UWB with Pulse Reordering:
Securing Ranging against Relay and Physical-Layer Attacks

Mridula Singh
ETH Zurich

Patrick Leu
ETH Zurich

Srdjan Čapkun
ETH Zurich

Abstract

Physical-layer attacks allow attackers to manipulate (spoof) ranging and positioning. These attacks had real-world impact and allowed car thefts, executions of unauthorized payments and manipulation of navigation. UWB impulse radio (UWB-IR) has emerged as a prominent technique for precise ranging that allows high operating distances despite power constraints by transmitting multi-pulse symbols. Unfortunately, longer symbols make UWB-IR vulnerable to physical-layer attacks. Currently, none of the existing systems is precise, performant and secure at the same time. We present *UWB with pulse reordering* (UWB-PR), the first modulation scheme that secures distance measurement between two mutually trusted devices against all physical-layer attacks without sacrificing performance and irrespective of the environment or attacker. We analyze the security of UWB-PR under the attacker that fully controls the communication channel and show that UWB-PR resists even such a strong attacker. We evaluate UWB-PR within a UWB system built on IEEE 802.15.4f and show that it achieves distances of up to 93m with 10cm precision (LoS).

1 Introduction

Proximity and distance have been so far used in a number of security and safety-critical applications. Proximity can indicate an intent to open cars, offices, execute payments, establish cryptographic keys and access data. Measurement of distances and position helps devices navigate, find other devices and optimize message routing. Numerous wireless ranging and localization techniques have been developed in the last decade. These are based on time of arrival, time difference of arrival, phase [1] as well as RSSI measurements [2]. However, these techniques have been shown to be vulnerable to physical-layer attacks [3]; most notable examples include spoofing attacks on GPS [4, 5], relay attacks on passive entry/start systems in cars [6] and credit card payments [7]. Those vulnerabilities have real-world implications, as shown by a recent car theft that found widespread media attention [8].

In attacks on ranging, manipulations on the physical layer allow the attacker to reduce distances that devices measure, therefore violating the security of the systems that rely on this information (e.g., allowing the car to be unlocked and started [6]). At the logical layer, such manipulations, called *Mafia Fraud* Attacks are easily prevented using distance-bounding protocols [9]. Unlike logical-layer attacks that use manipulations of message bits, physical-layer attacks involve the manipulation of signal characteristics with the goal of fooling the receiver into decoding incorrect bits or incorrectly measuring signal phase, amplitude or time of arrival. A number of ranging systems have been shown to be vulnerable to physical-layer attacks: e.g., UWB 802.15.4a to Cicada attack [10], Phase ranging [11] to phase manipulation [12] and early detect / late commit (ED/LC) [13], Chirp Spread Spectrum to ED/LC [14]. These attacks are effective despite authentication and distance-bounding protocols [9, 15], since they target the physical layer and do not change the message content.

Prior research in the prevention of physical-layer attacks [16, 17] has shown that these attacks can be prevented using short symbols (typically UWB pulses) for precise time-of-flight (ToF) measurements. This results in modulations that encode each symbol as a single UWB pulse [16]. Instantaneous transmit power in any practical UWB system faces constraints originating from both regulatory bodies as well as hardware integration concerns. This results in limitations on the amount of energy that can be placed in a short time frame and renders single pulse systems inadequate for non-line-of-sight (NLoS) and long-distance communication. Therefore, for distance measurement under such conditions, we need longer symbols with multiple pulses per symbol. However, increasing the symbol length has shown to be vulnerable to ED/LC [13], enabling a distance reduction attack by an untrusted (i.e. external) man in the middle. This is essentially a comeback of Mafia Fraud, an attack assumed to be solved on the logical (bit-) level through a rapid bit exchange, this time executed purely on the symbol level, in a way independent of guarantees provided by distance-bounding protocols. With respect to this attack, existing systems can be either secure or performant, in terms of their range and resilience to NLoS conditions under power constraints, but not both.

In this work, we address this problem and propose *UWB with pulse reordering* (UWB-PR), the first modulation scheme that secures distance measurement between two mutually trusted devices against all physical-layer distance reduction attacks and enables long-range distance measurements. UWB-PR prevents Mafia-Fraud-like attacks at the physical layer. UWB-PR uses pulse reordering and cryptographic pulse blinding to prevent physical-layer attacks, allowing UWB systems to securely scale to longer symbols (multiple pulses per bit) for long distance and performance. UWB-PR is compatible with 802.15.4f UWB as well as FCC and ETSI regulations. It provides quantifiable probabilistic security guarantees without making any assumptions regarding channel conditions or attacker positions. Finally, UWB-PR combines data transfer and distance measurement and allows secure distance measurement on multi-bit nonces. It is therefore compatible with the majority of existing distance-bounding protocols [9, 18].

We analyze the security of UWB-PR analytically and through simulations. We show that, at any symbol length, UWB-PR allows to extract security guarantees from longer nonces n_{VE} and n_{PR} in two ways. First, more bits interleaved by means of the reordering operation lower an attacker's chances of guessing any individual bit. Second, longer overall nonces decrease the chances of an attacker guessing the entire sequence n_{VE} or n_{PR}, as all bits have to be guessed correctly.

We further implemented UWB-PR within a UWB transceiver and show that it achieves a range of 93m with a precision of 10cm.

This work shows that a number of assumptions that were made with respect to the design and implementation of distance-bounding protocols are not correct. In particular, we show that these protocols do not need to rely on the rapid bit-exchange. We discuss this further in Section 6.2.

The remainder of this paper is organized as follows. In Section 2, we provide some background on distance-bounding protocols and introduce different physical-layer attacks. Section 3 outlines the existing conflict between performance and security in UWB-IR systems. We introduce our approach in Section 4 and analyze its security in Section 5. Section 6 discusses the performance and security of our 802.15.4f-compatible proposal in relation to the 802.15.4a standard as well as implications and limitations of our approach.

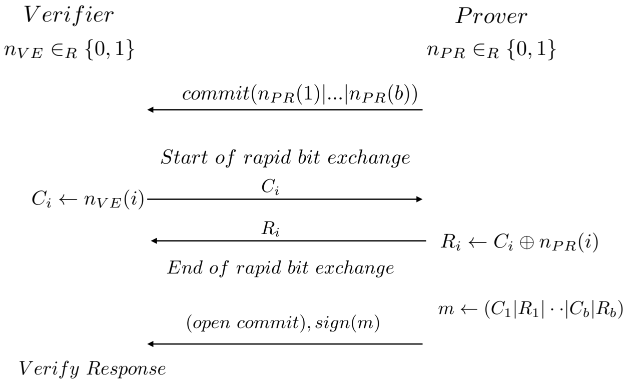
$Verifier$
$Prover$
$n_{VE} \in_R \{0,1\}$
$n_{PR} \in_R \{0,1\}$
$commit(n_{PR}(1)|...|n_{PR}(b))$
$Start\ of\ rapid\ bit\ exchange$
$C_i \leftarrow n_{VE}(i)$
C_i
R_i
$R_i \leftarrow C_i \oplus n_{PR}(i)$
$End\ of\ rapid\ bit\ exchange$
$m \leftarrow (C_1|R_1|\cdot\cdot|C_b|R_b)$
$(open\ commit), sign(m)$
$Verify\ Response$

Figure 1: The Brands-Chaum distance-bounding protocol provides security against Mafia Fraud at the logical layer.

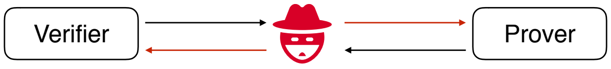

Figure 2: In Mafia Fraud, an external attacker reduces the distance measured between two mutually trusted parties.

2 Background

2.1 Distance-Bounding Protocols

Distance-bounding protocols are challenge-response protocols designed to determine an upper bound on the physical distance between two communicating parties, therefore preventing distance-reduction attacks. To secure ranging, distance-bounding protocols send cryptographically generated challenges and expect the correct response within a certain time window. The first distance-bounding protocol was proposed by Brands and Chaum and is illustrated in Figure 1. In this protocol, the verifier (VE) challenges the prover (PR) with a random nonce n_{VE} and measures the time until it receives the response, calculated by the prover using his secret n_{PR}. This time is then converted into an upper bound on the distance between the verifier and the prover. The Brands-Chaum protocol prevents distance reduction from an external attacker. This type of attacker model is known as Mafia Fraud and depicted in Figure 2. More recent distance-bounding protocols focus on other types of attacks, such as Terrorist Fraud and Distance Hijacking [19, 20, 21, 18].

