Christian Holzner, BSc.

Secure Ranging in the IEEE 802.15.4a Standard

Master's Thesis

to achieve the university degree of

Diplom-Ingenieur

Master's degree programme: Electrical Engineering and Business

submitted to

Graz University of Technology

Supervisor

Assoc.Prof. Dipl.-Ing. Dr., Witrisal Klaus

Signal Processing and Speech Communication Laboratory

Dipl.-Ing. Dr., Thomas Gigl

Graz,May 2015

STATUTORY DECLARATION

I declare that I have authored this thesis independently, that I have not used other than the declared sources/resources, and that I have explicitly indicated all material which has been quoted either literally or by content from the sources used. The text document uploaded to TUGRAZonline is identical to the present master‘s thesis dissertation.

Date: ______________________________ Signature: ______________________________

Abstract

So-called "Keyless-Entry" systems are very welcomed by many consumers and have become indispensable in many areas. They involve radio modules, which automatically grant access as soon as an authorized key is within a certain distance. In most cases, this distance is not measured directly, because e.g. a passive key is supplied only in the immediate vicinity of the car with enough energy trough electromagnetic coupling. Once the key responds it is assumed that it is located very close to the car.

Although such systems are very convenient for consumers, the safety aspect is often lost very quickly. There are numerous reports of so-called relay attacks that simply forward the signal and thus expand the acceptance radius for burglars.

The Ultra WideBand (UWB) technology opens the way for very effective and inexpensive data communication and ranging devices. Methods make use of the so-called Impulse Radio, in which very short pulses are sent (in the nanosecond range). The achieved time resolution allows to differentiate individual components (reflections) caused by the multipath propagation. The result is a highly accurate channel estimation, which is used for a Time of Flight (TOF) measurement to compute the distance between two devices.

For this purpose the IEEE 802.15.4a standard developed in 2007 a protocol that enables low-cost and energy-efficient devices for data communication, with the additional possibility of accurate positioning (<1m). The standard provides many parameters that allow manufactures to design secure equipment and to be compliant with the various regulatory authorities.

Of course, the TOF measurement makes such systems safer. Nevertheless it is still possible to distort the measurement. An attacker can manipulate the signal levels to achieve a time shift of the entire communication, which leads to a distance decrease. Thus, the key seems to be closer than it is in reality. Since such attacks occur on the physical layer, they bypass any cryptographic efforts introduced by developers.

In my work I deal with the energy detector, the simplest implementation of a localization system that implies with the standard. Due to its simplicity, the energy detector is particularly suitable for those "keyless entry" systems, because a keyfob is often limited in its size and power consumption. Nevertheless, this low complexity makes the energy detector also more vulnerable to relay attacks.

For this purpose a countermeasure has been developed which detects a manipulation of the signal levels. The method is based on a simple hypothesis test, which validates the authenticity of the received signal.

This countermeasure makes it virtually impossible for the attacker to manipulate the signal levels without being noticed, thus preventing the manipulation of the TOF measurement.

Kurzfassung

So genannte "Keyless-Entry"-Systeme finden in den letzten Jahren reißenden Absatz und sind mittlerweile aus manchen Sparten nicht mehr wegzudenken. Es handelt sich dabei um Funkmodule, welche automatisch Zugang gewähren, sobald sich ein autorisierter Schlüssel in einem bestimmten Abstand befindet.

In den meisten Fällen wird dabei der Abstand gar nicht direkt gemessen, da z.B. ein passiver Schlüssel nur in einem bestimmten Umkreis, über elektromagnetische Kopplung mit Energie versorgt wird. Sobald der Schlüssel antwortet wird also davon ausgegangen, dass er sich in unmittelbarer Nähe vom Auto befindet. Abgesehen vom Umstand, dass solche Systeme sehr praktisch für den Endverbraucher sind, geht dabei der Sicherheitsaspekt oft verloren. Es gibt zahlreiche Berichte über sogenannte Relay-Attacken, die das Signal einfach weiterleiten und so den Zugangsradius für Einbrecher erweitern.

