WIRELESS PHYSICAL-LAYER SECURITY PERFORMANCE OF UWB SYSTEMS

A Thesis Presented

by

MIYONG KO

Submitted to the Graduate School of the
University of Massachusetts Amherst in partial fulfillment
of the requirements for the degree of

MASTER OF SCIENCE IN ELECTRICAL AND COMPUTER ENGINEERING

September 2011

Electrical and Computer Engineering

WIRELESS PHYSICAL-LAYER SECURITY PERFORMANCE OF UWB SYSTEMS

A Thesis Presented

by

MIYONG KO

Approved as to style and content by:

Dennis L. Goeckel, Chair

Robert W. Jackson, Member

Patrick A. Kelly, Member

C. V. Hollot , Department Head
Electrical and Computer Engineering

To Jangwon and my family

ABSTRACT

WIRELESS PHYSICAL-LAYER SECURITY PERFORMANCE OF UWB SYSTEMS

SEPTEMBER 2011

MIYONG KO

B.S., SEOUL NATIONAL UNIVERSITY

M.S.E.C.E., UNIVERSITY OF MASSACHUSETTS AMHERST

Directed by: Professor Dennis L. Goeckel

Traditionally, spread-spectrum systems have been employed to provide low probability-of-intercept (LPI) and low probability-of-detection (LPD) performances at the physical layer, but the messages transmitted over such a system are still encrypted with a powerful cipher to protect their secrecy. Our challenge is to find a solution to provide an additional level of security at the physical layer so that simple systems such as RFID tags with limited resources can be secure without using standard encryption. It has recently been suggested that the cryptographic security of the system can be enhanced by exploiting physical properties of UWB signals. With an eavesdropper observing the communications over multipath channels between two legitimate partners sharing a secret key of a limited length, we consider both coherent and reference-based UWB schemes to enhance security. The security of the legitimate nodes is achieved by signal attributes based on the secret key, conferring an advantage over the adversary. We propose UWB signaling schemes to improve physical layer security when the transmission is intended for coherent reception and

TR reception. Among possible improvements, we consider removing the frame structure of the UWB coherent signaling scheme, resulting in pulses that can be located anywhere in the symbol period. Our proposed signaling schemes could potentially suggest a solution for applications relying on conventional cryptography, especially for low-data rate RFID systems.

TABLE OF CONTENTS

LIST OF TABLES

Table **Page**

LIST OF FIGURES

Figure **Page**

CHAPTER 1

INTRODUCTION

Securing the transmission of any message in wireless systems poses challenges since the signal is not physically constrained. In general, encryption for securing such messages is required at the digital layer via some sort of powerful ciphers. However, low-power wireless systems such as radio frequency identification (RFID) systems lack sufficient power and resources to operate powerful encryption algorithms. Thus, it has recently been suggested that some level of cryptographic security of the system can be enhanced at the physical layer by exploiting physical properties of wideband signals [14]. This could prove highly desirable in extremely low-power RFID systems; hence, marrying a lighter-weight cryptographic protocol to an enhancing physical layer is attractive.

In particular, as one way to use characteristics of wideband signals for increased security at the physical layer, consider the case of the transmitter and receiver sharing a common key. This common key could be used to establish the hopping pattern of a frequency-hopped (FH) system or the spreading code in a code-division multiple-access (CDMA) system. However, a frequency-hopped system wherein relatively narrowband signals are hopped across a wide bandwidth consumes considerable power for hopping over the large bandwidth. In a direct-sequence spread-spectrum, on the other hand, signals are significantly shorter in time and wider in frequency. However, like the FH system, the CDMA system is problematic for a low-power system because of the energy expended for a given level of security. Both of these systems are not power efficient for encryption done at the physical layer; thus, they cannot perform as the power-saving solutions for extremely low-

power RFID applications. We hereby advocate an extremely low-power ultra-wideband (UWB) architecture for encryption at the physical layer.

UWB systems must follow strict federal communications commission (FCC) regulations limiting the UWB bandwidth, power spectral density emission and data rates in order to avoid interference with other existing systems. Accordingly, UWB systems have been proven to consume very low power due to power limitations imposed by the FCC. The extremely large bandwidth of UWB signals makes UWB transmissions more resistant to interference than narrow band transmissions. Furthermore, UWB transmission has been widely adopted in recent years because of increasing demand for portable devices providing high data rates at lower power for short range wireless applications. Accordingly, ultra-wideband (UWB) communication systems have attracted considerable attention both because of their extremely low-power architecture, thereby avoiding interference by conventional receivers, and a potentially robust physical layer security as a consequence of their large bandwidth.

In this work we propose signaling models for providing some level of encryption at the physical layer by using an extremely low-power UWB architecture, which can be a lower power solution than traditional encryption algorithms for the same level of security assurance. Then, we investigate the abilities of UWB systems employing a pulse of an ultra-wideband spectrum bandwidth to provide such physical layer cryptographic security. The proposed signaling models are based on a time-hopping (TH) method and binary pulse amplitude modulation. We assume that a randomly generated secret key is shared by two communicating parties, i.e., an RFID tag and a legitimate receiver. This shared key is used to determine the UWB pulse locations. The utility of the proposed UWB signaling models is based on the legitimate receiver's identifying the pulse locations via the secret key, thus conferring an advantage over any adversary lacking any knowledge of the time slots employed to transmit a data bit. Thus, we examine the security performance in terms

of the ability of the legitimate receiver to decode data versus the ability of the eavesdropper to ascertain the key as directed by potential cryptographic protocols [7].

Our proposed thesis work is divided into two research studies. The first part proposes UWB signaling models with the standard frame structure as a means to secure physical transmission. That is, in order to convey symbol bits, there are multiple frames in one symbol period with only one pulse being located in each frame. In this study we consider two receiver implementations in UWB systems: a coherent UWB communication system and a UWB transmitted-reference (TR) noncoherent communication system. In UWB systems, performance, receiver complexity, power consumption and cost are all considered in deciding whether to utilize coherent or noncoherent reception. Coherent UWB systems call for a sophisticated receiver design in order to estimate channel information. Thus, the complexity of coherent UWB communication systems tends to increase in order to achieve robust performance. In general, coherent UWB systems are regarded as superior to noncoherent UWB systems in performance but at the expense of significant receiver complexity. In contrast, noncoherent UWB systems can provide a simpler receiver structure by avoiding the complicated channel estimation inherent in extreme bandwidth. The performance of coherent and noncoherent UWB systems has been analyzed [10, 5]. However, to the best of our knowledge, there have been no studies investigating the ability of UWB systems to support higher-layer cryptographic protocols. In particular, the tradeoffs between security performance and receiver complexity in multipath fading channels have not yet been examined. Therefore, we provide an accurate security performance analysis of the baseline UWB system intended for coherent reception and of the baseline UWB system intended for reference-based reception with both systems using the proposed UWB signaling schemes. We utilize a numerical evaluation to rate the security performance of the legitimate receiver in decoding data versus the adversary to ascertain the key.

The second part of our research explores improving the signaling schemes proposed in the first part. The proposed schemes can be improved in numerous ways. Among them

we consider removal of the frame structure in both the UWB coherent and TR signaling models. For simplicity, we consider only coherent reception. Thus, we propose a UWB signaling model of a frameless structure designed for coherent reception. In general, in a UWB system intended for coherent reception, one symbol is represented by a sequence of pulses with each pulse being located in an interval designated a frame. That is, the typical frame is composed of multiple time slots among which only one pulse is assigned. However, we investigate removing this frame structure so that the multiple pulses representing one bit can be placed anywhere in one symbol period without restriction. We expect that doing so may make it more challenging for the adversary to detect the pulses because of expanded pulse search space. To evaluate this, we investigate the ability of the adversary to detect the pulses correctly when the signal scheme of a frameless structure intended for coherent reception is adopted. Then, we compare performance to that of the UWB coherent signaling scheme with a frame structure previously employed in the first portion of our research. By doing so, we study whether this frameless signaling scheme provides better security performance than the conventional framed signaling scheme.

In this chapter we will first present a brief background helpful to understanding our framework, and then we will summarize our contributions.

1.1 Background

Ultra-wideband (UWB) communication systems have recently received considerable attention in academia and industry for short-range, low-power applications in wireless systems. UWB communications involve the transmission of impulses with a large bandwidth at a low transmission power. This extremely low-power transmission of UWB signals insuring that impulse radio signals do not interfere with already-existing narrowband radio systems has motivated the FCC to allocate a UWB spectrum in the range of 3.1 GHz to 10.6 GHz, some of which is already dedicated to other radios. More specifically, the UWB pulses possess a bandwidth over 500 MHz or exceeding 20% of the system cen-

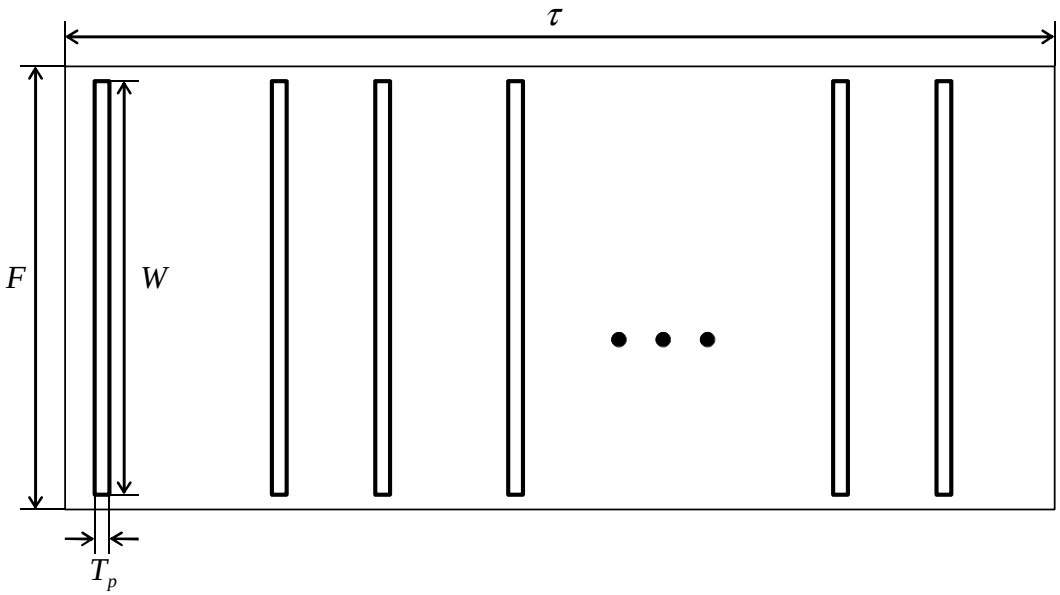

Figure 1.1. Picture of the time (horizontal) and frequency (vertical) space of dimension τ x F with an ultra-wideband time-hopped approach to allocation

ter frequency. Such a large bandwidth offers low probability-of-intercept (LPI) and low probability-of-detection (LPD) in conjunction with the extremely low power spectral density. Each symbol is transmitted at a low duty cycle over a large number of frames with only one pulse per frame in order to concentrate sufficient symbol energy for reliable detection while maintaining very low-power density.

The system of interest exploits a low-power transmitter of ultra-wideband with a large time-bandwidth space to provide the desired cryptographic solution. Consider a time-hopping UWB system employing a pulse with an ultra-wide bandwidth. Assume that the goal of this system is to convey N_b data bits through a large bandwidth of size F in τ seconds. For wideband systems, each data bit is generally conveyed by a sequence of N_p pulses. The pulse of a duration T_p is employed, which has bandwidth given by $W = g/T_p$, where g is slightly larger than one. Thus, each pulse occupies a rectangular tile of size T_p x W in a time x frequency plane. As shown in Fig. 1.1, we employ a pulse spanning the entire band with nominal value of W = 7 GHz. The time space τ has multiple time slots.