Given the assumption that the attacker fully controls the communication channel between VE and PR, the attacker can always increase the measured time and therefore the measured distance. However, the attacker cannot trivially reduce this distance - unless it can guess n_{VE} or n_{PR} or manipulate the time of flight by attacking the physical layer. Longer nonces n_{VE} and n_{PR} lower an attacker's chances of guessing all bits.

The only remaining concern in these protocols are therefore physical-layer attacks by which an attacker can try to

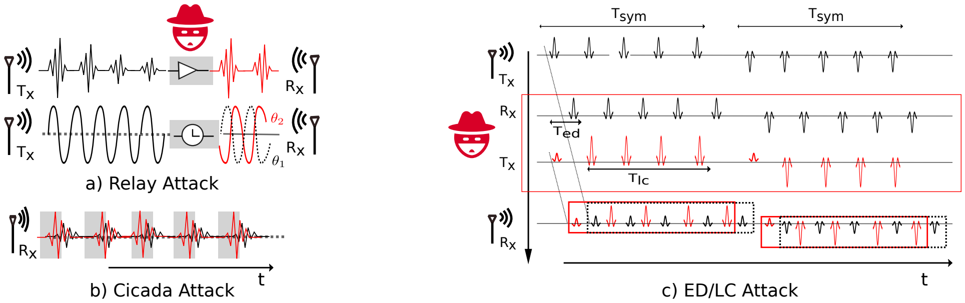

Figure 3: Existing distance-measurement techniques are all vulnerable to physical-layer attacks. RSSI and phase-based ranging have been shown to be vulnerable to relay attacks. Time-of-flight and time-delay-of-flight ranging have been attacked in Cicada and ED/LC attacks.

trick PR (resp. VE) to measure an earlier arrival time of n_{VE} (resp. n_{PR}). If this attack succeeds, the measured distance will be shorter than the actual distance. The success of such a physical-layer attack depends on the ranging system and on the modulation scheme that supports it. As we show in the review below, all existing ranging schemes are vulnerable to physical-layer attacks.

2.2 Physical-Layer Attacks

Existing ranging systems are typically vulnerable to one of three types of attacks: Relay, Cicada [3] and Early-Detect/Late-Commit. These are illustrated in Figure 3.

Relay Attack: In a relay attack, the signal is fed through an alternative signal propagation path by an attacker, allowing the attacker to exert control over some physical properties of the signal. Specifically, the attacker can control signal strength as well as the signal phase. To attack an RSSI based ranging system, the attacker simply amplifies the signal close to the transmitter until the received signal strength is consistent with the expected path loss over the claimed distance. Similarly, the signal phase can be manipulated by the attacker in order to be consistent with the propagation delay introduced by the claimed distance. Relay attacks are conceptually simple and have been successfully performed in a number of systems including WiFi [22], PKES systems [6] and NFC [7]. It is important to note that a relay by definition serves to extend the communication path, thereby increasing the time of flight of the signal. Therefore, any ranging system relying on a signal's time of flight is inherently resistant to a relay attack, no matter the capability of the relay (e.g., it being duplex or not).

Early-Detect and Late-Commit (ED/LC) Attack: In this attack, the attacker learns symbol values early and commits them late in order to fool receivers about the signal arrival time. An attacker thereby relies on the predictability of the inner signal structure of a symbol. In an early-detection phase, the adversarial receiver detects a symbol using only the initial part of the symbol - i.e., within time $T_{ED} < T_{sym}$. The detection of the symbol is possible within T_{ED} as the attacker can position his receiver close to the transmitter and get a higher SNR than the legitimate receiver. In a late-commit phase, the adversary forges the symbol such that the small initial part of the symbol is noncommittal (i.e., does not indicate a bit), whereas the last part of the symbol T_{LC} corresponds to one of the bits. In this way, the attacker can start sending a symbol before knowing which symbol should be sent. This attack has been demonstrated on time-of-flight-based systems, such as 802.15.4a Chirp Spread Spectrum [14] and 802.15.4a IR-UWB [23, 24]. Section 6 discusses in more detail the implications of ED/LC attacks in the context of IEEE 802.15.4a.

Cicada Attack: Time-of-flight (ToF)-based ranging systems rely on fine time resolution to estimate distance precisely. The Cicada attack [10] exploits the search algorithm that is used in UWB ToF systems which first detects the peak pulse and then performs a search to find the leading pulse edge. In this attack, the attacker injects pulses ahead of the legitimate pulses that are exchanged between the communicating devices. When receivers then detect the time of arrival of the pulse, they will perform a search, now extended due to attackers injected signals, and will, therefore, register an earlier arrival time. This attack has been demonstrated on 802.15.4a IR-UWB [10]. Limiting the search window can prevent this attack, but it affects the performance of the system. The Cicada attack shows that a careful design of time-of-arrival detection is needed in the design of secure distance measurement radios.

3 Problem Statement

Impulse-radio UWB systems are ideal candidates for high-precision ranging, and low-power IR-UWB ranging systems are becoming commercially available [25, 26]. IR-UWB ranging systems rely on signal time-of-flight for distance measurement. ToF ranging systems are inherently secure against relay attacks. A relay serves the attacker to extend the communication range, which increases the time of flight.

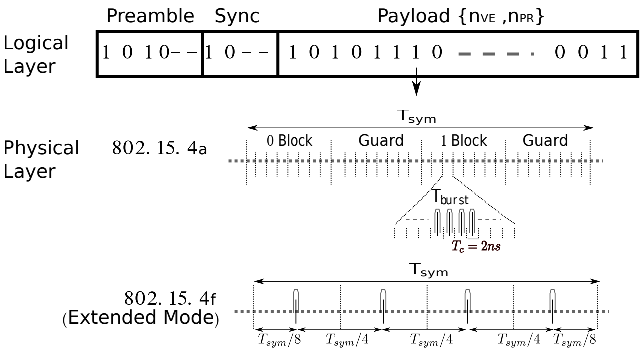

Figure 4: 802.15.4a and 802.15.4f propose different modulations for mapping a ranging packet to a physical signal. This illustration refers to the respective modes geared towards long distances.

Another attack type introduced, the Cicada attack, can be prevented by the receiver limiting the search window. The only remaining threat to be addressed is the ED/LC attack, especially at increasing symbol lengths. Cryptographic operations in distance-bounding protocols are currently limited to the logical layer (i.e., the bit-level) and, hence, cannot address this problem. The goal of this work is to close this gap towards full ED/LC resistance by cryptographically securing the underlying modulation.

3.1 IR-UWB

IEEE 802.15.4a and IEEE 802.15.4f have standardized IR-UWB as the most prominent technique for precision ranging. These standards allow the use of a 500MHz-bandwidth channel located in a frequency range between approximately 3GHz and 10GHz. Transmit power is limited by FCC and ETSI regulations. The standards do not specify transmitter or receiver implementations. Nevertheless, they propose different modulation schemes and receivers suitable for ranging. Both standards include separate operating modes for long and short-range use. 802.15.4a uses pulse position modulation and longer symbols. This increases robustness but makes the modulation vulnerable to ED/LC attacks [23]. 802.15.4f supports a base mode that encodes each bit in one pulse (on-off keying) as well as extended and long-range modes that encode each bit in multiple UWB pulses. The modulations as proposed in IEEE 802.15.4a and 802.15.4f are illustrated in Figure 4.

A short symbol given by a single narrow pulse (1-2ns) can be considered secure against an ED/LC attack and is, therefore, a good basis for secure ranging. In [13], Clulow et al. conclude that a system relying on longer symbols is inherently vulnerable to ED/LC attacks. They propose to minimize symbol length, leaving little room for an ED/LC attack. These considerations suggest the base mode of IEEE 802.15.4f be secure against ED/LC attacks. However, due to the limit on transmit power, its use is constrained to short-range LoS scenarios. The extended and long-range modes of 802.15.4f rely on more pulses per bit, increasing the range and providing robustness in indoor NLoS scenarios. Unfortunately, due to long symbol lengths and predictable symbol structures, these modes are vulnerable to ED/LC attacks. The problems in IEEE 802.15.4a seem more fundamental and will be discussed in Section 6. In any case, the need for multiple pulses seems to be vital for increased communication distance or when dealing with NLoS conditions.

