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

Mridula Singh
Dept. of Computer Science
ETH Zurich
mridula.singh@inf.ethz.ch

Patrick Leu
Dept. of Computer Science
ETH Zurich
patrick.leu@inf.ethz.ch

Srdjan Capkun
Dept. of Computer Science
ETH Zurich
srdjan.capkun@inf.ethz.ch

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, standardized within 802.15.4a,f, has emerged as a prominent technique for precise ranging that allows high operating distances despite power constraints by transmitting multi-pulse symbols. Security of UWB ranging (in terms of the attacker's ability to manipulate the measured distance) has been discussed in the literature and is, since recently also being addressed as a part of the emerging 802.15.4z standard. However, all research so far, as well as security enhancements proposed within this emerging standard face one main limitation: they achieve security through short symbol lengths and sacrifice performance (i.e., limit the maximum distance of measurement), or use longer symbol lengths, therefore sacrificing security. 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 distance shortening attacks without sacrificing performance, therefore simultaneously enabling extended range and security. We analyze the security of UWB-PR under the attacker that fully controls the communication channel and show that UWB-PR resists such strong attackers. We evaluate UWB-PR within a UWB system built on top of the IEEE 802.15.4 device and show that it achieves distances of up to 93m with 10cm precision (LoS). UWB-PR is, therefore, a good candidate for the extended mode of the new 802.15.4z Low Rate Pulse standard. Finally, UWB-PR shows that secure distance measurement can be built on top of modulation schemes with longer symbol lengths - so far, this was considered insecure.**

I. 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 [34] as well as RSSI measurements [7]. However, these techniques have been shown to be vulnerable to physical-layer attacks [27]; most notable examples include spoofing attacks on GPS [24], [19], relay attacks on passive entry/start systems in cars [15] and credit card payments [16]. Those vulnerabilities have real-world implications, as shown by a recent car theft that found widespread media attention [5].

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 [15]). At the logical layer, such manipulations, called *Mafia Fraud* Attacks are easily prevented using distance-bounding protocols [8]. 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 [25], Phase ranging [3] to phase manipulation [23] and early detect / late commit (ED/LC) [12], Chirp Spread Spectrum to ED/LC [28]. These attacks are effective despite authentication and distance-bounding protocols [8], [20], since they target the physical layer and do not change the message content.

UWB impulse radio, standardized within 802.15.4a,f, has emerged as a prominent technique for precise ranging. Prior research [32], [12] has shown UWB IR can be used to prevent distance manipulation attacks by using short UWB pulses for precise and secure time-of-flight (ToF) measurements. This results in modulations that encode each bit as a single UWB pulse [32]. Instantaneous transmit power in any practical UWB system faces constraints originating from both regulatory bodies as well as hardware integration concerns. Namely, the energy of the pulse is limited therefore limiting the range. In addition, standards imposed limitations on the amount of energy that can be placed in a short time frame further rendering 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 bit. However, increasing the symbol length has shown to be vulnerable to ED/LC [12], enabling distance reduction attacks by an untrusted (i.e., external) man in the middle. This is essentially a comeback

The first two authors contributed equally to this work.

Network and Distributed Systems Security (NDSS) Symposium 2019
24-27 February 2019, San Diego, CA, USA
ISBN 1-891562-55-X
https://dx.doi.org/10.14722/ndss.2019.23109
www.ndss-symposium.org

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 but not both.

Security of UWB ranging is since recently being addressed as a part of the emerging 802.15.4z standard [2]. Existing 802.15.4z proposals, however, achieve security through short symbol lengths thus by limiting the maximum distance of measurement, or use longer symbol lengths, therefore, risking attacks.

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 802.15.4 UWB as well as FCC and ETSI regulations. This makes it a good candidate for the Low Rate Pulse mode of the upcoming 802.15.4z standard. In the follow-up work, the authors have used similar cryptographic operations to solve a related problem – distance enlargement [31].

UWB-PR 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 [8], [17].

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.

Finally, UWB-PR shows that a number of assumptions that were made with respect to the design and implementation of distance-bounding protocols [12] are not correct. In particular, we show that these protocols do not need to rely on the rapid bit-exchange nor do they have to be implemented on top of modulation schemes that have short symbol lengths. UWB-PR shows that secure distance measurement can be built on top of modulation schemes with longer symbol lengths. In the existing literature [12] this was considered insecure. We discuss this further in Section VII.

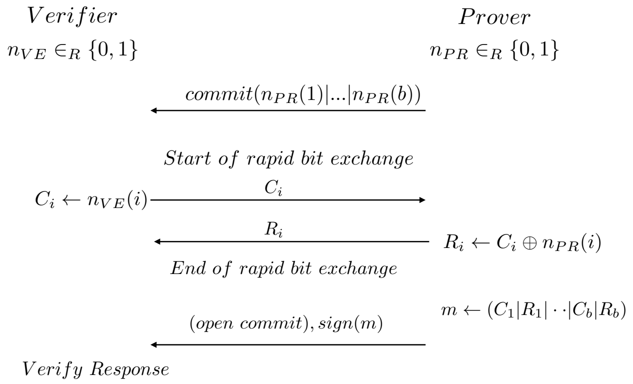
$Verifier$
$Prover$
$n_{VE} \in_R \{0,1\}$
$n_{PR} \in_R \{0,1\}$
$commit(n_{PR}(1)|...|n_{PR}(b))$
$Start\ of\ rapid\ bit\ exchange$
$C_i \leftarrow n_{VE}(i)$
C_i
R_i
$R_i \leftarrow C_i \oplus n_{PR}(i)$
$End\ of\ rapid\ bit\ exchange$
$m \leftarrow (C_1|R_1|\cdot\cdot|C_b|R_b)$
$(open\ commit), sign(m)$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

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

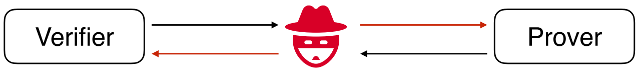

Fig. 2. In Mafia Fraud, an external attacker reduces the distance measured between two mutually trusted parties.

