cédric Lauradoux, Benjamin Martin, Jorge Munilla, Alberto Peinado, et al. Security of distance-bounding: A survey. *ACM Computing Surveys (CSUR)*, 51(5):94, 2019.

[ABK+11] Gildas Avoine, Muhammed Ali Bingöl, Süleyman Kardas, Cédric Lauradoux, and Benjamin Martin. A framework for analyzing RFID distance bounding protocols. *Journal of Computer Security*, 19(2):289–317, 2011.

[BBD+91] Samy Bengio, Gilles Brassard, Yvo G Desmedt, Claude Goutier, and Jean-Jacques Quisquater. Secure implementation of identification systems. *Journal of Cryptology*, 4(3):175–183, 1991.

[BC93] Stefan Brands and David Chaum. Distance-bounding protocols (extended abstract). In *EUROCRYPT*, pages 344–359, 1993.

[BD90] Thomas Beth and Yvo Desmedt. Identification tokens - or: Solving the chess grandmaster problem. In *Advances in Cryptology - CRYPTO '90, 10th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1990, Proceedings*, volume 537 of *Lecture Notes in Computer Science*, pages 169–177. Springer, 1990.

[BMV14] Ioana Boureanu, Aikaterini Mitrokotsa, and Serge Vaudenay. Towards secure distance bounding. In Shiho Moriai, editor, *Fast Software Encryption*, pages 55–67, Berlin, Heidelberg, 2014. Springer Berlin Heidelberg.

[BMV15] Ioana Boureanu, Aikaterini Mitrokotsa, and Serge Vaudenay. Practical and provably secure distance-bounding. *Journal of Computer Security*, 23(2):229–257, 2015.

[BRGD20] Pepijn Boer, Jac Romme, Jochem Govers, and Guido Dolmans. Performance of high-accuracy phase-based ranging in multipath environments. pages 1–5, 05 2020.

[CHKM06] Jolyon Clulow, Gerhard Hancke, Marku Kuhn, and Tyler Moore. So near and yet so far: Distance-bounding attacks in wireless networks. In *Proceedings of the 3rd European Workshop on Security and Privacy in Ad Hoc and Sensor Networks (ESAS '06)*, volume LNCS 4357 of *Lecture Notes in Computer Science*, pages 83–97. Springer-Verlag, 2006.

[CK01] Ran Canetti and Hugo Krawczyk. Analysis of key-exchange protocols and their use for building secure channels. In *EUROCRYPT*, volume 2045 of *LNCS*, pages 453–474. Springer, 2001.

[CK02] Ran Canetti and Hugo Krawczyk. Security analysis of IKE's signature-based key-exchange protocol. In *CRYPTO*, volume 2442 of *LNCS*, pages 143–161. Springer, 2002.

[Des88] Y. Desmedt. Major security problems with the "Unforgble" (Feige)-Fiat-Shamir proofs of identity and how to overcome them. In *SecuriCom*, pages 15–17, 1988.

[DM07] Saar Drimer and Steven J Murdoch. Keep your enemies close: Distance bounding against smartcard relay attacks. In *USENIX security symposium*, volume 312, pages 87–102, 2007.

[FDC11] Aurélien Francillon, Boris Danev, and Srdjan Capkun. Relay attacks on passive keyless entry and start systems in modern cars. In *Proceedings of the 18th Network and Distributed System Security Symposium (NDSS)*, 2011.

[FHMM10] Lishoy Francis, Gerhard Hancke, Keith Mayes, and Konstantinos Markantonakis. Practical NFC peer-to-peer relay attack using mobile phones. In *International Workshop on Radio Frequency Identification: Security and Privacy Issues*, pages 35–49. Springer, 2010.

[GTG+05] Sinan Gezici, Zhi Tian, Georgios B Giannakis, Hisashi Kobayashi, Andreas F Molisch, H Vincent Poor, and Zafer Sahinoglu. Localization via Ultra-Wideband radios: a look at positioning aspects for future sensor networks. *IEEE signal processing magazine*, 22(4):70–84, 2005.