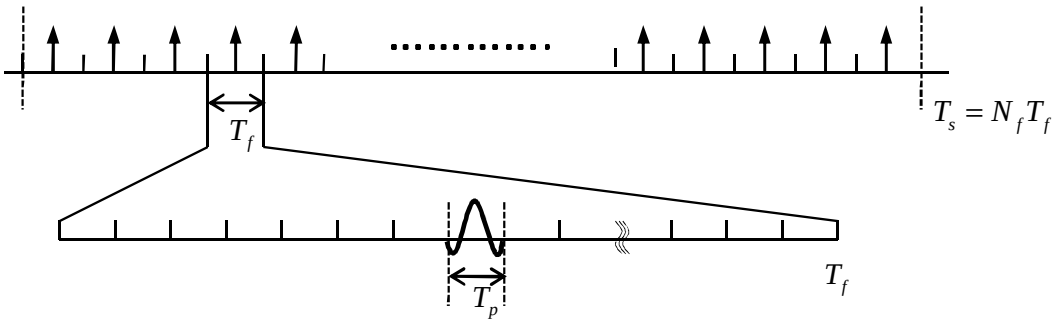

Figure 1.2. Conventional time-hopping UWB signaling scheme

The shared secret key determines which time slots are filled. Obviously, since a UWB pulse signal transmitted at lower power is buried in noise, this makes it difficult for the receiver to extract the signal. However, the intended receiver knows where to look since the receiver knows the sequence of timings employed. This is a linear search using a template to find the correct timing offset of the bit sequence start. When the receiver notes a large energy spike in the output of its template matching, it presumes it has detected the correct timing. However, the challenge for the adversary is greater due to no knowledge of the time slots employed. We assume no limitation on the computational power of the adversary. The adversary is also able to completely sample the bandwidth of the system at all times. Even with this, the adversary has to confront a number of hypothesis testing problems to find the correct $N_b N_p$ transmission slots. This difference between the abilities of the intended receiver and the adversary, thereby rendering some level of encryption at the physical layer, is what we intend to exploit.

For example, assume that a train of UWB pulses to represent one data bit is transmitted in one symbol period with one pulse being located in each frame as shown in Fig. 1.2. The pulse location in each frame is determined by the b-bit secret key shared by the transmitter and the intended receiver. Thus, each pulse in each frame is located at the same time slot designated by the secret key. The intended receiver does not need to run the hypothesis test to determine which time slot has the data pulse. However, the adversary has to perform a

large number of hypothesis tests due to its lacking the secret key. For example, assume that 10-bit secret key is used. In this case, finding the correct time slots is an 2^{10} hypothesis testing problem, which means that the number of hypotheses dramatically escalates. Even if we ignore the computational constraint, the probability of finding the correct sequence of time slots rapidly diminishes to zero.

1.2 Contribution

Our major contributions in this work are as follows:

- Proposing low-power UWB signaling schemes to provide some level of encryption at the physical layer when the transmission of signals is intended for coherent reception and TR reception,
- Suggesting that the UWB TR systems outperform the coherent UWB systems in terms of performance of the desired receiver versus that of the adversary, and
- Proposing a frameless signaling scheme when the transmission is intended for coherent reception to offer enhanced physical layer security.

1.3 Organization

In Chapter 2, we introduce UWB signaling schemes for both the system intended for coherent reception and the TR system. Next, we derive error probabilities of the legitimate receiver and the adversary when the transmission is intended for coherent reception and TR reception. Then, we present numerical evaluation of the physical layer security performance for both systems operating in IEEE 802.15.4a environments. In Chapter 3, we propose a UWB signaling scheme with a frameless structure when the transmission is intended for coherent reception. In addition, we derive the tradeoffs in the security performance of the UWB coherent system employing this frameless signaling scheme and the

UWB coherent system of a framed structure previously proposed in Chapter 2. Finally, in Chapter 4 we summarize our thesis work based on the results from Chapters 2 and 3.

CHAPTER 2

PHYSICAL LAYER SECURITY PERFORMANCE OF BASELINE COHERENT AND TR SIGNALING SCHEMES

In this chapter we propose UWB signaling models to enhance secure transmission by utilizing physical properties of UWB signals. The proposed signaling models are based on a time-hopping (TH) method and binary pulse amplitude modulation. It is assumed that a randomly generated secret key is shared by two communicating parties, i.e., an RFID tag and a legitimate receiver. This shared key is used to determine the UWB pulse locations. We examine the security performance in terms of the ability of the legitimate receiver to decode data versus the ability of the eavesdropper to ascertain the key as motivated by potential cryptographic protocols [7].

We derive the error probabilities of both the legitimate UWB receiver and adversary when the transmission is intended for coherent reception, and then those of the legitimate UWB receiver and adversary when the transmission is intended for reference-based reception. Since the quantities of interest are in integral form, analytical evaluation is very difficult. Accordingly, we present numerical results for systems operating in IEEE 802.15.4a environments [4]. Finally we discuss our proposed schemes as a possible solution for the near-far problem that plagues PHY-based security in the wireless environment and consider ways to further improve security of signal transmission using the UWB schemes.

The proposed scheme may offer a potentially effective solution for applications which rely on conventional cryptography for secure communications. In particular, the proposed UWB signaling schemes can be adapted to a low-data rate RFID system with a simple tag but with a reader of higher complexity, thereby making available possible UWB TR

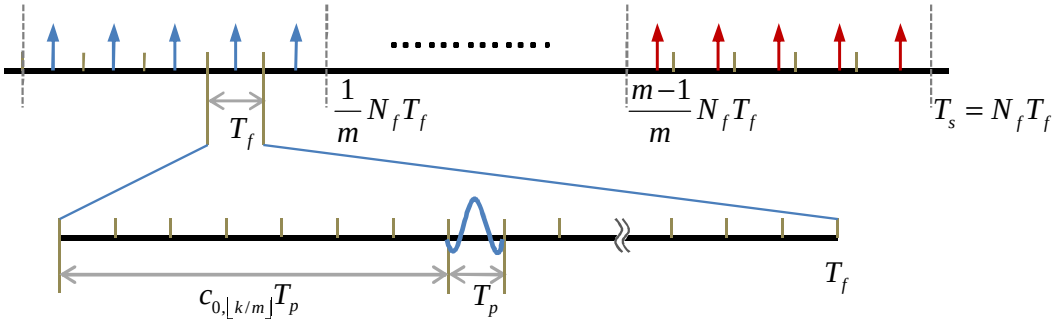

Figure 2.1. UWB signaling scheme intended for coherent reception

approaches and perhaps coherent approaches, both of which would be difficult in low-power integrated circuits [6].

2.1 System Models

Given peak power constraints on UWB hardware, particularly in emerging CMOS technologies with small feature sizes, there will often be a large number of short UWB pulses to convey a data bit [10, 8]. Assume that a randomly generated b-bit secret key K is shared by a transmitter and a legitimate receiver. A single user that employs a TH method and binary pulse amplitude modulation will be assumed throughout this work. Without loss of generality, a signal carrying the first data bit b_0 mapped to $\{-1, 1\}$ with equal probability in the first symbol period is considered.

2.1.1 UWB signaling scheme intended for coherent reception

We employ the b-bit secret key K to position the UWB pulses within the symbol period T_s. In contrast to traditional spread-spectrum systems, we do not employ a shift register with connections determined by the key to produce a longer pseudo-random noise (PN) sequence, since this does not improve the cryptographic strength of the system [12]. Fig. 2.1 illustrates a UWB signaling scheme intended for coherent detection. Ideally, each pulse would be independently located using key bits, but keys are generally not long enough to support such. Hence, we divide the b-bit shared key K into m parts $K = (\kappa_1, \kappa_2, ..., \kappa_m)$

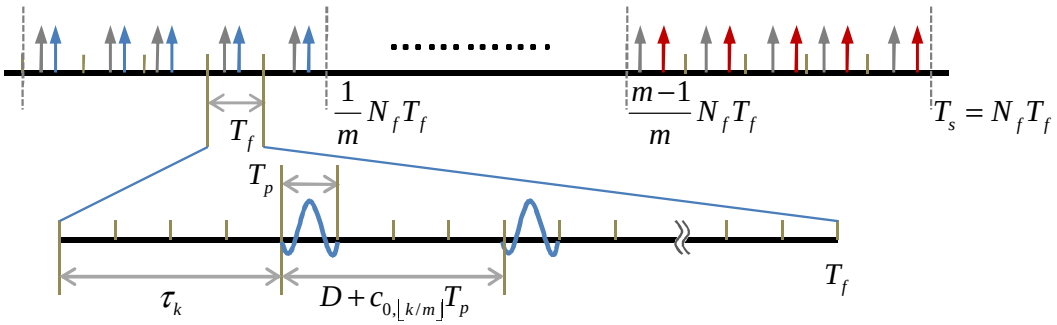

Figure 2.2. UWB signaling scheme intended for TR reception

to utilize the limited key bits, and each κ_i consisting of b/m bits, $i \in \{1, 2, ..., m\}$, is used to select a position index in $\{0, 1, ..., \ 2^{b/m} - 1\}$ that is shared by the pulses in the corresponding N_f/m frames.

More formally, a transmitted signal $s_0(t)$ carrying the first information bit b_0 over the first symbol period as shown in Fig. 2.1 is considered, and the signal transmitted by a single user can be expressed by:

$$s_0(t) = \sum_{k=0}^{N_f-1} (-1)^{b_0} \sqrt{E_p}\, p(t - kT_f - c_{0,\lfloor k/m \rfloor} T_p), \tag{2.1}$$

where $p(\cdot)$ is a normalized standard UWB pulse of approximate duration T_p and $\int_{-\infty}^{+\infty} |p(t)|^2 dt = 1$. The transmission energy of each pulse is $E_p = E_s/N_f$ where E_s is the symbol energy and N_f is the number of frames in one symbol period. The symbol period $T_s = N_f T_f$, T_f is the frame period, and $\{c_{0,\lfloor k/m \rfloor}\}_{k=1}^{N_f-1}$ is the TH sequence. Specifically, the TH code element $c_{0,\lfloor k/m \rfloor} \in \{0, 1, ..., \ 2^{b/m} - 1\}$ for positioning the UWB pulse in the kth frame is determined by the b/m key bits $\kappa_{\lfloor k/m \rfloor + 1}$. Hence, the pulse location in frames $0, 1, ..., \ m - 1$ is determined by κ_1, the pulse location in frames $m, m + 1, ..., \ 2m - 1$ is determined by κ_2, etc.

2.1.2 UWB TR signaling scheme

Fig. 2.2 illustrates the UWB TR signaling scheme, where each frame consists of two pulses: a reference pulse and a data pulse. A transmitted signal $s_{0,tr}(t)$ of a UWB TR system over the first symbol interval can be written as:

$$s_{0,tr}(t) = \sum_{k=0}^{N_f-1} (\sqrt{E_s/2}\, p(t - kT_f - \tau_k) + (-1)^{b_0} \sqrt{E_s/2}\, p(t - kT_f - \tau_k - D - c_{0,\lfloor k/m \rfloor} T_p)), \quad (2.2)$$

where the previous parameters specified in (2.1) hold in (2.2). In frame k, the reference pulse is transmitted first and the data pulse follows with a delay $D + c_{0,\lfloor k/m \rfloor} T_p$. Thus, unlike the UWB signaling scheme for coherent reception shown in Fig. 2.1, the key bits κ_i are used to determine not the data pulse locations but rather the time delay $c_{0,\lfloor k/m \rfloor} T_p$ between the reference pulse and the data pulse. Thus, the time delay $c_{0,\lfloor k/m \rfloor} T_p$ in each group of N_f/m frames remains invariant. The fixed time delay D, $D > \tau_{max}$, is employed to prevent inter-pulse interference between the reference pulse and the data pulse after passing through the channel, where τ_{max} is the maximum delay spread of the channel. The variable τ_k indicates the starting time of the reference pulse in the *k*th frame, which varies in a true random manner in the proposed UWB TR signaling scheme. For example, although a time separation $c_{0,0} T_p$ between the reference and data pulses determined by the first key bits κ_1 is constant in the first N_f/m frames, the actual location in *each* frame will vary according to the random offsets. These random offsets keep the UWB TR adversary from detecting the transmitted signal coherently by using the reference pulse to estimate channel information. Note that a transmitter can generate this true random location with extremely low-power circuitry (0.57 pJ/bit) [11], and that a TR receiver does not require knowledge of the offset τ_k (and, hence, these random bits) to decode the signal.