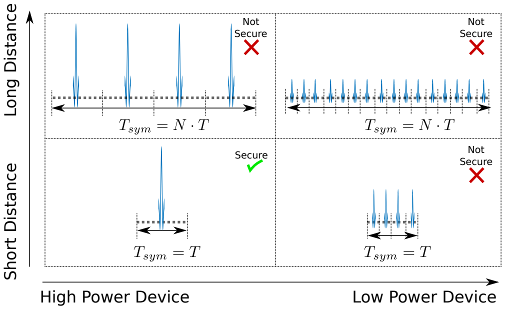

Figure 5: There are two independent causes driving the need for more pulses per symbol: Low instantaneous power and high performance in terms of energy per symbol, both under compliance with regulatory constraints.

3.2 Single-Pulse vs. Multi-Pulse Systems

Because UWB systems operate over wide segments of licensed spectrum, they have to be compliant with stringent regulatory constraints. Firstly, the power spectral density cannot exceed -41.3dBm/MHz, averaged over a time interval of 1ms. Secondly, the power measured in a 50MHz-bandwidth around the peak frequency is limited to 0dBm.

Long symbols are associated with unfavorable outcomes in ED/LC attacks. Therefore, a reasonable assumption might be that a system aiming primarily for security and long distance will first try to maximize the power per pulse and then the pulse repetition frequency (PRF), in order to guarantee highest possible energy per symbol while keeping the symbol as short as possible. Optimally, such a system would hence exactly meet both constraints. Maxing out the average constraint can only be done for certain PRFs, however. Specifically, all PRFs below 187.5 kHz are less than optimal due to the power per pulse saturating under the peak power constraint [27].

Consequently, a single pulse per bit sent at a PRF of 187.5kHz could theoretically be considered optimal in terms of security and performance. In practice, there exist legitimate incentives for higher PRFs and also increased numbers of pulses per bit, however. Data rates exceeding 187.5kbps can only be offered at higher PRFs since the bit rate cannot exceed the pulse rate in binary pulse-position modulation (PPM) or on-off keying (OOK), which are the modu-

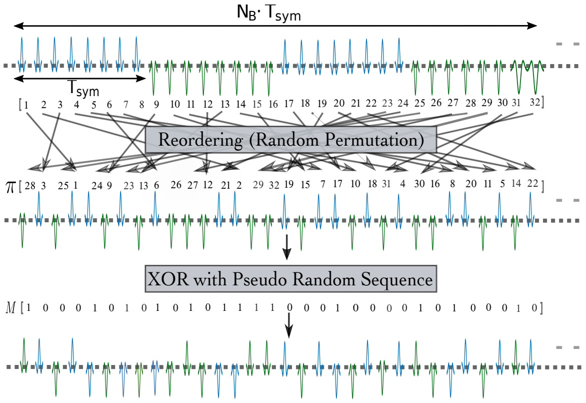
$N_B \cdot T_{sym}$
T_{sym}
[1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32]
Reordering (Random Permutation)
π [28 3 25 1 24 9 23 13 6 26 27 12 21 2 29 32 19 15 7 17 10 18 31 4 30 16 8 20 11 5 14 22]
XOR with Pseudo Random Sequence
M [1 0 0 0 1 0 1 0 1 0 1 0 1 1 1 1 0 0 0 1 0 0 0 0 1 0 1 0 0 0 1 0]

Figure 6: UWB-PR randomly reorders UWB pulses associated with N_B consecutive bits and cryptographically blinds their polarities before transmission. UWB-PR employs OOK, however, for visualization purposes, off-slots are shown as pulses with negative polarity.

lations used by 802.15.4a and 802.15.4f. Moreover, the instantaneous power can be a serious limitation imposed by the hardware, especially at high integration densities. Likely to accommodate for the latter, 802.15.4a, for instance, offers a range of different configurations, each with similar energy per symbol, but varying PRFs and energy levels per pulse. This underscores the practical necessity of spreading out energy across pulses, even if regulations might not require it.

Given a certain PRF, increased performance and distance can always be achieved by increasing the symbol length. This fact gets reflected well in the extended mode of 802.15.4f, where a symbol consists of four pulses as compared to only one pulse in the base mode. However, the PRF remains unchanged (and, in particular, uniform).[1] As a consequence, this approach allows to achieve virtually arbitrary symbol energy, without violating regulatory and other power constraints, by constructing ever longer symbols.[2] Due to this property, we built on 802.15.4f with UWB-PR. We will discuss this choice at greater lengths in Section 6. However, without securing the modulation, what essentially constitutes repetition coding is still highly vulnerable to ED/LC attacks. This is the problem addressed in UWB-PR.

We conclude that a) irrespective of the PRF, longer symbols and more pulses per symbols reliably provide higher distances and b) maxing out pulse power according to regulations might not be viable due to hardware constraints. This means that, for meaningful distances, a practical, highly integrated system will likely use multi-pulse symbols (and therefore be vulnerable to ED/LC attacks on the symbol level). These considerations are summarized in Figure 5.

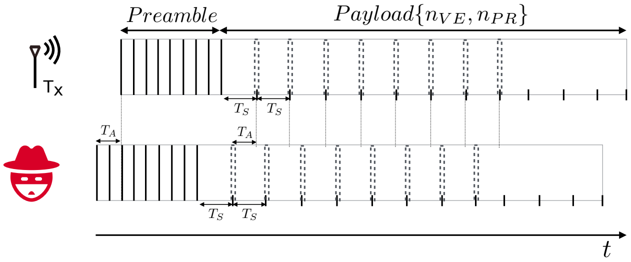

Figure 7: In a distance commitment, the timing of the preamble is binding w.r.t. the timing of subsequent secret information.

4 UWB with Pulse Reordering

UWB-PR is a new modulation technique that enhances the extended mode of 802.15.4f with pulse reordering and cryptographic pulse blinding to prevent all physical-layer attacks on ranging, including ED/LC, while retaining the range and performance of the extended mode. To the best of our knowledge, UWB-PR is the first modulation to prevent ED/LC attacks independently of communication range offered.

The main intuition behind UWB-PR is provided in Figure 6 and can be summarised as follows. UWB-PR randomly reorders the UWB pulses that are associated with each bit and cryptographically blinds their polarity before transmission. Since a successful ED/LC attack is based on the attacker knowing the shape of the symbol as well as when the symbol starts and ends, pulse reordering prevents this attack by blinding the pulse polarity, through XOR with a preshared sequence, and by reordering pulses such that the attacker does not know which pulse belongs to which bit (i.e., where each bit starts/ends).

In ED/LC, the attacker implicitly relies on deterministic mappings between symbol positions and bits. In both 802.15.4a and 802.15.4f, this assumption is justified, since symbols consist of consecutive UWB pulses. UWB-PR introduces uncertainty for an ED/LC attacker in both assessing past symbols and deciding when to interfere in the future (in order to affect a certain bit). While ED/LC attacks require an attacker being able to effectively decouple timing from cryptographic uncertainty, the reordering of UWB-PR cryptographically couples the random bits and pulse timings. As a consequence, an attacker has to guess correctly both the symbol values and symbol timings in order to guess a bit and is uncertain about the progress of the attack at any time.

Distance Measurement with UWB-PR While UWB-PR secures the payload of each transmission, the structure of the preamble at the beginning of each bit sequence is no secret. The receiver relies on this preamble for time synchronization. In the context of distance bounding, the timing of the preamble equated to a distance commitment as introduced in [16] and illustrated in Figure 7. While an attacker can

[1] Because the (local) PRF does not depend on the symbol duration here.
[2] Assuming that the oscillator drift remains reasonably bounded.

trivially send the preamble early in an attempt to reduce the distance, he still has to guess subsequent protected symbols to be successful. The preamble does not contain any information about the nonces n_{VE} and n_{PR}. The timing of the preamble simply tells the receiver when to expect this secret information. Correct detection and verification then depend on this time offset being consistent with the actual timing of the UWB-PR pulses constituting n_{VE} and n_{PR}. The timing of the preamble is therefore binding. If the preamble is sent early, each subsequent pulse will be expected earlier by the receiver, essentially forcing an attacker to guess each pulse for successful verification. If the preamble alone is sent early, the receiver will detect the inconsistency in the timing of the preamble and the secret payload or might not be able to recover the data at all, dismissing the claim in both cases.