[Han06] Gerhard P Hancke. Practical attacks on proximity identification systems. In *2006 IEEE Symposium on Security and Privacy (S&P'06)*, pages 6–pp. IEEE, 2006.

[HK05] Gerhard P. Hancke and Markus G. Kuhn. An RFID Distance Bounding Protocol. In *Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks*, SECURECOMM '05, pages 67–73, Washington, DC, USA, 2005. IEEE Computer Society.

[HK08] Gerhard P Hancke and Markus G Kuhn. Attacks on time-of-flight distance bounding channels. In *Proceedings of the first ACM conference on Wireless network security*, pages 194–202. ACM, 2008.

[KAK+08] Chong Hee Kim, Gildas Avoine, François Koeune, François-Xavier Standaert, and Olivier Pereira. The Swiss-Knife RFID distance bounding protocol. In *International Conference on Information Security and Cryptology*, LNCS, pages 98–115. Springer, 2008.

[KL14] Jonathan Katz and Yehuda Lindell. *Introduction to modern cryptography*. Chapman and Hall/CRC, 2014.

[Kra03] Hugo Krawczyk. SIGMA: The 'SIGn-and-MAc' approach to authenticated Diffie-Hellman and its use in the IKE-protocols. In *CRYPTO 2003*, LNCS, pages 400–425, 2003.

[Li] Qinghua Li. Attacks to Fully Random OFDM Sounding Signal.

[LZP11] Steven Lanzisera, David Zats, and Kristofer SJ Pister. Radio frequency time-of-flight distance measurement for low-cost wireless sensor localization. *IEEE Sensors Journal*, 11(3):837–845, 2011.

[Mau12] Rainer Mautz. Indoor positioning technologies. *Habilitation Thesis*, 2012.

[MP08] Jorge Munilla and Alberto Peinado. Distance bounding protocols for RFID enhanced by using void-challenges and analysis in noisy channels. *Wireless communications and mobile computing*, 8(9):1227–1232, 2008.

[ORC17] Hildur Olafsdóttir, Aanjhan Ranganathan, and Srdjan Capkun. On the security of carrier phase-based ranging. In *CHES*, volume 10529 of *LNCS*, pages 490–509. Springer, 2017.

[Rap15] Jacek Rapiński. The application of ZigBee phase shift measurement in ranging. *Acta Geodynamica et Geomaterialia*, 12(291780), 2015.

[RCHBC09] Kasper Bonne Rasmussen, Claude Castelluccia, Thomas S. Heydt-Benjamin, and Srdjan Capkun. Proximity-based access control for implantable medical devices. In *Proceedings of the 16th ACM Conference on Computer and Communications Security*, CCS '09, pages 410–419, 2009.

[RDC15] Aanjhan Ranganathan, Boris Danev, and Srdjan Capkun. Proximity verification for contactless access control and authentication systems. In *Proceedings of the 31st Annual Computer Security Applications Conference*, ACSAC 2015, pages 271–280, New York, NY, USA, 2015. ACM.

[RS15] Jacek Rapinski and Michal Smieja. ZigBee ranging using phase shift measurements. *The Journal of Navigation*, 68(4):665–677, 2015.

[RTŠ+12] Aanjhan Ranganathan, Nils Ole Tippenhauer, Boris Škorić, Dave Singelée, and Srdjan Čapkun. Design and implementation of a terrorist fraud resilient distance bounding system. In Sara Foresti, Moti Yung, and Fabio Martinelli, editors, *Computer Security – ESORICS 2012*, volume 7459 of *LNCS*, pages 415–432, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

[Rv10] Kasper Bonne Rasmussen and Srdjan Čapkun. Realization of RF distance bounding. In *Proceedings of the 19th USENIX Conference on Security*, USENIX Security'10, pages 25–25, Berkeley, CA, USA, 2010. USENIX Association.

[SP07] Dave Singelée and Bart Preneel. Distance bounding in noisy environments. In *European Workshop on Security and Privacy in Ad-Hoc and Sensor Networks (ESAS)*, LNCS, pages 101–115. Springer-Verlag, 2007.

