

UWB Impulse Radio Based Distance Bounding

Marc Kuhn¹, Heinrich Luecken¹, and Nils Ole Tippenhauer²

¹Communication Technology Laboratory, ²System Security Group

ETH Zurich, CH-8092 Zurich, Switzerland

{kuhn, luecken}@nari.ee.ethz.ch, tinils@inf.ethz.ch

Abstract—Today’s communication systems are often vulnerable to wormhole or relaying attacks, leading to severe security problems. Distance Bounding (DB) protocols are authentication protocols designed to protect against these attacks. They determine an upper bound on the physical distance between two communication parties — the verifier \mathcal{V} (e.g. a door requiring an access key) and the prover \mathcal{P} (e.g. a wireless key device). UWB technology promises an innovative wireless implementation of DB protocols, using low cost components. A crucial aspect for DB algorithms, besides a high temporal resolution, is the processing delay of \mathcal{P} between receiving a challenge from \mathcal{V} and transmitting the answer to \mathcal{V} . Even current UWB transceivers may add a considerable processing delay, which decreases the provided security. We propose and analyze a novel analog UWB transceiver architecture which is able to both detect incoming UWB pulses and transmit answers with minimal delay.

I. INTRODUCTION

With proliferation of wireless communication to security-related systems, design and analysis of security protocols are essential. Considering for example access control to buildings, it is desirable to use a low-complexity wireless device working as a key. The door, here referred to as the *verifier* \mathcal{V} and the key (*prover* \mathcal{P}) share a secret, which legitimates an authorized person to enter. A well-known vulnerability of these systems are *relay or wormhole attacks* (cf. Fig. 1): The attacker \mathcal{A} establishes communication between \mathcal{V} and a distant \mathcal{P}_2 by forwarding the respective messages. Using this attack, the attacker can open the door without having to decrypt messages or guessing the shared key. One solution to protect against these attacks is *distance bounding* [1]–[3]: An authorized \mathcal{P} is only allowed to open the door if it proves to be not further from \mathcal{V} than a certain maximum distance d_{\max} by replying to several single bit challenges.

The high bandwidth of UWB enables time-of-arrival measurements with high resolution [4]. Moreover, UWB impulse radio enables the implementation of low complexity and low power transceivers. In particular, noncoherent receivers can be implemented very efficiently [5]. In [6], the authors presented an energy detection (ED) based ultra-low power UWB system design with an overall estimated current consumption of less than 1 mW. The theoretical feasibility of the presented design respecting FCC power limits [7] together with transmission of only one pulse per bit (very important for our DB approach) has been shown by means of computer simulation and over the air [8]. This makes an UWB impulse radio (IR) design based on the ED a very promising candidate for the implementation of DB protocols. The resulting transceiver of \mathcal{P} would com-

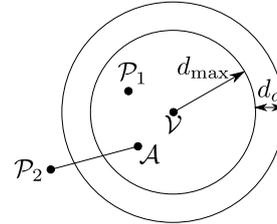


Fig. 1. Wormhole attack: the attacker \mathcal{A} relays communication between the distant \mathcal{P}_2 and \mathcal{V} although \mathcal{P}_2 is outside the secure distance d_{\max} .

bine low complexity and low power consumption with fast response/ low delay that is essential for DB hardware. In this paper, we investigate the application of such a UWB IR system design for DB.

Contributions: We present a system concept for DB based on an analog UWB IR transceiver using the ED of [6] and the original DB protocol [1]. We analyze the false acceptance and false rejection ratio of the system when transmitting compliant to the FCC regulation and investigate in which distances the system shows acceptable performance. Furthermore, we identify the disadvantages of the common binary pulse position modulation (BPPM) approach for UWB IR. Eventually, we propose improvements of the system leading to higher accuracy of the DB while keeping the low complexity.

II. DISTANCE BOUNDING

A. The Distance Bounding Protocol

DB techniques use measurements of the distance between the verifier \mathcal{V} and the prover \mathcal{P} to detect wormhole attacks. If the DB protocol finishes successfully, \mathcal{V} will conclude that \mathcal{P} is closer than a certain distance d_{\max} . In this paper, we propose the following three phases approach based on [1]:

In the *initialization phase*, the protocol first establishes a connection between \mathcal{V} and \mathcal{P} on the physical layer. This includes a synchronization of both nodes and channel estimation at \mathcal{V} . Further, \mathcal{V} sends on a secure channel a fresh and random nonce $\mathbf{s} = [s_1, \dots, s_R] \in \{0, 1\}^R$ to \mathcal{P} to be used as a shared secret in this protocol execution. This secure channel has to guarantee the authenticity, integrity and secrecy of the messages sent on it, which can be achieved e.g. by SSL [9].

The protocol uses this secret in the second phase, the *rapid bit exchange*. At the start of this phase, \mathcal{V} generates another fresh and random nonce $\mathbf{c} = [c_1, \dots, c_R] \in \{0, 1\}^R$ to use as R single bit challenges for \mathcal{P} . This is done by transmitting \mathbf{c} in R single UWB IR pulses with a sufficient inter-pulse

spacing allowing for the answers of \mathcal{P} in between. As shown in Fig. 2, immediately after receiving each of these challenges, \mathcal{P} computes a reply r_i using the received challenge bit \hat{c}_i and the current shared secret bit s_i , and transmits this reply to \mathcal{V} as soon as possible. \mathcal{V} measures the total round trip time between challenge and response and checks the response bit according to c_i and s_i . This process is repeated until all R challenge bits are transmitted and the R challenge responses are received at \mathcal{V} . In general, the round trip time T is two times the propagation delay τ between \mathcal{V} and \mathcal{P} , plus the prover delay T_p , which includes all delays such as signal processing time at \mathcal{P} , the pulse duration etc.:

$$T = 2\tau + T_p$$

In each round, an upper bound on the distance d can be computed by neglecting the prover delay T_p ,

$$d \leq \frac{T}{2}c, \quad (1)$$

where c is the propagation speed. An estimate \hat{d} of the actual distance of a prover \mathcal{P} with unmodified hardware can be determined assuming a maximal delay T_{\max} at \mathcal{P} as

$$\hat{d} = \frac{T - T_{\max}}{2}c \leq d. \quad (2)$$

After the R rapid bit exchanges, the DB protocol uses a third phase — the *challenge retransmission*. In this phase, \mathcal{P} transmits all received bit challenges to \mathcal{V} . This is done using a secure channel, e.g. the same channel used to send s in the initialization phase. The challenge retransmission is necessary to ensure that the challenges \hat{c}_i received at \mathcal{P} were indeed sent by \mathcal{V} .