The remainder of this paper is organized as follows. In Section II, we provide some background on distance-bounding protocols, introduces different physical-layer attacks and outlines the existing conflict between performance and security in UWB-IR systems. Section III details the threat model. Section IV establish that longer symbol cannot be avoided. We introduce our approach in Section V and analyze its security in Section VI. In Section VII we inspect the implications of the proposed approach. Section VIII discusses the performance and security of our 802.15.4f-compatible proposal in relation to the 802.15.4a standard as well as limitations of our approach.

II. Background and Related Work

A. 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 [21], [9], [29], [17].

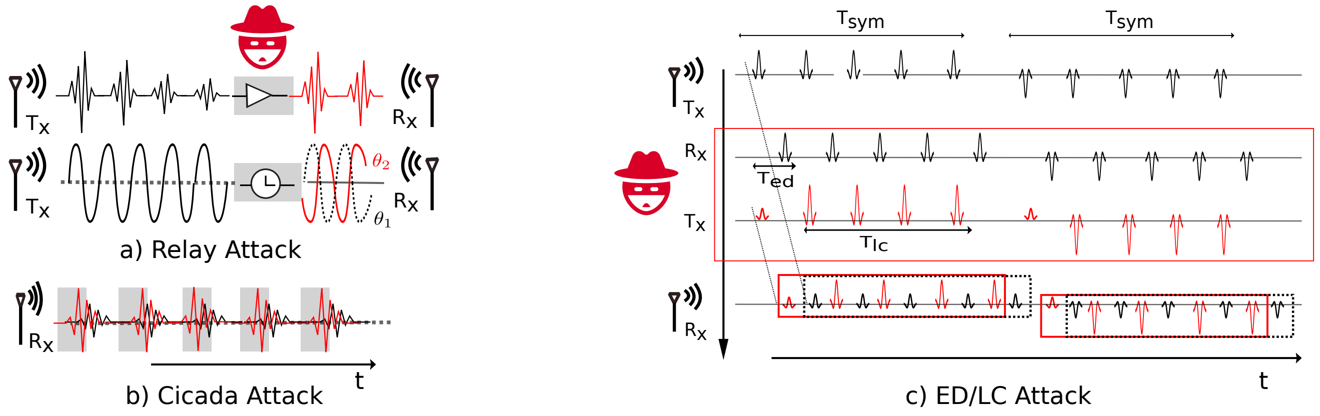

Fig. 3. Existing distance-measurement techniques are all vulnerable to physical-layer attacks. RSSI and phase-based ranging have been shown to be vulnerable to relay attacks. Time-of-flight and time-delay-of-flight ranging have been attacked in Cicada and ED/LC attacks.

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 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.

B. Physical-Layer Attacks

Existing ranging systems are typically vulnerable to one of three types of attacks: Relay, Cicada [27] 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 [33], PKES systems [15] and NFC [16]. 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 [28] and 802.15.4a IR-UWB [13], [26]. Section VIII 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 [25] 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 [25]. 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.

C. UWB-IR

Impulse-radio UWB systems are ideal candidates for high-precision ranging, and low-power IR-UWB ranging systems are becoming commercially available [1], [4]. 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 with different pulse repetition frequency (PRF), separate operating modes for long and short-range, and receivers suitable for ranging. The modulations as proposed in IEEE 802.15.4a and 802.15.4f are illustrated in Figure 4. 802.15.4a uses burst position modulation (BPM) and binary phase shift keying (BPSK), to accommodate for both coherent and noncoherent receivers. 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. 802.15.4f achieve lower complexity, in term of low power consumption and low cost by using OOK modulation and non-coherent receiver design.

The symbol length (T_{sym}) depends on the modulation scheme, the number of pulses in symbol, and the PRF. The motivation of different PRF stems from the fact that the device operates in different environments with widely varying delay spread. The 802.15.4a device should support mandatory low (3.9 MHz) and high PRF (15.6 MHz) and can adapt PRF based on the channel condition. 802.15.4f supports only low-PRF (1-2 MHz) which reduces location ambiguity and improves the performance of the non-coherent receiver in the high multipath environment. The security of the UWB ranging is recently being discussed as the part of the 802.15.4z standard [2]. The 802.15.4z propose enhanced high rate pulse (HRP) and low rate pulse (LRP) as the physical layers. The details of the modulation schemes are yet under discussion.[1] We will see further in Section IV that the choice of the modulation scheme, PRF, and receiver design have a direct effect on the performance and security of the system.

D. Physical-Layer Attacks on UWB systems

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. 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. The feasability of ED/LC attacks is shown in [13], [12], [28]. In [12], Clulow et al. conclude that a system relying on longer symbols is inherently vulnerable to ED/LC attacks, the only way to prevent ED/LC attack is by using a short symbol length. In [32], Tippenhauer et. al. designed a system to process short symbols. To minimize symbol length, they allocate energy within a time frame as short as feasible. This leaves little room to an attacker to shorten the time measured. Existing proposals against ED/LC attack provide the choice between longer symbols (longer distance) or security.

