EPFL-REPORT-150112[♭]

Distance Bounding with IEEE 802.15.4a: Attacks and Countermeasures

Marcin Poturalski[†*], Manuel Flury[†*],
Panos Papadimitratos[‡], Jean-Pierre Hubaux[†], Jean-Yves Le Boudec[†]

[†]Laboratory for Computer Communications and Applications
EPFL, Switzerland
firstname.lastname@epfl.ch

[‡]School of Electrical Engineering
KTH, Stockholm, Sweden
papadim@kth.se

***Abstract*—Impulse Radio Ultra-Wideband, in particular the recent standard IEEE 802.15.4a, is a primary candidate for implementing distance bounding protocols, thanks to its ability to perform accurate indoor ranging. Distance bounding protocols allow two wireless devices to securely estimate the distance between themselves, with the guarantee that the estimate is an upper-bound on the actual distance. These protocols serve as building blocks in security-sensitive applications such as tracking, physical access control, or localization.**

We investigate the resilience of IEEE 802.15.4a to physical-communication-layer attacks that decrease the distance measured by distance bounding protocols, thus violating their security. We consider two attack types: malicious prover (internal) and distance-decreasing relay (external). We show that if the honest devices use energy-detection receivers (popular due to their low cost and complexity), then an adversary can perform highly effective internal and external attacks, decreasing the distance by hundreds of meters. However, by using more sophisticated rake receivers, or by implementing small modifications to IEEE 802.15.4a and employing energy-detection receivers with a simple countermeasure, honest devices can reduce the effectiveness of external *distance-decreasing relay attacks* to the order of 10m. The same is true for malicious prover attacks, provided that an additional modification to IEEE 802.15.4a is implemented.

***Index Terms*—security, ranging, distance bounding, impulse radio, ultra-wideband**

I. Introduction

One of the distinguishing features of Impulse Radio Ultra-Wideband (IR-UWB) is its capability of high precision indoor ranging, even in dense multi-path environments [1]. This was also one of the main reasons for including an IR-UWB physical layer (PHY) in the IEEE 802.15.4a standard. The ability to measure the distance between two devices with a precision of less than one meter is an enabler for many location-aware applications and services, such as physical access control, tracking of goods and people, or indoor localization. Many of these applications are security-sensitive: They require trustworthy distance measurements, even in the presence of an adversary interfering with the ranging process.

Secure range estimation is the domain of *distance-bounding* (DB) protocols [2]. They allow a *verifier* to obtain a secure *upper-bound* on the distance to a *prover*. DB protocols are cryptographic in nature, which means that they consider an adversary that manipulates and injects messages on the bit level. However, DB protocols abstract away from the PHY details and are therefore susceptible to PHY attacks, in which an adversary manipulates PHY symbols, rather than bits [3]. Such attacks can bypass any cryptographic mechanisms and allow a malicious prover or an external adversary mounting a relay attack to violate DB security by decreasing the measured distance.

Because of its unique ranging capabilities, IR-UWB is often mentioned as an ideal candidate for a DB PHY. In addition, IR-UWB can incorporate very short symbols, which mitigates PHY attacks [3]. One approach is to design an IR-UWB DB PHY from scratch. An alternative approach, which we investigate in this paper, is to use an existing PHY, such as IEEE 802.15.4a. The latter approach has a number of advantages. First, PHYs are typically designed with performance in mind, and a DB protocol would benefit from the performance optimization provided by such a PHY. Another important benefit is the ease of deployment on devices compatible with an established PHY. However, a thorough evaluation of resilience of the PHY to PHY attacks is crucial: Often, features improving benign-case performance create vulnerabilities.

This is exactly the problem we address in this paper: We adapt the distance-decreasing PHY attacks introduced in [3] (*early detection* and *late commit*) to the IEEE 802.15.4a standard and evaluate their effectiveness. We extend our previous work [4] by considering different types of receivers, and malicious prover attacks (internal) in addition to distance-decreasing relay attacks (external). We also examine countermeasures that can mitigate PHY attacks, while minimally degrading the benign-case performance. We make the following new contributions:

► We unveil an anomaly in the convolutional code employed in IEEE 802.15.4a, which can be exploited by an adversary equipped with a rake receiver that attacks energy-detection receivers. It allows the adversary to decrease the distance

*Equally contributing authors.

[♭]This technical report is an extended version of the paper published under the same title in *IEEE Transactions on Wireless Communications*.

The work presented in this paper was supported (in part) by the National Competence Center in Research on Mobile Information and Communication Systems (NCCR-MICS), a center supported by the Swiss National Science Foundation under grant number 5005-67322.

more substantially than the attacks in [4], or to mount an *undetectable* attack with a more modest, but still substantial distance-decrease. The anomaly can be patched with a small modification to IEEE 802.15.4a.

► We show that time-hopping used in IEEE 802.15.4a allows a malicious prover to augment the distance-decrease of PHY attacks at the cost of decreasing the probability of attack success. A rake-equipped malicious prover can also similarly exploit the combination of BBPM and BPSK employed in IEEE 802.15.4a. The time-hopping vulnerability can be patched with a small modification to IEEE 802.15.4a.

► We observe that by increasing the length of nonces used in a DB protocol, we can improve its performance and preserve the security level. We use this observation to advocate a simple, efficient, and standard-compliant countermeasure to PHY attacks. Employed in an energy-detection receiver, along with the convolutional code patch, this countermeasure effectively limits the distance-decrease of distance-decreasing relay attacks to around 10m. Employed in an energy-detection receiver or in a rake receiver, along with the convolutional code and time-hopping patches, it limits the effectiveness of malicious prover attacks to around 10m.

The paper is organized as follows: In Section II we describe the related work. In Section III we discuss our assumptions about DB protocols, and describe a general method to balance performance and security. In Section IV we introduce the IEEE 802.15.4a PHY and the receivers we consider, and explain implementing DB within IEEE 802.15.4a. We show a range of PHY attacks in Section V, and evaluate their performance in Section VI. In Section VII we discuss countermeasures, before concluding in Section VIII.

II. Related work

Distance bounding was first proposed by Brands and Chaum in [2]. The first proposal tolerating errors in the bit-exchange was [5]. A number of other DB protocols are proposed, addressing aspects such as mutual ranging [6], [7], resilience to the terrorist fraud (see Section III) [8], [9], [10], efficiency [11], privacy [12], and formal verification [13], [14].

Physical layer attacks against distance bounding were first introduced in [3]. The effectiveness of these attacks against concrete PHYs is studied in [15] (ISO 14443 RFID and wireless sensor networks) and [4] (IEEE 802.15.4a). Another type of PHY attacks against IR-UWB ranging was introduced in [16]. The attack is based on introducing malicious interference to manipulate the time-of-arrival estimation, thus decreasing the measured distance.

An IR-UWB architecture for implementing DB protocols is proposed in [17]. The maximum distance-decrease an adversary can gain against this PHY is $3-6$m. This is achieved with the short symbol duration of 20ns, which limits the applicability of this PHY in dense multi-path environments for which IEEE 802.15.4a was designed. An ID-based distance bounding protocol is implemented on proprietary IR radios in [18]. Beyond IR-UWB, DB PHYs tailored to narrow-band RFID systems are proposed in [9], [19], [20], and a DB PHY for smartcards (wire-line) is introduced in [21].

III. Distance Bounding

Distance bounding (DB) protocols are cryptographic protocols that allow one device, the *verifier V*, to compute an upper-bound on the distance to another device, the *prover P*, in an adversarial setting. Like regular ranging protocols, DB protocols perform distance estimation based on time-of-flight measurements of *ranging messages*: the *challenge(s)* sent by V and the *response(s)* of P. Additional messages are employed to guarantee authentication. Three threat scenarios are traditionally considered [22], [8]. In the *mafia fraud*, the adversary interferes with a DB session between an honest V and an honest P, and decreases the measured distance below the actual distance. In the other scenarios, a malicious P convinces V that it is closer than it actually is, working alone (*distance fraud*), or in collusion with other malicious devices (*terrorist fraud*).

A. Security Level and Performance

The challenge and response messages in a DB protocol (Figure 1) are typically nonces (of length N_{nonce} each), unpredictable to the adversary. At the end of the protocol execution, the verifier learns both the true and the received values of these nonces. The verifier accepts a distance measurement only if the received challenge and response messages contain less than N_{err} erroneous bits each. The parameters $N_{\text{nonce}}, N_{\text{err}}$ jointly determine 1) the maximum bit error rate (BER) that the protocol tolerates and 2) the security level.

The security level of a DB protocol is defined as the probability that the adversary will succeed in decreasing the measured distance below the actual distance. Let us set aside physical layer attacks, and assume that the DB protocol is cryptographically secure and that the authenticator is too long to be guessable. Then, the adversary is limited to guessing attacks on the nonces: 1) a malicious P guesses the challenge or response and replies early to V's challenge; 2) an external adversary guesses the response and replies early in place of the honest P; 3) an external adversary guesses the challenge, sends it to P to extract the correct response, and sends this response to V. The success probability of such guessing attacks is:

$$P_{\text{guess}} = F_{\text{BIN}}(N_{\text{err}}|N_{\text{nonce}}, \frac{1}{2}) \tag{1}$$

where $F_{\text{BIN}}(x|n,p)$ is the CDF of a binomial distribution with parameters n and p.