After the three phases, \mathcal{V} can decide based on the challenge responses and the estimated distances, if \mathcal{P} is within the distance d_{\max} . Depending on the expected Bit Error Rate (BER) variation, \mathcal{V} can tolerate a certain number of wrong reply bits. To aggregate the distances measured in each round of the rapid bit exchange, the max-function should be used for maximum security.

B. Attacker Models

In our security analysis, we will discuss standard DB-attacks by an external attacker \mathcal{A} (referred to as *Mafia fraud* in the literature) or a misbehaving \mathcal{P}_m (*Distance fraud*). The goals of these two attackers are the same: to shorten the measured distance between \mathcal{V} and the prover and thus to make \mathcal{V} believe that the prover is closer than he really is. The difference between both attacker models is the following: The misbehaving \mathcal{P}_m is in possession of the shared secret s , but more than d_{\max} away from \mathcal{V} and therefore has to cheat to successfully complete the protocol. The external attacker \mathcal{A} is not in possession of the secret s , but close enough to \mathcal{V} to run the protocol successfully. The case of a misbehaving prover sharing s with an external attacker is also referred to as *Terrorist Attack* and will not be discussed here; distance bounding protocols can be extended to protect against this attack in general [10], if needed.

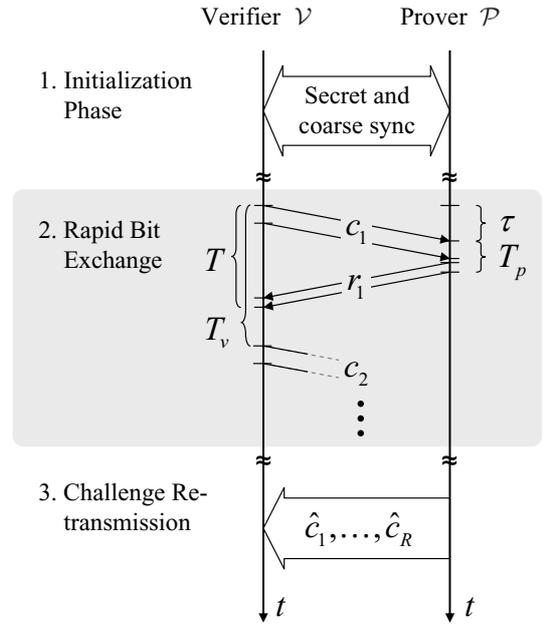


Fig. 2. Schematic figure of protocol timeline.

C. Standard Attacks on Distance Bounding

In this subsection, we will describe relevant standard attacks on round trip time based distance measurement protocols and how to either minimize their impact or to defeat them fully.

Relay or Wormhole attacks: In case of a relay attack, the attacker forwards communication to a distant \mathcal{P} . This is detected by the proposed protocol, because the signal propagation speed is limited to c . Therefore, the attacker can not speed up the transmission of the forwarded message, resulting in a high additional transmission delay which will be detected by \mathcal{V} . Therefore, relay attacks are defeated by the distance bounding protocol. This fundamental conclusion is analyzed in more detail in [11], [12].

Minimizing T_p : If an estimate \hat{d} of the distance between \mathcal{V} and \mathcal{P} is computed under consideration of the maximal prover delay T_{\max} , using (2), then a malicious \mathcal{P}_m can shorten this distance by shortening the delay T_p , e.g. by using more sophisticated transceiver hardware. The maximal distance advantage an attacker can gain using sophisticated hardware which minimizes T_p is

$$d_a = \frac{T}{2}c - \frac{T - T_{\max}}{2}c = \frac{T_{\max}}{2}c. \quad (3)$$

This effectively extends the radius of the circle in which \mathcal{P}_m has to reside to successfully run the protocol (see also Figure 1).

For this reason, minimizing the processing time at \mathcal{P} is essential for DB because it allows for smaller values of T_{\max} and consequently allows smaller d_a . UWB seems to be ideal for this purpose because it allows for short pulse durations and low delay receiver architectures.

Guessing attacks: Both an external attacker impersonating \mathcal{P} and a malicious \mathcal{P}_m can try to send the replies before

actually receiving the respective challenges. As the proposed protocol is based on an i.i.d. random sequence of R equally distributed bits, the chance to guess each of the R replies correctly is 2^{-R} .

Verifier Impersonation Attack: An external attacker \mathcal{A} close to \mathcal{V} could also try to obtain s by sending R random challenges c'_1, \dots, c'_R to \mathcal{P} before \mathcal{V} starts the actual rapid bit exchange. Then, \mathcal{P} computes the correct replies to these challenges and sends them to \mathcal{A} . When \mathcal{V} starts sending the proper challenge bits, \mathcal{A} can impersonate \mathcal{P} by using \mathcal{P} 's earlier replies. If the function to compute the replies from the challenge and secret is bijective, knowing the replies to c'_i will allow \mathcal{A} to perfectly answer any c_i sent by \mathcal{V} . If the function is not bijective, \mathcal{A} will still improve his chances compared to random guessing only. This attack may result in a shorter distance measured because \mathcal{A} is closer to \mathcal{V} than \mathcal{P} .

In case of the proposed DB protocol, \mathcal{V} can detect this fraud because of the challenge retransmission phase in which \mathcal{P} reports all received challenges \hat{c}_i to \mathcal{V} . Unless \mathcal{A} guesses all challenges correctly (with a chance 2^{-R}), the attack will be detected.

Early detection attacks: More sophisticated attacks are the early detection and late commit attacks [3], [13]. Early detection attacks try to obtain information of a symbol earlier than a normal receiver. On the signal processing level, the attacker could modify the demodulator such that the decision for the current symbol's data content is given earlier than usually, either by using a superior demodulator or accepting a higher BER. This way, the attacker would get an advantage of a fraction of the symbol length, which can be a problem for symbols with low bandwidth. Therefore, the distance bounding implementation should have symbols as short as possible to mitigate this attack.

Late commit attacks: The late commit attacks exploit the fact that an honest sender will only start sending a message when the content is ready. Instead of using the correct transmit signal, a malicious sender could use an alternative waveform, which is constructed such that the decision at the receiver is determined not by the full symbol, but only a part at the end [3], [13]. Similar to early detection attacks, this can yield an advantage of up to the symbol duration for the attacker and can be mitigated by choosing short symbols.

III. MINIMAL DELAY UWB TRANSCEIVER FOR DISTANCE BOUNDING

In the rapid bit exchange, it is essential to detect UWB pulses and transmit answers with minimal delay. Current UWB transceiver systems detect incoming signals using digital signal processing. These approaches may add a considerable delay to the response of \mathcal{P} . Therefore, the proposed receiver structure has to be able to perform signal processing in analog domain. We propose a noncoherent energy detection (ED) receiver for \mathcal{P} , which is motivated by stringent requirements on low complexity and low power consumption. It is based on the receiver design according to [6] and consists of a bandpass filter and a squaring device followed by an integration filter.