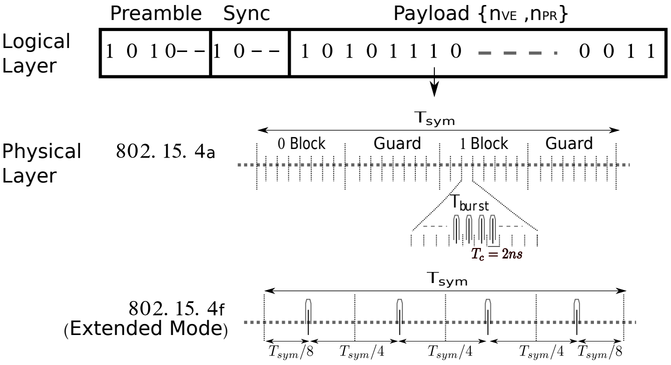

Fig. 4. 802.15.4a and 802.15.4f propose different modulations for mapping a ranging packet to a physical signal. This illustration refers to the respective modes geared towards long distances.

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. This suggests that the base mode of IEEE 802.15.4f be secure against ED/LC attacks. The extended and long-range modes of 802.15.4f rely on more pulses per bit. 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 VIII.

E. Formalization

In [22], the authors formally define Message Time of Arrival Codes (MTACs), addressing the security requirements for the prevention of distance reduction and enlargement attacks. UWB-PR, as introduced in this work, is an example of an MTAC that prevents a distance reduction attack. This claim is in line with the results of the security analysis in Section VI.

III. Threat Model

We focus on a scenario where two mutually trusted nodes are interested in measuring the distance between them. The nodes perform ToF measurements, relying on UWB signals for precise time resolution. These nodes have a shared secret and are assumed to have access to commonly-used encryption standards and protocols to attain confidentiality. They can secretly share logical-layer data and other information required for secure ranging.

The attacker's objective is to reduce the perceived distance between these nodes. She can have different incentives to perform such a distance-reduction attack, such as opening a car, gaining access to an office, or stealing money from a credit card, etc. We consider that the attacker has access to sophisticated hardware and processing capabilities. She can eavesdrop on messages transmitted by honest nodes, and get information at the granularity of the UWB-pulse

[1] LRP and HRP modes of 802.15.4z will use variations of 802.15.4f and 802.15.4a as underlying schemes.

level, i.e., phase, frequency and amplitude of each pulse. A malicious node can synchronize her transmission to ongoing transmissions and can adapt the transmission power of the signal. However, we assume a malicious node not to have access to any secret information and not being able to steal the identity of honest nodes. The attacker controls the communication channel, and she can prevent all direct communication between the honest nodes or eavesdrop on the data they are transmitting, but she will receive encrypted data. The attacker's inability to predict this secret information prevents her from performing a reduction attack at the logical layer. However, the use of sophisticated hardware and processing power allows her to perform an ED/LC attack at the physical layer.

The problem of ED/LC attack arises due to predictable symbols and is amplified by long symbols. To address this problem, we first establish that longer symbols cannot be avoided, and then look at the possibility of designing a secure physical layer. We propose UWB-PR - a secure modulation scheme to prevent ED/LC attacks. We look at possible attacks on UWB-PR, involving an attacker that detects pulses from honest transmitters and reacts accordingly.

IV. Design Space

A. 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 [14].

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 the burst position modulation (BPM) or on-off keying (OOK), which are the modulations 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.

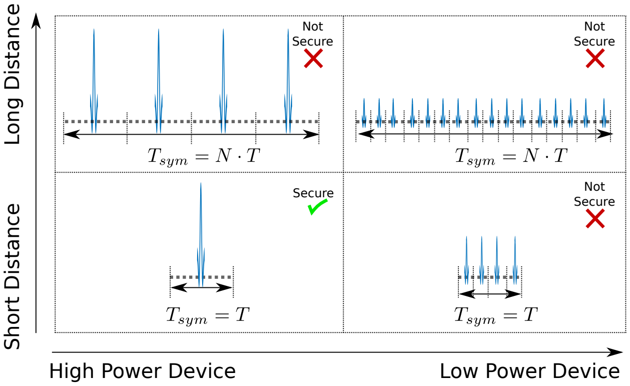

Fig. 5. Two independent causes are driving the need for more pulses per symbol: Low instantaneous power and high performance in terms of energy per symbol, both under compliance with regulatory constraints. The higher energy per symbol is needed for the longer distance and NLoS measurements. However, longer and deterministic symbol structure make the system vulnerable to ED/LC attack.

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).[2] As a consequence, this approach allows to achieve virtually arbitrary symbol energy, without violating regulatory and other power constraints, by constructing ever longer symbols.[3] 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.

B. Physical-Layer Cryptographic Operations

Multi-pulse UWB systems need to be secured against physical-layer attacks on ToF measurement by means of dedicated, physical-layer cryptographic operations. Encrypting the data bits exchanged as part of distance-bounding protocols is not sufficient. An ED/LC attacker can exploit redundant, multi-pulse signal structures despite knowing nothing about the data being exchanged.

On the other hand, individual UWB pulses are too short for a meaningful ED/LC attack, as the theoretically achievable reduction would be less than 1m. Therefore, the focus of

[2] Because the (local) PRF does not depend on the symbol duration here.

[3] Assuming that the oscillator drift remains reasonably bounded.