4.1 Tx/Rx Chain

Previous considerations make an OOK modulation as used in 802.15.4f a reasonable choice for our system. In the following, we introduce the major steps involved in transmission and reception of a bit sequence with UWB-PR. This involves the encoding, which accommodates our main security features, as well as the continuous time signal representation and subsequent decoding.

Pulse Reordering As part of the encoding, we introduce a reordering of pulses that interleaves symbols of multiple consecutive bits. Consider first a deterministic encoding with N_P UWB pulses per bit. The reordering function R reorders the pulses of N_B consecutive bits as defined by a permutation π. π specifies the mapping between pulse positions before and after reordering. Π denotes the set of all possible reorderings. There are $|\Pi| = (N_P \cdot N_B)!/(N_P)^{N_B}$ ways to assign the pulses to bits, all equally probable from the attacker's point of view. We design the system to choose a fresh, random reordering $\pi \in \Pi$ for each frame. This secret is assumed to be shared between verifier and prover before the ranging phase. The reordering function subject to some permutation is defined as

$$R(P,\pi) = (p_{\pi(0)}, ..., p_{\pi(N_P \cdot N_B - 1)}).$$

The reordered pulse sequence can in general be defined as

$$\hat{P} = R(P,\pi),\ \pi \overset{UAR}{\leftarrow} \Pi.$$

The choice of π being a secret shared by transmitter and receiver, an attacker has no knowledge that allows to link pulse positions to bits. From an attacker's point of view all $|\Pi|$ reorderings are equally probable.

Pulse Blinding In addition to randomizing the pulse positions, we suggest to XOR the resulting sequence with a random bitmask M. We define the UWB-PR pulse sequence as the XOR of the reordererd pulse sequence and a random bitmask:

$$\tilde{P} = \hat{P} \oplus M,\ M \overset{UAR}{\leftarrow} \mathscr{M}$$

The idea behind this is to guarantee high entropy in the resulting pulse sequence, irrespective of the choice of codes and bit sequences n_{VE} or n_{PR} at higher protocol layers. Again, we assume that M is chosen randomly for each exchange and shared between prover and verifier befor the ranging phase.

Modulation In OOK, a binary sequence is encoded as a pulse either being present or absent at a known time. We consider regularly spaced pulse positions with period T_P. Under these assumptions, the transmit signal for a pulse sequence $\tilde{P}^{(b_1,...,b_{N_B})}$ of N_B interleaved bits consisting of N_p pulses each can be written as

$$s(t) = \sum_{k=0}^{N_B \cdot N_P - 1} \tilde{P}^{(b_1,...,b_{N_B})}[k] g(t - kT_P),$$

for a UWB base pulse g.

Demodulation The receiver optimally collects the energy at time kT_P by applying a matched filter $h = g(-t)$ as

$$y[k] = (s * h)(kT_P) = ||g||^2 \tilde{P}^{(b_1,...,b_{N_B})}[k],$$

where $*$ denotes the convolution operation. The receiver can construct the energy profiles for the bit-0 hypothesis

$$\tilde{P}_{H_0^k} = R((...|| \underbrace{P^0}_{k\text{-th bit}} ||...),\pi) \oplus M,$$

and the bit-1 hypothesis as

$$\tilde{P}_{H_1^k} = R((...|| \underbrace{P^1}_{k\text{-th bit}} ||...),\pi) \oplus M,$$

by applying the same randomness π and M for reordering and cryptographic blinding as on the tranmsit side.

The sufficient statistics for the bit-wise hypothesis can be obtained by correlating the received energy with the expected energy profiles for each hypothesis:

$$\sigma^k = \sigma_1^k - \sigma_0^k = \langle y, \tilde{P}_{H_1^k} \rangle - \langle y, \tilde{P}_{H_0^k} \rangle$$

Because the codes are orthogonal and of equal parity, and neglecting all channel nonidealities, the ideal statistic at the receiver evaluates to

$$\sigma^k = \begin{cases} ||g||^2 N_P N_B/2, & \text{if } b_k = 1 \\ -||g||^2 N_P N_B/2, & \text{if } b_k = 0 \end{cases},$$

suggesting optimal detection of the k-th bit as

$$\hat{b}_k = \text{sign}(\sigma^k).$$

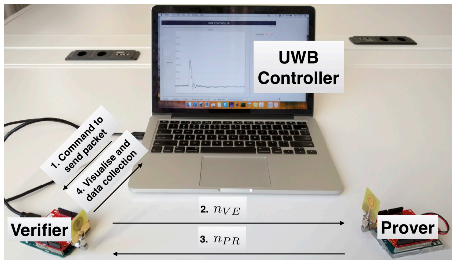

Figure 8: For our experimental setup, we chose LoS conditions and adapted the transmit power in order to simulate increasing path loss.

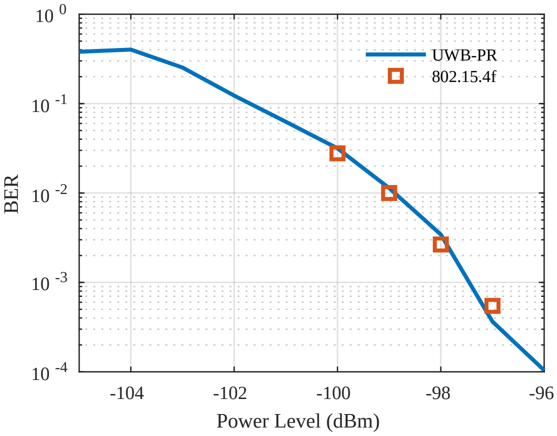

Figure 9: BER performance of UWB-PR as compared to 802.15.4f. Our experiments do not suggest any effect of the blinding and reordering operations on the bit error rate.

4.2 Proof-of-concept implementation

We evaluated UWB-PR in a prototype system transmitting OOK UWB pulses at a system bandwidth of 500MHz. The pulses are sent at a peak pulse repetition frequency (PRF) of 4MHz, i.e., with a spacing of 250ns. In terms of the regulatory transmission power constraints, this places UWB-PR in the regime dominated by the average constraint of -41.3dBm/MHz[3] [27].

The link budget of the resulting system depends on the number of pulses per symbol. Our implementation provides us with an equivalent link budget[4] of about 79dB if it relies on a single pulse per bit. Within this margin, it can tolerate additional losses due to distance and shadowing. For instance, this configuration would allow operations up to distances of ca. 32m under LoS conditions. Robustness of signal transmission and, in turn, the maximum operating distance can be further improved by increasing the number of pulses per bit.

For the experimental evaluation, we relied on 16 pulses per bit. This improves the link budget by 9dB to 88dB and results in an almost threefold maximum operating distance of 93m. There is no fundamental limitation to even longer symbols and corresponding distance improvements.

We evaluated the bit error rate for both a standard 802.15.4f-mode (i.e. without reordering) and a UWB-PR-mode relying on blinding and reordering over groups of four bits. Figure 8 shows our experimental setup. As the reordering can be configured in our prototypes we were able to use the same hardware for both runs. The results for the bit error rate as presented in Figure 9 do not indicate any difference between legacy and UWB-PR systems. We also note that the ranging precision of 10cm (LoS) is not affected by the reordering operation since the distance measurement is executed on the preamble in both cases and is therefore independent of this operation.

5 Security Analysis

UWB-PR is designed with the goal to provide performant ranging while guaranteeing quantifiable security against an external attacker. In particular, such an attacker should not succeed in reducing the distance between two mutually trusted parties, be it by means of a relay or by conducting any other physical-layer attack. A well designed ToF distance-bounding protocol is inherently resistant to a relay attack. Moreover, a Cicada attack can be prevented by limiting the search window for pulse detection, i.e. its success depends purely on receiver configuration. The only remaining option for an attacker to reduce the distance measured is by advancing the signals representing the nonces (n_{VE} and n_{PR}), i.e. by means of an ED/LC attack.