2.2 Performance of Systems Intended for Coherent Reception

Consider the transmission of the signal $s_0(t)$ over a frequency-selective multipath channel appropriate for the wireless UWB system. The channel impulse response will be given by a standard discrete-path model as:

$$h(t) = \sum_{l=0}^{L-1} h_l \delta(t - \tau_l), \tag{2.3}$$

where h_l denotes the attenuation factor, τ_l is the time delay associated with the *l*th propagation path, and L is the number of multipath components. Assume that the channel is time-invariant over one symbol period so that all of the pulses in a symbol period will go through the same channel.

The received signal can be expressed as:

$$r_0(t) = h(t) * s_0(t) + n(t) \tag{2.4}$$

where $n(t)$ is a zero-mean white Gaussian noise with two-sided power spectral density $N_0/2$.

2.2.1 Legitimate receiver

Since precise timing is required by the legitimate receiver, we will assume that beacons have allowed for timing and channel estimation for both the legitimate UWB receiver and adversary. A template signal perfectly matched to the pulse sequence of the received signal in the first symbol period is given by:

$$s_{temp}(t) = \frac{1}{\sqrt{N_f}} \sum_{j=0}^{N_f-1} p(t - jT_f - c_{0,\lfloor j/m \rfloor} T_p). \tag{2.5}$$

Assuming a maximal ratio combining approach, the decision statistic after combining the outputs of the correlators can be written as:

$$\begin{aligned} y_0 &= \sum_{l=0}^{L-1} h_l \int_0^{T_s} r_0(t)\ s_{temp}(t-\tau_l)\ dt \\ &= \sum_{l=0}^{L-1} h_l \int_0^{T_s} (h(t) * s_0(t))\ s_{temp}(t-\tau_l)\ dt + n_0, \end{aligned} \tag{2.6}$$

where $n_0 = \sum_{l=0}^{L-1} h_l \int_0^{T_s} n(t) s_{temp}(t-\tau_l) dt$ is Gaussian-distributed with zero mean and variance $\frac{N_0}{2} \sum_{l=0}^{L-1} {h_l}^2$. Thus, the decoding error probability for the legitimate receiver with knowledge of the data pulse locations when conditioned on $\{h_l\}_{l=0}^{L-1}$ is given in [2] by:

$$P_{e,\,rcv} = E_{\underline{h_l}} \left[Q\left(\sqrt{\frac{2E_s \sum_{l=0}^{L-1} h_l^2}{N_0}} \right) \right]. \tag{2.7}$$

2.2.2 Adversary

Since a UWB signal at a low power level is buried in noise, finding the information data pulse can be very challenging without knowledge of the pulse locations. In order to provide a lower bound on security performance, we consider the worst case scenario to the legitimate receiver where the adversary knows the transmitted bit. This might occur, for example, if the adversary is able to exploit some sort of packet structure. More formally, consider the first N_f/m frames, where data pulses are located at the identical time slot in each frame, and thus a template signal when the pulse is in the time slot i is given by:

$$s_{temp,i}(t) = (-1)^{b_0} \frac{1}{\sqrt{N_f}} \sum_{j=0}^{N_f/m-1} p(t - jT_f - \tilde{c}_{0,i} T_p), \tag{2.8}$$

where $i \in \{0, 1, ...,\ 2^{b/m} - 1\}$. Assuming the adversary uses the maximal ratio combining technique, the decision statistic after combining the outputs of the correlators for the first N_f/m frames is given by:

$$y_{0,i} = \sum_{l=0}^{L-1} h_l \int_0^{N_f T_f/m} r_0(t)\ s_{temp,i}(t-\tau_l)\ dt$$
$$= \sum_{l=0}^{L-1} h_l \int_0^{N_f T_f/m} (h(t) * s_0(t))\ s_{temp,i}(t-\tau_l)\ dt + n_{0,i}, \tag{2.9}$$

where $n_{0,i} = \sum_{l=0}^{L-1} h_l \int_0^{N_f T_f/m} n(t) s_{temp,i}(t-\tau_l) dt$ is Gaussian-distributed with zero mean and variance $\frac{N_0}{2} \sum_{l=0}^{L-1} {h_l}^2$. The adversary has to confront a large number of hypotheses, since there is only one data pulse but many empty slots in each frame due to the extreme bandwidth expansion. We assume the adversary employs the template at various delays, and picks the output with the largest value. The adversary with the assumed knowledge of the channel could instead perform a sophisticated hypothesis test, but our main conclusion is based on the adversary performing well in the coherent case, and thus a lower bound to the adversary performance suffices.

Noting

$$y_{0,c_{0,0}} \sim N(\mu_0, \sigma^2)$$
$$\text{and} \qquad y_{0,i} \sim N(\mu_i, \sigma^2), \qquad i \neq c_{0,0},$$

where

$$\mu_0 = \frac{E_s}{m} \sum_{l=0}^{L-1} h_l^2$$

$$\mu_i = \begin{cases} \frac{E_s}{m} \displaystyle\sum_{l=0}^{L-|i-c_{0,0}|-1} h_l h_{l+|i-c_{0,0}|}, & c_{0,0} - L < i < c_{0,0} + L, \\ 0, & \text{otherwise} \end{cases}$$

and

$$\sigma^2 = \frac{N_0}{2} \sum_{l=0}^{L-1} h_l^2,$$

the probability of finding the correct pulse position in the first N_f/m frames conditioned upon $\{h_l\}_{l=0}^{L-1}$ is easily extended from the coherent reception of orthogonal signals [9]:

$$
\begin{aligned}
&P_{c,\,adv,\,0|\underline{h_l}} \\
&= P(y_{0,i} < y_{0,c_{0,0}}, \forall i \neq c_{0,0} | \underline{h_l}) \\
&= \int_{-\infty}^{\infty} \prod_{i=0, i\neq c_{0,0}}^{2^{b/m}-1} \left(1 - Q\left(\frac{r-\mu_i}{\sigma}\right)\right) \cdot \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(r-\mu_0)^2}{2\sigma^2}}\, dr.
\end{aligned} \tag{2.10}
$$

Since the TH codes for each group of N_f/m frames are independently assigned by each of $\kappa_1, \kappa_2, ..., \kappa_m$, the probability of error of the adversary for finding the entire key is obtained by averaging over the channel realization:

$$
P_{e,\,adv} = 1 - E_{\underline{h_l}}\left[(P_{c,\,adv,\,0|\underline{h_l}})^m\right]. \tag{2.11}
$$

Note that partial keys also yield some utility to the adversary, since they weaken the system security if key refresh schemes are not employed, but we adopt the probability of obtaining the whole key since partial key capture can be combatted at higher layers.

2.3 Performance of TR Systems

For performance analysis, assume the channel is constant over the symbol period, although we hasten to note that the system functions well if the channel is constant only over the frame duration so that the reference pulse in each frame goes through the same channel as the data pulse. The maximum delay spread of the channel τ_{max} is assumed to be smaller than the minimal separation D in order to avoid interference between the reference and data pulses, and T_f is assumed large enough to assure no inter-frame interference. Note that these assumptions are easily satisfied in the relatively low-data rate RFID applications envisioned.

The received signal passes through a noise-limiting low-pass filter with sufficiently wide bandwidth W at the front end of the receiver. The filtered received signal is given by:

$$
\tilde{r}_{0,tr}(t) = h(t) * s_{0,tr}(t) + \tilde{n}(t), \tag{2.12}
$$

where $\tilde{r}_{0,tr}(t)$ is $r_{0,tr}(t)$ filtered by the low-pass filter, $\tilde{n}(t)$ is a zero-mean Gaussian noise with power spectral density $S_n(f) = |H(f)|^2 \frac{N_0}{2}$, and $H(f)$ is the frequency response of the filter.

2.3.1 Legitimate receiver

Knowing the sequence $(c_{0,0}, c_{0,1}, ...)$ indicating the separations between the reference pulses and the data pulses, the legitimate UWB TR receiver correlates the filtered received signal $\tilde{r}_{0,tr}(t)$ with its delayed version $\tilde{r}_{0,tr}(t - D - c_{0,\lfloor k/m \rfloor} T_p)$ in the kth frame and sums over all frames; that is, the integrator output corresponding to the first symbol period is given by:

$$y_0 = \sum_{k=0}^{N_f - 1} \int_{kT_f}^{(k+1)T_f} \tilde{r}_{0,tr}(t)\ \tilde{r}_{0,tr}(t - D - c_{0,\lfloor k/m \rfloor} T_p)\ dt. \tag{2.13}$$

The error probability of the legitimate UWB TR receiver conditioned upon $\{h_l\}_{l=0}^{L-1}$ according to the Gaussian approximation can be derived in [6] and thus the decoding error probability of the legitimate UWB TR receiver when averaged over the multipath channel becomes:

$$P_{e,\,TR-rcv} = E_{\underline{h_l}} \left[Q \left(\frac{E_s \sum_{l=0}^{L-1} h_l^2}{\sqrt{4E_s N_0 \sum_{l=0}^{L-1} h_l^2 + 2T_s N_0^2 W}} \right) \right]. \tag{2.14}$$

Note that this receiver obtains this performance without requiring knowledge of the random offsets τ_k.

2.3.2 Adversary

We assume that the true random τ_k offsets keep the adversary from doing channel estimation based on methods such as template averaging [2]. Thus, the UWB TR adversary, lacking knowledge of the delay $D + c_{0,\lfloor k/m \rfloor} T_p$ between the reference and data pulses but with knowledge of the data bit b_0, correlates the filtered received signal $\tilde{r}_{0,tr}(t)$ with the

delayed version $(-1)^{b_0}\tilde{r}_{0,tr}(t - D - iT_p)$ for $i = 0, 1, ..., \ 2^{k/m} - 1$, and for each i, sums all of the correlation outputs corresponding to N_f/m pulses. The integrator output $y_{0,i}$ for the first N_f/m frames follows as:

$$y_{0,i} = (-1)^{b_0} \sum_{k=0}^{N_f/m-1} \int_{kT_f}^{(k+1)T_f} \tilde{r}_{0,tr}(t) \ \tilde{r}_{0,tr}(t - D - iT_p) \ dt. \tag{2.15}$$

The decision statistic $y_{0,i}$ can be approximated as a Gaussian random variable as suggested in [6, 1]. The adversary selects the index of the delay corresponding to the largest correlator output. As in the coherent case, a more sophisticated hypothesis test could be performed, but, in the TR case, this is further complicated and gains limited because of the lack of knowledge of the channel.