Durch die Ultra-Breitband-Technologie (UWB) ist es heute möglich, sehr effektiv und kostengünstig Entfernungen zu messen aber auch Daten zu übermitteln. Dabei bedient man sich dem sogenannten Impulse Radio, bei dem sehr kurze Impulse (im Nanosekundenbereich) ausgesandt werden. Die zeitliche Auflösung, die dadurch erreicht wird, ermöglicht die Unterscheidung von einzelnen Komponenten (Reflexionen), die durch die Mehrwegeausbreitung entstehen. Das Ergebnis ist eine sehr präzise Kanalschätzung, die für die Laufzeitmessung herangezogen wird, um die Entfernung zu messen.

Der IEEE 802.15.4a Standard hat 2007 zu diesem Zweck ein Protokoll entwickelt, das es ermöglicht preisgünstige und energieeffiziente Geräte zu entwerfen, die zusätzlich zur Datenkommunikation mit der Möglichkeit einer genauen Positionsbestimmung (<1m) ausgestattet sind. Der Standard stellt dabei sehr viele Parameter bereit die es den Herstellern erlauben untereinander kompatible und auch sichere Geräte zu entwerfen und dabei im Einklang mit den verschiedenen Regulierungsbehörden zu bleiben.

Die Laufzeitmessung macht solche Systeme zwar sicherer, aber trotzdem gibt es auch hier die Möglichkeit die Messung zu verfälschen. Ein Angreifer kann durch Manipulation der Signalpegel eine zeitliche Verschiebung der gesamten Kommunikation herbeiführen, was zu einer Reduzierung der gemessenen Laufzeit führt. Dadurch scheint der Schlüssel näher zu sein als er es in Wahrheit ist. Da solche Attacken an der niedersten physikalischen Ebene ansetzten, umgehen sie alle kryptografischen Bemühungen der Entwickler.

In meiner Arbeit beschäftige ich mich ausschließlich mit dem Energiedetektor, der einfachsten Implementation eines solchen Lokalisierungssystems, das aus dem Standard hervorgeht. Der Energie Detektor eignet sich der Einfachheit wegen besonders gut für solche "Keyless-Entry"-Systeme, da ein Schlüssel meistens in seiner Größe und seinem Energieverbrauch begrenzt ist. Die geringe Komplexität des Energiedetektors macht ihn aber auch anfälliger gegenüber solcher Relay-Attacken.

Um solche Attacken zu verhindern wurde eine Gegenmaßnahme entwickelt, welche eine Manipulation der Signalpegel erkennt. Die Methode basiert auf einen einfachen Hypothesen Test, welcher die Echtheit des Empfangenen Signals validiert. Diese Gegenmaßnahme macht es dem Angreifer nahezu unmöglich die Signalpegel zu verändern ohne das es bemerkt wird und verhindert so die Manipulation der Laufzeitmessung.

Acknowledgments

I want to thank Maxim, who gave me the opportunity to write my thesis on a very interesting and topical subject.

Special thanks for their patience and time spent also goes to my supervisors Thomas Gigl and Klaus Witrisal, without whose advice this would not have been possible. Furthermore, a big thank goes out to Paul Meissner and Bernhard Geiger for their helpful suggestions.

Finally, I would like to thank my mother for her support and trust during my years of study.

List of Abbreviations

AGC	Automatic Gain Control
ARX	Adversarial Receiver
ATX	Adversarial Transmitter
AWGN	Additive White Gaussian Noise
BER	Bit Error Rate
BPM	Burst Position Modulation
BPSK	Binary Phase Shift Keying
CIR	Channel Impulse Response
CLT	Central Limit Theorem
CSS	Chirp Spread Spectrum
DB	Distance Bounding
DPS	Dynamic Preamble Selection
ED	Early Detection
FOM	Figure of Merits
HRX	Honest Transmitter
HTX	Honest Transmitter
IEEE	Institute of Electrical and Electronics Engineers
IPI	Inter-Pulse-Interference
IR	Impulse Radio
ISI	Inter Symbol Interference
LC	Late Commit
LFSR	Linear feedback shift Register
LOS	Line Of Sight
LPRF	Low Pulse Repetition Frequency