Since UWB-PR relies on a distance commitment for distance measurement, the attacker has to advance both preamble and payload data. The preamble is no secret and the attacker can send it in advance. However, the payload is cryptographically generated. Upon locking to the preamble, the receiver samples the payload pulses at specific times. The attack is only successful if the pulses sent by the attacker at these very instants yield the same correlation output at the receiver as the legitimate pulses.

The ED/LC attack required to advance the payload bits involves the attacker predicting part of the symbol. Conventional multi-pulse UWB systems help an attacker with that due to their predictable symbol structure.

In UWB-PR, on the other hand, the pulses representing N_B bits are reordered and their polarity is XORed with a secret sequence. An attacker does not know the pulse-to-bit mapping and the polarity of the pulses, but can only try to *guess* this information. Guessing allows an attacker to send his pulse before observing the corresponding legitimate pulse. As we do not place any limit on the attacker's reception capabilities, we assume that he can resolve the legitimate signal at the pulse level. As a consequence, the attacker obtains

[3] This corresponds to -14.3dBm over the entire system bandwidth.

[4] The maximum attenuation that still allows for successful ranging with likelihood > 0.01 per attempt.

feedback on the correctness of his pulse-guess immediately, before transmitting the next pulse. Moreover, we assume that the decision of the receiver only depends on the attacker signal, i.e. the effect of the legitimate signal being negligible. This reflects a scenario where the legitimate prover is not in the vicinity of the verifier. An attacker guessing a polarity sequence P_A, transmitted with a sequence of power levels A, results for the k-th bit in the receiver statics

$$\sigma_A^k = \|g\|^2 \langle AP_A, \tilde{P}^{(0,\ldots,b_k,0,\ldots)} \rangle.$$

The attack on the entire group of bits is successful iff

$$\mathrm{sign}(\sigma_A^k) = \mathrm{sign}(\sigma^k),\ \forall k \in (0,\ldots,N_B - 1),$$

i.e. all bits decoded at the receiver based on the statistics produced by the attacker signal match the legitimate bits.

Without reordering and pulse blinding, the attacker knows the value of a bit after observing a small part of the symbol. As will be introduced in the following, in UWB-PR, the guessing attacker's knowledge is only probabilistic.

5.1 Attacker Knowledge

Since the secret reordering and blinding sequences are chosen randomly for each transmission, an attacker cannot learn anything by observing multiple frames. Therefore, the evolution of an attacker's knowledge is confined to the specific pulse sequence within a single frame.

Attack Sequence S At each time t during an attack, the attacker knows all his past contributions in terms of transmission power and polarity as well as the true pulse polarities sent by the legitimate transmitter. Therefore, the attacker knows at each time all his past contributions to the bit-wise decision statistics $\sigma_A^k, k \in \{1,\ldots,N_B\}$, at the receiver. We call all the time-wise contributions by the attacker to a particular frame at time t the *attack sequence* and define it as

$$S = (s_1,\ldots,s_t),$$

where the contribution at time k is

$$s_k = A[k] \cdot P_A[k] \cdot \tilde{P}^{(b_1,\ldots,b_{N_B})}[k].$$

As the attacker proceeds through the attack (i.e, the frame), after each pulse transmission and subsequent disclosure of the actual pulse polarity, he is able to update his knowledge by appending the most recent correlation contribution

$$s_t = \begin{cases} A[t], & \text{if } P_A[t] = \tilde{P}^{(b_1,\ldots,b_{N_B})}[t] \\ -A[t], & \text{if } P_A[t] \neq \tilde{P}^{(b_1,\ldots,b_{N_B})}[t] \end{cases}$$

to the existing attack sequence.

Attack State Although the attacker sees each correlation contribution during the course of the attack, he is uncertain as to which bit each value contributes to. Therefore, what we call the attack state; the bit-wise intermediate correlation result, is in general not known to the attacker. However, the attacker can model the attack state as a random variable with a distribution based on the attack sequence. The uncertainty stems from the random reordering, each of which is equally likely from the attacker's point of view. This way, the attack state $(\sigma^1,\ldots,\sigma^{N_B})$ can be modeled as the joint distribution of all N_B bit-wise correlations, each of which can be sampled as

$$\sigma^k =$$

$$\langle R(S,\pi), \overbrace{(\ldots\|0,\ldots,0\|\underbrace{1,\ldots,1}_{k\text{-th bit}}\|0,\ldots,0\|\ldots)}^{N_B \text{ bits}} \rangle,\ \pi \overset{UAR}{\leftarrow} \Pi,$$

given a reordering π drawn uniformly at random and some attack sequence S. Sampling each of the N_B correlation values for many reorderings allows the attacker to approximate the probability distribution of the attack state.

If the attacker is in a state with all bit-wise correlations strictly positive, he has won. Therefore, we call these states *winning states*.

Current Advantage P_{win} Given some attack sequence and the corresponding state distribution, the attacker is interested in his chances of having already won. This probability we call the attacker's current advantage. Having obtained the probability distribution over all states for an attack sequence S, we can find the current advantage simply by summing the probabilities of all winning states:

$$\sum_{\text{All winning states given S}} P(s)$$

This number essentially represents the attacker's confidence in his past interferences. Because of the reordering being unknown, the attacker is in general not able to tell with certainty whether he has already won or not.

Future Opportunity $\overline{P}_{win}$ At each time during the attack, the attacker can try to look ahead and consider all future progressions of the attack sequence. This involves building a model that serves to estimate his chances of winning if he continues playing. Evaluating this future opportunity helps the attacker in two ways. First, it allows the attacker to choose his next transmission power optimally, in particular as the argument maximizing the future opportunity conditioned on this choice. Second, by comparing the future opportunity against the current advantage, an attacker can make an informed stopping decision during the attack. This means that, if the expected chances in the next step are, irrespective of the current energy level choice, worse than the current advantage, the attacker will stop interfering. In any case, building a model for estimating the future opportunity is very complex as it contains uncertainty about the current state, the reordering as well as the future pulse polarities and requires the attacker to essentially simulate his own behavior for the entire remaining pulse sequence. Due to the random reordering and pulse blinding, the only information the attacker has about the future is the number of pulses remaining as well as some partial knowledge about the current attack state.

5.2 Attack Strategies

The knowledge that informs the strategy of a guessing attacker can be split into past observations and a model for the future. However, as discussed previously, the guessing attacker's knowledge about future pulses is very limited. We, therefore, argue that any strategy an attacker employs to maximize his success chances is predominantly based on his assessment of the past, i.e. the probability of having won P_{win}. This value will evolve during the attack based on the attacker's guessing luck and the power levels he chooses for his pulses. In terms of strategy, we argue that an attacker's 'degrees of freedom' are given by a) his decision when to terminate the attack and b) the power levels chosen for the pulses. In our model, for the former, we choose an over-approximation on the attacker's knowledge informing the attack termination. The latter we model by means of two extreme strategies. A *Single-Power* attacker that keeps his transmission level constant throughout the attack and a *Multi-Power* attacker that is not limited in the number of power levels to choose from. We introduce these choices in the following.

Optimal Attack Termination As the knowledge about the future is very limited, an attacker is in particular not able to anticipate if a certain probability of winning can be achieved at any time in the future. As an over-approximation for the attacker's capabilities of assessing the future, we assume the attacker to stop at the ideal time w.r.t. his estimate of P_{win}, subject to his energy allocation strategy and a given attack sequence.

Single-Power Attacker (SPA) This is an attacker that sends all pulses at the same transmission power.

Multi-Power Attacker (MPA) This model captures a more powerful attacker that can transmit at varying power levels. Having a limited number of chances to guess a bit correctly, the aim of this attacker is to compensate for any wrong interference as soon as possible. Any pulse guessed wrong will cause this attacker to double his power level for the next transmission. This way, each correctly guessed pulse results in a correct bit. Consequently, each correct guess improves P_{win} and, if things don't go so well, chances of still guessing the bit remain nonzero as long one pulse for each bit remains (i.e., as long as possible).

5.2.1 Attack Simulation and Results

Both attackers were simulated in MATLAB. For a given (legitimate) polarity sequence, both models result in a deterministic attack sequence. This allowed obtaining attack success probabilities by simulating attacks on randomly sampled polarity sequences and reorderings efficiently. For a sampled polarity sequence, P_{win} was calculated by randomly sampling pulse reorderings. As explained previously, the peak P_{win} over the entire attack sequence was chosen to characterize the attacker's chances of winning for this given sequence (*Optimal Attack Termination*).