Noting

$$\begin{aligned} & y_{0,c_{0,0}} \sim N(\mu_0, \sigma^2) \\ \text{and} \qquad & y_{0,i} \sim N(\mu_i, \sigma^2), \qquad i \neq c_{0,0}, \end{aligned}$$

where

$$\mu_0 = \frac{E_s}{2m} \sum_{l=0}^{L-1} h_l^2$$

$$\mu_i = \begin{cases} \frac{E_s}{2m} \displaystyle\sum_{l=0}^{L-|i-c_{0,0}|-1} h_l h_{l+|i-c_{0,0}|}, & c_{0,0} - L < i < c_{0,0} + L, \\ 0, & \text{otherwise} \end{cases}$$

and

$$\sigma^2 = \frac{E_s N_0}{m} \sum_{l=0}^{L-1} h_l^2 + \frac{T_s {N_0}^2 W}{2},$$

the probability for finding the separation employed by the TR system in the first group of N_f/m frames is found in an analogous fashion to (2.10):

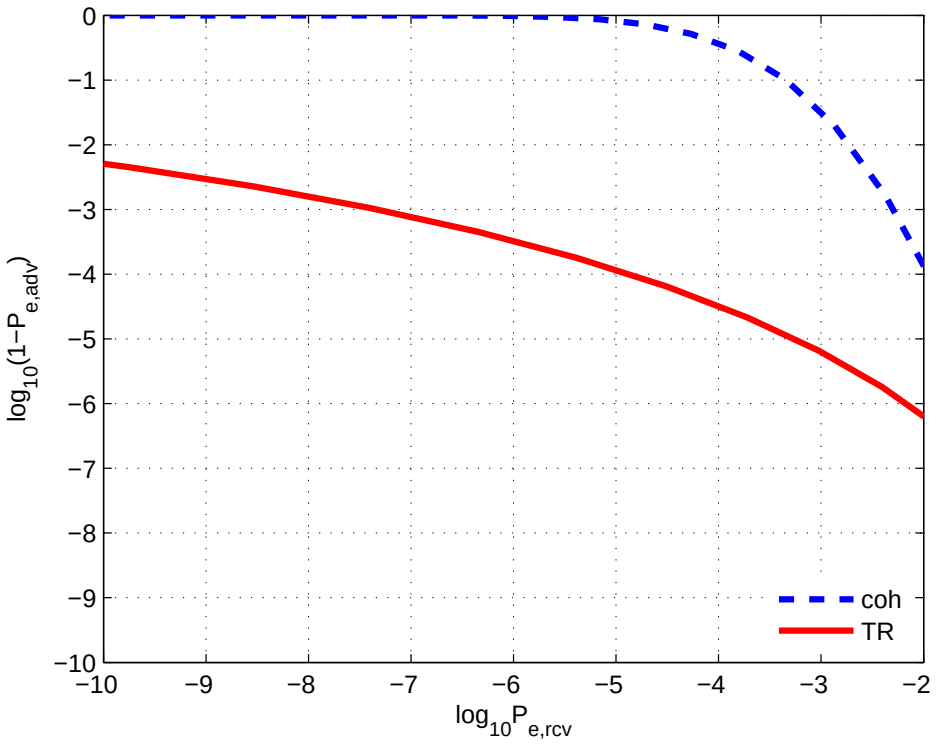

Figure 2.3. Comparison of security of UWB system intended for coherent reception and TR system in IEEE 802.15.4a LOS office environments. The x-axis denotes in log scale the error probability of the legitimate receivers in decoding the data bit while the y-axis denotes in log scale the probability of the adversaries correctly determining the key. At the same error probability for the legitimate receivers, the adversary in the coherent reception case is more effective.

$$P_{c,\,TR-adv,\,0|\underline{h}} = \int_{-\infty}^{\infty} \prod_{i=0, i\neq c_{0,0}}^{2^{b/m}-1} \left(1 - Q\left(\frac{r-\mu_i}{\sigma}\right)\right) \cdot \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(r-\mu_0)^2}{2\sigma^2}}\, dr. \tag{2.16}$$

Thus, the probability of the TR adversary not being able to determine the key over multipath channels is:

$$P_{e,\,TR-adv} = 1 - E_{\underline{h_l}}\left[\left(P_{c,\,tr-adv,\,0|\underline{h_l}}\right)^m\right]. \tag{2.17}$$

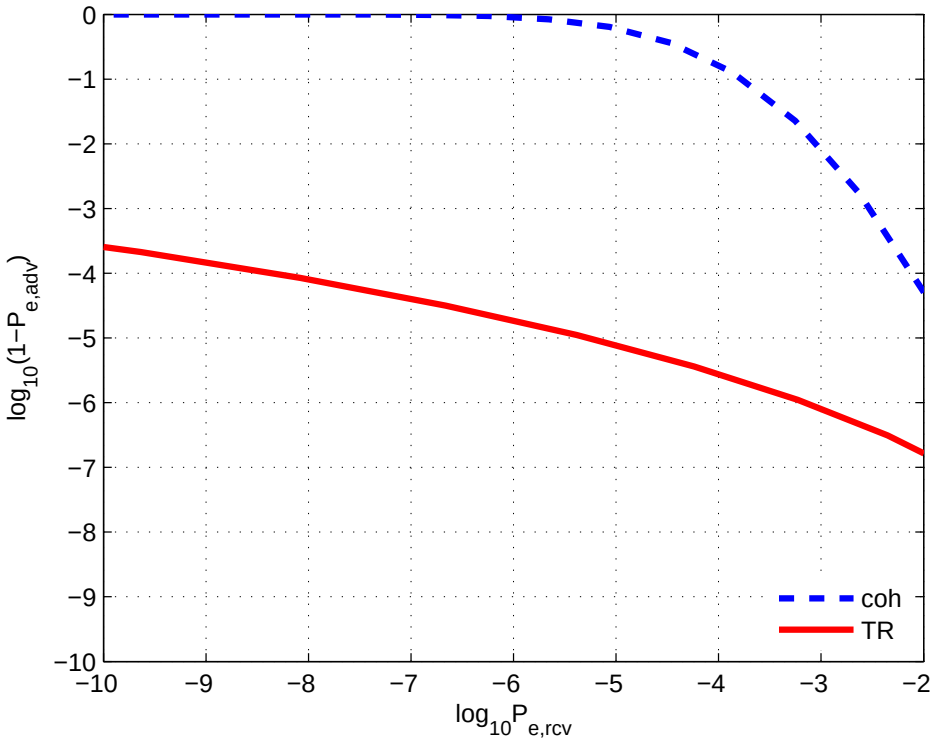

Figure 2.4. Comparison of security of UWB system intended for coherent reception and TR system in IEEE 802.15.4a LOS outdoor environments. The x-axis denotes in log scale the error probability of the legitimate receivers in decoding the data bit while the y-axis denotes in log scale the probability of the adversaries correctly determining the key. At the same error probability for the legitimate receivers, the adversary in the coherent reception case is more effective.

2.4 Semi-Analytic Simulations

The tradeoffs in performance of the legitimate receiver and the adversary for both coherent and TR reception are considered. For these plots, the received SNR is assumed to be the same at the intended receiver and the adversary. We consider the problem of a near adversary and far receiver below. IEEE 802.15.4a channel models [4] are considered.

Figs. 2.3 and 2.4 illustrate the security of the UWB systems when the proposed signaling schemes are used under IEEE 802.15.4a LOS office and LOS outdoor channel models, respectively. For the simulation parameters, we utilize a 30-bit secret key and divide it into 5 parts (m=5). Assume a low-data rate application of 100 $Kbps$. Each symbol period of 10 μs consists of 25 frames, each being 400 ns long. Therefore, each set of 6 bits is independently used to identify the pulse locations in the corresponding group of 5 frames. The bandwidth is 8 GHz yielding a pulse width of approximately 125 ps. For the simulation of the UWB TR system, we assume that D is fixed at 100 ns to assure no inter-pulse interference.

From the figures, the error probability of the difficult hypothesis test for the adversary is much worse than that of the legitimate receiver in both the system intended for coherent reception and the TR system. This is expected since finding the time slots with the randomly assigned data pulses is very difficult for adversaries without first learning the b-bit secret key. Note that the difficulty of the hypothesis test is caused not only by the large number of hypotheses, but also by the ringing of the UWB channel, which makes it difficult to separate hypotheses. Interestingly, both Figs. 2.3 and 2.4 demonstrate that the baseline UWB TR scheme provides better security than the baseline coherent UWB scheme. For example, at the low signal-to-noise (SNR) range in Fig. 2.3, when the error probability of the legitimate receivers in both systems is 10^{-2}, the error probabilities of the adversaries in the UWB system intended for coherent reception and UWB TR system are approximately $1 - 10^{-4}$ and $1 - 10^{-6}$, respectively.

The error probabilities of the legitimate receiver and adversary in the systems intended for coherent reception (2.7), (2.11) are not affected by the bandwidth W, whereas the error probabilities of the legitimate receiver and adversary in the TR systems (2.14), (2.17) are functions of the bandwidth W. The numerical results obtained by varying the bandwidth W show that the larger the bandwidth W used, the higher the probability of error for the adversary of TR reception, resulting in better security performance for the UWB TR systems.

2.5 Discussion

2.5.1 Near-far problem

One challenge to all physical-layer security protocols is the near-far problem. In particular, an eavesdropper near the transmitter can have a significant SNR advantage over the desired receiver. More troubling is that one often cannot assume knowledge of the receiver position, thus making it difficult to even choose the secrecy rate at which all of the recent schemes based on [13] should transmit. Hence, it is desirable to consider how robust the proposed schemes of the fixed rate are for eavesdroppers that have significant SNR advantages over the desired receiver.

Fig. 2.5 shows the error probabilities of the legitimate receiver and the adversary when the transmission is intended for coherent reception vs. the SNR. Consider when the error probability for both the legitimate receiver and the adversary is 10^{-1}. The legitimate receiver obtains $30.79\ dB$ for the error probability of 10^{-1} while the adversary needs 43.36 dB to obtain the same error probability. Since the energy is inversely proportional to the square of distance, if the legitimate receiver is not farther than 4.77 times the distance of the adversary from the transmitter, the error probability of the legitimate receiver is smaller than that of the adversary, circumventing any near-far problem.

Further numerical results (not shown) demonstrate it is very difficult for adversaries to detect a transmitted signal over a large SNR range. In particular, even when the re-

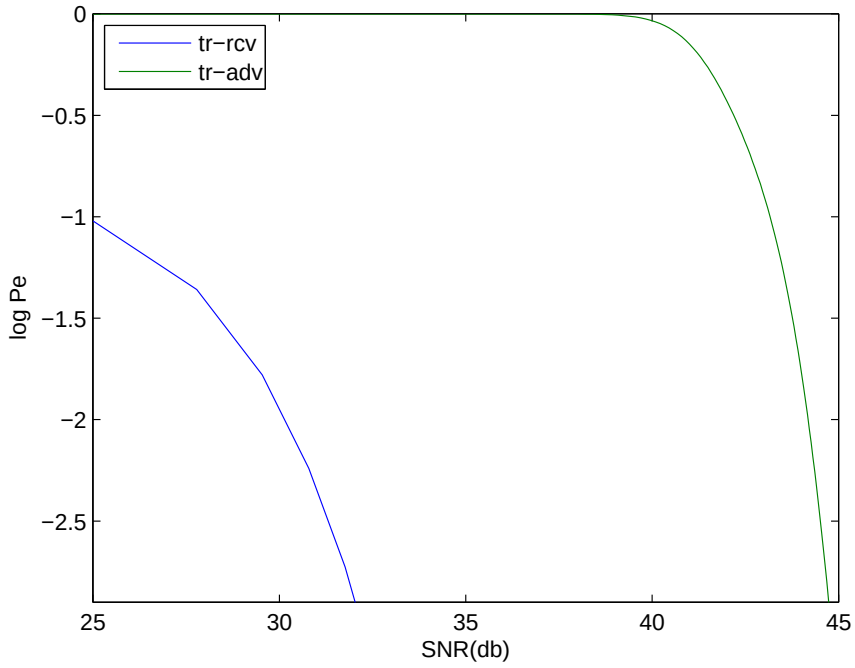

Figure 2.5. Error probabilities of UWB systems intended for TR reception vs. SNR. The x-axis denotes SNR (dB) while the y-axis denotes the error probabilities of the legitimate receiver and the adversary when transmission is intended for coherent reception.

ceived SNR of the desired receiver is driven very high (corresponding to extremely low probabilities of error), the minimum error probability of the adversary is still high. This demonstrates that even when an adversary is near the transmitter while a legitimate receiver is located distantly from the transmitter, the adversary will have difficulty in detecting the transmitted signal. This complication for the adversary comes from the long "ringing" of the UWB channel, which is particularly hard for the adversary to deal with, even with sophisticated receivers, in the TR case. Longer keys and wider bandwidths will also improve this promising near-far resiliency.