Inverting the CDF yields the maximum N_{err} achieving a desired security level P_{guess}:

$$N_{\text{err}} = F^{-1}_{\text{BIN}}(P_{\text{guess}}|N_{\text{nonce}}, \frac{1}{2}) \tag{2}$$

Interestingly, for a fixed security level, this allows a DB protocol to operate at virtually any bit error rate by simply increasing N_{nonce} and N_{err}. (We will see in Section VII why this is an important property for potential countermeasures). Indeed, we have that:

$$\begin{aligned}\lim_{N_{\text{nonce}}\to\infty} N_{\text{err}} &= \lim_{N_{\text{nonce}}\to\infty} F^{-1}_{\text{BIN}}(P_{\text{guess}}|N_{\text{nonce}}, 1/2) = \\ &= \lim_{N_{\text{nonce}}\to\infty} F^{-1}_{\mathcal{N}}(P_{\text{guess}}|N_{\text{nonce}}/2, N_{\text{nonce}}/4)\end{aligned} \tag{3}$$

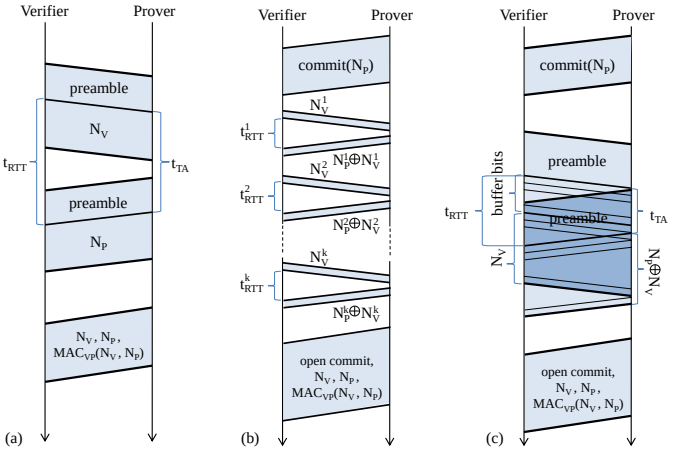

Fig. 1. Examples of distance bounding protocol: (a) is secure only against the mafia fraud, (b) and (c) are secure against the distance fraud and the mafia fraud. (b) achieves distance fraud resilience with the rapid-bit-exchange (RBE), (c) replaces RBE with full-duplex transmission. All protocols are simplified for the sake of clarity, in reality both the Verifier, **V**, and Prover, **P**, need to be aware that they are engaging in a distance bounding session with each other. **V** estimates the distance to **P** with the formula $d_{VP} = c(t_{\mathrm{RTT}} - t_{\mathrm{TA}})/2$, where c is the channel propagation speed. $\mathrm{MAC_{VP}}$ stands for Message Authentication Code with a symmetric key shared between **V** and **P**, N_V and N_P are freshly generated nonces, t_{TA} is a constant turn-around time that **V** and **P** know, and which is assumed 0 for protocol (b), and t_{RTT} is the round-trip-time measured by **V**.

where $F_{\mathcal{N}}^{-1}(x|\mu,\sigma^2)$ is the inverse of the CDF of a normal distribution with mean μ and variance σ^2 and the second equality follows from the central limit theorem. The protocol succeeds as long as there are no more than N_{err} errors in a nonce of length N_{nonce}, resulting in a bit error rate of $\mathrm{BER}^{\max} = N_{\mathrm{err}}/N_{\mathrm{nonce}}$. From (3) it then follows that, as the length of the nonce increases, the maximum sustainable bit error rate $\mathrm{BER}^{\max}$ tends to the worst case of $1/2$, i.e.,

$$\lim_{N_{\mathrm{nonce}}\to\infty} \mathrm{BER}^{\max} = \lim_{N_{\mathrm{nonce}}\to\infty} \frac{N_{\mathrm{nonce}}/2 + \sqrt{N_{\mathrm{nonce}}/4}\,\Phi^{-1}(P_{\mathrm{guess}})}{N_{\mathrm{nonce}}} = \frac{1}{2} \tag{4}$$

where $\Phi^{-1}(x)$ denotes the inverse CDF of a standard normal distribution.

B. Choosing the Nonce Length

DB protocols make use of both ranging and communication packets. We have seen in the preceding section that ranging packets carrying nonces can support very high bit error rates and still achieve the desired security level P_{guess}, provided that the coding rate is properly adjusted through the parameters N_{nonce} and N_{err}. In contrast, communication packets do not necessarily offer the same flexibility because the coding rate can be fixed (as in the case of IEEE 802.15.4a, see Section IV-A3). Consequently, if we define a performance goal in terms of the maximum tolerable packet error rate for communication packets of a given length $\mathrm{PER}_{\mathrm{comm}}$, there is a minimum signal-to-noise ratio (SNR) $\mathrm{SNR}_{\mathrm{min}}$ required to reach this goal. Given $\mathrm{PER}_{\mathrm{comm}}$, $\mathrm{SNR}_{\mathrm{min}}$ can be established analytically or with simulations.

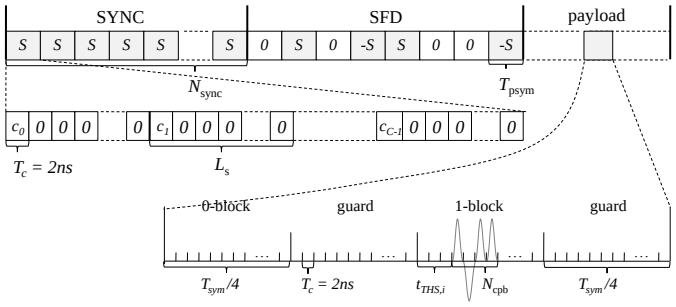

Fig. 2. IEEE 802.15.4a packet structure: preamble and payload.

We can define a similar performance goal for ranging packets by fixing their maximum tolerable packet error rate $\mathrm{PER}_{\mathrm{db}}$. Now, if ranging and communication ought to have the same operating range, ranging packets should achieve $\mathrm{PER}_{\mathrm{db}}$ at $\mathrm{SNR}_{\mathrm{min}}$. To guarantee this, we can first establish (again analytically or with simulations) the bit error rate $\mathrm{BER}_{\mathrm{db}}$ that ranging messages experience at $\mathrm{SNR}_{\mathrm{min}}$. A ranging packet of length N_{nonce} subject to $\mathrm{BER}_{\mathrm{db}}$ is considered to be in error if it contains more than N_{err} errors. We can thus derive N_{nonce} and N_{err} by solving the system of equations formed by (2), that ensures the desired security level, and

$$N_{\mathrm{err}} = F_{\mathrm{BIN}}^{-1}(1 - \mathrm{PER}_{\mathrm{db}} | N_{\mathrm{nonce}}, \mathrm{BER}_{\mathrm{db}}) \tag{5}$$

that ensures the required $\mathrm{PER}_{\mathrm{db}}$.

IV. IR-UWB System Model and Assumptions

A. IEEE 802.15.4a PHY

IEEE 802.15.4 is a standard for low-rate wireless personal area networks (WPAN). The IEEE 802.15.4a amendment [23] defines an IR-UWB PHY that allows for low-rate communication and high precision ranging. Because of the ultrawideband nature of this PHY, the transmitting power is significantly limited by regulation. This results in a relatively low communication range (20-30 m). We focus on one of the mandatory modes of the standard, LPRF (*low pulse repetition frequency*). However, our results are easily transferable to other modes (which use different parameter values). All parameter values are publicly known.

An IEEE 802.15.4a packet (Figure 2) is composed of a preamble followed by a payload part.

1) Preamble: The preamble consists of a SYNC part and the start frame delimiter (SFD). The SYNC part is composed of $N_{\mathrm{sync}} = 64$ identical preamble symbols of duration $T_{\mathrm{psym}} = 3968$ ns. The SFD is composed of a particular sequence of $N_{\mathrm{sfd}} = 8$ preamble symbols. Each preamble symbol is formed by C code symbols that consist of L_{s} chips of duration $T_{\mathrm{c}} = 2$ ns. Pulses are sent in the first chip of every code symbol and modulated according to a ternary preamble code of length C. The received signal during reception of a preamble and after filtering with a bandpass filter of bandwidth B is given by:

$$r_{\mathrm{pre}}(t) = \sum_{i=1}^{N_{\mathrm{sync}}+N_{\mathrm{sfd}}} s_i \sum_{j=1}^{C} c_j \cdot h(t - jL_{\mathrm{s}}T_{\mathrm{c}} - iT_{\mathrm{psym}} - \nu_0) + w(t) \tag{6}$$

where $h(t)$ is the unknown channel response (including the transmitted waveform, the response of the multi-path channel and the bandpass filter) assumed invariant for the duration of one packet, $w(t)$ is a zero-mean AWGN process with power spectral density $N_0/2$, $c_j \in \{-1, 0, +1\}$ are the elements of the preamble code and ν_0 is the propagation delay. Each preamble symbol is modulated by the sequence $s_i = [1, \ldots, 1, 0, 1, 0, -1, 1, 0, 0, -1]$ whose last eight elements denote the SFD.

2) Payload: The payload is modulated using a combination of *Binary Pulse Position Modulation* (*BPPM*) and *Binary Phase-Shift Keying* (*BPSK*). In addition, time-hopping is used to allow for multiple-access and every symbol is signalled through the transmission of a burst of N_{cpb} pulses. The signal received during the i-th payload symbol is:

$$r_i(t) = w(t) + \tag{7}$$
$$(2a_i - 1) \sum_{j=1}^{N_{\text{cpb}}} b_{ij} \cdot h(t - iT_{\text{sym}} - d_i T_{\text{sym}}/2 - t_{\text{THS},i} - jT_{\text{c}} - \nu_0)$$

where a_i is the polarity bit (BPSK), d_i the position bit (BPPM), $T_{\text{sym}} = 1024ns$ is the symbol duration, $t_{\text{THS},i} \in [0, t_{\text{THS}}^{\max}]$, where $t_{\text{THS}}^{\max} = T_{\text{sym}}/4 - N_{\text{cpb}} \cdot T_{\text{c}}$, defines the pseudo-random time-hopping offset, and the scrambling sequence b_{ij} defines the polarity of the j-th pulse of the i-th burst. Both the time-hopping and the scrambling sequences are derived from a fixed and publicly known linear feedback shift register that is initialized to a publicly known state at the beginning of every packet. Both sequences are thus the same for every packet.