Figure 10 shows the attack success probabilities for different configurations of N_B and N_P. The results show that the security offered by UWB-PR increases for higher numbers of bits grouped together for reordering. For the configuration geared towards long distance, using 16 pulses per symbol, reordering of all bits reduces the single- and multi-power attacker success to no more than $4.5 \cdot 10^{-5}$ and $1.1 \cdot 10^{-3}$, respectively. The typical length of nonces n_{VE} and n_{PR} as used in distance-bounding protocols amounts to 20 bits. Extrapolating from our results, reordering all 20 nonce bits will decrease the attacker's chances of success further, likely below the 10^{-6} mark for the single-power attacker.

A system implementing UWB-PR faces the choice of how to split up the nonces into groups of bits that are reordered. Either all bits of the nonce can be reordered (i.e. $N_B = |n_{VE}| = |n_{PR}|$), or the nonces can be split into groups before reordering (i.e. $N_B < |n_{VE}| = |n_{PR}|$). Although increasing N_B shows to be the better choice for security, in some scenarios smaller groups might be favorable (such as when memory is limited). Important to note is that this does not necessarily get in the way of overall security, as the nonces can be chosen longer for compensation. In Table 1 we list the minimum required nonce lengths for both attackers and different configurations of UWB-PR, such that an attacker's success chances are below 10^{-6}.

5.3 Reordering is Key

Our simulation results show that the number of bits grouped together is an important security parameter, reducing the attacker's success chances rapidly. We can also observe that, for small numbers of bits reordered, the multi-power attacker becomes very strong, guessing the bits with probability close to one if the reordering is done on only two bits. It seems as if security is lost altogether without reordering, despite the attacker not knowing the polarity of individual pulses due to the pulse blinding. Indeed, if a system chooses not to reorder at all, an attacker that can increase transmit power at will has very high chances of guessing the bit. Specifically, he has N_P

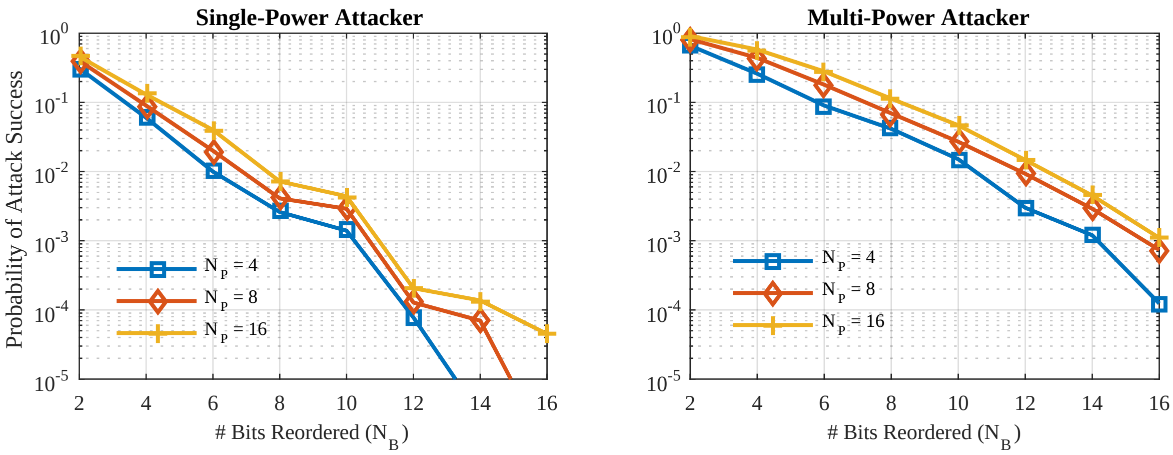

Figure 10: Grouping more bits together for reordering (i.e., increasing N_B) makes it harder for both attackers to guess any of the bits, reducing their probabilities of success. This allows compensating for the detrimental effects of longer symbols (higher N_P) on security.

	$N_P = 4$			$N_P = 8$			$N_P = 16$		
	$N_B = 2$	$N_B = 4$	$N_B = 6$	$N_B = 2$	$N_B = 4$	$N_B = 6$	$N_B = 2$	$N_B = 4$	$N_B = 6$
$\lvert n_{VE}\rvert$, $\lvert n_{PR}\rvert$ (SPA)	24	20	18	32	24	24	36	28	28
$\lvert n_{VE}\rvert$, $\lvert n_{PR}\rvert$ (MPA)	68	44	36	140	68	54	294	104	66

Table 1: Depending on the attacker and configuration of UWB-PR, different minimum nonce lengths are required to drive the overall attack probability below 10^{-6}. Besides reordering more bits, using longer nonces can serve to compensate the detrimental effects on security by longer symbols (higher N_P).

independent attempts, each with probability 0.5, since he can stop guessing once he has guessed one pulse correctly. The probability of guessing the entire bit follows as $1-0.5^{N_P}$, which amounts to 0.99998 for $N_P = 16$. Given that the simulated multi-pulse attacker is essentially an extension of this attacker type over reordered bits, and can be contained for more bits reordered, we argue that the reordering is vital in addressing this existing shortcoming in multi-pulse UWB systems. In consequence, security against ED/LC attacks requires the reordering to be a shared secret between verifier and prover, and unknown to the attacker.

6 Discussion

In the following, we first relate our proposal to the 802.15.4a standard. Then we discuss implications of our findings w.r.t. prevalent assumptions in the literature. We close the section by addressing the limitations of our approach.

6.1 802.15.4a with PR?

Until now, we assumed some form of OOK modulation to underly our system. As explained earlier, OOK seems a good fit for our system due to its simplicity. In the following, we investigate if some other modulation, e.g., as used in 802.15.4a, would also suit our requirements and could potentially form the basis of our scheme. To this end, we first describe the assumptions our security features in UWB-PR place on the underlying modulation. At the core of our system, for all security properties, we rely on the modulation consisting of basic energy units that are individually not vulnerable to ED/LC attacks. Typically, such a unit can be thought of as a pulse or group of pulses. These basic energy units have to satisfy the following requirements:

- *Atomicity*: An attacker cannot both detect and interfere with the signal due to its short duration. An ED/LC attack on this unit is therefore not possible.[5]
- *Associativity* w.r.t correlation: All reorderings of a sequence of units result in the same correlation output at the receiver. This is a requirement for guaranteed robustness of the system under all possible reorderings.
- *Bandwidth*: Precise ranging asks for high signal bandwidth.

[5] Under the assumption that the attacker's processing time is lower bounded by a few nanoseconds.

802.15.4a and 802.15.4f both specify UWB PHY modulations with bandwidths upwards of 500MHz. In general, this translates to nanosecond time resolution which satisfies requirements for centimeter-precision ranging. Therefore, the bandwidth requirement we consider met by both standards. Before we check if the other criteria could potentially be satisfied by 802.15.4a, we introduce some existing issues with its modulation.

Security problems of 802.15.4a In its 2007 amendment for ranging, 802.15.4a relies on a mix of burst position modulation (BPM) and binary phase shift keying (BPSK) to accommodate for both coherent and noncoherent transmitters and receivers. In BPM, time-wise coding gain is achieved by repeating a pulse within a short interval many times. In case of coherent operation, the burst is also associated with a polarity (phase). Fundamentally, and in comparison to 802.15.4f, we can think of basic energy units given by bursts of pulses instead of individual pulses. Due to the high rate of these pulses (499.2MHz) as well as channel multipath, it is unlikely for a non-rake receiver to resolve individual pulses. More likely, a receiver will just integrate the energy over the entire time slot of a burst, and obtain the timing and phase as an aggregate over all the pulses of a burst. This means that the shape of a burst does not contain any relevant information. Individual bursts can, in consequence, become a target for ED/LC attacks due to their unspecific and, hence, predictable structure. It has indeed been observed that, in 802.15.4a, an attacker can always decrease the distance by some value slightly smaller than the distance corresponding to the burst duration [24].