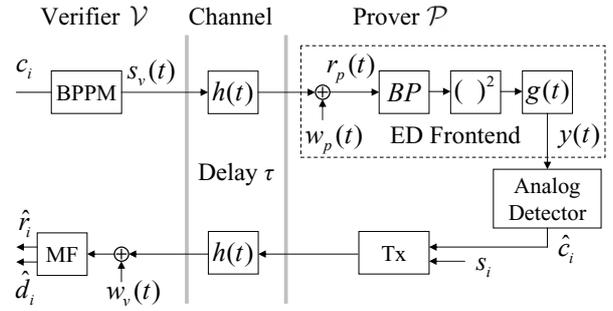


Fig. 3. System model: Verifier and prover.

This filter is implemented as a first-order low-pass. Besides the low duty cycle operation also the usage of low complexity resonant circuits in the analog part is important for the transceiver to achieve low power consumption. This requires a moderate relative bandwidth. Hence, the frequency range from 3.5 to 4 GHz has been chosen. The duty cycle of the receiver can be reduced to 1%, i.e. the analog components of the receiver can be switched most of the time to save power, cf. [6]. As a further advantage, the ED receiver is robust to jitter of the symbol clock, which is trained in the first phase of the DB protocol. For the forward path from \mathcal{V} to \mathcal{P} the challenges are transmitted using UWB IR with Binary Pulse Position Modulation (BPPM) or Security Enhanced Modulation (SEM). We choose a BPPM symbol duration of 20 ns, i.e. 10 ns per PPM half frame. This is motivated by channel measurements of the rms delay spread (cf. [14], [15]). For this choice the ED receiver shows acceptable performance for the considered scenario, even when multipath is considered.

Since \mathcal{V} may not be limited in terms of complexity and power consumption, we propose to use Binary Phase Shift Keying (BPSK) for the backward path from \mathcal{P} to \mathcal{V} and coherent detection, i.e. a channel matched filter receiver, at \mathcal{V} . This enables a better BER performance and also reduces the effects of late commit attacks.

A. System Model

The system model of the UWB DB system is shown in Fig. 3. At \mathcal{V} , the challenge bits c_i are binary pulse position modulated with transmit pulse $p(t)$. For $c_i = 0$ the pulse is transmitted in the first time slot and for $c_i = 1$ the pulse is transmitted in the second time slot. The polarity of the transmit pulse $a_i = \pm 1$ is chosen randomly to avoid discrete spectral lines in the spectrum of the transmit signal. Otherwise, the FCC rules for UWB could not be exploited to the full extent. Thus, the transmit signal is given by

$$s_v(t) = \sum_{i=1}^R a_i p(t - c_i T_{\text{ppm}} - iT_v),$$

where $T_{\text{ppm}} = 10$ ns denotes the duration of the PPM half frame and T_v the challenge repetition time, which has to be larger than the round trip time of a single challenge bit. The number of transmitted bits is R . As transmit pulse shape $p(t)$

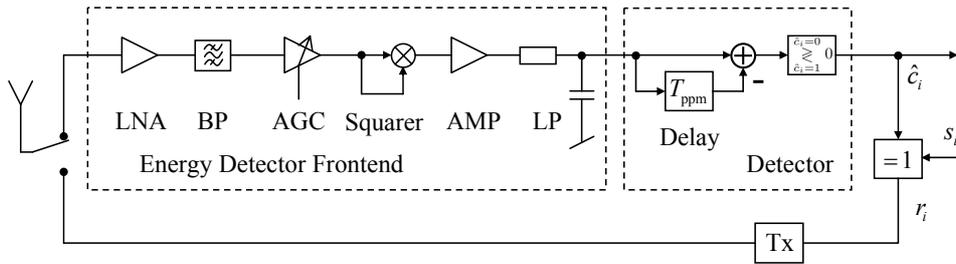


Fig. 4. Block diagram of prover architecture.

we choose the impulse response of a third order butterworth filter with energy E_b , center frequency $f_c = 3.75$ GHz, and bandwidth $B = 500$ MHz. To comply with FCC regulation [7], the transmit power is limited to $P_{\text{FCC}}^{\text{av}} = -14.3$ dBm by the average power constraint and $P_{\text{FCC}}^{\text{p}} = 0$ dBm by the peak power constraint. Depending on the pulse rate either the first or the second constraint may be limiting [5]. For a duty cycle of 1%, the maximal allowed transmit power equals 0 dBm.

The multipath channel is modeled as convolution of the transmit signal $s(t)$ with channel impulse response $h(t)$. It is assumed that the channel is static during the complete protocol run. The line-of-sight (LOS) path of the frequency selective channel exhibits a delay of $\tau = \frac{d}{c}$, where c denotes the speed of light. At prover \mathcal{P} , the receive signal is perturbed by additive white Gaussian noise (AWGN) with spectral power density $\frac{N_0}{2}$. Hence, the receive signal is given by

$$r_p(t) = s(t) * h(t) + w_p(t).$$

The data detection at \mathcal{P} is based on a generalized energy detector frontend followed by analog detection. The generalized energy detector frontend consists of a bandpass filter, a squaring device and an integration filter. Thus, we have at the output of the generalized energy detector

$$y(t) = \int_{-\infty}^{\infty} g(\tau) \tilde{r}_p^2(t - \tau) d\tau,$$

where $\tilde{r}_p(\cdot)$ denotes the bandpass filtered receive signal and $g(\cdot)$ the impulse response of the integration filter.

The analog detector consists of a delay element, subtraction and a threshold device. The energy of the first time slot is compared to the energy of the second time slot. This is done by subtracting the values and comparing to threshold zero. The decision rule for challenge bit i is modeled as

$$y(iT_v) - y(iT_v + T_{\text{ppm}}) \underset{\hat{c}_i=1}{\overset{\hat{c}_i=0}{\geq}} 0.$$

It is the inherent advantage of BPPM that the threshold is zero and independent of the channel conditions and must not be adapted. We assume for the rapid bit exchange phase perfect symbol synchronization at prover \mathcal{P} . The synchronization is established during the training phase before the rapid bit exchange starts. Synchronization algorithms for the considered receiver structure are presented e.g. in [16].

To compute the reply bits r_i , the estimated challenge bits \hat{c}_i are XORed with the secret s_i :

$$r_i = \hat{c}_i \oplus s_i$$

The reply bits are transmitted back to the verifier \mathcal{V} by BPSK. Thus, the transmit signal at \mathcal{P} can be written as

$$s_p(t) = \sum_{i=1}^N (2r_i - 1) \cdot p(t - \tau - T_p - iT_v),$$

where we assume to use the same transmit pulse $p(t)$ with energy E_b as in the forward path. The channel is assumed to be the same in both directions. At \mathcal{V} , white Gaussian noise $w_v(t)$ with power spectral density $\frac{N_0}{2}$ is added and the reply bits \hat{r}_i as well as the delay \hat{d}_i are estimated with a channel matched filter (MF) receiver. As stated before, the constraints on complexity, power consumption and costs are not limiting for \mathcal{V} . Hence, we refer here to standard algorithms for coherent channel and timing estimation and detection [17].