LR	Low Rate
MAC	Media Acess Control
MAE	Mean Average Error
MPC	Multi Path Component
NLOS	Non-Line Of Sight
OOK	On-Off Keying
PDP	Power Delay Profile
PHR	Physical Header
PHY	Physical Layer
PPDU	Physical Protocol Data Unit
PPM	Pulse Position Modulation
PRF	Pulse Repetition Frequency
PSD	Power Spectral Density
PSDU	Physical Service Data Unit
RAP	Range Authentication Packet
RDEV	Ranging Device
RFRAME	Ranging Frame
RKS	Remote Keyless System
RMARKER	Ranging Marker
RNG	Ranging Packet Bit
RS	Reed Solomon
RTT	Round Trip Time
RV	Random Variable
SDS	Symmetric Double Sided
SEM	Security Enhanced Modulation
SFD	Start of Frame Delimiter

SHR	Synchronization Header
SNR	Signal to Noise Ratio
SYNC	Synchronization
TOA	Time of arrival
TOF	Time of Flight
TPS	Ternary Preamble Sequence
TWR	Two Way Ranging
UHF	Ultra High Frequency
UWB	Ultra WideBand
WPAN	Wireless Personal Area Network

Contents

1. Introduction

1.1. Motivation

For a better understanding of how such a relay attack can be mounted on an actual Remote Keyless System (RKS) system, Fig.1.1 illustrates a possible configuration. It is started with the assumption that the owner of the car puts his keyfob (Honest Transmitter (HRX)) on the desk inside the house and outside of the acceptance radius (green dashed circle). Therefore the base station in the car Honest Transmitter (HTX) checks the distance between the car and the keyfob and locks the car because HRX is out of range.

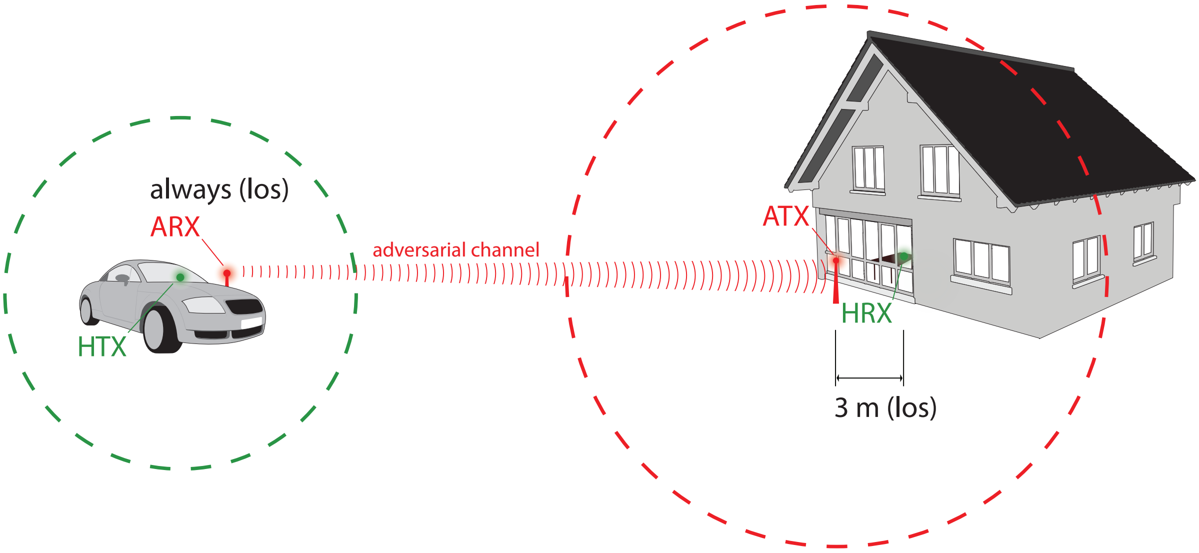


Figure 1.1.: Example of an relay attack against a RKS system

Then it is assumed that an attacker could initialize a new detection process by pressing the door handle of the car. But now the attacker relays the signal on the constructed adversarial channel over several meters and therefore expands the acceptance radius to his favour (red dashed circle). The car now admits the attacker access to the car and depending on the system, he could also start the engine and drive away.

In Fig.1.1 only a one-way transmission is given; the attacker, of course has to equally transfer the signal responses of HRX to HTX to achieve the desired distance reduction. However, this is not a problem for the attacker because he only has to implement 2 transceivers that switch their roles.

The assumption that the attacker can move very closely to the honest devices is well understood, because he can hide his setup e.g. in a suitcase. Therefore we can suppose that the attacker can always force a Line Of Sight (LOS) transmission. The attacker can also choose the configuration of his channel. Of course he does not need to worry about any regulations in terms of emitted energy or frequency bands and he can in principle also use a wired channel.