3) Channel Coding: A systematic rate $1/2$ convolutional code with generator polynomials $g_1 = (0, 1, 0)$ and $g_2 = (1, 0, 1)$ is used. Denote the bits to be transmitted by x_i. Then the position bit is $d_i = x_i$ and the polarity bit is $a_i = x_{i-1} \oplus x_{i+1}$, where $\oplus$ denotes modulo two addition. With this construction, an energy-detection receiver, which cannot recover the polarity bit, can still decode the transmitted bit sequence x_i; whereas a coherent receiver, which can recover both bits, can apply convolutional decoding to improve performance. IEEE 802.15.4a also applies a systematic (55,63) Reed-Solomon (RS) code before modulation.

B. Wireless Transceivers

Honest devices are equipped with an IEEE 802.15.4a compliant receiver and transmitter. The choice of transmitter is of little consequence to our investigation, any standard-compliant transmitter is acceptable, e.g., [24], [25]. We consider two types of receivers: a low-complexity and low-cost non-coherent energy-detection receiver, and a sophisticated coherent rake receiver.

Adversarial devices are equipped with transmitters similar to the honest devices, but able to send non-standard-compliant pulse sequences and to ignore regulatory transmission power limits. The adversary may further equip his devices with high gain antennas, thus allowing him to increase the SNR observed by both adversarial and honest devices. Such an increase in SNR can also be achieved by the adversary moving his devices closer to the honest devices. The receivers used by the adversary are modified versions of the receivers presented next (see Section V).

1) Energy-Detection Receiver: The energy-detection receiver (we also use the term *energy detector*) squares and integrates the received signal $r(t)$. The integrator outputs a discrete time sample every $T = T_{\text{c}} = 2$ ns. Such a sampling rate is high enough to allow for precise ranging.

The receiver employs a traditional synchronization algorithm based on a correlation with the known preamble sequence. After a coarse synchronization, usually achieved on the strongest multi-path component, the receiver undertakes a verification phase. If successful, fine synchronization is performed using a back-search algorithm, to obtain a better estimate of the beginning of the signal. The receiver then performs a period of channel estimation where it estimates the energy-delay profile of the channel by averaging a number of preamble symbols. At the same time it also begins to look for the SFD.

To demodulate the i-th BPPM bit d_i of the payload, the receiver uses the optimum decision rule from [26], [27], comparing the (weighted) energies in the first and second half of the symbol:

$$\sum_{m=0}^{M-1} y_{m,i} \cdot p_m \underset{d_i=1}{\overset{d_i=0}{\gtrless}} \sum_{m=0}^{M-1} y_{m+\frac{T_f}{2T_{\text{c}}},i} \cdot p_m \tag{8}$$

where $y_{m,i}$ denotes the m-th discrete sample of the i-th symbol. The weighting coefficients p_m are derived from the energy-delay profile of the channel. The number of samples to combine is $M = t_{\text{det}}/T$, where t_{det} defines the *detection time*: the length of the received signal (per half-symbol) that the receiver uses to demodulate the bits; t_{det} is chosen to be large enough to account for the channel delay spread. In our simulations we use the non-line-of-sight residential channel model from [28] and set $t_{\text{det}} = 60$ns accordingly.

2) Rake Receiver: The receiver with optimal performance (in a benign setting), but also with the highest complexity, is an all-rake receiver using maximum ratio combining (MRC) [29]. The convolutional code is decoded with the optimal symbol-wise branch metric for BPPM/BPSK given in [30]. For this paper, the crucial difference between an energy-detection receiver and a rake receiver is that the latter can recover the polarity bits a_i during payload demodulation. This diminishes the effectiveness of payload PHY attacks against rake receivers (Section V-C), but also opens a new space for payload attacks if a rake receiver is used against energy-detection receivers. In our analysis of the rake receiver, we therefore focus on the payload, assuming perfect synchronization and channel estimation.

Similar to the energy-detection receiver, an important parameter for our analysis is the detection time t_{det}, denoting the portion of the received signal that the rake receiver uses to demodulate a bit. We chose t_{det} large enough to account for the channel delay spread.

C. Distance Bounding with IEEE 802.15.4a

DB protocols that are secure only against the mafia fraud, such as the protocol in Figure 1(a), are directly compatible

with IEEE 802.15.4a. This is because they employ a standard packet format for ranging messages [6], [13]. However, protocols that are also secure against the distance fraud or the terrorist fraud are typically not directly compatible with IEEE 802.15.4a. Such protocols need to prevent a malicious prover from decreasing the measured distance by responding prematurely. This is traditionally achieved with a *rapid bit exchange* (*RBE*), in which V sends single bit challenges, to which the prover should respond instantly (Figure 1(b)). An IEEE 802.15.4a implementation of the RBE – which requires prefixing every bit with a lengthy preamble – is not only inefficient, but also opens a space for packet-level attacks [3]. Nevertheless, recent proposals [12] show that with full duplex transmission, regular packet formats can be used in place of the rapid-bit-exchange. Applying this principle in IEEE 802.15.4a requires adding a number of "buffer" bits at the beginning of the challenge's payload, of total duration equal to the duration of the preamble (Figure 1(c)). This is necessary because the prover cannot start sending the response preamble before it synchronizes and detects the SFD of the challenge preamble, whereas security requires that every response symbol is transmitted *instantly* after the corresponding challenge symbol.

We define t_{res} as the time interval at the prover between the start of the reception of a challenge bit and the start of the transmission of the corresponding response bit. To make the response as "instant" as possible with IEEE 802.15.4a, we assume that $t_{\text{res}} = T_{\text{sym}}/2 + t_{\text{THS}}^{\text{max}} + t_{\text{det}}$. This is the smallest t_{res} sufficient to demodulate symbols with maximal time-hopping offsets.

We assume that the DB protocol has access to the received bit sequence before it is decoded with the error correcting codes (Reed-Solomon, convolutional). In a receiver implementation, this assumption can easily be met as these bits have to be received from the channel in any case. If this assumption is violated, the success probability of guessing attacks increases, because coding can mask some of the erroneously guessed bits.

V. Distance-decreasing Attacks

Physical layer (PHY) attacks were first introduced as a potential attack vector against distance bounding (DB) in [3]. These attacks rely on two primitives: 1) In *early detection* (*ED*), an adversarial receiver (ARX) detects a PHY symbol (e.g., payload symbol) of duration t_{sym} based only on the beginning part of this symbol of duration $t_{\text{ED}} < t_{\text{sym}}$, where t_{ED} is the *ED delay*. This leads to a detection which is less reliable, but also faster than that of a normal receiver (which takes $t_{\text{res}} > t_{\text{ED}}$ of the PHY symbol into account for detection). 2) In *late commit* (*LC*), only the $(t_{\text{sym}} - t_{\text{LC}})$-long end-part of the PHY symbol is modulated based on the intended value of the symbol (e.g., whether it encodes a 0 bit or a 1 bit), and the beginning part is modulated independently of this value. This allows an adversarial transmitter (ATX) to delay the decision about which symbol it transmits by t_{LC}, where t_{LC} is the *LC delay*. The PHY symbols generated with LC typically differ from regular symbols, but, if appropriately chosen, they can be demodulated by an honest receiver, albeit with some performance loss.

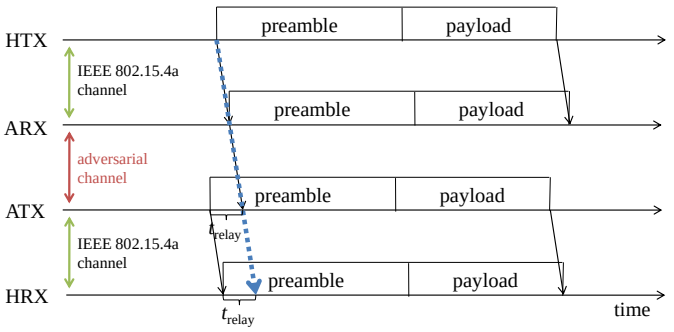

Fig. 3. Overview of the distance-decreasing relay attack. ARX and ATX are assumed to be located on a line between HRX and HTX. The thick dotted arrow indicates time-of-arrival corresponding to the actual distance between HTX and HRX.

The first type of PHY attack we consider is an internal attack mounted by a *malicious prover* (consisting of an ARX and an ATX), which can be used in a distance/terrorist fraud. In this attack, a malicious prover uses ED, LC or their combination to respond prematurely to the verifier's V challenge. This decreases the propagation time measured by V by an offset t_{gain} that we call the *time-gain*. The time-gain is equal to $(t_{\text{C}} + t_{\text{res}} - t_{\text{ED}})/2$ for an ED-only attack, $(t_{\text{LC}} + t_{\text{res}} - t_{\text{D}})/2$ for an LC-only attack, and $(t_{\text{LC}} + t_{\text{res}} - t_{\text{ED}})/2$ for an ED+LC attack, where t_{D} and t_{C} are, respectively, the detection delay and commit delay when the attacker chooses not to perform ED and LC. (Note: it is possible that $t_{\text{D}} < t_{\text{res}}$ and $t_{\text{C}} > 0$ if time-hopping is involved.) The time-gain translates into a *distance-decrease* of $c \cdot t_{\text{gain}}$, where c is the speed of light.