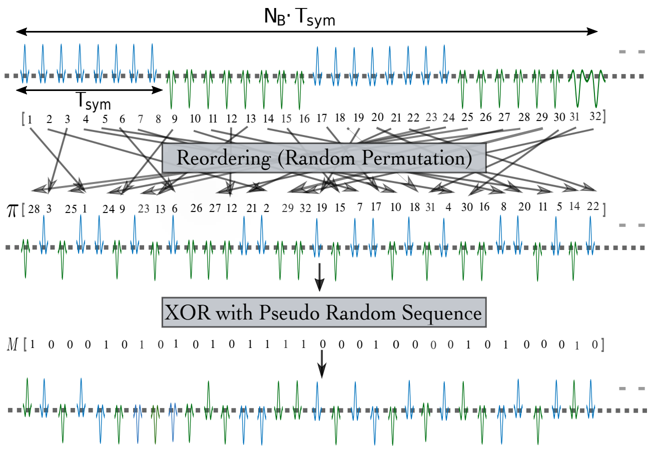
$N_B \cdot T_{sym}$
T_{sym}
[1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32]
Reordering (Random Permutation)
π [28 3 25 1 24 9 23 13 6 26 27 12 21 2 29 32 19 15 7 17 10 18 31 4 30 16 8 20 11 5 14 22]
XOR with Pseudo Random Sequence
M [1 0 0 0 1 0 1 0 1 0 1 0 1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

Fig. 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.

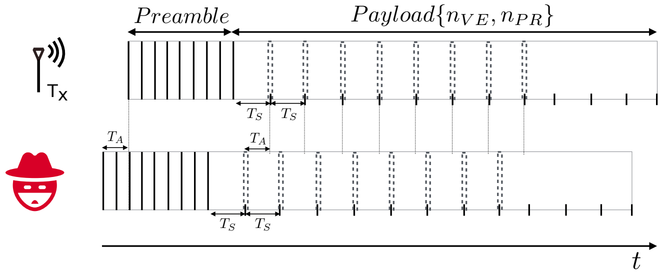

Fig. 7. In a distance commitment, the timing of the preamble is binding w.r.t. the timing of subsequent secret information.

cryptographic operations is to make it impossible for an attacker to exploit the redundant encoding of information bits in multiple consecutive pulses. This is equivalent to hiding the way a receiver generates information bits from a train of UWB pulses. Physical-layer cryptographic operations are not related to the data transmitted on the logical-level (i.e., the bits). In the same sense that bit-level cryptography does not protect against physical-layer ED/LC attack, bit-level data is not affected by the specific secrets used for physical-layer encryption. These operations, therefore, add an additional layer of security, specifically to protect against those attacks. Physical-layer cryptographic operations randomize the pulse sequence, given some bit-sequence to be transmitted.

Irrespective of how the information is encoded in the pulses (OOK, FSK, PSK), we can model each pulse as having two polarities. We argue that physical-layer cryptographic operations can be concerned with a) XORing the pulse polarities with a random sequence[4] and b) hiding the timing of pulses belonging to a given bit. UWB-PR relies on the first and employs the latter mechanism by reordering[5] the pulses of consecutive bits.

V. UWB with Pulse Reordering

UWB-PR is a new modulation technique that enhances the extended mode of 802.15.4f with cryptographic operations at pulse level 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.

a) 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 [32] and illustrated in Figure 7. While an attacker can 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] freshly generated for each transmission

[5] also, freshly generated for each transmission

A. 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.

a) 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.

b) 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 reordered pulse sequence and a random bitmask:

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

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 before the ranging phase.

c) 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.

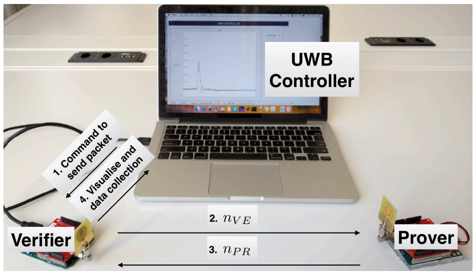

Fig. 8. Illustration of our experimental setup. Actual measurements were obtained over a LoS channel for varying distances.

d) 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

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

B. 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[6] [14].

The link budget of the resulting system depends on the number of pulses per symbol. Our implementation provides

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

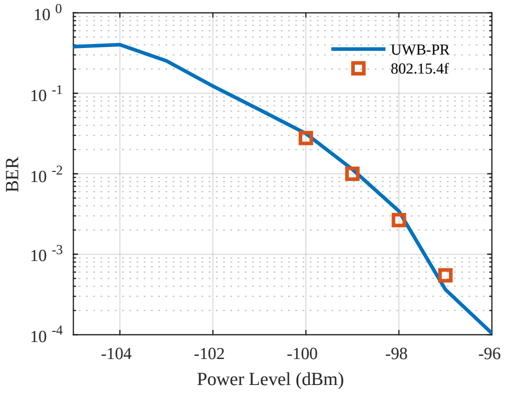

Fig. 9. BER performance of UWB-PR as compared to 802.15.4f. Our experiments do not suggest any effect of the blinding and reordering operations on the bit error rate.

us with an equivalent link budget[7] 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 approximately 32m under LoS conditions. Robustness of signal transmission and, in turn, the maximum operating range 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.

VI. 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 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

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

The attack on the entire group of bits is successful iff

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

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.