Anyone who thinks that these assumptions are only far-fetched, is mistaken because several cases with stolen cars and abandoned enemy equipment have been reported. There are many cars on the road that contain such insecure systems still based on Ultra High Frequency (UHF) technology. An attack on a UWB system is much more complicated, but still possible, due to the fact that the main principle of the relay attack is applicable.

The attack bases on the manipulation of the signal levels, which allows a shift of the whole data packet and therefore a distance decrease. This distance decrease depends mainly on the symbol length that is introduced by the modulation scheme of the used system.

Countermeasures proposed so far try to minimize the obtained distance decrease by changing the symbol length or switching to a other modulation schemes. This is always obtained with a deeper intervention in the system, which usually degrades the behaviour of the system.

The countermeasure that I propose leaves the system unchanged and focuses on the main problem, which is to detect the manipulation of the signal levels.

The goal of this work is to explain the developed method to counter this attacks and then to simulate it against different attack scenarios to show the effectiveness of the countermeasure.

It will always be focused on a realization with a non coherent receiver because thinking over the size of a keyfob makes it obvious that the system is restricted in terms of complexity and, moreover, in terms of power consumption.

Finally, I would like to refer the interested reader to [2][3] and the Ècole Polytechnique Fèdèrale de Lausanne, which have investigated such attacks in a more extended way and on several systems.

1.2. UWB-Technology for RKS

Ultra-wideband (UWB) Impulse Radio (IR) has become a popular research topic in wireless communications in recent years. The time-resolution introduced by the extremely short impulses, enables an accurate channel estimation and makes it therefore a perfect candidate for ranging devices. UWB signals are usually defined as signals having a bandwidth of at least $500MHz$ or at least 20% of the center frequency. The transmitted Power Spectral Density (PSD) is typically regulated by a peak limit of $0\,dBm/50MHz$ and an average limit of $-41.3\,dB$ averaged over $1ms$.

Sophisticated Rake receivers can deal very well with the pulse spreading, introduced by the multipath channel. Concerning the complexity of such receivers, they can be taken out of consideration for many applications.

Non-coherent receivers such as the energy detector, although labelled as sub-optimal, have many advantages over coherent receivers, where low-complexity and low-power plays an important role. Due to the loss of the phase information there follows a decreased Bit Error Rate (BER) performance, reduced spectral efficiency and reduced capability to exploit the multipath channel diversity compared to coherent receivers.

The IEEE 802.15.4a standard focuses on ultra-low power consumption, low cost, and localization with accuracies better than $1m$. The fact that the standard comprises a combination of Binary Phase Shift Keying (BPSK) and Pulse Position Modulation (PPM) modulation, makes it feasible to operate with both receiver structures. Moreover, the standard introduces a high variety of parameters, which is very helpful for manufacturers since they do not have to develop a system from scratch.

Especially the automotive sector focuses on RKSs, to provide their costumers with an additional service. These systems are mainly based on UHF technology, which makes them more susceptible to relay attacks. There are many studies on this subject, revealing relay distances up to several kilometers (see [1]). This reason and also the more precise ranging capability, forces many producers to switch to the UWB technology and the given standard. Naturally UWB devices are more robust to such attacks due to the very short pulses, but there always remains space for attackers since the bit decision is spread over several nanoseconds.

In this work it will by tried to evaluate these attacks against non-coherent receivers, always focusing on the mandatory mode that the standard proposes. Of course, the evaluation will be based on already given studies and then a countermeasure to the relay attack will be developed.

1.3. Outline

Chapter 2 shows the receiver architecture and the signal and channel model that are used in the remainder of the work and necessary for the following considerations. Afterwards the general approach of a distance decrease relay attack is described, which is then adapted on the standard. Moreover an alternative attack is defined that exploits the nature of the non coherent energy detector in the simplest way. Then a vulnerability of the standard is shown that leads to a diversification of the different receiver architectures and relay types that are incurred by.

Chapter 3 initially shows countermeasures that were proposed so far. Afterwards the developed countermeasure against the described relay attacks is explained step by step. Finally, an example of the implementation is shown.