2.5.2 Comments on the comparison and improvement of each scheme

The comparison provided in this thesis work considers only baseline systems and thus should be carefully considered before making firm decisions on eventual utility. Here we comment on this comparison and future directions for improving each of the systems.

First, consider each of the systems when the adversary employs a more complicated hypothesis test that takes into account the confusion of the hypotheses caused by the channel. For the system intended for coherent reception, it is relatively straightforward for the UWB adversary to use the equations presented in this work to conduct such a hypothesis test, although we could complicate this somewhat with a more complicated mapping to pulse locations from the key bits. However, since the UWB TR adversary is not able to estimate the channel parameters, it would be much harder for the adversary to perform such a hypothesis test from the analogous set of equations in that case.

We also have assumed perfect timing for both the receiver and the adversary in both the system intended for coherent reception and in the TR system. In the system intended for coherent reception, this is reasonable since the assumed beacons easily provide such. However, in a TR system, the reader and adversary would have to perform such. Since the TR system knows the key, this is a standard exercise, but the adversary would have a much more difficult task to figure out not only symbol boundaries, but also the locations where the system switches from one part of the key to another.

Finally, we are considering future enhancements that will facilitate improvement on the baseline systems employing coherent and reference-based reception. One could easily argue that the comparison here is not fair to the coherent system, since a given tradeoff on its performance curves in Figs. 2.3 and 2.4 might come at a lower transmit power than the one compared to on the TR curve. Increasing the pulse power in the coherent system to try to equalize such does not help, because it just moves one along the performance curves in Figs. 2.3 and 2.4. However, there are multiple possibilities to employ excess power.

One potential scheme is to produce dummy pulses in some of the frames to confuse the adversary. The adversary would be just as likely to choose a dummy pulse as the real one, and the reader would only be mildly affected by inter-pulse interference on the pulse in which it is interested.

For example, Fig. 2.6 illustrates the security of the UWB systems intended for coherent reception for a different number of dummy pulses and TR system in IEEE 802.15.4a LOS office environments. Since the UWB system intended for coherent reception uses less transmit power, extra dummy pulses can be generated with excess power. For comparison, the UWB systems intended for coherent reception generating a different number of dummy pulses in each frame with excess power is considered. As the number of chaff pulses in each frame increases, the error probability of the adversary increases since the adversary has no knowledge of the real data pulse location among the transmitted pulses.

Consider the case that the error probability of the legitimate receiver is 10^{-2}. To obtain this error probability, the energies used to transmit pulses in one symbol period in the UWB systems intended for coherent reception and TR reception are respectively $7.78\ dB$ and $33.80\ dB$. This implies the coherent system could employ many dummy pulses to confuse the adversary if synchronization is not affected. Up to a maximum of 2 dummy pulses, security performance of the UWB TR system still remains superior to that of the coherent UWB system for the error probability of the legitimate receiver of 10^{-2}. However, if there are more than 2 dummy pulses generatedin the coherent system, then the coherent UWB system outperforms the UWB TR system.

One another possible improvement being considered is to remove the frame structure in both the UWB coherent and TR signaling models. In UWB coherent signaling, pulses can be placed anywhere in one symbol period based on the entire secret key. In UWB TR signaling, the key could be mapped to a tuning of the autocorrelation function of the transmitted signal across an entire symbol period. Doing so in either signaling scheme may make it more challenging for the adversary to detect pulses because of the expanded search

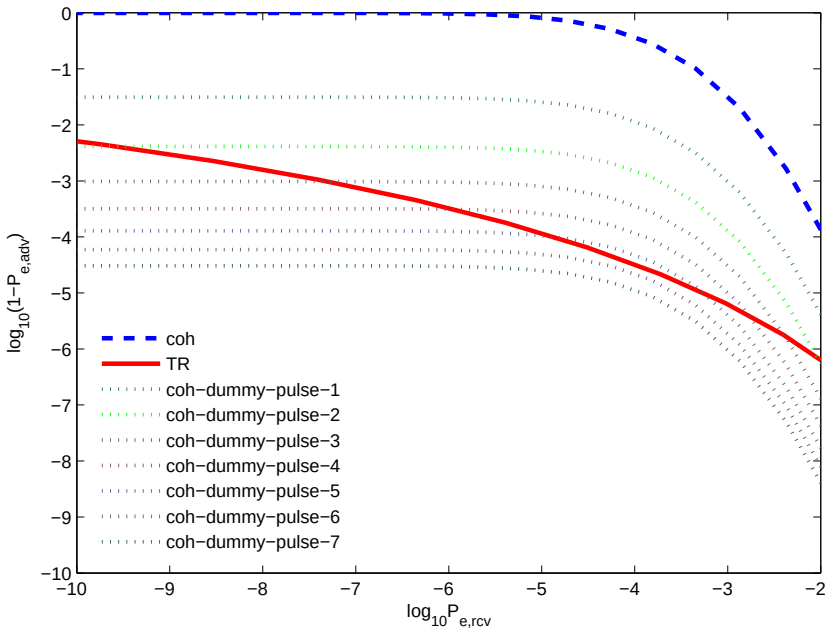

Figure 2.6. Comparison of security of UWB systems intended for coherent reception generating dummy pulses and TR system in IEEE 802.15.4a LOS office environments. The x-axis denotes in log scale the error probability of the legitimate receivers in decoding the data bit while the y-axis denotes in log scale the probability of the adversaries correctly determining the key.

space. In the following chapter we investigate whether removing the frame structure in UWB coherent signaling can provide better security performance.

2.6 Conclusion

In this thesis work we proposed a UWB signaling model to strengthen physical layer security. We examined the security performance of both baseline coherent and TR signaling schemes numerically in IEEE 802.15.4a environments. These numerical results demonstrate that, for the baseline systems considered, the security performance of the TR system is better than that of the system intended for coherent reception. There are numerous ways in which each of the schemes can be improved and many adversary models that can be adopted. We are currently pursuing such in conjunction with lightweight cryptographic protocols to be employed over the UWB system. We hope this work also motivates further work of others in this important area.

CHAPTER 3

FRAMELESS UWB

In this chapter we propose a UWB signaling scheme with a frameless structure when the transmission is intended for coherent reception. As in the previous chapter, the proposed signaling scheme is based on a TH method and binary pulse amplitude modulation. We assume that a randomly generated b-bit secret key K is used to determine the UWB pulse positions in both the framed and frameless signaling schemes to allow comparison of their security performances. Here we consider the transmission of the signals over the additive white gaussian noise (AWGN) channel. Like those in the previous chapter, a signal carrying the first data bit b_0 mapped to $\{-1, 1\}$ with equal probability in the first symbol period is considered.

Since the legitimate receiver shares the secret key K and thus knows where to search for the pulses, the probability of the legitimate receiver not being able to decode the data remains the same for both signaling schemes. We examine the security performance in terms of the ability of the adversary using the signaling scheme with a frame structure to detect the key versus the ability of the adversary using the signaling scheme with a frameless structure to ascertain the key when both signaling schemes are intended for coherent reception.

First, we derive the cumulative distribution function (CDF) for the number of key bits that the adversary can detect when the signaling scheme is based on a framed structure intended for coherent reception as shown in Fig. 3.1 which is similar to that of Fig. 2.1 in Chapter 2. For simplicity, we do not consider repetition of the pulses. We obtain an analogous CDF when the frameless signaling scheme is intended for coherent reception as

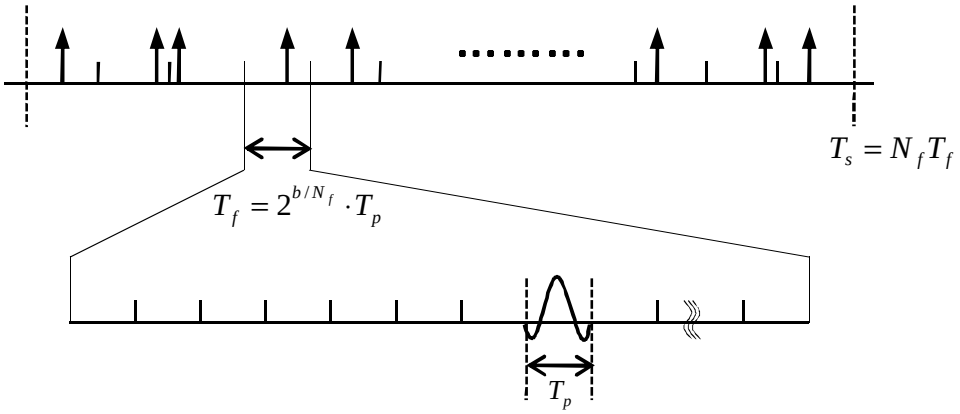

Figure 3.1. Signaling scheme with a frame structure intended for coherent reception

illustrated in Fig. 3.2 is employed. We first assume that both systems use the same secret key K to locate data pulses, resulting in a different number of pulses in each signaling scheme. On the other hand, we can consider the case that there is no constraint on the secret key length. Here, we assume that the same number of data pulses is generated in both the framed and frameless signaling schemes.

3.1 SYSTEM MODEL

3.1.1 Signaling scheme with a frame structure

Fig. 3.1 illustrates a frame UWB signaling scheme intended for coherent reception. Given the b-bit secret key K constraint, we aim to generate N_f pulses in one symbol period T_s, each of which uses $k = b/N_f$ bits to specify a pulse position in each frame. As described in the previous chapter, a transmitted signal $s_0(t)$ carrying the first information bit b_0 over the first symbol period is considered. Thus the signal transmitted by a single user can be written as:

$$s_{0,frame}(t) = \sum_{i=0}^{N_f-1} (-1)^{b_0} \sqrt{E_p}\, p(t - iT_f - c_{0,i}T_p), \tag{3.1}$$

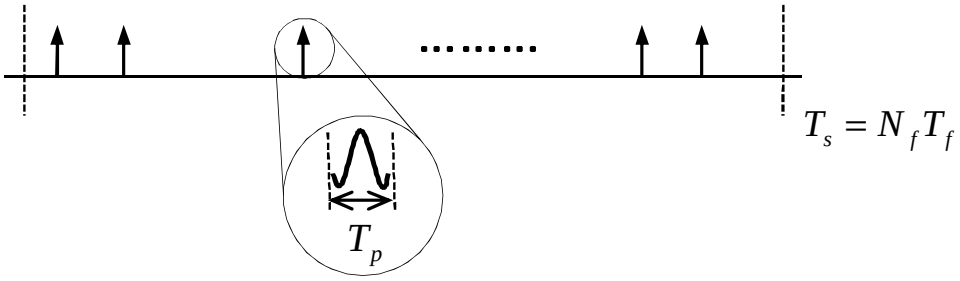

Figure 3.2. Signaling scheme with a frameless structure intended for coherent reception

where the parameters specified in the previous chapter hold in (3.1). Here, assuming the pulse duration T_p and the frame duration T_f, the number of bits k used to select a position index in $\{0, 1, ..., \ 2^k - 1\}$ in each frame can be expressed as:

$$k = \log_2(T_f/T_p). \tag{3.2}$$

Accordingly, the total number of pulses in one symbol period specified by the b-bit secret key K is given by:

$$N_f = b/k = \frac{b}{\log_2(T_f/T_p)}. \tag{3.3}$$

3.1.2 Signaling scheme with a frameless structure

Fig. 3.2 illustrates a frameless UWB signaling scheme intended for coherent reception. We assumed that this frameless signaling scheme is constrained by the b-bit secret key K and the total number of time slots N_t in one symbol period. In this signaling scheme with a frameless structure, pulses can be located within any time slot in each symbol period. Therefore, since there are $N_t = 2^k \cdot N_f = T_s/T_p$ time slots in one symbol period, $k + \log_2 N_f$ bits are used to specify a pulse location. The total number of pulses transmitted in one symbol period N_p is given by:

$$N_p = \frac{b}{k + \log_2 N_f} = \frac{b}{\log_2(T_s/T_p)}. \tag{3.4}$$

Since the frameless signaling scheme uses extra bits $\log_2 N_f$ to decide the pulse location, fewer pulses than those with a frame structure are supported by the constraint of the b-bit secret key K. We also consider a transmitted signal $s_{0,frameless}(t)$ carrying the first information bit b_0 over the first symbol period. Thus the signal transmitted by a single user can be expressed by:

$$s_{0,frameless}(t) = \sum_{i=0}^{N_p-1} (-1)^{b_0} \sqrt{E_p}\, p(t - e_{0,i}T_p), \tag{3.5}$$

where $e_{0,i} \in \{0, 1, ..., \ N_t - 1\}$ and the parameters specified in the previous chapter hold in (3.1). The TH code element $e_{0,i}$ is to position the UWB pulse over the time slots in one symbol period.