A. 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.

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

a) 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 $\sigma_A^k, k \in \{1, ..., N_B\}$, 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

$$S = (s_1, ..., s_t),$$

where the contribution at time k is

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

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

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

to the existing attack sequence.

b) 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 $(\sigma^1, ..., \sigma^{N_B})$ can be modeled as the joint distribution of all N_B bit-wise correlations, each of which can be sampled as

$$\sigma^k =$$

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

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*.

c) 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:

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

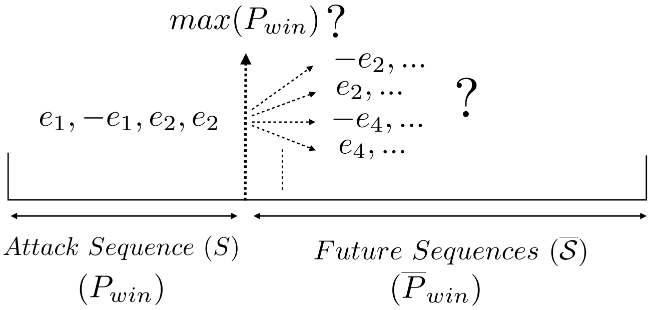

Fig. 10. The knowledge of a guessing attacker can be split into his assessment of the past and his model of the future.

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.

d) 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.

B. Attack Strategies

The knowledge that informs the strategy of a guessing attacker can be split into past observations and a model for the future, as illustrated in Figure 10. 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' is 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

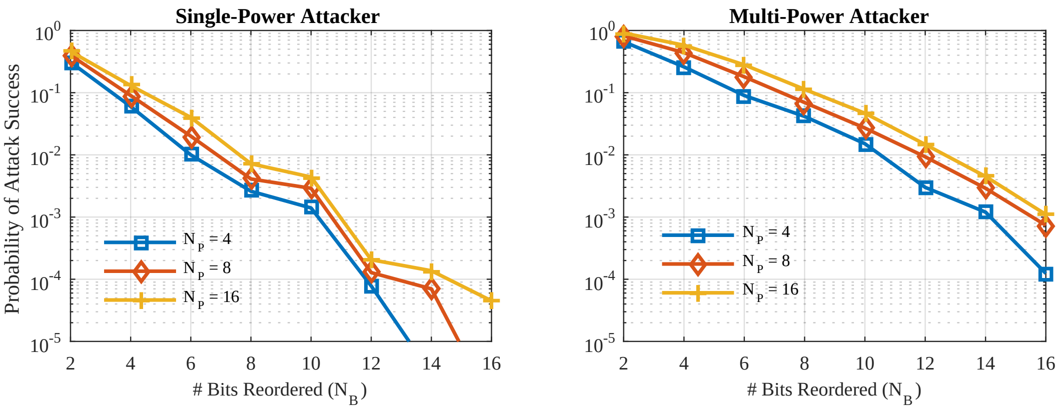

Fig. 11. Grouping more bits together for reordering (i.e., increasing N_B) makes it harder for both attackers to guess any of the bits, reducing their probabilities of success. This allows compensating for the detrimental effects of longer symbols (higher N_P) on security.

	$N_P = 4$			$N_P = 8$			$N_P = 16$		
	$N_B = 2$	$N_B = 4$	$N_B = 6$	$N_B = 2$	$N_B = 4$	$N_B = 6$	$N_B = 2$	$N_B = 4$	$N_B = 6$
$\lvert n_{VE}\rvert$, $\lvert n_{PR}\rvert$ (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 I
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).

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).

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 11 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 the 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 I 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

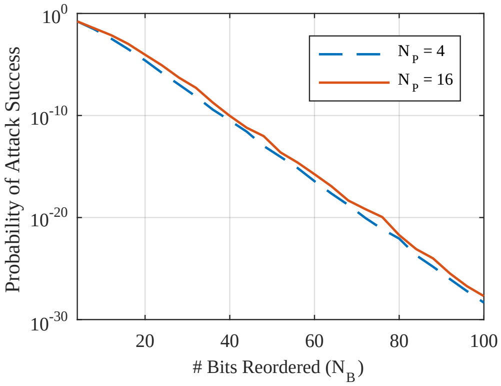

Fig. 12. Simulation results for structured reorderings: The attack success rates decrease exponentially as the number of bits reordered is increased. The attacker has knowledge about the statistical distribution of bits and pulses, and is given the optimal point of attack termination.

10^{-6}.

Structured Reordering Giving an attacker partial knowledge about the set of reorderings decreases his chances of winning overall. This becomes evident by comparing previous results (Figure 11) to Figure 12, which represents simulation results for a partially structured reordering. The knowledge about this partial structure is given to the attacker. The details on the simulations for a structured reordering are provided in the Appendix. In particular, the pulses of all bits occur in groups according to their position in their respective bit. The attacker's uncertainty is therefore limited to the bit each pulse belongs to. As in previous simulations, the attacker's chances of success are maximized by providing the optimal point of attack termination. In the same figure, we also see that the trend of the attack chances for more bits reordered is an exponential decrease. As this captures a scenario in which an attacker has structural knowledge about the reorderings, respectively, the set of possible reorderings is vastly reduced, we conclude that the attacker's success chances must decrease at least exponentially for increased numbers of bits in the general case, too. In other words, the attacker's success probability is negligible in N_B, which is within the security definition of a Message Time of Arrival Code (MTAC) as introduced in [22]. UWB-PR, therefore, is a candidate for an MTAC.

C. 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 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.

VII. Re-visiting principles for secure distance measurements

Clulow et al. [12] proposed principles for secure distance measurement. They restricted the choice of communication medium, communication format to single bit messages, symbol length to narrow and protocols to error-tolerant versions. These restrictions increase hardware complexity, introduce challenges in implementing secure distance bounding, and there is a limit on the distance we could measure using these implementations. These might be reasons that none of the commercially available UWB ranging systems adhere to these principles [4], [6], [1].

With the possibility of distance commitment and cryptographic operations at the physical layer, we need to revisit these principles. We will see that the changes in these principles will help in constructing performant and secure ranging systems.