The second type of attack we consider is a *distance-decreasing relay attack* between two honest devices. This attack is mounted by an external adversary using a combination of ED and LC and it can be classified as a mafia fraud. The general setup for the relay attack is shown in Figure 3. The adversary should mount the distance-decreasing relay attack on all ranging messages (challenge, response); other messages, being not time-critical, can be relayed in an arbitrary fashion. Without loss of generality, we focus on the exchange of a single ranging message. In this case one of the honest devices acts as a transmitter (HTX) and the other one as a receiver (HRX), whereas one adversarial device acts as an early detection receiver (ARX), and another as a late commit transmitter (ATX). The channel from HTX to ARX, and from ATX to HRX is the IEEE 802.15.4a channel. ARX and ATX communicate using a dedicated, out-of-band adversarial channel. The propagation speed of both channels is c, the speed of light.

In a distance-decreasing relay attack the adversary relays messages between HTX and HRX in such a way that to HRX they seem "shifted back in time" by a positive offset $t_{\text{relay}} = t_{\text{LC}} - t_{\text{ED}}$ that we call the *relay time-gain* (Figure 3). The distance measured by V is then reduced by the *relay distance-decrease* $c \cdot t_{\text{relay}}$. (Assuming that ARX and ATX are located on a line between HTX and HRX. In other configurations the distance decrease will be smaller. Note, however, that the choice of the configuration rests with the adversary.) In the relay attack, ATX needs to begin the transmission of the

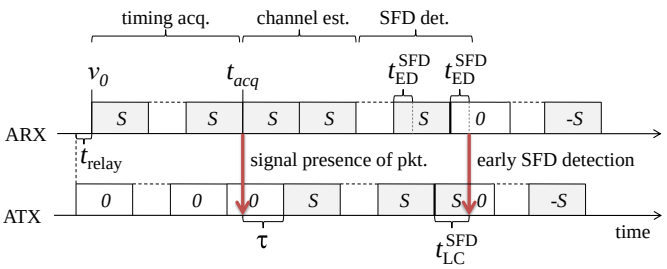

Fig. 4. Distance-decreasing relay attack on the preamble.

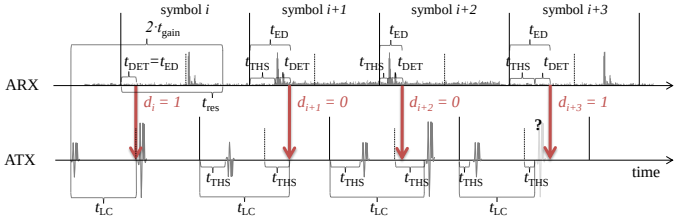

Fig. 5. Example of a malicious prover ED+LC attack on the payload. The first two symbols use equal time-hopping offsets for corresponding symbols, hence their time-gain is identical. The maximal time-gain for the 3rd symbol is larger than the packet-wide time-gain chosen of the adversary. The time-gain for the 4th symbol is smaller than the packet-wide time-gain, and the adversary is forced to guess.

preamble at time $t_0 - t_{\text{relay}}$, *before* ARX begins receiving the preamble from HTX a time t_0. However, the adversary learns t_0 only *after* synchronizing to the preamble of HTX. (Guessing t_0 is not practical at the nanosecond precision required.) To escape this vicious circle, the adversary needs to mount some form of ED and LC on the preamble, in addition to ED and LC on the payload. In contrast, the preamble attacks are not necessary in the case of malicious prover attacks.

Note that the distance-decrease that the adversary might wish to obtain is not limited by the low communication range of IEEE 802.15.4a. Indeed, a malicious prover can increase his communication range by using a high gain antenna and transmitting with non-regulatory power to reach a remote prover. Further, in a relay attack, the adversary can "connect" remote HRX and HTX by placing ARX close to HTX and ATX close to HRX, and using a long-range ATX–ARX link to which the range limitations of IEEE 802.15.4a do not apply.

We consider three scenarios, in which the adversary uses different types of receivers against different types of receivers used by the honest devices: Energy Detector against Energy Detector, Rake against Energy Detector, and Rake against Rake. For each scenario we first analyze the delay of the ED and LC primitives. Then, we elaborate on the use of these primitives for malicious prover attacks and relay attacks. Table I summarizes the upper-bounds on the time-gain and distance-decrease of various variants of PHY attacks. Note that the preamble attack is only presented in Section V-A1, as this attack is applicable and sufficient in the two other scenarios (it can achieve the relay time-gains of the magnitude required for the payload attack).

A. Energy Detector against Energy Detector

1) Attack on the Preamble: The attack, which is part of the distance-decreasing relay attack, is depicted in Figure 4; for clarity of presentation, we assume the distance between ARX and ATX to be 0. ARX performs packet detection, timing acquisition, and channel estimation in the same fashion as an honest receiver. ARX then signals the fact that it has acquired timing to ATX. Deviating from honest receivers, ARX performs *early SFD detection*: It chooses an early SFD detection delay $t_{\text{ED}}^{\text{SFD}}$ and tries to detect the presence of the SFD by deliberately considering only the first $t_{\text{ED}}^{\text{SFD}}$ ns of every received preamble symbol. As the SFD starts with a 0 modulated preamble symbol, as opposed to a 1 modulated symbol used during the SYNC part, early SFD detection boils down to on-off keying (OOK) demodulation.

At the other end of the relay, ATX chooses a late SFD commit delay $t_{\text{LC}}^{\text{SFD}}$ and remains silent until ARX signals that timing acquisition has been successful. Then, after an appropriately chosen (we explain how shortly) delay $\tau < T_{\text{psym}}$, ATX begins transmitting a sequence of preamble symbols S. This is repeated until ARX signals that the SFD was detected. Immediately afterwards, ATX switches to the transmission of a standard compliant SFD, beginning from $t_{\text{LC}}^{\text{SFD}}$ into the SFD. This concludes the distance-decreasing attack on the preamble.

In contrast to a standard-compliant preamble, the SYNC part of the preamble generated by ATX begins with a number of 0 modulated preamble symbols; The beginning of the SFD corresponds to a 1 modulated preamble symbol for a duration of $t_{\text{LC}}^{\text{SFD}}$, instead of having no signal contribution. The relay time-gain achieved by this attack is $t_{\text{relay}} = t_{\text{LC}}^{\text{SFD}} - t_{\text{ED}}^{\text{SFD}}$. This determines the choice of τ, as $T_{\text{psym}} - \tau = t_{\text{relay}} \mod T_{\text{psym}}$.

2) Attack on the Payload: Payload attacks are performed on a symbol basis. As we are considering energy-detection receivers, which are blind to the signal polarity, only the position bit d_i is relevant.

a) ED: ARX performs ED by deciding on the value of d_i^{RX} after an *early detection delay* $t_{\text{ED}}(d_i^{\text{RX}}) = t_{\text{THS},i}^{\text{RX}} + t_{\text{det}}^{\text{A}} < T_{\text{sym}}/2$, where $t_{\text{det}}^{\text{A}}$ denotes the detection time of ARX and $t_{\text{THS}}^{\text{RX}}$ is the time-hopping offset sequence of the received message. This implies that ARX replaces BPPM demodulation with on-off keying (OOK) demodulation. The time $t_{\text{det}}^{\text{A}}$ can be made arbitrarily short, it determines the attack's performance. If ARX chooses not to perform ED, the detection delay is $t_{\text{D}}(d_i^{\text{RX}}) = T_{\text{sym}}/2 + t_{\text{THS},i}^{\text{RX}} + t_{\text{det}}$.

b) LC: In the LC attack, ATX always transmits a burst of pulses with energy E_0 (shifted by the appropriate time-hopping offset). In the second half of the symbol, ATX acts according to the value of d_j^{TX}: If $d_j^{\text{TX}} = 0$, ATX transmits nothing in the second part of the symbol; if $d_j^{\text{TX}} = 1$, ATX transmits a burst of pulses with energy $E_1 > E_0$. This attack exploits the fact that HRX performs a simple energy comparison to demodulate. The *late commit delay* for d_j^{TX} is $t_{\text{LC}}(d_j^{\text{TX}}) = T_{\text{sym}}/2 + t_{\text{THS},j}^{\text{TX}} + t_{\text{PLC}}$, where $t_{\text{THS}}^{\text{TX}}$ is the time-hopping offset sequence of the transmitted message, and $t_{\text{PLC}} < t_{\text{det}}$ is the *pulse LC delay*, by which the transmission of the pulse can be additionally delayed, similar to the LC attacks discussed in [3], [15]. Throughout most of the paper, notably Section VI, we assume $t_{\text{PLC}} = 0$. If ATX chooses to send standard-compliant symbols, it can still delay committing

to the transmitted symbol by $t_{\mathrm{C}}(d_j^{\mathrm{TX}}) = t_{\mathrm{THS},j}^{\mathrm{TX}}$.