3.2 Performance of the systems

Consider the transmission of the signal $s_{0,frame}(t)$ and $s_{0,frameless}(t)$ over the AWGN channel.

The received signals after passing through the front-end filter at the receiver can be expressed as:

$$y_{0,frame}(t) = s_{0,frame}(t) * c(t) + n(t) * c(t) \tag{3.6}$$

$$y_{0,frameless}(t) = s_{0,frameless}(t) * c(t) + n(t) * c(t) \tag{3.7}$$

where $c(t)$ is the impulse response of the front-end filter to eliminate the out-of-bandwidth noise and $n(t)$ is a zero-mean white Gaussian noise with two-sided power spectral density $N_0/2$.

3.2.1 Performance of adversary: UWB system with frames

Let the number of pulses that the adversary finds correctly in one symbol period be the random variable X. X takes on a value less than or equal to $d \in \{0, 1, 2, ..., N_f -$

$1\}$. Similar to the systems intended for coherent reception in the previous chapter, the probability of finding the correct pulse position in one is easily derived from the coherent reception of orthogonal signals [9]:

$$\begin{aligned} p_{c,\,adv} &= p(y_{0,i} < y_{0,c_{0,0}}, \forall i \neq c_{0,0}) \\ &= \int_{-\infty}^{\infty} \left[1 - Q\left(\frac{v+\mathcal{E}_s}{\sqrt{\frac{N_0}{2}}}\right)\right]^{2^{b/N_f}-1} \cdot \frac{1}{\sqrt{\pi N_0}} e^{-\frac{v^2}{N_0}}\, dv \\ &= \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} [(1-Q(x))^{2^{b/N_f}-1}] e^{-\frac{(x-\sqrt{\frac{2\mathcal{E}_s}{N_0}})^2}{2}}\, dx \end{aligned} \tag{3.8}$$

where $x = \frac{v+\mathcal{E}_s}{\sqrt{\frac{N_0}{2}}}$.

Noting

$$\begin{aligned} & y_{0,c_{0,0}} \sim N(\sqrt{\mathcal{E}_s}, N_0/2) \\ \text{and} \qquad & y_{0,i} \sim N(0, N_0/2), \qquad i \neq c_{0,0}. \end{aligned}$$

Now, the cumulative distribution function (CDF) for the random variable X can be derived as:

$$\mathrm{P}(X \leq d) = \sum_{d=0}^{N_f-1} \binom{N_f-1}{d} {p_{c,\,adv}}^d (1-p_{c,\,adv})^{(N_f-1-d)}, \tag{3.9}$$

where $d \in \{0, 1, 2, ..., N_f - 1\}$.

3.2.2 Performance of adversary: UWB system without frames

The noise random variable is drawn from a zero-mean normal distribution with a variance $N_0/2$, whereas the signal random variable has a normal distribution with a mean $\sqrt{\mathcal{E}_s}$

and a variance $N_0/2$. The probability density functions (pdfs) of the signal and the noise are given, respectively, by:

$$g(n) = \frac{1}{\sqrt{2\pi}} e^{-n^2/2} \tag{3.10}$$

$$f(s) = \frac{1}{\sqrt{2\pi}} e^{-(s-\sqrt{\mathcal{E}_s})^2/2}. \tag{3.11}$$

On the other hand, the adversary, lacking knowledge of the b-bit secret key K, selects the largest N_p values among the received signals and assumes them to be the correct data pulses. We use order statistics to obtain the CDF of the random variable X, the number of pulses that the adversary finds correctly in one symbol period. There are N_p observed values of the signal random variable and $2^k \cdot N_f - N_p$ observed values of the noise random variable. Here, the order statistic of rank l is the l^{th} smallest value in the value set and is denoted $S_{(l)}$ or $N_{(l)}$.

Note in particular that the minimum and maximum values considered are:

$$S_{(1)} = min\{S_1, ..., S_{N_p}\} \tag{3.12}$$

$$S_{(N_p)} = max\{S_1, ..., S_{N_p}\} \tag{3.13}$$

$$N_{2^k \cdot N_f - N_p} = max\{N_1, ..., N_{2^k \cdot N_f - N_p}\}. \tag{3.14}$$

Therefore, the pdf of $S_{(i)}$, the i^{th} smallest of $S_1, ..., S_{N_p}$, is given as in [3] by:

$$f_{(i)}(s) = N_p f(s) \binom{N_p - 1}{i - 1} (F(s))^{i-1} (1 - F(s))^{(N_p - i)}, \tag{3.15}$$

and the pdf of $N_{(j)}$, the j^{th} smallest of $N_1, ..., N_{2^k \cdot N_f - N_p}$, is given as in [3] by:

$$g_{(j)}(n) = (2^k \cdot N_f - N_p) g(n) \binom{2^k \cdot N_f - N_p - 1}{j - 1} (G(n))^{j-1} (1 - G(n))^{(2^k \cdot N_f - N_p - j)} \tag{3.16}$$

Then, the cumulative distribution function (CDF) of the random variable X can be derived as:

$$
\begin{aligned}
\mathrm{P}(X \leq d) &= \mathrm{P}(\text{more than } N_p - d \text{ noises are in the largest } N_p \text{ slots}) \\
&= \mathrm{P}(((2^k \cdot N_f - N_p) - (N_p - d - 1))^{th} \text{ smallest noise} > (N_p - d)^{th} \text{ smallest signal}) \\
&= \mathrm{P}(N_{(2^k \cdot N_f - 2N_p + d + 1)} > S_{(N_p - d)}) \\
&= E_{S_{(N_p-d)}}[\mathrm{P}(N_{(2^k \cdot N_f - 2N_p) + d + 1)} > s_{(N_p-d)})] \\
&= E_{S_{(N_p-d)}}[\int_s^\infty g_{(2^k \cdot N_f - 2N_p + d + 1)}(n) dn] \\
&= \int_{-\infty}^{\infty} f_{(N_p-d)}(s) \int_s^\infty g_{(2^k \cdot N_f - 2N_p + d + 1)}(n) dn ds
\end{aligned}
$$

3.3 Numerical Evaluation

In this section, we compare the ability of the adversary under the framed signaling scheme to detect the key versus the ability of the adversary under the frameless signaling scheme to ascertain the key. The abilities of the adversaries for both framed and frameless signaling schemes intended for coherent reception are represented in terms of the corresponding CDF of X. Since the final expressions for the CDFs are in integral form, we present numerical evaluation results. The frameless signaling scheme may offer better performance than the framed signaling scheme since the adversary in the frameless signaling scheme has to search not only for the time slots in each frame but rather the entire time slots in one symbol period to find the data pulse. However, as mentioned earlier, if we assume that the same b-bit secret key K is available and there are the same number of time slots provided in one symbol period, the frameless signaling scheme intended for coherent reception has a lesser number of data pulses than those in the framed signaling scheme. First, given the constraint of b-bit secret key K, we investigate whether the security of the frameless signaling scheme outperforms that of the framed signaling scheme despite the

difference in the number of pulses used to transmit data. Next, we assume that there is no constraint on the secret key bits and thus the same number of data pulses is used in one symbol period.

3.3.1 Same number of key bits used for both framed and frameless structures

b	k	N_f	N_p	Performance
64	4	16	8	Framed is better: See Fig. 3.3
160	5	32	16	Framed is better: See Fig. 3.4
168	21	8	7	Frameless is better: See Fig. 3.5
192	12	16	12	Framed is better: See Fig. 3.6
352	11	32	22	Framed is better: See Fig. 3.7
384	6	64	32	Framed is better: See Fig. 3.8

Table 3.1. Experimental parameters in case of using the same number of secret key bits

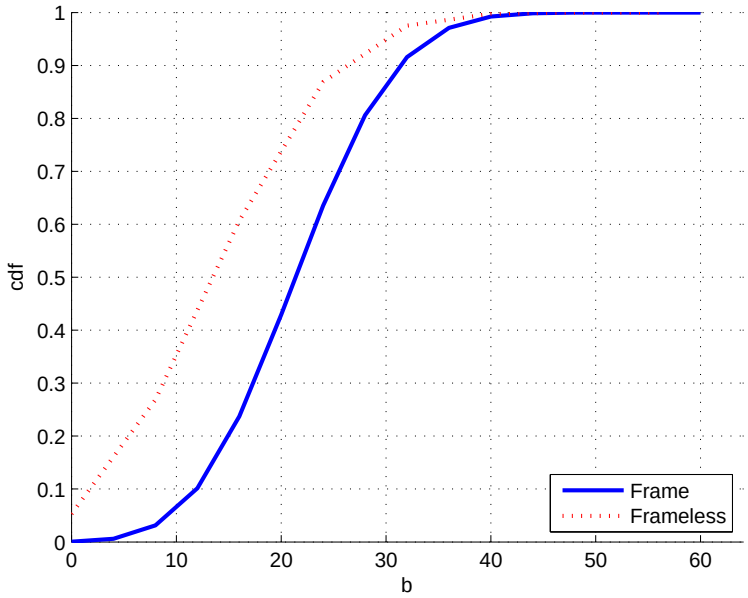

Figure 3.3. CDFs of the number of bits that the adversary detects. b=64, k=4, N_f=16 and N_p=8

Numerical results are presented here to compare the CDFs of the adversaries previously obtained. For simplicity, only integer parameters are considered. Table 3.1 presents the ex-

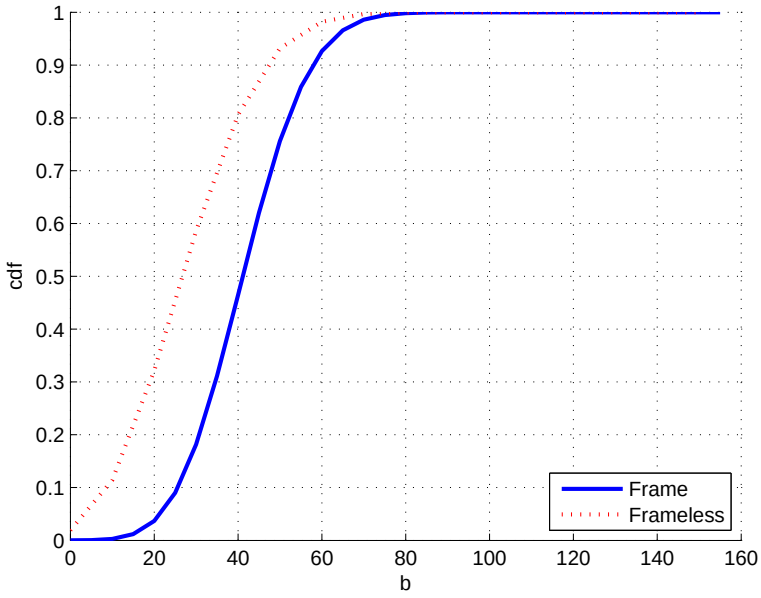

Figure 3.4. CDFs of the number of bits that the adversary detects. b=160, k=5, N_f=32 and N_p=16