B. Energy Detection Receiver

Due to the stringent requirements on the hardware of \mathcal{P} in terms of complexity, power consumption and costs, we describe the receiver structure of \mathcal{P} in detail in this section. A block diagram of the proposed design of \mathcal{P} is depicted in Fig. 4 and main parameters of the components are summarized in Table I.

The receive signal from the antenna is first amplified by a low-noise amplifier (LNA) with a gain of 20 dB. To model the hardware imperfections of the LNA, a noise figure of 5 dB is assumed for this component. Subsequently, the signal is bandpass filtered by a third order butterworth filter with an attenuation of 5 dB. The automatic gain control (AGC) is essential to allow for a high dynamic range of the receiver, i.e. when \mathcal{P} is close to \mathcal{V} (high receive power), the squaring device must be prevented from strong signal degradation due to non-linear effects and clipping. Hence, the AGC supports a variable gain between 26 and 46 dB, which is automatically adjusted according to the receive power level. The noise figure of the AGC is assumed to be 10 dB. The squaring device attenuates the signal by 5 dB and is modeled with a noise figure of 20 dB. Then, the signal is amplified in a third stage by 20 dB with noise figure 10 dB.

The standard energy detector would assume a running integrator after the squaring device, i.e. a rectangular integration filter. However, due to complexity reasons, here the integration filter is implemented as first order low pass. The impulse response of the first order low pass is given by

$$g(t) = \begin{cases} \frac{g_{LP}}{T_0} \exp\left(-\frac{t}{T_0}\right) & \text{for } t > 0 \\ 0 & \text{else,} \end{cases}$$

with time constant $T_0 = (2\pi f_{LP})^{-1}$ and f_{LP} denoting the low-pass cut-off frequency. The cut-off frequency is chosen to $f_{LP} = 100$ MHz. The voltage gain g_{LP} is modeled such that the attenuation of the low-pass filter is 3 dB.

After low-pass filtering, the signal is in baseband and the components of the detector are not required to support an ultra wide bandwidth. The delay element can be implemented as sample and hold circuit and the threshold device detects the polarity of the difference voltage between delay element and actual output. We assume that the hardware imperfections of the delay element, subtraction and detection of polarity are negligible. An exhaustive study on the power consumption of this energy detector frontend is presented in [6]. The overall noise figure of the energy detector frontend is approximately 5.4 dB.

TABLE I

COMPONENT PARAMETERS OF ENERGY DETECTOR FRONTEND [6]

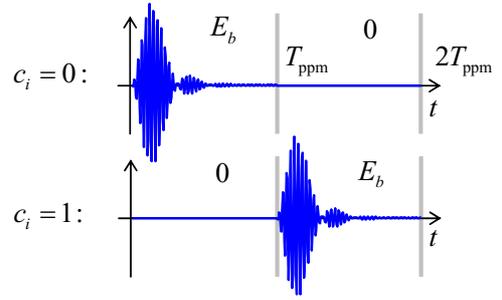
Component	Gain	Noise Figure	Group Delay
LNA	20 dB	5 dB	0.25 ps
Bandpass	-5 dB		1.798 ns
AGC	26-46 dB	10 dB	0.25 ps
Squaring Device	-5 dB	20 dB	320 ps
AMP	20 dB	10 dB	0.25 ps
Low-Pass	-3 dB		1.592 ns

C. Processing Time/ Minimal Delay Receiver

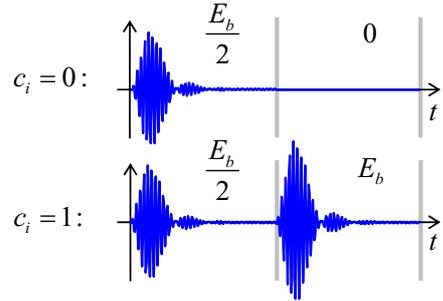
An approximation of the processing time based on an exhaustive literature survey for the proposed prover architecture is given in [18]. The processing time is estimated by the group delay of the components in the receiver chain (see Table I). UWB amplifiers show very small delays in the pico seconds range. Moreover, the squaring device as well as the detector and XOR show negligible delays. However, it is concluded that the group delay of the bandpass filter and the low-pass filter are the main contributions to the processing delay of the receiver. With a group delay of $\tau_{BP} \approx 1.8$ ns for the third order bandpass and $\tau_{LP} \approx 1.6$ ns for the lowpass filter, the processing time of the receiver is approximated to

$$T_{\text{proc}}^{\text{min}} = 3.71 \text{ ns.}$$

Note that this is value is only an approximation or a lower bound of the receiver processing time based on the single components and neglecting the transmitter at \mathcal{P} .



a) Binary Pulse Position Modulation (BPPM)



b) Security Enhanced Modulation (SEM)

Fig. 5. Data modulation for transmission from \mathcal{V} to \mathcal{P} .

D. Security Enhanced Modulation (SEM)

For data transmission from \mathcal{V} to \mathcal{P} , the use of BPPM is advantageous to support the non-coherent receiver structure of \mathcal{P} . In particular, the threshold for data detection must not be adapted and therefore the design requirements of very low complexity and very low power consumption can be met. However, concerning attacks on the distance bounding protocol, the application of BPPM yields also vulnerabilities. As shown in Fig. 5a, the overall duration to transmit a single challenge bit becomes $T_s = 2T_{\text{ppm}}$, i.e. for the chosen system parameters $T_s = 20$ ns. The energy detection receiver at \mathcal{P} waits until the end of the second time slot for the symbol decision.

Due to the inherent structure of the BPPM symbol, the signal can be predicted. If there is no pulse in the first time frame, there will be one transmitted in the second time frame and vice versa. For early detection attacks, this gives an advantage of at least $T_{\text{ppm}} = 10$ ns and in worst case $T_s = 20$ ns. This can lead to a severe accuracy loss of the distance bounding system. As a countermeasure, we propose an improved modulation for the forward path, which leads to a higher accuracy of the distance bounding while keeping the complexity low. As shown in Fig. 5b, Security Enhanced Modulation (SEM) transmits a pulse in the first time slot independent of the transmit symbol. The pulse is scaled by $\frac{1}{\sqrt{2}}$ leading to an energy of $\frac{E_b}{2}$. Then in the second time slot, for $c_i = 0$ nothing is transmitted and for $c_i = 1$ the pulse with energy E_b . This way, the first time slot does not allow to predict the overall signal. Additionally, SEM still enables

non-coherent demodulation and is suited for the proposed low-complexity receiver without any modifications. However, the downside of SEM lies in the increased bit error probability at the receiver. The energy difference of the first and second time slot of SEM is reduced to $\pm \frac{E_b}{2}$, i.e. a factor of $\frac{1}{2}$ compared to BPPM, which leads to a loss of 3 dB in bit error rate performance. Note that this enables an interesting trade-off between range and accuracy of the distance bounding system. Depending on the application requirements, we propose to use BPPM for a larger range and SEM for a system, which aims for higher accuracy. By using SEM the relevant symbol duration is reduced to $T_s = T_{\text{ppm}} = 10$ ns.