[TAO] TAOGLAS WDMP.2458.A. https://www.taoglas.com/product/wdma-2458-a-2-45-8ghz-mechanical-patch-antenna/.

[TLKC15] Nils Ole Tippenhauer, Heinrich Luecken, Marc Kuhn, and Srdjan Capkun. UWB rapid-bit-exchange system for distance bounding. In *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, page 2. ACM, 2015.

[Tv09] Nils Ole Tippenhauer and Srdjan Čapkun. ID-based secure distance bounding and localization. In *Proceedings of the 14th European Conference on Research in Computer Security*, volume 5789 of *LNCS*, pages 621–636, Berlin, Heidelberg, 2009. Springer-Verlag.

[Woo19] Martin Woolley. Bluetooth direction finding: A technical overview, 2019.

[ZRG+19] Pouria Zand, Jac Romme, Jochem Govers, Frank Pasveer, and Guido Dolmans. A high-accuracy phase-based ranging solution with Bluetooth Low Energy (BLE). In *IEEE Wireless Communications and Networking Conference (WCNC) 2019*. IEEE, 2019.

A MCPD Range Estimation

It is well known that the phase shift introduced by a pure Line-of-Sight (LOS) radio channel on a radio signal is a linear function of both frequency (f_i) and range (r) [ZRG+19, BRGD20], i.e.,

$$\phi(f_i, r) = -2\pi f_i r/c \mod 2\pi\,, \tag{10}$$

where c is the speed of light and $i \in \{1, \cdots, N\}$ is an integer denoting the frequency being used. One can use this property to estimate the range between two nodes as follows.

The verifier transmits a tone signal (continuous wave signal) at a given frequency to which the prover may lock its LO and retransmits the signal back to the verifier or instead of phase locking, the prover can measure the phase difference between its LO and the received signal without modifying the phase and then transmits back a tone signal that has a phase that depends solely on the prover's LO. Hence, the verifier and the prover will measure the following phase, respectively,

$$\phi_V(f_i, r) = -2\pi f_i \left(\frac{r}{c} - \Delta_t\right) + \theta_i \mod 2\pi \tag{11}$$

$$\phi_P(f_i, r) = -2\pi f_i \left(\frac{r}{c} - \Delta_t\right) - \theta_i \mod 2\pi\,, \tag{12}$$

where Δ_t is the time-offset between the verifier and the prover, and θ_i is the phase difference between the two LOs signal at the verifier and the prover at frequency i. After summing the measured phase at the verifier and prover, the resulted two-way phase difference will be independent of the time offset, Δ_t, and phase offset, θ_i. Hence, the phase difference is,

$$\phi_{2W}(f_i, r) = \phi_V(f_i, r) + \phi_P(f_i, r) = -4\pi f_i r/c \mod 2\pi\,. \tag{13}$$

We should note that the phase measurements taken at the verifier and the prover should be available at one of the nodes, typically the verifier. We should also note that the range ambiguity now becomes half a wavelength. In order to resolve the range ambiguity, the phase shift at two (or more) distinct tones is measured. In this case, the range ambiguity will depend on the frequency difference (Δ_f) of both tones

$$\Delta_{\phi(N)} = \phi_{2W}(f_N, r) - \phi_{2W}(f_{N-1}, r) = -\frac{4\pi\Delta_f}{c} r \mod 2\pi\,. \tag{14}$$

Hence the estimate for the range is,

$$\hat{r} = -\frac{c}{4\pi\Delta_f}\hat{\Delta}_{\phi(N)} \mod \frac{c}{2\Delta_f}, \tag{15}$$

where $c/2\Delta_f$ is the range ambiguity. This procedure can be performed on N tones where the average phase difference is obtained as,

$$\hat{\Delta}_\phi = \frac{1}{N-1} \sum_{i=1}^{N-1} \hat{\Delta}_\phi[i] \mod 2\pi \,. \tag{16}$$

Hence, by transmitting multiple tone signals at different frequencies, the bandwidth has effectively been increased by a factor of $N-1$, without reducing the unambiguous range.