c) Malicious Prover: The time-gain of the ED-only malicious prover attack for corresponding challenge and response symbols i and j is $t_{\mathrm{gain}}(i,j) = (t_{\mathrm{C}}(d_j^{\mathrm{TX}}) + t_{\mathrm{res}} - t_{\mathrm{ED}}(d_i^{\mathrm{RX}}))/2 = (T_{\mathrm{sym}}/2 + t_{\mathrm{THS}}^{\max} + t_{\mathrm{det}} - t_{\mathrm{det}}^{\mathrm{A}})/2 + (t_{\mathrm{THS},j}^{\mathrm{TX}} - t_{\mathrm{THS},i}^{\mathrm{RX}})/2 = C + (t_{\mathrm{THS},j}^{\mathrm{TX}} - t_{\mathrm{THS},i}^{\mathrm{RX}})/2$, where C is a constant not dependent on i and j. The time-gain of other malicious prover attacks can also be expressed as $C + (t_{\mathrm{THS},j}^{\mathrm{TX}} - t_{\mathrm{THS},i}^{\mathrm{RX}})/2$. The latter term varies from $-t_{\mathrm{THS}}^{\max}/2$ to $t_{\mathrm{THS}}^{\max}/2$, because $t_{\mathrm{THS}}^{\mathrm{TX}} \neq t_{\mathrm{THS}}^{\mathrm{RX}}$ if different channels are used for for RX and TX, but also because $i \neq j$ due to the "buffer" bits (Figure 1(c)). However, the structure of the attack demands that the adversary chooses a constant time-gain t_{gain} for all symbols. This leaves the adversary with a strategic decision: The adversary can set the time-gain conservatively, to make sure there is enough time to perform ED and/or LC on every symbol (i.e., choose $t_{\mathrm{gain}} \leq t_{\mathrm{gain}}(i,j)$ for all corresponding i,j index pairs). Alternatively, the adversary can set the time-gain more aggressively, which will force him to guess the bits with unfavorable time-hopping offsets (i.e., i,j pairs for which $t_{\mathrm{gain}}(i,j) < t_{\mathrm{gain}}$). This is illustrated in Figure 5. In this way, the adversary can trade-off a larger time-gain (up to $2 \cdot t_{\mathrm{THS}}^{\max}/2$) for a lower attack success probability. Figure 6 shows this trade-off for one particular case ($N_{\mathrm{nonce}} = 42, N_{\mathrm{err}} = 2$, mandatory LPRF mode).

d) Relay: For the relay attack, the time-gain is $t_{\mathrm{relay}}(i,j) = t_{\mathrm{LC}}(d_j^{\mathrm{TX}}) - t_{\mathrm{ED}}(d_i^{\mathrm{RX}}) = T_{\mathrm{sym}}/2 + t_{\mathrm{PLC}} + t_{\mathrm{THS},j}^{\mathrm{TX}} - t_{\mathrm{THS},i}^{\mathrm{RX}} - t_{\mathrm{det}}^{\mathrm{A}}$. However, in the case of the relay attack $t_{\mathrm{THS}}^{\mathrm{RX}} = t_{\mathrm{THS}}^{\mathrm{TX}}$ and $i = j$. Hence, the time gain is $t_{\mathrm{relay}} = T_{\mathrm{sym}}/2 + t_{\mathrm{PLC}} - t_{\mathrm{det}}^{\mathrm{A}}$ for every symbol. This is also the upper-bound on the overall time-gain of the relay attack, as the time-gains achievable for the preamble are larger.

B. Rake against Energy Detector

1) ED and LC: If honest devices use energy detectors, using a rake receiver allows the adversary to perform an ED attack with *negative* delay t_{ED} by extracting d_i^{RX} from the (*i-1*)-th symbol. This attack exploits the structure of the convolutional code: The (*i-1*)-th payload symbol carries the position bit d_{i-1}^{RX} and the polarity bit $a_{i-1}^{\mathrm{RX}} = d_{i-2}^{\mathrm{RX}} \oplus d_i^{\mathrm{RX}}$. With a rake receiver, ARX can decode both bits, and obtain d_i^{RX} by computing $a_{i-1}^{\mathrm{RX}} \oplus d_{i-2}^{\mathrm{RX}}$. This is all that is necessary to transmit the corresponding j-th symbol: The adversary can compute d_j^{TX} from d_i^{RX}, and a_j^{TX} can be set arbitrarily, as polarity bits cannot be demodulated by an energy-detection receiver. The delay of the rake ED attack extracting d_i from the (*i-1*)-th symbol is $t_{\mathrm{ED}}(d_i^{\mathrm{RX}}) = -(1 - d_{i-1}^{\mathrm{RX}}) \cdot T_{\mathrm{sym}}/2 - T_{\mathrm{sym}}/2 + t_{\mathrm{THS},i-1}^{\mathrm{RX}} + t_{\mathrm{det}}^{\mathrm{A}}$. HRX is an energy-detector as in Section V-A2, hence the same LC attack applies.

2) Malicious Prover and Relay: With the rake ED attack, the malicious prover attacks, but also the relay attack (as $i = j - 1$ in this case) are subject to per-symbol variability of the time-gain due to time-hopping offsets. An additional time-gain variability is due to BPPM, i.e., the term "$-(1 - d_{i-1}^{\mathrm{RX}}) \cdot T_{\mathrm{sym}}/2$" of the ED delay. As in Section V-A2, this presents the adversary with a trade-off between the distance-decrease, and the probability of a successful attack. For example, the additional time-gain of the relay attack is at most $T_{\mathrm{sym}}/2 + 2 \cdot t_{\mathrm{THS}}^{\max}$, and Figure 6 shows the trade-off for a particular set of parameters. See Table I for the malicious prover attack.

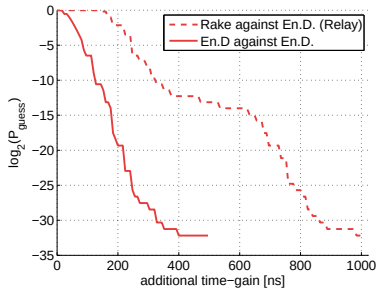

Fig. 6. Example trade-off between guessing probability and additional time-gain achievable with 1) Malicious prover attacks in the scenario "Energy Detector against Energy Detector" 2) Distance-decreasing relay attack in the scenario "Rake against Energy Detector". The guessing probability $P_{\mathrm{guess}}(t_{\mathrm{gain}}^{+}) = F_{\mathrm{BIN}}(N_{\mathrm{err}}|B(N_{\mathrm{nonce}}, t_{\mathrm{gain}}^{+}), \frac{1}{2})$, where $B(N_{\mathrm{nonce}}, t_{\mathrm{gain}}^{+})$ is the number of bits out of N_{nonce} that the adversary must guess to obtain an additional time-gain t_{gain}^{+}. The timing parameter values (notably the time-hopping sequence) correspond to the mandatory LPRF mode of IEEE 802.15.4a, and $N_{\mathrm{nonce}} = 42$, $N_{\mathrm{err}} = 2$ (corresponds to security level 2^{-32})

Furthermore, a negative ED delay allows for an ED-only distance-decreasing relay attack to be mounted. Although it has a lower time-gain than an ED+LC relay attack, the ED-only attack circumvents any countermeasures that prevent LC attacks, e.g., the countermeasure advocated in Section VII.

C. Rake against Rake

To mitigate the effects of the rake ED attack, an honest rake receiver must demodulate and check the correctness of both positions bits d_i and polarity bits a_i (without applying convolutional decoding, see assumption in Section IV-C). With this precaution in place, ATX cannot transmit symbol j (with or without LC) without knowing a_j^{TX}.

1) ED and LC: The ED delay of demodulating the polarity bit a_i^{RX} is $t_{\mathrm{ED}}(a_i^{\mathrm{RX}}) = d_i^{\mathrm{RX}} \cdot T_{\mathrm{sym}}/2 + t_{\mathrm{THS},i}^{\mathrm{RX}} + t_{\mathrm{det}}^{\mathrm{A}}$. The LC delay of committing to a_j^{TX} is $t_{\mathrm{LC}}(a_j^{\mathrm{TX}}) = t_{\mathrm{THS},j}^{\mathrm{TX}} + d_j^{\mathrm{TX}} \cdot T_{\mathrm{sym}}/2 + t_{\mathrm{PLC}}$. Note that both delays depend on the value of the position bit d. The delays for ED of d_i^{RX} and LC of d_j^{TX} are as in Section V-B.

2) Malicious Prover and Relay: The time-gain is computed as the minimum of the time-gain for the position bits d and the time-gain for the polarity bits a. In the relay attack, $i = j$, $d^{\mathrm{RX}} = d^{\mathrm{TX}}$, $a^{\mathrm{RX}} = a^{\mathrm{TX}}$, and $t_{\mathrm{THS}}^{\mathrm{RX}} = t_{\mathrm{THS}}^{\mathrm{TX}}$, hence the relay time-gain is $t_{\mathrm{relay}} = t_{\mathrm{PLC}} - t_{\mathrm{det}}^{\mathrm{A}} < t_{\mathrm{det}}$, which translates to at most 10m assuming $t_{\mathrm{det}} = 32$ns (see Section VI-B). This is an order of magnitude lower than the attacks presented so far. The time-gain of malicious prover attacks, without guessing, is of the same order of magnitude, see Table I. However, a malicious prover (but not a relaying adversary) can increase the distance-decrease by as much as $T_{\mathrm{sym}}/2 + t_{\mathrm{THS}}^{\max}$, by lowering the probability of success.