IV. FIGURES OF MERIT

In this section, we introduce the *false rejection ratio*, the *false acceptance ratio* and the *effective distance bound* as measures to evaluate the performance of the proposed DB implementation.

The goals of the DB protocol are to estimate the distance between \mathcal{V} and \mathcal{P} , and to decide if \mathcal{V} should authenticate \mathcal{P} . After finishing all three phases of the DB protocol, \mathcal{V} counts the number of the following *security relevant errors (SRE)* in the R protocol rounds:

(i) \mathcal{V} detects a wrong challenge reply in the rapid bit exchange, (ii) \mathcal{V} detects a wrong bit in the challenge retransmission phase, (iii) \mathcal{V} detects both, i.e. a challenge reply bit in the second round is wrong as well as the corresponding bit in the third phase.

In principle, \mathcal{V} could reject \mathcal{P} if one security relevant error is detected in any of the R rounds of the DB protocol. However, such an error may also be caused by the nature of the wireless channel, rather than due to a not legitimate \mathcal{P} . Hence, the DB protocol has to be able to cope with bit errors on the wireless channel – particularly, as there is no channel coding in the rapid bit exchange phase. To achieve this, \mathcal{V} may allow for a certain number of unsuccessful rounds in the DB protocol, i.e. for a certain number N of security relevant errors. In the third phase of the protocol, the challenge retransmission, the communication between \mathcal{V} and \mathcal{P} is not time-critical. Hence, we assume a significantly lower bit error probability $p_{e,r}$ in this phase due to the use of appropriate channel coding.

A. False Rejection Ratio

The *false rejection ratio (FRR)* is given by the probability p_{FR} that a legitimate prover \mathcal{P} will not gain access, although he answered all challenges correctly as defined by the DB protocol, and he is not further from \mathcal{V} than d_{max} . The FRR depends on the bit error probability and on the number N of tolerated security relevant errors. In the following, we assume that the round trip time is determined correctly, i.e. the distance measurement is perfect.

We denote the probability of a bit error on the forward transmission path with $p_{e,f}$ and a bit error on the backward path with $p_{e,b}$. We assume that these two bit error events are independent of each other and independent of an error in the challenge retransmission phase. The probability p_e of an SRE

event during the rapid bit exchange due to a bit error on either way is given by:

$$p_e = p_{e,f} + (1 - p_{e,f})p_{e,b}$$

Note that because of the challenge retransmission phase any error in forward direction leads to a security relevant error. The FRR of a legitimate \mathcal{P} is given by the probability:

$$p_{\text{FR}} = 1 - (1 - p_{e,r}) \sum_{i=0}^N \binom{R}{i} p_e^i \cdot (1 - p_e)^{R-i}$$

Accepting no security relevant error ($N = 0$) and using the assumption that $p_{e,r}$ can be made arbitrarily small by channel coding, this equals to

$$p_{\text{FR}} = (1 - p_e)^R.$$

B. False Acceptance Ratio

The *false acceptance ratio (FAR)* is given by the probability p_{FA} that an attacker \mathcal{A} is able to gain access; it depends on the attacker strategy and on the number N of tolerated SREs. We investigate the standard attacks on DB: Mafia frauds and distance frauds. To derive the FAR, we start with the case that an attacker inside the secure range d_{max} establishes a wormhole to an authorized \mathcal{P} outside the secure range (cf. Fig. 1). As the proposed DB protocol protects reliably against standard wormhole attacks, \mathcal{A} has to use guessing strategies. We start with two of these strategies. The distance fraud case of a malicious prover \mathcal{P}_m outside the secure range will be considered afterwards.

For convenience, we define the following Bernoulli random variables:

$$\begin{aligned} VA &= \begin{cases} 1 & \text{“Bit error occurred on the path } \mathcal{V} \text{ to } \mathcal{A}.” \\ 0 & \text{“No bit error on the path } \mathcal{V} \text{ to } \mathcal{A}.”} \\ AV &= \begin{cases} 1 & \text{“Bit error occurred on the path } \mathcal{A} \text{ to } \mathcal{V}.” \\ 0 & \text{“No bit error on the path } \mathcal{A} \text{ to } \mathcal{V}.”} \\ AP &= \begin{cases} 1 & \text{“Bit error occurred on the path } \mathcal{A} \text{ to } \mathcal{P}.” \\ 0 & \text{“No bit error on the path } \mathcal{A} \text{ to } \mathcal{P}.”} \\ PA &= \begin{cases} 1 & \text{“Bit error occurred on the path } \mathcal{P} \text{ to } \mathcal{A}.” \\ 0 & \text{“No bit error on the path } \mathcal{P} \text{ to } \mathcal{A}.”} \end{cases} \end{cases} \end{aligned}$$

For the probability of $P[X = k]$ we will use the shorthand notation $p_X(k)$. Note that all these probabilities need not to be the same as the ones for a legitimate prover, since the attacker does not need to comply with FCC regulation and may use a more complex system design.

a) *Strategy A - Guessing of Replies:* The probability of guessing the right response bit in one round is given by $p_{\text{guess}} = 1 - p_{\text{guess}} = \frac{1}{2}$. Hence, the probability $p_{\text{fake,A}}$, that \mathcal{A} is able to give a correct answer in one rapid bit exchange, is

$$\begin{aligned} p_{\text{fake,A}} &= p_{\text{guess}} p_{AV}(0) + (1 - p_{\text{guess}}) p_{AV}(1) \\ &= p_{\text{guess}} p_{AV}(0) + p_{\text{guess}} p_{AV}(1) \\ &= p_{\text{guess}} (p_{AV}(0) + p_{AV}(1)) = p_{\text{guess}}. \end{aligned}$$

The probability $p_{\text{fake},A}$ does not depend on the bit error probability of the path \mathcal{V} to \mathcal{A} . Knowing the correct challenge bit does not provide any advantage for the attacker's guessing. For the same reason a bit error on the path \mathcal{A} to \mathcal{V} does not have impact on the guessing.