Principle 1. Use a communication medium with propagation speed close to physical limit through space-time, i.e., the speed of light in vacuum. This principle is still valid and is important. Relaxing this constraint will allow the possibility of relay attacks on ToF-based ranging systems.

Principle 2. "Short symbols (preferably one pulse per symbol) are necessary for secure ranging." With UWB-PR, we show that longer symbols are secure to use. The restriction of narrow symbols was applied due to the threat of ED/LC attacks. This constraint limits the communication range of the system. UWB-PR performs cryptographic operations at the pulse level to prevent ED/LC attacks. This allows scaling to better performance and increased distance without compromising on security.

Principle 3. "Rapid pulse exchange is necessary for secure ranging." UWB-PR shows that a multi-pulse-multi-bit system can be secured against an external attacker. Earlier, multi-bit systems were considered vulnerable to ED/LC attacks. Rapid bit-exchange was required for security, where the transmitter would send a single bit, and the recipient would react instantly. In our design, we show that multiple bits can be a part of a single frame used for secure distance measurement, by using a distance commitment. In a distance commitment, the receiver performs timing acquisition on the preamble, and checks for the consistency of the bits with respect to the committed time, i.e., all bits should be advanced at the same time. Due to this check, both single and multi-bit systems have to adhere to the time consistency. Without a secure physical layer, both systems are equally vulnerable to ED/LC attacks. We argue that performance and resistance to ED/LC attacks are physical-layer concerns that need to be addressed at this level of abstraction, as done using UWB-PR. In UWB-PR, the association between information bits and pulses is cryptographically hidden. The transmission of a multi-bit nonce with a distance commitment over a secure physical layer is secure. This shows that the multi-bit challenge-response distance-bounding protocol such as Hu/Perrig/Johnson [18], Sastry/Shankar [30] and Capkun/Hubaux [10], [11] which were considered broken due to ED/LC attacks, are secure if run over a secure physical layer. Multi-bit systems also reduce hardware complexity, as timing acquisition needs to be done only once at the preamble, and the verification of the pulses follows afterward.

Principle 4. "Special bit-error tolerant protocols are required at the logical layer." Multi-pulse-multi-bit systems can be designed to prevent bit errors by increasing the symbol length, i.e., relying on more power per symbol. Error tolerance is not necessary at the protocol level, as it can be provided by a robust physical layer. The BER of UWB-PR is identical to a standard 802.15.4f implementation, as shown by our proof-of-concept implementation. The special protocol with error resistance was needed due to short symbols and rapid bit exchange. We should prevent error correction at the logical layer; bit errors can occur due to an attack attempt. In case of such an error, the system should again perform ranging with longer symbols and more bits interleaved.

VIII. Discussion

In the following, we first relate our proposal to the 802.15.4a standard. We close by discussing limitations of the approach.

A. 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.[8]
- *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.

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.

a) 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 [26].

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 13 for all mandatory configurations, where it is contrasted with the constantly small decrease possible in UWB-PR [9]. 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 [14]. 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

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

[9] 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 [14].

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 13 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 [26]. 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 II, 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 13.

	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 II
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 III
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 III.

B. 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.

IX. CONCLUSION

In this paper, we presented UWB-PR, a modulation scheme that secures ranging against all physical-layer attacks that

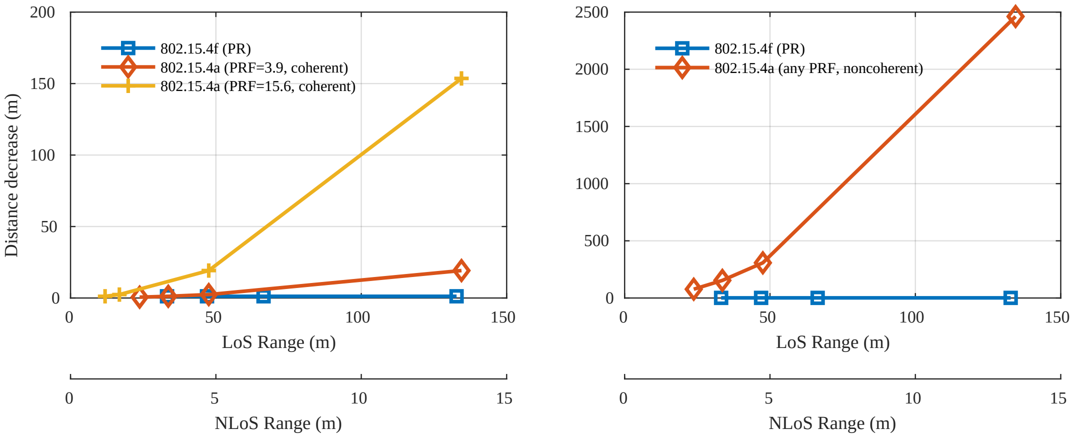

Fig. 13. Distance decrease in the coherent (left) and noncoherent (right) scenario as a function of the estimated range offered. For comparability, all systems are assumed to use 500MHz bandwidth. NLoS refers to a scenario with 20dB attenuation of the direct path. Non-idealities of the measurement hardware were not considered.

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.

Acknowledgment

The authors would like to thank Dr. Boris Danev and Dr. David Barras from 3db Access for their invaluable inputs and help in the implementation of the prototype.

References

[1] "3db Access AG - 3DB6830 ("proximity based access control")," https://www.3db-access.com/Product.3.html, [Online; Accessed 23. October 2017].