Furthermore, in the case of the relay attack, if only one of the honest devices uses an energy-detection receiver, notably without any countermeasures deployed, (and even though the other one uses a rake receiver) the adversary can achieve a significant time-gain. Even assuming that the distance-decrease against the rake receiver is negligible, the overall

		No guessing		Max. guessing gain	
		(relay) time-gain	distance-decrease	(relay) time-gain	distance-decrease
En.D. against En.D.					
Malicious Prover	ED-only	$T_{\text{sym}}/4 + (t_{\text{det}} - t_{\text{det}}^{\text{A}})/2$	86m	$+\, t_{\text{THS}}^{\text{max}}$	$+\,74$m
	LC-only	$T_{\text{sym}}/4 + t_{\text{PLC}}/2$	86m	$+\, t_{\text{THS}}^{\text{max}}$	$+\,74$m
	ED+LC	$T_{\text{sym}}/2 + (t_{\text{PLC}} + t_{\text{det}} - t_{\text{det}}^{\text{A}})/2$	171m	$+\, t_{\text{THS}}^{\text{max}}$	$+\,74$m
Relay Attack	ED+LC	$T_{\text{sym}}/2 + t_{\text{PLC}} - t_{\text{det}}^{\text{A}}$	171m	$+\,0$	$+\,0$m
Rake against En.D.					
Malicious Prover	ED-only	$T_{\text{sym}}/2 + (t_{\text{det}} - t_{\text{det}}^{\text{A}})/2$	162m	$+\, T_{\text{sym}}/4 + t_{\text{THS}}^{\text{max}}$	$+\,151$m
	ED+LC	$3/4 \cdot T_{\text{sym}} + (t_{\text{PLC}} + t_{\text{det}} - t_{\text{det}}^{\text{A}})/2$	248m	$+\, T_{\text{sym}}/4 + t_{\text{THS}}^{\text{max}}$	$+\,151$m
Relay Attack	ED+LC	$T_{\text{sym}} - t_{\text{THS}}^{\text{max}} + t_{\text{PLC}} - t_{\text{det}}^{\text{A}}$	251m	$+\, T_{\text{sym}}/2 + 2 \cdot t_{\text{THS}}^{\text{max}}$	$+\,302$m
	ED-only	$T_{\text{sym}}/2 - t_{\text{THS}}^{\text{max}} - t_{\text{det}}^{\text{A}}$	79m	$+\, T_{\text{sym}}/2 + 2 \cdot t_{\text{THS}}^{\text{max}}$	$+\,302$m
Rake against Rake					
Malicious Prover	ED-only	$(t_{\text{det}} - t_{\text{det}}^{\text{A}})/2$	5m	$+\, T_{\text{sym}}/4 + t_{\text{THS}}^{\text{max}}$	$+\,151$m
	LC-only	$t_{\text{PLC}}/2$	5m	$+\, T_{\text{sym}}/4 + t_{\text{THS}}^{\text{max}}$	$+\,151$m
	ED+LC	$(t_{\text{det}} + t_{\text{PLC}} - t_{\text{det}}^{\text{A}})/2$	10m	$+\, T_{\text{sym}}/2 + t_{\text{THS}}^{\text{max}}$	$+\,228$m
Relay Attack	ED+LC	$t_{\text{PLC}} - t_{\text{det}}^{\text{A}}$	10m	$+\,0$	$+\,0$m
En.D./Rake against En.D./Rake with ED-countermeasure (Section VII-A3) and convolutional code patch					
Malicious Prover	ED-only	$(t_{\text{det}}^{\text{C}} - t_{\text{det}}^{\text{A}})/2$	5-6m	$+\, t_{\text{THS}}^{\text{max}}$	$+\,74$m
	LC-only	$t_{\text{PLC}}^{C}/2$	5-6m	$+\, t_{\text{THS}}^{\text{max}}$	$+\,74$m
	ED+LC	$(t_{\text{PLC}}^{C} + t_{\text{det}}^{\text{C}} - t_{\text{det}}^{\text{A}})/2$	10-12m	$+\, t_{\text{THS}}^{\text{max}}$	$+\,74$m
Relay Attack	ED+LC	$t_{\text{PLC}} - t_{\text{det}}^{\text{A}}$	10-12m	$+\,0$	$+\,0$m
En.D./Rake against En.D./Rake with ED-countermeasure and convolutional code and time-hopping patches					
Malicious Prover	ED-only	$(t_{\text{det}}^{\text{C}} - t_{\text{det}}^{\text{A}})/2$	5-6m	$+\,0$	$+\,0$m
	LC-only	$t_{\text{PLC}}^{C}/2$	5-6m	$+\,0$	$+\,0$m
	ED+LC	$(t_{\text{PLC}}^{C} + t_{\text{det}}^{\text{C}} - t_{\text{det}}^{\text{A}})/2$	10-12m	$+\,0$	$+\,0$m
Relay Attack	ED+LC	$t_{\text{PLC}} - t_{\text{det}}^{\text{A}}$	10-12m	$+\,0$	$+\,0$m

TABLE I

Upper-bound on (relay) time-gain and (relay) distance-decrease of various PHY attacks in various "adversarial receiver against honest receiver" configurations. The left column presents conservative attacks, that work with 100% success probability. The right column presents the maximal additional time-gain/distance-decrease that can be achieved by combining PHY attacks and guessing attacks (when time guessing probability approaches the guessing probability of pure guessing attacks). Time-gain is expressed in terms of T_{sym} – payload symbol duration, $t_{\text{ED}} = 48\text{-}60ns$ – detection time of honest receivers without ED-countermeasure, $t_{\text{det}}^{\text{A}}$ – detection time of the adversary, $t_{\text{PLC}} < t_{\text{det}}$ – pulse LC delay, $t_{\text{THS}}^{\text{max}}$ – maximum time-hopping offset, $t_{\text{det}}^{C} = 48\text{-}60ns$ – detection time of honest receiver with ED-countermeasure, $t_{\text{PLC}}^{C} < t_{\text{det}}^{C}$ – pulse LC delay if countermeasure is deployed. The corresponding distance-decrease is shown for the IEEE 802.15.4a mandatory modes and delay values that maximize the distance-decrease.

distance-decrease of the relay attack is $c \cdot t_{\text{relay}}^{\text{En.D.}}/2$, where $t_{\text{relay}}^{\text{En.D.}}$ is the time-gain of the attack against an energy detector.

D. Processing Delays

An additional factor that reduces the time-gain of all attacks are the processing delays at ARX and ATX. A detailed discussion of these delays can be found in [4]. In short, it should be feasible to keep these delays in the order of 10-30ns (below 10m).

VI. Performance Evaluation

We evaluate the effectiveness of the distance-decreasing attacks with packet-based system simulations. We simulate a full IEEE 802.15.4a system including all the operations necessary to receive a packet: timing acquisition, estimation of the channel energy-delay profile, SFD detection, and data decoding. The physical layer is simulated with an accuracy of 100 ps. We use the residential non-line-of-sight channel model [28] with a channel delay spread $T_{\text{spread}} \approx 60$ ns. The signal to noise ratio (SNR) is defined as $\text{SNR} = \frac{E_p}{N_0}$ where E_p is the received energy *per pulse* (after the convolution of the pulse with the impulse response of the channel). We assume a desired security level of $P_{\text{guess}} = 2^{-32}$, and performance goals $\text{PER}_{\text{comm}} = \text{PER}_{\text{db}} = 10^{-2}$. According to Section III-B, this results in ranging packets of length $N_{\text{nonce}} = 42$ with a maximum of $N_{\text{err}} = 2$ tolerable bit errors.

A. Energy Detector against Energy Detector

For the energy detector against energy detector setting, a detailed performance evaluation of the ED and LC components, as well as of their combination in the case of the relay attack, was already presented in our previous paper [4] as well as in [31]. For a detailed discussion of the results, as well as alternative energy-detection receivers (which show similar performance), we therefore refer the reader there. In the following we give a summary of our main findings:

► In all attack scenarios, an adversary can decrease the distance by an amount that is close to the upper-bounds given in Table I. Furthermore, it can do so with an impressive success rate of 99% and at a cost of just a few dB in SNR with respect

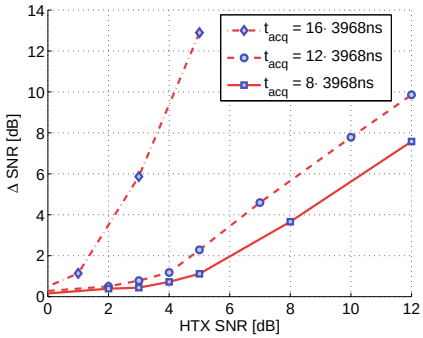

Fig. 7. Non-shielded HTX. We show the relative cost ΔSNR of the LC attack (both preamble and payload) versus SNR of HTX, for different timing acquisition delays t_{acq}.

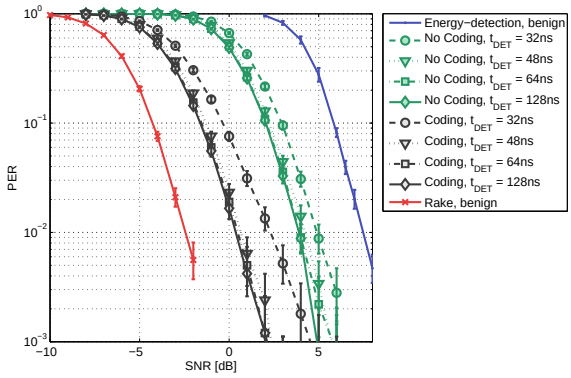

Fig. 8. Performance of early detection attack on the payload if the adversary uses an rake receiver. Early detection can be performed by decoding the convolutional code using partial information ("Coding") or by neglecting the convolutional code completely ("No Coding").

to normal system operation. A further increase in SNR allows the adversary to make the success rate arbitrarily large.

► For example, to mount an ED attack on the payload, achieving a distance-decrease of 77 m ($t_{\text{det}} = t^{\text{A}}_{\text{det}}$ in the order of the channel delay spread) with a success rate of 99%, the adversary requires an SNR at ARX that is 1.6 dB higher than in benign-case operation. A LC attack on the payload achieving the same distance-decrease (i.e., $t_{\text{PLC}} = 0$) costs 4 dB in SNR.

► A relay attack, including attacks on both preamble and payload, and achieving a distance-decrease of 144 m ($t_{\text{PLC}} = 0, t^{\text{A}}_{\text{det}} = 32$ ns), requires 6 dB higher SNR at ARX and 4 dB higher SNR at HRX, compared to benign-case operation.