However, \mathcal{A} must ensure that the challenge will arrive correctly at the legitimate prover, otherwise the attack could be detected in the challenge retransmission phase. The probability to achieve this goal is given by:

$$p_{\text{chall},A} = p_{VA}(0)p_{AP}(0) + p_{VA}(1)p_{AP}(1)$$

The attacker's probability to cause no SRE for a given round of the DB protocol is therefore:

$$p_{\text{succ},A} = p_{\text{fake},A} \cdot p_{\text{chall},A} = p_{\text{guess}} \cdot p_{\text{chall},A}$$

The path \mathcal{P} to \mathcal{A} is irrelevant for the rapid bit exchange, since the replies of \mathcal{P} arrive too late at \mathcal{A} to be delivered timely to the verifier \mathcal{V} .

With the previously defined N and R the false acceptance ratio of Strategy A is given by the probability:

$$p_{\text{FA},A} = (1 - p_{e,r}) \sum_{i=0}^N \binom{R}{i} (1 - p_{\text{succ},A})^i p_{\text{succ},A}^{R-i} \quad (4)$$

Allowing no SRE ($N = 0$) leads to:

$$p_{\text{FA},A} = (1 - p_{e,r}) p_{\text{succ},A}^R$$

If we further assume perfect challenge retransmission $p_{e,r} \approx 0$ and that a sophisticated attacker is able to minimize the BER on all channels, this will yield as expected:

$$p_{\text{FA},A} = p_{\text{guess}}^R \quad (5)$$

b) Strategy B - Guessing of Challenges: This is a verifier impersonating attack. The attacker \mathcal{A} tries to guess the challenges rather than the correct replies with the intention that the correct answer of \mathcal{P} will arrive through the wormhole early enough for him to reply to \mathcal{V} . We will assume in the following that the reply will always arrive early enough. With a similar reasoning as above we can compute the probability to cause no SRE in a given rapid bit exchange round as:

$$p_{\text{succ},B} = p_{\text{fake},B} \cdot p_{\text{chall},B}$$

The latter term describes the probability to find a correct challenge bit in the retransmission and equals

$$p_{\text{chall},B} = p_{\text{guess}} p_{AP}(0) + (1 - p_{\text{guess}}) p_{AP}(1).$$

Using $1 - p_{\text{guess}} = p_{\text{guess}}$ we can simplify this to

$$p_{\text{chall},B} = p_{\text{guess}}.$$

In order to get a correct challenge retransmission, the channel \mathcal{V} to \mathcal{A} is of no importance, since the attacker has to guess the right challenges *before* he receives the actual challenges from the verifier. However, this channel is relevant for the probability to reply correctly in the corresponding rapid bit

exchange round. The probability $p_{\text{fake},B}$ to reply correct in the respective round is given by:

$$p_{\text{fake},B} = p_{VA}(0) (p_{PA}(0) p_{AV}(0) + p_{PA}(1) p_{AV}(1)) \\ + p_{VA}(1) (p_{PA}(1) p_{AV}(0) + p_{PA}(0) p_{AV}(1))$$

Hence, the false acceptance ratio of Strategy B is given by

$$p_{\text{FA},B} = (1 - p_{e,r}) \sum_{i=0}^N \binom{R}{i} (1 - p_{\text{succ},B})^i p_{\text{succ},B}^{R-i},$$

which is in general different from equation (4). However, with $N = 0$, $p_{e,r} \approx 0$ and the assumption that the attacker will be able to lower the BER on all channels to approximately zero, this simplifies to

$$p_{\text{FA},B} = p_{\text{guess}}^R.$$

c) Access Request by a Distant Prover \mathcal{P}_m : This distance fraud scenario is different from the previously discussed wormhole-attacks. Because the malicious prover \mathcal{P}_m is outside the secure range, he has to guess the challenge bits and reply preemptively. Again, we denote the probability of a bit error on the forward transmission path \mathcal{V} to \mathcal{P}_m by $p_{e,f}$ and analogous on the backward path \mathcal{P}_m to \mathcal{V} by $p_{e,b}$. Furthermore, we assume that these two bit error probabilities are independent of each other. The probability of causing no SRE in one given round of the rapid bit exchange phase is given by:

$$p_{\text{succ},\text{mal}} = (p_{\text{guess}}(1 - p_{e,b}) + (1 - p_{\text{guess}})p_{e,b}) \cdot (1 - p_{e,f}) \\ = p_{\text{guess}}(1 - p_{e,f})$$

Consequently the false acceptance probability for this scenario amounts to

$$p_{\text{FA},\text{mal}} = (1 - p_{e,r}) \sum_{i=0}^N \binom{R}{i} (1 - p_{\text{succ},\text{mal}})^i p_{\text{succ},\text{mal}}^{R-i}.$$

With $N = 0$, $p_{e,r} \approx 0$ this leads to

$$p_{\text{FA},\text{mal}} = (p_{\text{guess}}(1 - p_{e,f}))^R,$$

which is different from the case of wormhole attackers. In case the prover \mathcal{P}_m uses the regular hardware, he cannot enhance the BER. Therefore, for an advanced attacker using better hardware, the false acceptance probability will be higher than for a malicious prover with regular transceiver.

C. Effective Distance Bound

An important performance criterion is the effective distance bound that the proposed DB protocol can provide. However, if an attack on the protocol is successful, there will not be any guaranty for a distance bound. If the attacker has replied preemptively, he could reside far outside the distance bound without being noticed. The distance bound is therefore given only with the probability $1 - p_{\text{FA}}$.

In case of a low false acceptance probability, the distance bound can be considered as reliable. Preemptive replies (guessing attacks) are not an option for an attacker. In this case, the worst case scenario is given by a certain distance fraud attack of an adversary knowing the secret but still residing

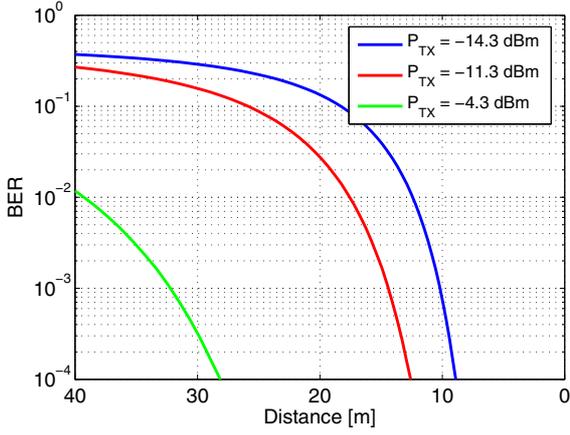


Fig. 6. Bit error ratio BER vs. distance between \mathcal{V} and \mathcal{P} , parameter is the FCC compliant transmit power P_{TX} (BPPM).

outside the secure distance d_{max} : The malicious prover \mathcal{P}_m is able to minimize the processing time T_{proc} and uses early detection/late commits as described in section II-C. The upper bound on the distance d between \mathcal{V} and \mathcal{P}_m according to (1) is still valid (with probability $1 - p_{\text{FA}}$). The effective distance bound is determined by the maximal distance advantage given in (3) and depends on T_{max} , and therefore on the prover delay T_p , which is achievable with the chosen implementation of the DB protocol.