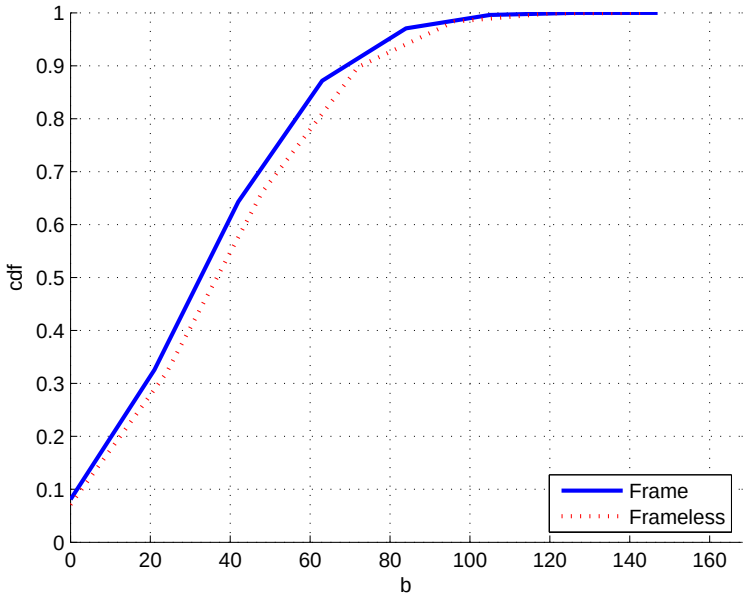

Figure 3.5. CDFs of the number of bits that the adversary detects. b=168, k=21, N_f=8 and N_p=7

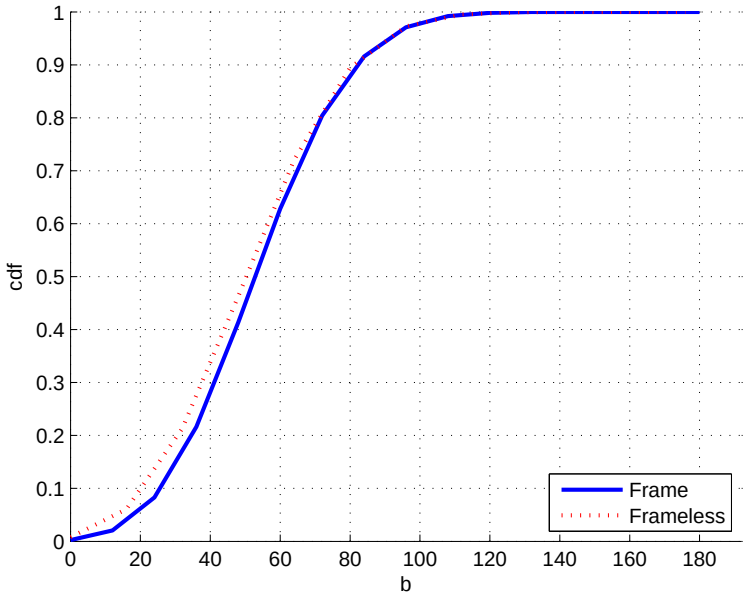

Figure 3.6. CDFs of the number of bits that the adversary detects. b=192, k=12, N_f=16 and N_p=12

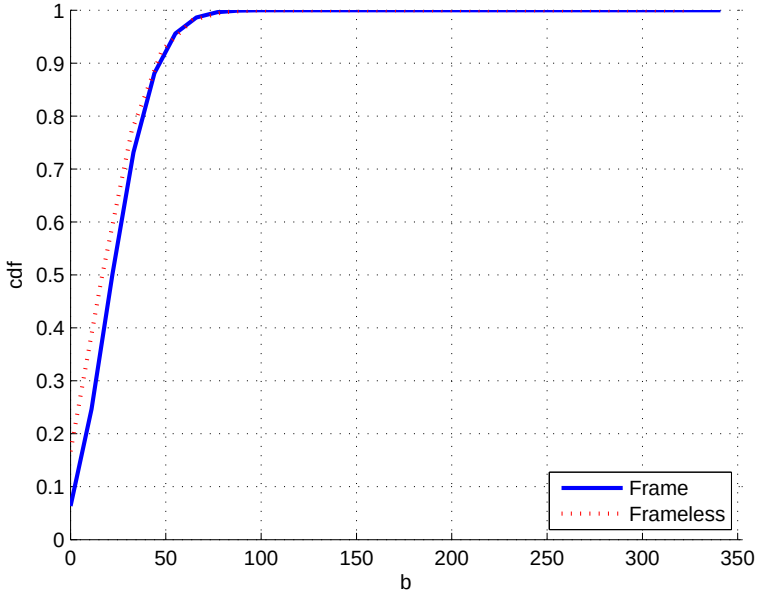

Figure 3.7. CDFs of the number of bits that the adversary detects. b=352, k=11, N_f=32 and N_p=22

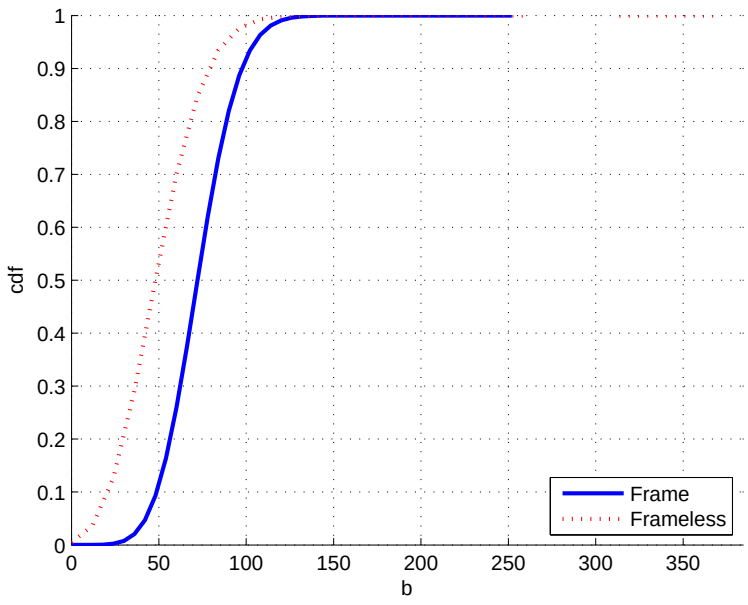

Figure 3.8. CDFs of the number of bits that the adversary detects. b=384, k=6, N_f=64 and N_p=32

perimental integer parameters satisfying the relationships of b, k, N_f and N_p if the same b-bit secret key K is used for both the framed and frameless signaling schemes. Comparisons of the CDFs are illustrated in Figs. 3.3 to 3.8. The upper curve indicates the superior ability of the adversary to detect the secret key correctly. As seen from Fig. 3.5, the frameless signaling scheme slightly outperforms the framed signaling scheme at least one case. In this case, the number of pulses generated to transmit data is almost the same since N_f=8 and N_p=7 as shown in Table 3.1. Otherwise, the framed signaling scheme performs better than the frameless signaling scheme. If there is no significant difference between the numbers of the generated pulses, the security performance of the frameless structure inherently outperforms that of the framed structure since the adversary has difficulty in finding the pulses due to the expanded search window. However, if considerably more pulses satisfying the relationships of b, k, N_f and N_p are generated in the framed signaling scheme, finding all the pulses in the framed signaling scheme becomes more challenging than finding the pulses with the expanded search window in the frameless signaling scheme.

3.3.2 No limitation on key bits

Now we present the simulation result when the same number of pulses is generated in both signaling schemes so that only the structure of the signaling scheme affects security performance. We assume, given the number of pulses N_f in the framed signaling scheme and total time slots N_t in one symbol period, that the same number of pulses $N_p = N_f$ is generated in one symbol period in the frameless structures. That is, we have sufficient secret key bits for positioning pulses, and thus $N_p = N_f$. Table 3.2 shows the experimental parameters when $N_p = N_f$. Figs. 3.9 to 3.13 compare the CDFs of the number of bits intercepted by the adversary for both the framed and frameless structures. As shown in Figs. 3.9 to 3.13, the curve of the CDF in the framed signaling scheme is slightly above that of the CDF in the frameless signaling scheme, meaning the frameless structure has slightly better security performance than the framed signaling scheme. This is expected; although there is the same number of pulses for the adversary to detect, the adversary in the frameless case has to search the entire set of time slots in one symbol period to detect the pulses with no structure.

b	k	$N_f = N_p$	Performance
64	8	8	Frameless is better: See Fig. 3.9
128	8	16	Frameless is better: See Fig. 3.10
128	16	8	Frameless is better: See Fig. 3.11
192	8	24	Frameless is better: See Fig. 3.12
192	16	12	Frameless is better: See Fig. 3.13

Table 3.2. Experimental parameters in case of the same number of pulses

3.4 Conclusion

In this chapter we proposed a frameless UWB signaling model to further strengthen physical layer security by removing unnecessary structure from the transmitted signal. Given the b-bit secret key K constraint, the numerical results demonstrates that the security performance of the system of a frameless structure is superior to that of the system of a

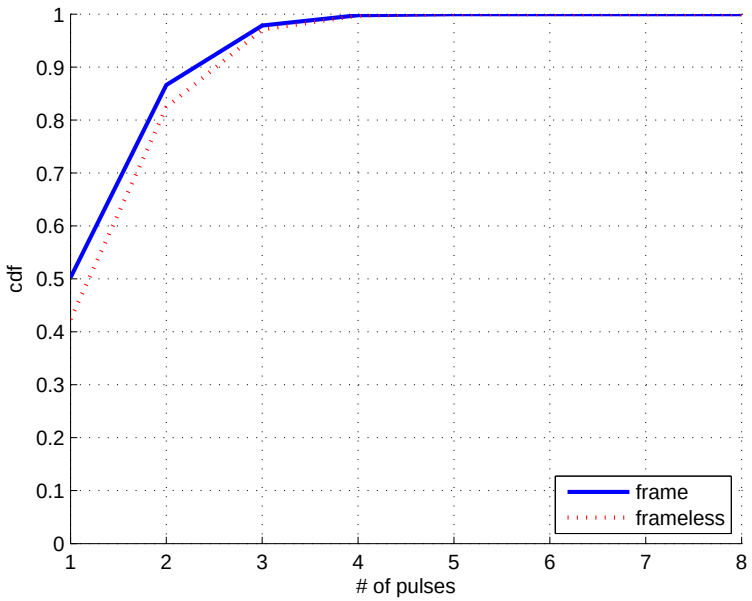

Figure 3.9. CDFs of the number of pulses that the adversary detects. b=64, k=8, N_f=N_p=8