1) HRX Not Isolated From HTX: In our threat model, we assume that the honest receiver, HRX, cannot receive signals sent by the honest transmitter, HTX. This is inherent in some scenarios, e.g., picking virtual pockets [32], but there are other scenarios where HTX will be in range of HRX. In this case, the adversary can prevent communication between the honest devices through shielding, by placing one of the honest devices in a Faraday cage (such as a "booster bag" coated with aluminium foil [33]). One adversarial device would then be connected via a wired link to the second adversarial device placed outside the Faraday cage.

However, in some scenarios HTX will be in range of HRX, and it might not be feasible for the adversary to shield HRX from HTX. We show here that the attack is still possible, but the cost of the attack (in terms of SNR) increases.

To make sure that HRX locks on the adversarial preamble, and not the preamble of HTX, ATX needs to start transmitting the preamble before HRX acquires HTX's signal. For the algorithms we assume, this happens no sooner than 18 preamble symbols into the preamble. The sooner ATX starts the transmission, the lower the cost (as usual, the cost is measured in terms of SNR necessary to achieve a PER of 10^{-2}).

Figure 7 shows the relative cost (in comparison with the LC attack where HRX is shielded from HTX) as a function of the SNR obtained by HTX at HRX, and when ARX starts the preamble transmission with a delay of 8, 12 and 16 preamble symbols. For the former two, the cost is in the order of HTX's SNR, but for 16 the cost grows much faster. Furthermore, ARX needs to perform early timing acquisition to make this attack possible. The cost, in comparison with regular acquisition after 18 symbols, is 6dB, 3dB and 2dB, for acquisition before 8, 12 and 16 preamble symbols, respectively.

B. Rake against Energy Detector

We evaluate the rake ED attack for an optimal all-rake receiver with perfect synchronization and channel estimation. Figure 8 shows the PER for an adversary performing the ED attack. When mounting the ED attack, ARX has the option to ignore ("No Coding") or take advantage of the convolutional code ("Coding"). For reference, the performance of a benign energy-detection receiver and a benign rake receiver are shown as well. The benign rake receiver decodes the convolutional code at the end of the packet as in [30], when the full decoding trellis is available. With ED and taking the code into account, only a partial trellis containing information about the symbols received so far is available at the time of decoding. This contributes to the higher cost (in terms of required SNR) of the attack with respect to the benign rake receiver operation. Ignoring the convolutional code is simpler and less computationally expensive, but results in an additional 3.5dB increase of the attack cost.

The adversary also has the choice of $t^{\text{A}}_{\text{det}}$. Optimal performance is experienced for $t^{\text{A}}_{\text{det}} = 64$ns, in the order of channel spread. $t^{\text{A}}_{\text{det}} = 48$ns results in a very minor performance loss, $t^{\text{A}}_{\text{det}} = 32$ns results in noticeable performance loss (around $1-2$dB). Assuming $t^{\text{A}}_{\text{det}} = 48$ns, the attack costs 2.8dB (at a PER of 10^{-2}, corresponding to an attack with a success rate of 99%) if coding is taken into account and the relay attack achieves a time-gain of $t_{\text{relay}} = 728$ns (distance-decrease of 218 meters). At the same cost, the alternative, ED-only attack achieves a time-gain of $t^{\text{ED-only}}_{\text{relay}} = 216$ns (distance-decrease of 65 meters).

VII. Countermeasures

When investigating countermeasures and patches, we consider their effectiveness (the maximum relay time-gain the adversary can achieve with the countermeasure in place),

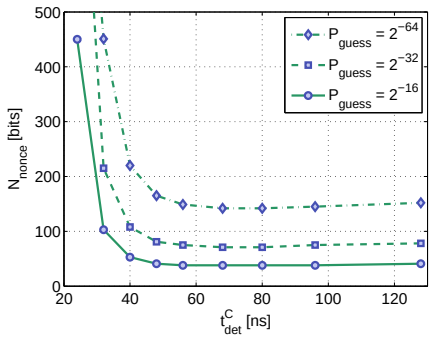

Fig. 9. Cost of Section VII-A3 countermeasure when the energy-detection receiver decides on the bit value using OOK demodulation at time $t^{\mathrm{C}}_{\mathrm{det}}$.

the effects they have on benign-case performance, and their compatibility with IEEE 802.15.4a. We discuss here the countermeasures which, in our opinion, provide the best trade-off between these factors. Then, we discuss out investigation of alternative countermeasures.

A. Recommended Countermeasures

1) Convolutional Code Patch: The rake ED attack is possible due to the specific combination of BPPM/BPSK with the convolutional code that IEEE 802.15.4a uses. The attack can be avoided with a different convolutional code, for which the polarity bit a_i does not reveal information about future position bits d_j, where $j > i$. The code should not allow for decoding a_{i+1} from the i-th symbol i, as this would enable an effective LC attack against a rake receiver. We refer to this solution as the *convolutional code patch*. Alternatively, the convolutional code can be removed altogether. The former is not compatible with IEEE 802.15.4a, whereas the latter is compatible to a very limited extent: Although IEEE 802.15.4a provides a few optional modes that do not use the convolutional code, these modes cannot be used with energy-detection receivers, because, for these modes, polarity carries data information.

2) Time-Hopping Patch: Time-hopping allows a malicious prover to trade-off attack success probability for additional time-gain. A simple way to remove this vulnerability is to modify the time-hopping sequence such that the corresponding challenge and response symbols have identical time-hopping offsets. Removing time-hopping is also a solution, but an inferior one, as it significantly degrades IEEE 802.15.4a multi-user access properties.

3) Early Detection at Honest Receiver: The honest energy-detection receiver can choose to only take into account the beginning of the symbol [15], essentially performing early detection with OOK demodulation at an offset $t^{\mathrm{C}}_{\mathrm{det}}$ from the beginning of the symbol. Then, t_{LC} is reduced from $T_{\mathrm{sym}}/2$ to $t^{C}_{\mathrm{PLC}} < t^{\mathrm{C}}_{\mathrm{det}}$, and the (malicious prover) time-gain due to ED is limited to $(t^{\mathrm{C}}_{\mathrm{det}} - t^{\mathrm{A}}_{\mathrm{det}})/2$ (assuming that the Prover sends the response symbol immediately after the early detection is done). This countermeasure does not induce inter-symbol interference and is compliant with the mandatory modes of the standard.

Moreover, the mild performance loss that this countermeasure entails due to the ignoring of half of the symbol, can be compensated for by increasing the length of the nonces N_{nonce}. We can derive the required nonce length by using the method introduced in Section III-B. Figure 9 plots the resultant N_{nonce} as a function of $t^{\mathrm{C}}_{\mathrm{det}}$ for performance goals $\mathrm{PER}_{\mathrm{comm}} = \mathrm{PER}_{\mathrm{db}} = 10^{-2}$ and 3 security levels. For example, by employing the countermeasure with $t^{\mathrm{C}}_{\mathrm{det}} = 40ns$ and increasing the number of bits per nonce from 42 to 108 we can bring the maximum theoretically achievable time-gain to 40ns (distance decrease of about 12 m) maintaining security level $P_{\mathrm{guess}} = 2^{-32}$. At the same time, this countermeasure does not reduce the performance in terms of PER and we also keep the same security level against guessing attacks. The only drawback is generating, sending and receiving of the additional bits required for the longer nonces. As every IEEE 802.15.4a payload carrying a nonce is preceded by a preamble of considerable length, and as a good deal of receiver complexity during reception stems from synchronization, we argue that the cost of adding a few bits to the payload is in most cases acceptable.

Furthermore, this countermeasure can be employed by both energy-detection and rake receivers to prevent the adversary from exploiting the BPPM variability (Section V-B). See Table I for upper-bounds on the attack time-gains with the countermeasure and patches deployed.

B. Alternative Countermeasures

1) Decrease Payload Symbol Duration: A straightforward countermeasures is to decrease payload symbol duration T_{sym} [3], as the time-gain of any PHY attack is at most T_{sym}. This countermeasure can be even implemented within the IEEE 802.15.4a standard, as some non-mandatory modes have symbols as short as 32 ns. However, reducing T_{sym} to a value where the attack is not a threat (i.e.,, the maximum achievable distance-decrease is only a few meters), is detrimental to benign performance. Inter-symbol interference (ISI) manifests itself if the symbol duration is close to or below the channel delay spread. Low-complexity non-coherent receivers cannot cope well with ISI and even if some solutions exist, they entail a loss of $5 - 10$ dB in the benign-case [34]. Furthermore, shorter symbols have less resilience to multi-user interference.

2) Secret Spreading Codes: To make preamble ED harder, if not infeasible within the constrained time budget available to the adversary, the honest devices could generate preamble codes from a shared secret. It is uncertain, but worth investigating, how such random codes without nice auto-correlation properties would affect the benign-case performance. Alternatively, secret time-hopping sequences could be used to make ED of payload symbols more difficult. This also requires further investigation. Naturally, both approaches can only prevent relay attacks, as a malicious prover would know the secret spreading codes.

Furthermore, both approaches are not directly compliant with the current IEEE 802.15.4a standard. The standard includes an optional private ranging mode, in which the ranging devices can secretly agree on a preamble code, but there exist only eight publicly known preamble codes to choose from. This offers little security: The adversary can guess both codes

with decent probability, or perform detection using, in parallel, all eight allowable codes. (This can be done entirely in the digital domain by correlating the received signal with each of the 8 codes and choosing the one with the highest correlation output.)

3) Detect Payload LC: We investigated a countermeasure that detects the non standard signal sent by the adversary during the payload LC attack. With this countermeasure, the receiver records, for every bit, the energy in the fist half of the symbol, and compares the distribution of these energies for the 0 bits (bits that were decoded as a 0) with the 1 bits (decoded as a 1). In the benign case, the first halves of the 0 bits carry more energy, whereas under attack these energies are the same. To distinguish these cases, one can use a robust statistical test, such as the Mann-Whitney-Wilcoxon test. This countermeasure prevents the attack presented in Section V-A2 with virtually no degradation of benign case performance. However, an adversary can modify the attack (vary the energy levels between symbols) to severely degrade the performance of this countermeasure.