[2] "802.15.4z - standard for low-rate wireless networks amendment: Enhanced high rate pulse (hrp) and low rate pulse (lrp) ultra wide-band (uwb) physical layers (phys) and associated ranging techniques," https://standards.ieee.org/develop/project/802.15.4z.html, [Online; Accessed 7. August 2018].

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

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

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

[6] "Time Domains PulsON ("p440")," http://www.timedomain.com/products/pulson-440/, [Online; Accessed 23. October 2017].

[7] P. Bahl and V. N. Padmanabhan, "RADAR: an in-building RF-based user location and tracking system," in *IEEE INFOCOM*, vol. 2, 2000, pp. 775–784.

[8] S. Brands and D. Chaum, "Distance-bounding protocols," in *EUROCRYPT*. Springer, 1994, pp. 344–359.

[9] A. Brelurut, D. Gerault, and P. Lafourcade, "Survey of Distance Bounding Protocols and Threats," in *Foundations and Practice of Security (FPS)*, 2015, pp. 29 – 49. [Online]. Available: https://hal.archives-ouvertes.fr/hal-01588557

[10] S. 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*, vol. 3. IEEE, 2005, pp. 1917–1928.

[11] ——, "Secure positioning in wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 221–232, 2006.

[12] J. Clulow, G. P. Hancke, M. G. Kuhn, and T. 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*, ser. ESAS'06. Springer, 2006, pp. 83–97. [Online]. Available: http://dx.doi.org/10.1007/11964254_9

[13] M. Flury, M. Poturalski, P. Papadimitratos, J.-P. Hubaux, and J.-Y. Le Boudec, "Effectiveness of distance-decreasing attacks against impulse radio ranging," in *Proceedings of the Third ACM Conference on Wireless Network Security*, ser. WiSec '10. ACM, 2010, pp. 117–128.

[14] R. J. Fontana and E. A. Richley, "Observations on low data rate, short pulse uwb systems," in *Ultra-Wideband, 2007. ICUWB 2007. IEEE International Conference on*. IEEE, 2007, pp. 334–338.

[15] A. Francillon, B. Danev, and S. Capkun, "Relay attacks on passive keyless entry and start systems in modern cars," in *Network and Distributed System Security Symposium (NDSS)*, 2011.

[16] L. Francis, G. Hancke, K. Mayes, and K. Markantonakis, "Practical relay attack on contactless transactions by using nfc mobile phones," 2012.

[17] G. P. Hancke and M. G. Kuhn, "An rfid distance bounding protocol," in *Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks*, ser. SECURECOMM '05. IEEE Computer Society, 2005, pp. 67–73. [Online]. Available: http://dx.doi.org/10.1109/SECURECOMM.2005.56

[18] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in *INFOCOM 2003*, vol. 3. IEEE, 2003, pp. 1976–1986.

[19] T. Humphreys, B. Ledvina, M. Psiaki, B. O'Hanlon, and P. Kintner, *Assessing the spoofing threat: Development of a portable gps civilian spoofer*, 2008, vol. 2, pp. 1198–1209.

[20] A. M. Ioana Boureanu and S. Vaudenay, "Towards secure distance bounding," *IACR Cryptology ePrint Archive*, vol. 2015, p. 208, 2015. [Online]. Available: http://eprint.iacr.org/2015/208

[21] C. H. Kim, G. Avoine, F. Koeune, F.-X. Standaert, and O. Pereira, "The swiss-knife rfid distance bounding protocol." in *ICISC*, vol. 5461. Springer, 2008, pp. 98–115.

[22] P. Leu, M. Singh, and S. Capkun, "Message time of arrival codes: A fundamental primitive for secure distance measurement," 2019. [Online]. Available: https://www.research-collection.ethz.ch/handle/20.500.11850/310393

[23] H. Ólafsdóttir, A. Ranganathan, and S. Čapkun, "On the security of carrier phase-based ranging," in *International Conference on Cryptographic Hardware and Embedded Systems*. Springer, 2017, pp. 490–509.

[24] P. Papadimitratos and A. Jovanovic, "Gnss-based positioning: Attacks

and countermeasures," in *MILCOM 2008 - 2008 IEEE Military Communications Conference*, 2008, pp. 1–7.

[25] M. Poturalski, M. Flury, P. Papadimitratos, J. P. Hubaux, and J. Y. L. Boudec, "The cicada attack: Degradation and denial of service in ir ranging," in *2010 IEEE International Conference on Ultra-Wideband*, 2010, pp. 1–4.

[26] ——, "Distance bounding with ieee 802.15.4a: Attacks and countermeasures," *IEEE Transactions on Wireless Communications*, pp. 1334–1344, 2011.

[27] A. Ranganathan and S. Capkun, "Are we really close? verifying proximity in wireless systems," *IEEE Security Privacy*, vol. 15, no. 3, pp. 52–58, 2017.

[28] A. Ranganathan, B. Danev, A. Francillon, and S. 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*. ACM, 2012, pp. 15–26.

[29] J. Reid, J. M. G. Nieto, T. Tang, and B. Senadji, "Detecting relay attacks with timing-based protocols," in *Proceedings of the 2Nd ACM Symposium on Information, Computer and Communications Security*, ser. ASIACCS '07. ACM, 2007, pp. 204–213. [Online]. Available: http://doi.acm.org/10.1145/1229285.1229314

[30] N. Sastry, U. Shankar, and D. Wagner, "Secure verification of location claims," in *Proceedings of the 2nd ACM workshop on Wireless security*. ACM, 2003, pp. 1–10.