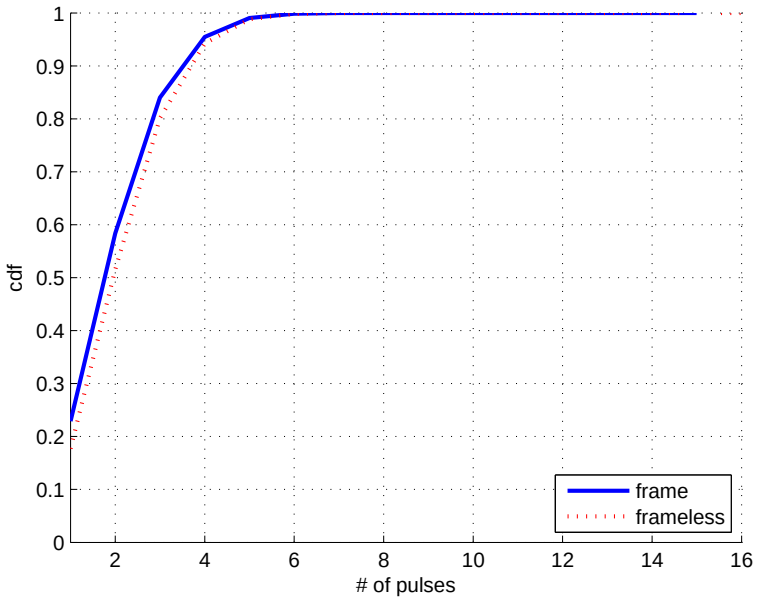

Figure 3.10. CDFs of the number of pulses that the adversary detects. b=128, k=8, N_f=N_p=16

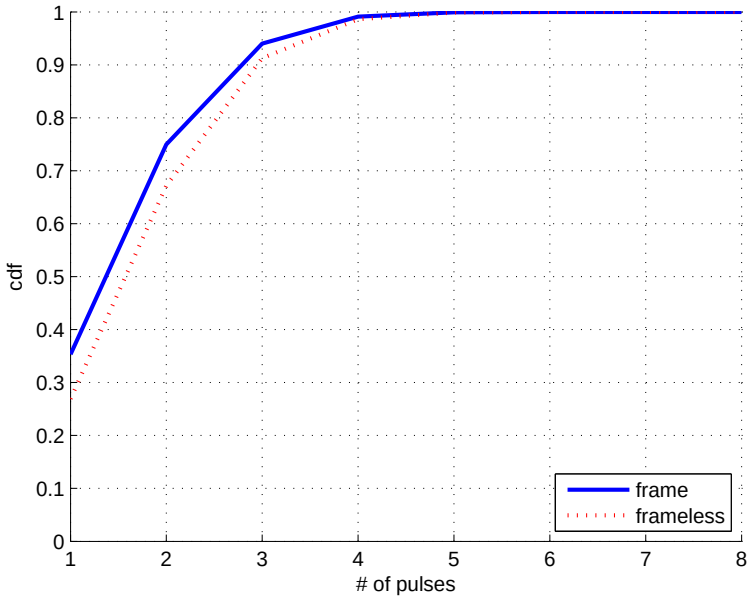

Figure 3.11. CDFs of the number of pulses that the adversary detects. b=128, k=16, N_f=N_p=8

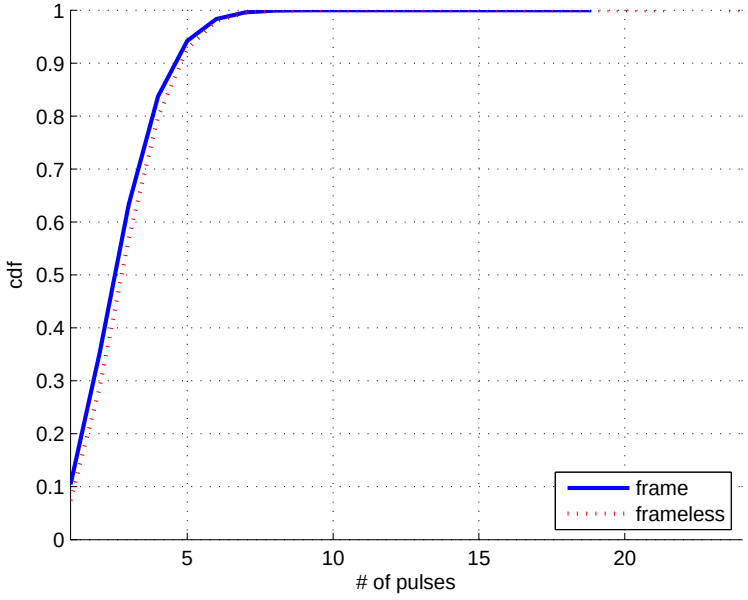

Figure 3.12. CDFs of the number of pulses that the adversary detects. b=192, k=8, N_f=N_p=24

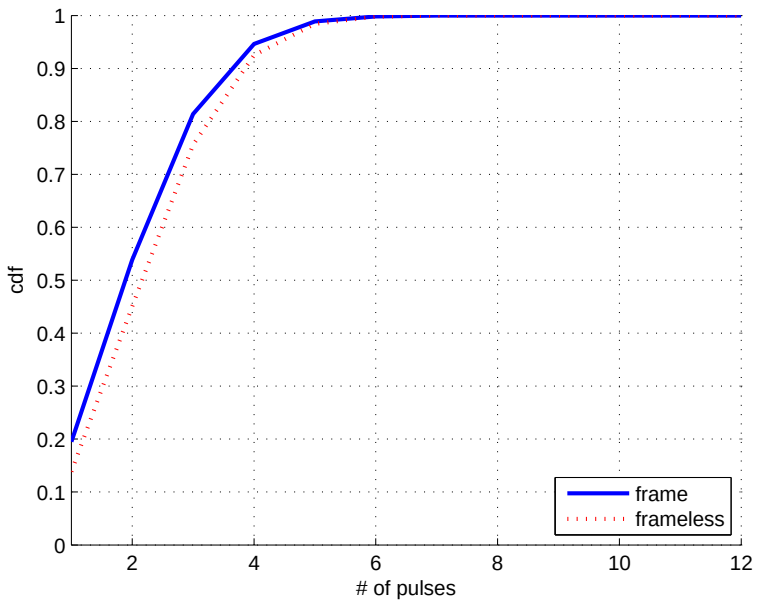

Figure 3.13. CDFs of the number of pulses that the adversary detects. b=192, k=16, N_f=N_p=12

framed structure only if there is no significant difference between the numbers of the pulses N_f and N_p positioned in one symbol period. Otherwise, quite surprisingly, the framed signaling scheme outperforms the frameless signaling scheme. We also examined the security performance of both systems when there is the same number of pulses in one symbol period. The security performance of the frameless signaling scheme outperforms that of the framed signaling scheme, since the adversary in the case of the frameless signaling scheme experiences difficulty in detecting the pulses due to the expanded search window.

CHAPTER 4

CONCLUSION

Traditionally, spread-spectrum systems have been employed to provide low probability-of-intercept (LPI) and low probability-of-detection (LPD) performances at the physical layer, but the messages transmitted over such a system are still encrypted with a powerful cipher to protect their secrecy. Our challenge is to find a solution to provide an additional level of security at the physical layer so that simple systems such as RFID tags with limited resources can be secure without using standard encryption. It has recently been suggested that the cryptographic security of the system can be enhanced by exploiting physical properties of UWB signals. With an eavesdropper observing the communications over multipath channels between two legitimate partners sharing a secret key of a limited length, we consider both coherent and reference-based UWB schemes to enhance security. The security of the legitimate nodes is achieved by signal attributes based on the secret key, conferring an advantage over the adversary.

In particular, in the first part, we propose UWB signaling schemes to improve physical layer security when the transmission is intended for coherent reception and TR reception. To evaluate the signaling schemes, we derive the error probabilities for the legitimate receivers and the adversaries for both transmission cases. Then we weigh the tradeoffs in security performance of both baseline coherent and TR signaling schemes numerically in IEEE 802.15.4a environments. Critical to the TR scheme is employing true randomness to keep a sophisticated adversary from decoding the signal coherently. We investigate the physical layer security performance of UWB systems intended for coherent reception and UWB TR systems in IEEE 802.15.4a multipath environments. Numerical results for IEEE

802.15.4a channel models reveal not only that the proposed schemes provide promising support for higher-layer cryptographic protocols, but also, surprisingly, that the baseline UWB TR system can demonstrate better security tradeoffs than the baseline UWB system intended for coherent reception under the IEEE 802.15.4a channel model. Further, there are numerous ways in which each of the schemes can be improved as well as in the many adversary models that can be adopted. Among possible improvements, we could consider removing the frame structure in both the UWB coherent and TR signaling schemes.

Accordingly, in the second part of the thesis, we consider removing the frame structure of the UWB coherent signaling scheme, resulting in pulses that can be located anywhere in the symbol period. Our hypothesis is that the frameless signaling scheme can make it more difficult for the adversary to detect the pulses. For this, we first compare the CDFs of the number of bits which the adversary can detect when the signaling schemes are based on both the framed structure and the frameless structure given the same size secret key to position the pulses. The numerical results demonstrate that the frameless structure slightly outperforms the framed structure unless there is a significant difference between the numbers of pulses in both signaling structures. However, if there is no constraint on the size of the secret key and thus, for example, there are the same number of pulses located in one symbol period, the results reveal that the frameless structure is superior to the framed structure in every example tested to date.

Our proposed signaling schemes could potentially suggest a solution for applications relying on conventional cryptography, especially for low-data rate RFID systems.

BIBLIOGRAPHY

[1] Chao, Y.-L., and Scholtz, R.A. Ultra-wideband transmitted reference systems. *IEEE Transactions on Vehicular Technology 54*, 5 (Sept. 2005), 1556–1569.

[2] Choi, J. D., and Stark, W. E. Performance of ultra-wideband communications with suboptimal receivers in multipath channels. *IEEE Journal on Selected Areas in Communications 20* (2002), 1754–1766.

[3] David, H.A., and Nagaraja, H.N. *Order Statistics*, 3rd ed. Wiley, 2003.

[4] De Nardis, L., and Di Benedetto, M.-G. Overview of the IEEE 802.15.4/4a standards for low data rate wireless personal data networks. In *4th Workshop on Positioning, Navigation and Communication* (March 2007), pp. 285–289.

[5] Durisi, G., and Benedetto, S. Comparison between coherent and noncoherent receivers for UWB communications. *EURASIP J. Appl. Signal Process.* (2005), 359–368.

[6] Goeckel, D.L., and Zhang, Qu. Slightly frequency-shifted reference ultra-wideband (UWB) radio: TR-UWB without the delay element. In *Military Communications Conference* (Oct. 2005), pp. 3029–3035.

[7] Juels, A., and Weis, S.A. Authenticating pervasive devices with human protocols. In *Crypto 2005* (Aug. 2005), pp. 293–308.

[8] Morrison, K., Capar, C., Lai, Z., Goeckel, D., and Jackson, R. A unified framework for reference-based ultra-wideband signaling. In *IEEE International Conference on Ultra-Wideband* (Sept. 2009), pp. 290–294.

[9] Proakis, J. G., and Salehi, M. *Digital Communications*, 5th ed. McGraw-Hill, New York, 2008, pp. 741–743.

[10] Scholtz, R. A., Pozar, D. M., and Namgoong, W. Ultra-wideband radio. *EURASIP J. Appl. Signal Process.* (2005), 252–272.

[11] Srinivasan, S., Mathew, S., Erraguntla, V., and Krishnamurthy, R. A 4gbps 0.57pj/bit process-voltage-temperature variation tolerant all-digital true random number generator in 45nm cmos. In *VLSI Design, 2009 22nd International Conference on* (Jan. 2009), pp. 301–306.

[12] Talbot, J., and Welsh, D. *Complexity and Cryptography: An Introduction*. Cambridge University Press, New York, 2006.

[13] Wyner, A. D. The wire-tap channel. *Bell System Technical Journal 54*, 8 (Oct. 1975), 1355–1367.

[14] Yu, P., Schaumont, P., and Ha, D. Securing rfid with ultra-wideband modulation. In *RFIDSec 2006* (July 2006).