The standard advocates the use of more pulses per symbol for increased robustness and distance. However, an attacker's distance decrease improves with the amount of such temporal coding gain. This dependency is shown in Figure 11 for all mandatory configurations, where it is contrasted with the constantly small decrease possible in UWB-PR [6]. There we also see that, at high PRFs, more robustness comes at a high price in terms of security. This effect characterizes the regime of PRF>1MHz, where the power per pulse is limited by the regulatory constraint on average power [27]. Specifically, the comparably high PRFs supported by 802.15.4a are associated with small marginal SNR increases per pulse added. But each pulse added to the burst will proportionally increase its length T_{burst}, and give the attacker more time. This results in an unfavorable trade-off between performance and security, especially at high PRFs. Consequently, an 802.15.4a ranging system can be geared towards either security or performance, but not both.

In particular, all configurations place less energy on each pulse than the extended mode of 802.15.4f. This requires configurations to compensate excessively with temporal diversity in order to achieve comparable receive SNR. Indeed, the standard allows for long burst durations of up to roughly 256ns (125 times the minimum), along with proportionally increasing symbol durations. Unfortunately, for the highest mandatory PRF of 15.6MHz, this leads to a potential 153.6m and 2461.6m distance decrease by an ED/LC attacker in a coherent or noncoherent setting, respectively. Although one could argue that the option for shorter burst duration exists, a system opting for robust communication over distances exceeding a few meters will have no other choice than introducing temporal diversity and, due to FCC/ETSI regulations, longer symbol lengths. This becomes evident in Figure 11 when considering the NLoS path loss model which assumes a 20dB signal attenuation to an object (e.g., human body) blocking the direct path. We note that temporal diversity for meaningful operating distances is essential in any UWB system and also strongly incentivized by the 802.15.4a standard. We argue that 802.15.4a does even more so than 802.15.4f, since it operates with each pulse well below the peak power constraint of 0dBm per 50MHz, thereby relying even more on the temporal spreading of transmitting power. The core weakness of 802.15.4a, however, is that temporal diversity can only be gained by increasing the burst duration T_{burst}, which is not secure.

We exemplify this problem by comparing configurations of 802.15.4a and UWB-PR operating over identical bandwidths and allocating similar symbol energy under regulatory constraints. This way, we aim to compare configurations expected to offer similar ranges. With our proposed 16 pulses per symbol and mean pulse repetition frequency (PRF) of 2MHz in UWB-PR, we find in the 802.15.4a-configuration using 32 pulses per burst over a symbol duration of 8205.13ns our closest fit. In the coherent scenario, denoted as 802.15.4a (C), an attacker can decrease the distance by close to 20m, as compared to only less than 1m in UWB-PR. Even worse, if the system chooses to not convey any information in the signal phase, the modulation reduces to pure BPM, and the attacker can guess the symbol value ca. half a symbol duration in advance [24]. An attacker can then simply adapt his transmission power in the second symbol half to what he observes in the first half of the legitimate symbol. Correspondingly, the maximum distance decrease goes up to 2461.6m in this noncoherent scenario 802.15.4a (NC). This kind of attack represents a fundamental limitation of any noncoherent PPM/BPM system and its success is independent of the shape and duration of the pulse burst. Both results are listed in Table 2, where they are compared to the distance decrease possible under UWB-PR. Irrespective of the configuration chosen in 802.15.4a, higher symbol energy comes at the cost of longer symbol duration which is, in turn, associated with higher distance decreases in a noncoherent setting. This behavior is compared to UWB-PR in Figure 11.

[6] In this analysis, we use a simplified model on signal energy under regulatory constraints which do not consider non-idealities of the measurement hardware as introduced in [27].

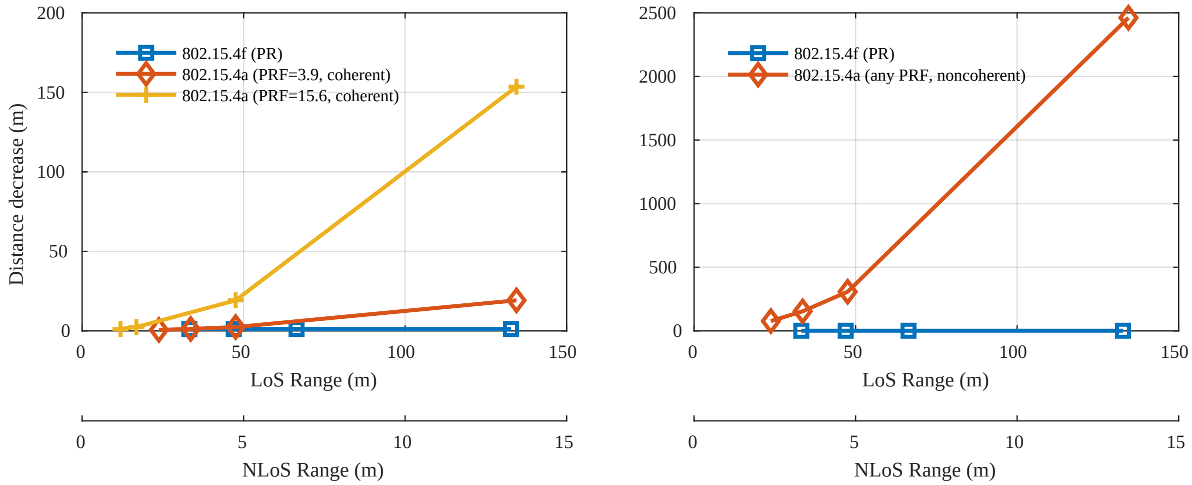

Figure 11: Distance decrease in the coherent (left) and noncoherent (right) scenario as a function of the estimated range offered. For comparability, all systems are assumed to use 500MHz bandwidth. NLoS refers to a scenario with 20dB attenuation of the direct path. Non-idealities of the measurement hardware were not considered.

	Law	**Decrease**
802.15.4a (NC)	$\sim 2\cdot(T_{sym}/2)$	2461.6m (8205.2ns)
802.15.4a (C)	$\sim 2\cdot T_{burst}$	38.46m (128.2ns)
802.15.4f (PR)	$\sim 2\cdot T_{pulse}$	1.2m (4ns)

Table 2: Ideal, non-guessing distance decrease for coherent (C) and noncoherent (NC) operation of 802.15.4a and our proposed UWB-PR. We assume 16 pulses (802.15.4a) per symbol.

	ISI (IPI)	**Precision**	**Range**	**ED/LC**
802.15.4a	×	√	√	×
802.15.4f (BM)	√	√	×	√
802.15.4f (EM)	√	√	√	×
UWB-PR	√	√	√	√

Table 3: UWB-PR is resistant to all physical-layer attacks while avoiding interference among pulses (respectively inter-symbol-interference, when reordering is considered) and providing long communication range.

We can summarise our insights as follows. With cryptographic reordering and blinding missing, the deterministic time-coding of 802.15.4a and 802.15.4f make both approaches vulnerable to ED/LC attacks. In 802.15.4f, we find a modulation scheme that provides atomic building blocks that can be effectively interleaved for security. That is why UWB-PR builds on 802.15.4f and introduces reordering of pulses among bit-wise time intervals in order to gain resistance against all physical-layer attacks, including ED/LC attacks. An overview of these considerations is provided in Table 3.

6.2 Implications

Clulow et al. [13] see in the rapid bit-exchange with single-pulse bits a design principle for secure distance-bounding systems. They argue that this design is necessary to prevent ED/LC attacks, i.e. distance reduction attacks that leverage multi-pulse symbols. With UWB-PR, we demonstrate that this assumption does not hold. Multiple bits can be part of a single frame used for secure distance measurement by using a distance commitment. In UWB-PR, the association between information bits extracted by the verifier and pulses observed by an attacker is cryptographically hidden. This way, ED/LC attacks can be prevented even if a bit is encoded redundantly in time, e.g., as multiple pulses. This allows scaling to better performance and increased distance without compromising on security. We argue that performance and resistance to ED/LC attacks are physical-layer concerns that also need to be addressed at this level of abstraction. A secure physical layer, such as UWB-PR, does not place constraints on the protocol layer, irrespective of performance (i.e., distance). In particular, multi-bit, robustly encoded nonces can be secured. Finally, fully decoupling physical-layer security from the protocol layer allows redeeming the security properties of existing distance-bounding protocols that have come under threat by ED/LC attacks. Namely, in [13], the authors claimed that, given ED/LC attacks, multi-bit challenge-response distance bounding and protocols such as proposed by Hu/Perrig/Johnson [28], Sastry/Shankar [29] and Capkun/Hubaux [30, 31] are broken. This work shows that this is not correct and that those protocols, when used on top of the secure physical layer (such as UWB-PR), resist ED/LC attacks.