Chapter 4 is devoted to the test statistics of the introduced receiver architecture and the simplifications specified therein. Thereafter the channel estimation process is described which is then needed for the ranging process and the countermeasure.

Chapter 5 contains the simulation results and a comparison to the statistical analysis. Finally, different attack scenarios are simulated and the performance of the countermeasure is evaluated.

2. Attacks Against the Physical Layer

Nowadays it often happens that Ranging Devices (RDEVs) operate in very security sensitive environments, for example in physical access control, localization or tracking of goods. For this applications it is absolutely crucial that the distance estimate of the two RDEVs can not be modified by fraudulent intruders.

The problem of attacks against facilities, was first apprehended by Brands and Chaum in [4]. To counter this attacks they invented a cryptographic Distance Bounding (DB) protocol to guarantee secure ranging. Such DB protocols allow a verifier to obtain a secure upper-bound on the distance to a prover. The essential element of a DB protocol is quite simple and consists of a single bit challenge and rapid-bit response. The advantage of this principle is that each bit of the prover is sent out immediately after receiving a bit from the verifier. The delay time for the responses enables the verifier to compute the upper-bound of the distance.

Due to the fact that in the IEEE 802.15.4a standard, every data packet has a fixed preamble, this rapid bit exchanges is outside the scope of the standard. The prefixing of the data packets by several preamble symbols opens a space for packet-level attacks.

In the remainder of this Chapter, first the receiver architecture and the channel model will be described in detail to give the reader a better understanding, how these attacks are mounted on the standard. Then the main principle of a general distance decreasing attack is explained briefly and next step this principle is adapted to the standard resulting in the distance decreasing relay attack that is focused on.

2.1. Receiver Architecture

The conventional energy detector, illustrated in Fig.2.1, measures the energy associated with the received signal over a specified time duration and bandwidth.

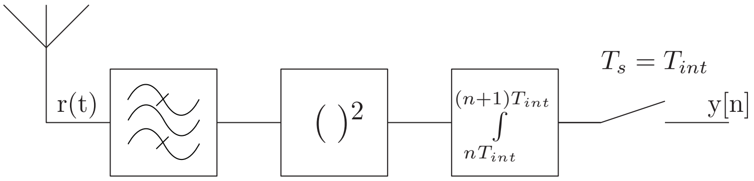


Figure 2.1.: Energy Detector

The received signal first passes a band-pass filter, followed by a square law device. After squaring, the signal is integrated for a fixed time interval T_{int}, which is equal to the sampling time T_s of the energy detector. For ranging purpose, the integration interval should not be too long to ensure an adequate resolution ($T_{int} = 2ns \approx 30cm$). For communication, the obtained samples can then be added up for a certain window, considering the delay spread of the channel. Summing up samples is therefore equal to increasing the integration interval.

In case of the energy detector, any information on the symbol phase is lost. Therefore it can not cope with the additional bit introduced by the BPSK modulation of the standard. On the other side the energy detector is less sensitive to inaccurate synchronization. Another advantage is that it does not need to sample the received signal at Nyquist rate, which is twice the signal bandwidth.

Of course, an attacker is not restricted to use this receiver architecture to reach his desired distance decrease, he also can use a more sophisticated coherent receiver. A experimental characterization of such a coherent receiver and a comparison to less complex receiver architectures is given in [5].

2.2. Signal Model

The generic signal model of the standard, is described more accurately in Appendix A. For the SHR preamble only the Synchronization (SYNC) part is considered because the Start of Frame Delimiter (SFD) only signals the transition to the data part and leaves no further information. Therefore the preamble part is described as