[31] M. Singh, P. Leu, A. Abdou, and S. Capkun, "UWB-ED: distance enlargement attack detection in ultra-wideband," 2018. [Online]. Available: https://www.research-collection.ethz.ch/handle/20.500.11850/309346

[32] N. O. Tippenhauer, H. Luecken, M. Kuhn, and S. Capkun, "Uwb rapid-bit-exchange system for distance bounding," in *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, ser. WiSec '15. ACM, 2015, pp. 2:1–2:12. [Online]. Available: http://doi.acm.org/10.1145/2766498.2766504

[33] H. T. T. Truong, X. 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)*, 2014, pp. 163–171.

[34] D. Vasisht, S. Kumar, and D. Katabi, "Decimeter-level localization with a single wifi access point," in *USENIX NSDI*, 2016, pp. 165–178. [Online]. Available: https://www.usenix.org/conference/nsdi16/technical-sessions/presentation/vasisht

APPENDIX

To understand the impact of the reordering on attack success, we analyze a particular instance of UWB-PR. The idea is to determine the probability of attack success for different numbers of bits reordered under the multi-power attacker model and an optimal attack termination-point.

Reordering Process: Instead of reordering all pulses randomly, we follow a specific process. We create N_P subsets, and each subset has N_B pulses, where N_P is the number of pulses per symbol and N_B the number of bits reordered. The N_B pulses of each subset belong to exactly N_B different bits. However, each subset hides the mapping differently, by using a different reordering and XOR sequence. Figure 14 shows an example of this reordering process.

Attack Strategy: The attacker is aware of the statistical distribution, i.e., N_B and N_P, and knows that each pulse of the subset belongs to the different bit. This knowledge gives a bias to the attacker, even towards the end of the attack, the attacker has a non-zero probability of producing a positive contribution on each bit. However, he doesn't know reordering and XOR sequence applied on the subset. To maximize the likelihood of positive net power per bit, an attacker needs to decide energy levels for the attack on each pulse and the point of attack termination. For the choice of the energy level, we suggest the following:

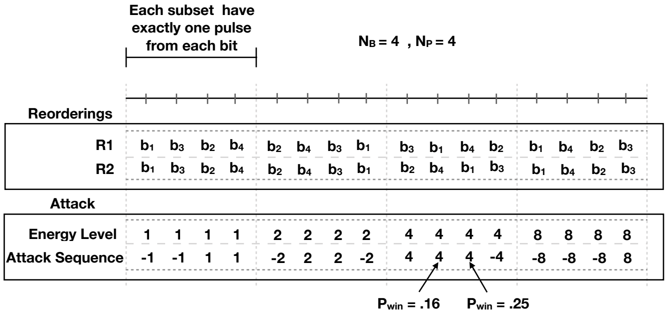
Each subset have exactly one pulse from each bit
$N_B = 4$, $N_P = 4$
Reorderings
R1 b_1 b_3 b_2 b_4 b_2 b_4 b_3 b_1 b_3 b_1 b_4 b_2 b_1 b_4 b_2 b_3
R2 b_1 b_3 b_2 b_4 b_2 b_4 b_3 b_1 b_2 b_4 b_1 b_3 b_1 b_4 b_2 b_3
Attack
Energy Level 1 1 1 1 2 2 2 2 4 4 4 4 8 8 8 8
Attack Sequence -1 -1 1 1 -2 2 2 -2 4 4 4 -4 -8 -8 -8 8
P_{win} = .16
P_{win} = .25

Fig. 14. Example for a Structured Reordering: There are N_P subsets, and each subset has N_B pulses. Each pulse of a subset belongs to a different bit, as is shown by reorderings R1 and R2. In order maximize the likelihood of correcting any previous negative contributions, the attacker uses the same energy level within the subset and doubles the transmission power upon transitioning from one subset to the next. For the reordering R2, the attack is successful if attack termination happens at the third position of the third subset (at $P_{win} = 0.25$). However, the attack fails for reordering R1, irrespective of the point of termination of the attack.

- Within a subset, the same energy level is used for each pulse. Given that all pulses belong to different bits, and the attacker does not know the pulse-to-bit mapping, all pulses are equally probable to belong to a certain bit.
- When transitioning from one subset to another, the attacker can decide to use the same, increase or decrease the energy level. In our model, we choose the minimum energy level that will maximize the likelihood of positive net power per bit, given that the next pulse polarity is guessed correctly. As long as negative per-bit correlations remain, this is equivalent to doubling the power per pulse upon transitioning.

The energy choice according to this model ensures that the correct guess of a pulse brings the attacker closer to winning and an incorrect guess can be corrected in the next subset. However, in the process of fixing a wrong interference of a bit, the attacker can end up interfering with another bit. Suppose in one subset the attacker guesses the polarity of $(N_B - 1)$ pulses correctly but guesses one wrong. To maximize his chances of success in the next subset, he needs to guess the polarity of the pulse of this particular bit correctly. In the process of correcting this bit, if the attacker attacks a pulse in the next subset, the probability of correcting this bit is $(0.5 \cdot 1/N_B)$, and causing a negative contribution to another bit is $(0.5 \cdot (N_B - 1)/N_B)$. By increasing the number of bits reordered, the probability of interfering with the wrong bit increases. An attacker also needs to be careful about the when to terminate the attack. In the example shown in Figure 14, an attacker can stop interfering after the second or third position of the third subset. After interfering with the second pulse of the third subset, the attacker already knows that P_{win} is .16. He can choose to proceed or terminate the attack at this point. For calculating the results, as shown in Figure 12, we assume that the attacker continues and terminates the attack at the third position of the third subset, where P_{win} is .25.