4) Detect Preamble LC: We experimented with countermeasures that attempt to detect the preamble under a LC attack. For example, a countermeasure could check if the first SFD symbol is entirely 0 (as it should be). However, this countermeasure can only reliably detect an attack with relatively high $t_{\text{LC}}^{\text{SFD}}$ (more S than 0 in the preamble symbol) at high SNR, but not attacks with low $t_{\text{LC}}^{\text{SFD}}$ (more 0 than S), especially in the lower SNR regions. A countermeasure could also detect the high number of 0 symbol at the beginning of the preamble – but this can be countered by the adversary by early time acquisition (which comes at some additional cost in terms of SNR, see Section VI-A1). Finally, countermeasures to preamble LC attacks cannot prevent malicious prover attacks.

VIII. Conclusion

We have investigated the vulnerability of the IEEE 802.15.4a standard to physical layer distance-decreasing attacks. We have demonstrated that if honest devices use energy-detection receivers without appropriate countermeasures, an adversary can decrease the measured distance by hundreds of meters, with a success rate arbitrarily close to 100%. However, minor modifications to IEEE 802.15.4a and implementing a simple countermeasure on energy-detection receivers used by honest devices, allow honest devices to reduce the effectiveness of distance-decreasing relay attacks to at most 10m. Alternatively, this can be achieved (even without IEEE 802.15.4a modifications) if honest devices use the more sophisticated rake receivers. Furthermore, to reduce the effectiveness of malicious prover attacks to around 10m, the honest receivers (energy detector and rake alike) should implement the same simple countermeasure, and a time-hopping patch should be applied to IEEE 802.15.4a. In conclusion, with appropriate countermeasures on the receivers and patches to the IEEE 802.15.4a standard, the standard can be used as a DB PHY.

More generally, our investigation has identified PHY features that, although improving system performance in the benign case, can create vulnerabilities against distance-decreasing PHY attacks if used carelessly. One such potential point of failure is the interaction between the modulation and the coding scheme. Another, perhaps more fundamental one, is payload time-hopping, which allows the adversary to additionally decrease the distance by lowering the attack's probability of success. Such features should be approached with caution, or not used at all, in any DB PHY.

References

[1] S. Gezici, Z. Tian, G. Giannakis, H. Kobayashi, A. Molisch, H. V. Poor, and Z. Sahinoglu, "Localization via ultra-wideband radios: a look at positioning aspects for future sensor networks," *IEEE Signal Process. Mag.*, vol. 22, no. 4, July 2005.

[2] S. Brands and D. Chaum, "Distance-bounding protocols," in *EUROCRYPT'93, Lect. Notes in Computer Science 765*, 1993.

[3] J. Clulow, G. P. Hancke, M. G. Kuhn, and T. Moore, "So near and yet so far: Distance-bounding attacks in wireless networks," in *Third European Workshop on Security and Privacy in Ad-hoc and Sensor Networks (ESAS)*, 2006. [Online]. Available: http://www.crysys.hu/ESAS2006/cfp.html

[4] M. Flury, M. Poturalski, P. Papadimitratos, J.-P. Hubaux, and J.-Y. Le Boudec, "Effectiveness of Distance-Decreasing Attacks Against Impulse Radio Ranging," in *3rd ACM Conference on Wireless Network Security (WiSec)*, 2010.

[5] G. Hancke and M. Kuhn, "An RFID distance bounding protocol," in *Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on*, 2005.

[6] S. Čapkun and J.-P. Hubaux, "Secure positioning in wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, 2006.

[7] D. Singelée and B. Preneel, "Distance bounding in noisy environments," in *European Workshop on Security and Privacy in Ad-Hoc and Sensor Networks (ESAS)*, 2007.

[8] L. Bussard, "Trust establishment protocols for communicating devices," Ph.D. dissertation, 2004.

[9] J. Reid, J. M. G. Nieto, T. Tang, and B. Senadji, "Detecting relay attacks with timing-based protocols," in *ASIAN ACM Symposium on Information, Computer and Communications Security*, 2007.

[10] C. H. Kim, G. Avoine, F. Koeune, F.-X. Standaert, and O. Pereira, "The swiss-knife RFID distance bounding protocol," in *International Conference on Information Security and Cryptology (ICISC)*, P. Lee and J. Cheon, Eds., 2008.

[11] C. H. Kim and G. Avoine, "RFID distance bounding protocol with mixed challenges to prevent relay attacks," in *8th International Conference on Cryptology and Network Security (CANS)*, 2009, paper http://www.uclouvain.be/sites/security/download/papers/KimA-2009-cans.pdf.

[12] K. B. Rasmussen and S. Čapkun, "Location privacy of distance bounding protocols," in *15th ACM conference on Computer and Communications Security (CCS)*, 2008.

[13] C. Meadows, R. Poovendran, D. Pavlovic, L.-W. Chang, and P. Syverson, "Distance bounding protocols: Authentication logic analysis and collusion attacks," in *Secure Localization and Time Synchronization for Wireless Sensor and Ad Hoc Networks*. Springer-Verlag, Series: Advances in Information Security, Vol. 30, 2007.

[14] P. Schaller, B. Schmidt, D. Basin, and S. Čapkun, "Modeling and verifying physical properties of security protocols for wireless networks," in *CSF '09: Proceedings of the 2009 22nd IEEE Computer Security Foundations Symposium*, 2009.

[15] G. P. Hancke and M. G. Kuhn, "Attacks on time-of-flight distance bounding channels," in *First ACM conference on Wireless network security (WiSec)*, 2008.

[16] 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 *Ultra-Wideband, 2010. ICUWB 2010. IEEE International Conference on*, 2010.

[17] M. Kuhn, H. Luecken, and N. Tippenhauer, "UWB impulse radio based distance bounding," in *Proceedings of the Workshop on Positioning, Navigation and Communication (WPNC)*, 2010.

[18] N. O. Tippenhauer and S. Čapkun, "Id-based secure distance bounding and localization," in *In Proceedings of ESORICS (European Symposium on Research in Computer Security)*, 2009.

[19] J. Munilla and A. Peinado, "Distance bounding protocols for RFID enhanced by using void-challenges and analysis in noisy channels," *Wireless Communications and Mobile Computing*, vol. 8, no. 9, 2008.

[20] G. Hancke, "Design of a secure distance-bounding channel for RFID," *Elsevier Journal of Network and Computer Applications*, 2010.

[21] S. Drimer and S. Murdoch, "Keep your enemies close: Distance bounding against smartcard relay attacks," in *Proceedings of the 16th USENIX Security Symposium*, 2007.

[22] Y. Desmedt, "Major security problems with the "unforgeable"(Feige-)Fiat-Shamir proofs of identity and how to overcome them," in *SecuriCom'88*, 1988.

[23] IEEE Computer Society, LAN/MAC Standard Committee, "IEEE P802.15.4a/D7 (amendment of IEEE std 802.15.4), part 15.4: Wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks," Jan. 2007.

[24] C. Duan, P. Orlik, Z. Sahinoglu, and A. F. Molisch, "A non-coherent 802.15.4a UWB impulse radio," in *Ultra-Wideband, 2007. ICUWB 2007. IEEE International Conference on*, September 2007, pp. 146–151.

[25] J. Ryckaert, G. Van der Plas, V. De Heyn, C. Desset, G. Vanwijnsberghe, B. Van Poucke, and J. Craninckx, "A 0.65-to-1.4nJ/burst 3-to-10GHz UWB digital TX in 90nm CMOS for IEEE 802.15.4a," *IEEE International Solid-State Circuits Conference (ISSCC 07)*, 2007.

[26] A. A. D'Amico, U. Mengali, and E. Arias-De-Reyna, "Energy-detection UWB receivers with multiple energy measurements," *IEEE Trans. Wireless Commun.*, vol. 6, no. 7, pp. 2652–2659, 2007.

[27] M. Flury, R. Merz, and J.-Y. Le Boudec, "An energy detection receiver robust to multi-user interference for ieee 802.15.4a networks," in *IEEE International Conference on Ultra-Wideband (ICUWB 2008)*, Hannover, 2008.

[28] A.-F. Molisch, K. Balakrishnan, C.-C. Chong, S. Emami, A. Fort, J. Karedal, J. Kunisch, H. Schantz, U. Schuster, and K. Siwiak, "IEEE 802.15.4a channel model - final report, document 04/662r1," November 2004.

[29] J. G. Proakis and M. Salehi, *Digital Communications*, 5th ed. McGraw–Hill, 2008.

[30] Z. Ahmadian and L. Lampe, "Performance analysis of the IEEE 802.15.4a UWB system," *Communications, IEEE Transactions on*, vol. 57, no. 5, pp. 1474–1485, 2009.

[31] M. Flury, "Interference Robustness and Security of Impulse-Radio Ultra-Wide Band Networks," Ph.D. dissertation, Lausanne, 2010. [Online]. Available: http://library.epfl.ch/theses/?nr=4698

[32] Z. Kfir and A. Wool, "Picking virtual pockets using relay attacks on contactless smartcard," in *Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on*, 2005.

[33] "http://www.realtechnews.com/posts/1366."

[34] F. Trösch and A. Wittneben, "MLSE post-detection for ISI mitigation and synchronization in UWB low complexity receivers," in *Vehicular Technology Conference, 2007. VTC2007-Spring. IEEE 65th*, april 2007, pp. 2915 –2919.