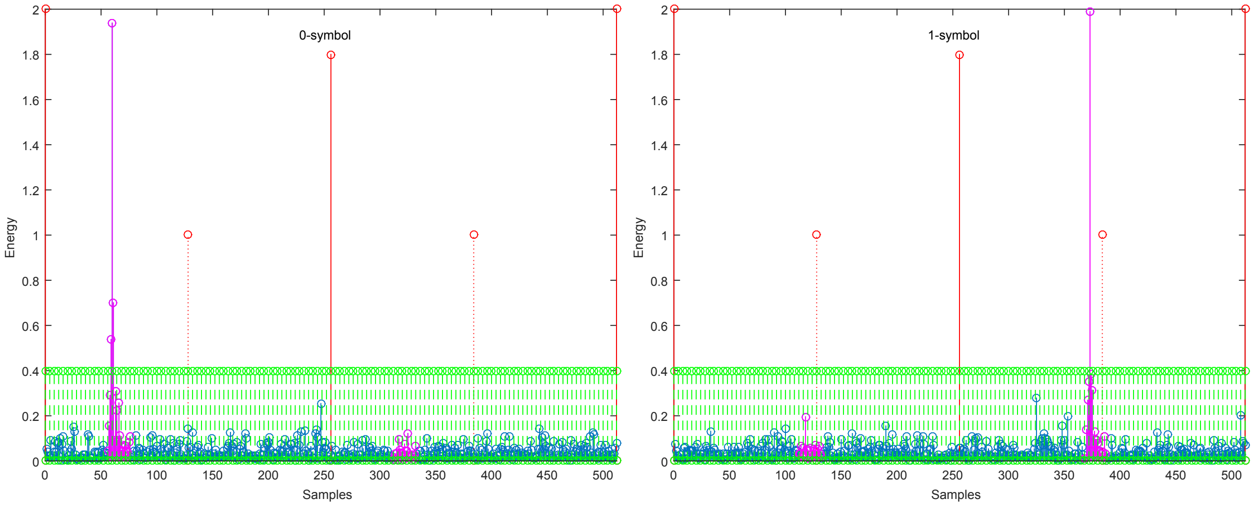
$$s_{preamble}(t) = \sqrt{\frac{2E_p}{N_{sync}N_N}} \Re\left\{\sum_{m=0}^{M-1} c_m\, \phi(t - mT_c)e^{j\omega_c t}\right\} \tag{2.1}$$

where N_{sync} is the number of symbols with N_N active chips per symbol, c_m is the mth element of the spreading code and ϕ is the used pulse shape.

The transmit waveform for the ith data symbol interval is given by

$$s_{data,i}(t) = \sqrt{2E_p}\Re\left\{(1 - 2g_{1,i}) \sum_{n=0}^{N-1} [(1 - 2s_{n+iN_{cpb}})\, \phi(t - g_{0,i}T_{BPM} - iT_{Burst} - nT_c)]e^{j\omega_c t}\right\} \tag{2.2}$$

where N_{cpb} is the number of chips per burst, $g_{0,i} \in \{0, 1\}$ represents the burst position and $g_{1,i} \in \{0, 1\}$ the burst polarity. $(1 - 2s_{n+iN_{cpb}})$ is the scrambling sequence derived from the linear feedback shift register and iT_{Burst} indicates the hopping position within the symbol interval. For an energy detector the position information $g_{0,i}T_{BPM}$, within one symbol represents the relevant data to decode.



(a) (b)

Figure 2.2.: Decoding process of the energy detector for a 0-symbol (a) and a 1-symbol (b)

In Fig.2.2 the decoding process of a 0-symbol (a) and a 1-symbol (b) for the energy detector is shown, where the green dashed lines represent the different hopping positions. The red lines show the boundaries of each symbol half and the red dotted lines the beginning of the