6.3 Limitations

UWB-PR prevents all physical-layer attacks that would allow an attacker to decrease the distance between the verifier and trusted prover (Relay Attack, Mafia Fraud). However, UWB-PR as such does not help against a malicious prover aiming to reduce the distance measured (Distance Fraud). An attacker that knows the reordering and XOR sequence cannot be prevented from transmitting the reply early. This attacker can send the appropriate response n_{PR} as soon as it has observed at least one pulse of each bit in n_{VE}.

However, the reordering operation could also be a vital part of a solution to this problem. We argue that distance fraud could be prevented by keeping the reordering secret from the prover. The prover would then intermingle its nonce with the verifier's challenge purely on the physical layer, for example by adding the n_{PR} signal onto the received n_{VE} signal before transmitting the combined signal back. Precise time alignment is guaranteed by the preamble and serves to convince the verifier that the secret challenge was actually handled by the prover. Because the reordering is not known to the prover, it is not able to decode the challenge. As a consequence, the early inference of the challenge bit sequence n_{VE} can be prevented.

7 Conclusion

In this paper, we presented UWB-PR, a modulation scheme that secures ranging against all physical-layer attacks that enable Mafia Fraud. We provided quantifiable probabilistic security guarantees without making any assumptions regarding channel conditions or attacker positions. We showed that UWB-PR is unique compared to existing UWB systems in that it allows long-distance ranging without compromising on security. Measurements obtained with a prototype implementation of UWB-PR were aligned with that finding.

References

[1] Deepak Vasisht, Swarun Kumar, and Dina Katabi. Decimeter-level localization with a single wifi access point. In 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16), pages 165–178, Santa Clara, CA, 2016. USENIX Association.

[2] P. Bahl and V. N. Padmanabhan. 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), volume 2, pages 775–784 vol.2, 2000.

[3] A. Ranganathan and S. Capkun. Are we really close? verifying proximity in wireless systems. IEEE Security Privacy, 15(3):52–58, 2017.

[4] P. Papadimitratos and A. Jovanovic. Gnss-based positioning: Attacks and countermeasures. In MILCOM 2008 - 2008 IEEE Military Communications Conference, pages 1–7, Nov 2008.

[5] Todd E. Humphreys, Brent M. Ledvina, Mark L. Psiaki, Brady W. O'Hanlon, and Paul M. Kintner. Assessing the spoofing threat: Development of a portable gps civilian spoofer, volume 2, pages 1198–1209. 2008.

[6] Aurélien Francillon, Boris Danev, and Srdjan Čapkun. Relay attacks on passive keyless entry and start systems in modern cars. In Network and Distributed System Security Symposium (NDSS), 2011.

[7] Lishoy Francis, Gerhard Hancke, Keith Mayes, and Konstantinos Markantonakis. Practical relay attack on contactless transactions by using nfc mobile phones, 2012.

[8] "mercedes 'relay' box thieves caught on cctv in solihull.". http://www.bbc.com/news/uk-england-birmingham-42132689. [Online; Accessed 29. November 2017].

[9] Stefan Brands and David Chaum. Distance-bounding protocols. In Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology, EUROCRYPT '93, pages 344–359, Secaucus, NJ, USA, 1994. Springer-Verlag New York, Inc.

[10] M. Poturalski, M. Flury, P. Papadimitratos, J. P. Hubaux, and J. Y. Le Boudec. The cicada attack: Degradation and denial of service in ir ranging. In 2010 IEEE International Conference on Ultra-Wideband, volume 2, pages 1–4, Sept 2010.

[11] Atmel phase difference measurement unit. http://www.atmel.com/Images/Atmel-8443-RTB-Evaluation-Application-Software-Users-Guide_Application-Note_AVR2152.pdf. [Online; Accessed 23. October 2017].

[12] Hildur Ólafsdóttir, Aanjhan Ranganathan, and Srdjan Capkun. On the security of carrier phase-based ranging. In International Conference on Cryptographic Hardware and Embedded Systems, pages 490–509. Springer, 2017.

[13] Jolyon Clulow, Gerhard P. Hancke, Markus G. Kuhn, and Tyler Moore. So near and yet so far: Distance-bounding attacks in wireless networks. In Proceedings of the Third European Conference on Security and Privacy in Ad-Hoc and Sensor Networks, ESAS'06, pages 83–97, Berlin, Heidelberg, 2006. Springer-Verlag.

[14] Aanjhan Ranganathan, Boris Danev, Aurélien Francillon, and Srdjan Capkun. Physical-layer attacks on chirp-based ranging systems. In Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks, pages 15–26. ACM, 2012.

[15] Ioana Boureanu, Aikaterini Mitrokotsa, and Serge Vaudenay. Towards secure distance bounding. IACR Cryptology ePrint Archive, 2015:208, 2015.

[16] 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, WiSec '15, pages 2:1–2:12, New York, NY, USA, 2015. ACM.

[17] Kasper Bonne Rasmussen and Srdjan Čapkun. Realization of rf distance bounding. In Proceedings of the USENIX Security Symposium, 2010.

[18] 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.

[19] Chong Hee Kim, Gildas Avoine, François Koeune, François-Xavier Standaert, and Olivier Pereira. The swiss-knife rfid distance bounding protocol. In ICISC, volume 5461, pages 98–115. Springer, 2008.

[20] Agnès Brelurut, David Gerault, and Pascal Lafourcade. Survey of Distance Bounding Protocols and Threats. In Foundations and Practice of Security (FPS), pages 29 – 49, Clermont Ferrand, France, October 2015.

[21] Jason Reid, Juan M. Gonzalez Nieto, Tee Tang, and Bouchra Senadji. Detecting relay attacks with timing-based protocols. In Proceedings of the 2Nd ACM Symposium on Information, Computer and Communications Security, ASIACCS '07, pages 204–213, New York, NY, USA, 2007. ACM.

[22] H. T. T. Truong, Xiang Gao, B. Shrestha, N. Saxena, N. Asokan, and P. Nurmi. Comparing and fusing different sensor modalities for relay attack resistance in zero-interaction authentication. In 2014 IEEE International Conference on Pervasive Computing and Communications (PerCom), pages 163–171, March 2014.

[23] Manuel Flury, Marcin Poturalski, Panos Papadimitratos, Jean-Pierre Hubaux, and Jean-Yves Le Boudec. Effectiveness of distance-decreasing attacks against impulse radio ranging. In Proceedings of the Third ACM Conference on Wireless Network Security, WiSec '10, pages 117–128, New York, NY, USA, 2010. ACM.

[24] M. Poturalski, M. Flury, P. Papadimitratos, J. P. Hubaux, and J. Y. Le Boudec. Distance bounding with ieee 802.15.4a: Attacks and countermeasures. IEEE Transactions on Wireless Communications, 10(4):1334–1344, April 2011.

[25] 3db Access AG - 3DB6830 ("proximity based access control"). `https://www.3db-access.com/Product.3.html`. [Online; Accessed 23. October 2017].

[26] DecaWave "dw1000 product description and applications". `https://www.decawave.com/products/dw1000`. [Online; Accessed 23. October 2017].

[27] Robert J Fontana and Edward A Richley. Observations on low data rate, short pulse uwb systems. In Ultra-Wideband, 2007. ICUWB 2007. IEEE International Conference on, pages 334–338. IEEE, 2007.

[28] Y-C Hu, Adrian Perrig, and David B Johnson. Packet leashes: a defense against wormhole attacks in wireless networks. In INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies, volume 3, pages 1976–1986. IEEE, 2003.

[29] Naveen Sastry, Umesh Shankar, and David Wagner. Secure verification of location claims. In Proceedings of the 2nd ACM workshop on Wireless security, pages 1–10. ACM, 2003.

[30] Srdjan Capkun and J-P Hubaux. Secure positioning of wireless devices with application to sensor networks. In INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE, volume 3, pages 1917–1928. IEEE, 2005.

[31] Srdjan Capkun and J-P Hubaux. Secure positioning in wireless networks. IEEE Journal on Selected Areas in Communications, 24(2):221–232, 2006.