V. PERFORMANCE ANALYSIS

A. BER, FRR and FAR

Fig. 6 shows the BER vs. distance between \mathcal{V} and \mathcal{P} for an AWGN channel and BPPM. An AWGN channel with a free space path loss model has been chosen to model a typical line-of-sight scenario with a dominant direct path; an example could be a badge legitimating to open a door. The plots are parameterized by three different values of the transmit power P_{TX} , all compliant to the FCC rules. We conclude that for distances up to about 15m the UWB IR system shows acceptable performance at very low transmit power.

The false rejection and false acceptance probabilities for $R = 20$ rounds of the DB protocol and $N = 0$ (no SRE tolerated) are shown in Fig. 7. Here, the transmit power was chosen to $P_{\text{TX}} = -14.3$ dBm. By exploiting the low duty cycle operation of the considered application, even $P_{\text{TX}} = 0$ dBm would meet the FCC regulations [18].

As an example we consider a secure range of $d_{\text{max}} = 10$ m. For this distance the FRR is about 10^{-2} (even for the considered very low transmit power) and the FAR according to (5) as well as the FAR of a malicious prover are below 10^{-6} . Tolerating one SRE ($N = 1$) leads to a significantly lower FRR (about 10^{-4}), while the FAR increases to about $2 \cdot 10^{-5}$.

B. Effective Distance Bound

We consider the following scenario: The goal of the DB protocol is to provide a secure range of $d_{\text{max}} = 10$ m. Hence,

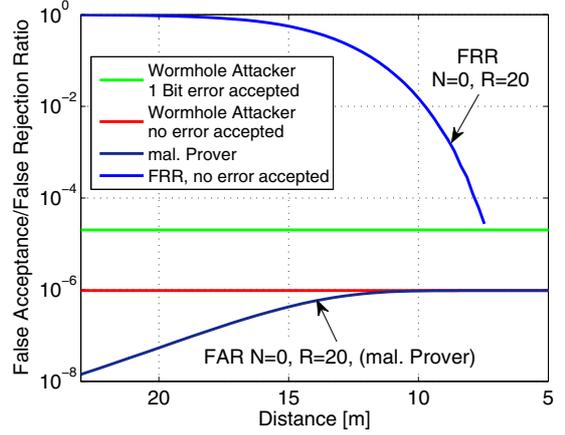


Fig. 7. False rejection/false acceptance probabilities vs. distance \mathcal{V} to \mathcal{P} for $P_{\text{TX}} = -14.3$ dBm (BPPM) and $R = 20$.

the maximal propagation time from the verifier \mathcal{V} to the prover \mathcal{P} and back is given by $T_{\text{prop}}^{\text{max}} \approx 66.67$ ns. The processing time is considered to be $T_{\text{proc}}^{\text{min}} \approx 4$ ns. On the forward path a BPPM transmission scheme with symbol time $T_{\text{S},f} = 20$ ns is used, whereas on the backward path a BPSK transmission scheme with symbol time $T_{\text{S},b} = 10$ ns shall be employed. Therefore the verifier will grant access if his measured round trip time fulfills:

$$T \leq T_{\text{prop}}^{\text{max}} + T_{\text{S},f} + T_{\text{S},b} + T_{\text{proc}}^{\text{min}} = 100.67 \text{ ns}$$

Relay or Wormhole attack: In a relay attack, the attacker is simply forwarding the challenges from \mathcal{V} to a distant \mathcal{P} further away than d_{max} as described in Section I. Even a perfect attacker, who forwards the original signals without any additional delay, will not be able to speed up the messages sent, and consequently fails to provide \mathcal{P} 's replies within the maximum round-trip-time.

Malicious Prover attack or Distance fraud: A powerful malicious \mathcal{P}_m might be able to reply to the challenges with zero processing delay by using superior hardware as discussed in Section II. This would allow the attacker to reply $T_{\text{proc}}^{\text{min}} \approx 4$ ns earlier, allowing him to correctly reply from a distance up to $d_a = 0.6$ m outside the secure range and still gain access.

Malicious Prover attack or Distance fraud with ideal transceiver: This attacker model extends the previous model by allowing the attacker to demodulate signals immediately after receiving a first fraction of the symbol (ideal early detection), and to allow the attacker to commit at the latest possible time to the value of a symbol (ideal late commit). If BPPM is used on the path from \mathcal{V} to \mathcal{P} , this can yield an advantage up to $T_{\text{S},f} = 20$ ns on the forward path and accordingly up to $T_{\text{S},b} = 10$ ns on the backward path. Considering the zero processing delay, a malicious \mathcal{P}_m would consequently be able to gain up to $T_{\text{S},f} + T_{\text{S},b} + T_{\text{proc}}^{\text{min}} = 34$ ns in time. This corresponds to a distance advantage of $d_a = 5.1$ m, which an attacker would be able to decrease the measured range.

If our proposed SEM is used, the influence $T_{\text{S},f}$ is decreased

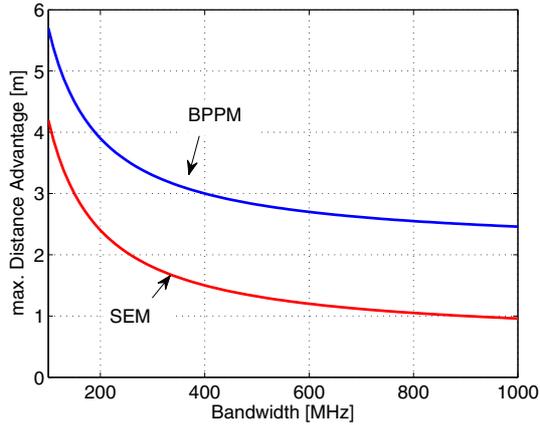


Fig. 8. Maximal distance advantage for malicious prover with ideal transceiver vs. bandwidth B of the UWB pulses; BPPM and SEM.

to 10 ns, reducing the maximum distance advantage to 24 ns or $d_a = 3.6$ m.

We conclude that even using the strongest possible attacker model our system provides a tight enough bound for most applications.

Until now we considered the worst case scenario in which ideal early detection attacks of \mathcal{A} could gain an advantage $2 \cdot T_{\text{ppm}} = 20$ ns of two PPM half frames. In this case, the analog detector of the receiver at \mathcal{P} decides, which bit has been received, after $T_s = 2 \cdot T_{\text{ppm}}$, i.e. after the second PPM half frame. To investigate the influence of the bandwidth of the used pulses, we consider a different scenario: The analog detector of the prover comes to the decision in the second PPM half frame immediately after the pulse duration T_{puls} . Hence, the maximal gain of ideal early detection attacks is $T_{\text{ppm}} + T_{\text{puls}} \leq 2 \cdot T_{\text{ppm}}$ for BPPM and $T_{\text{puls}} \leq T_{\text{ppm}}$ for SEM. For this scenario, Fig. 8 shows how the maximal distance advantage d_a depends on the used bandwidth in case of a malicious prover \mathcal{P}_m using an ideal transceiver. We assume that in the plotted range of bandwidths the processing time $T_{\text{proc}} = 4$ ns does not depend on the bandwidth. For the considered DB system with bandwidth $B = 500$ MHz this leads to a maximal distance advantage of less than 3 m for PPM, less than 1.5 m for SEM, even if the attacker is able to reply with zero processing delay and additionally uses ideal early detection and late commit.

VI. CONCLUSIONS

Due to the high signaling bandwidth and short symbol duration, UWB enables distance measurements with high accuracy. Furthermore, the use of UWB impulse radio allows for minimal delay DB transceiver based on noncoherent receiver structures. This makes UWB impulse radio a perfect candidate for the implementation of distance bounding systems. An energy detection receiver at the prover enables low complexity and low power consumption. We propose to use this in combination with a higher complexity coherent receiver at the verifier to improve the DB performance.

To analyze the performance of the proposed UWB DB implementation, the False Rejection Ratio and False Acceptance Ratio for different attacker models are the major figures of merit of the system. Based on evaluations of the performance of the protocol in typical application scenarios, we conclude that a low FAR is possible for a secure distance of up to 10 m, using a very low transmit power of $P_{\text{TX}} = -14.3$ dBm; this is even low compared to the transmit power allowed according to the FCC regulations. By using Security Enhanced Modulation (SEM) the impact of early detection attacks on the UWB IR distance bounding system can be reduced. Due to the low FAR, the accuracy of the DB system for a worst case attack is given by 3.6 m in case of SEM, or 5.1 m for the BPPM approach of UWB IR.

The presented novel system architecture enables the realization of efficient UWB impulse radio based distance bounding systems with very low power consumption at \mathcal{P} ; it offers efficient protection against wormhole attacks at low costs.

ACKNOWLEDGMENTS

This work was supported by the Zurich Information Security Center and by the Communication Technology Laboratory of ETH Zurich. It represents the views of the authors. The authors thank Armin Wittneben and Srdjan Čapkun for their support and valuable suggestions, as well as Michael Schaub and Felix Schulthess for their excellent work during their student project.

REFERENCES

- [1] S. Brands and D. Chaum, "Distance-bounding protocols," in *Workshop on the theory and application of cryptographic techniques on Advances in cryptology (EUROCRYPT)*. Springer, 1994, pp. 344–359.
- [2] G. P. Hancke and M. G. Kuhn, "An RFID Distance Bounding Protocol," in *Proceedings of the International Conference on Security and Privacy for Emerging Areas in Communications Networks (SecureComm)*. IEEE Computer Society, 2005, pp. 67–73.
- [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 *ESAS, ser. Lecture Notes in Computer Science*, L. Butty, V. D. Gligor, and D. Westhoff, Eds., vol. 4357. Springer, 2006, pp. 83–97.
- [4] S. Gezici, Z. Tian, G. Giannakis, H. Kobayashi, A. Molisch, H. Poor, and Z. Sahinoglu, "Localization via ultra-wideband radios: a look at positioning aspects for future sensor networks," *IEEE Signal Processing Magazine*, vol. 22, no. 4, pp. 70–84, July 2005.
- [5] K. Witrals, G. Leus, G. Janssen, M. Pausini, F. Troesch, T. Zasowski, and J. Romme, "Noncoherent ultra-wideband systems," *IEEE Signal Processing Magazine*, vol. 26, no. 4, pp. 48–66, July 2009.
- [6] F. Troesch, C. Steiner, T. Zasowski, T. Burger, and A. Wittneben, "Hardware aware optimization of an ultra low power UWB communication system," in *IEEE International Conference on Ultra-Wideband, ICUWB 2007*, September 2007, pp. 174–179.
- [7] FCC, "Revision of part 15 of the commission's rules regarding ultra-wideband transmission systems," *First Report and Order, ET Docket 98-153, FCC 02-48*, adopted/released Feb. 14/ Apr. 22 2002.
- [8] C. Steiner, H. Luecken, T. Zasowski, F. Troesch, and A. Wittneben, "Ultra low power UWB modem design: Experimental verification and performance evaluation," *Union Radio Scientifique Internationale, URSI*, Aug. 2008.
- [9] E. Rescorla, *SSL and TLS: Designing and Building Secure Systems*. Addison-Wesley Professional, Oct. 2000.
- [10] L. Bussard and W. Bagga, "Distance-bounding proof of knowledge to avoid real-time attacks," in *Proceedings of SEC*, 2005.
- [11] C. Meadows, R. Poovendran, D. Pavlovic, L. 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*, vol. 30. Springer, 2007.

- [12] P. Papadimitratos, M. Poturlski, P. Schaller, P. Lafourcade, D. Basin, S. Capkun, and J.-P. Hubaux, "Secure neighborhood discovery: A fundamental element for mobile ad hoc networking," *IEEE Communications Magazine*, vol. 40, no. 2, pp. 132–139, February 2008.
- [13] G. Hancke and M. G. Kuhn, "Attacks on 'Time-of-Flight' Distance Bounding Channels," in *Proceedings of the ACM Conference on Wireless Security (WiSeC)*. ACM, 2008.
- [14] T. Zasowski, F. Althaus, M. Staeger, A. Wittneben, and G. Troester, "UWB for noninvasive wireless body area networks: Channel measurements and results," in *IEEE Conference on Ultra Wideband Systems and Technologies, UWBST*, November 2003, pp. 285–289.
- [15] F. Althaus, F. Troesch, T. Zasowski, and A. Wittneben, "STS measurements and characterization," *PULSERS Deliverable D3b6a*, vol. IST-2001-32710 PULSERS, 2005.
- [16] H. Luecken, C. Steiner, and A. Wittneben, "ML timing estimation for generalized UWB-IR energy detection receivers," in *IEEE International Conference on Ultra-Wideband, ICUWB 2009*, Sept. 2009, pp. 829–833.
- [17] J. G. Proakis, *Digital Communications*, 4th ed. McGraw-Hill Higher Education, 2001.
- [18] M. Schaub and F. Schulthess, "UWB impulse radio: Secure ranging and distance bounding," ETH Zurich, Tech. Rep., 2009.