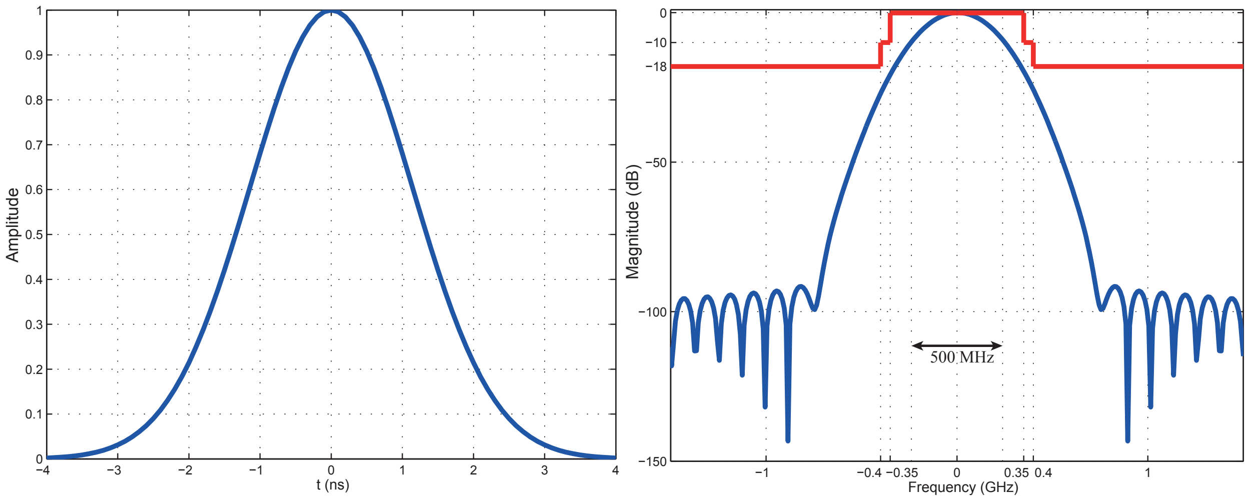


Figure 2.3.: Pulse shape in time domain (left) and frequency domain (right)

guard interval. The magenta samples are the N samples that are accumulated to the energy value of each symbol half that are given by the integration window $NT_s = T_{int}$. This 2 energy values are then compared to gain the decision over the whole symbol. The receiver works in the mandatory Low Pulse Repetition Frequency (LPRF) mode defined by the standard with a sampling time of $T_s = 2ns$ and uses an integration window of $T_{int} = 40ns$ to decode a single symbol.

After modulating the pulse shape illustrated in Fig.2.3 with the preamble and data sequence, the whole signal is modulated with a carrier waveform with frequency ω_c. The carrier frequency applied on the channel model, is fixed with $f_c = 4.5\,GHz$.

Throughout the whole simulations, a Gaussian pulse was used with a pulse duration of $T_p \approx 2ns$ and a $\beta = 4.3$. Mathematically, the pulse shape can be described as

$$\phi(t) = \frac{\sqrt{\pi}}{\alpha} e^{\frac{(-\pi t)^2}{\alpha^2}} \qquad with \qquad \alpha = \frac{\sqrt{\log 2}\beta T_p}{\sqrt{2}}. \tag{2.3}$$

With these parameters, the pulse fits optimally into the spectral mask defined by the standard and is therefore a compliant pulse. The 500 MHz bandwidth of the pulse is given at a magnitude of $-10\,dB$.

2.3. Channel Model

UWB propagation channels are characterized by strong clustering of the multipath component with respect to the time of arrival. The channel impulse response of the Saleh-Valenzuela model that is considered in this work, describes this processes as a tapped delay line as

$$h(t) = \sum_{l=0}^{L}\sum_{k=0}^{K} a_{k,l} e^{(j\varphi_{k,l})} \delta(t - T_l - \tau_{k,l}) \tag{2.4}$$

where $a_{k,l}$ is the tap weight of the k^{th} component in the lth cluster, T_l is the delay of the lth cluster, $\tau_{k,l}$ is the delay of the kth Multi Path Component (MPC) relative to the lth cluster arrival time. The phases $\varphi_{k,l}$ are uniformly distributed over the range $[0, 2\pi]$. L represents the number of clusters and is assumed to be Poisson-distributed.

The ray arrival times are modelled with a mixture of two Poisson processes as follows

$$\begin{aligned} p(\tau_{k,l}|\tau_{(k-1),l}) = {} & \beta\lambda_1\, exp\,[-\lambda_1(\tau_{k,l} - \tau_{(k-1),l})] \\ & + (\beta - 1)\lambda_2\, exp\,[-\lambda_2(\tau_{k,l} - \tau_{(k-1),l})] \qquad k \ > \ 0 \end{aligned} \tag{2.5}$$

where β is the mixture probability, while λ_1 and λ_2 are the ray arrival rates and in generally $T_0 = 0ns$ and $\tau_{0,l} = 0$.

The power of each multipath component decays exponentially, determined by Ω_l, the integrated energy of the lth cluster cluster and the intra-cluster decay time constant γ_l and is given as

$$E\{|a_{k,l}|^2\} = \Omega_l \, \frac{1}{\gamma_l[(1-\beta)\lambda_1 + \beta\lambda_2 + 1]} exp(-\tau_{k,l}/\gamma_l). \tag{2.6}$$

The cluster decay rates are found to depend linearly on the arrival time of the cluster

$$\gamma_l \propto k_\gamma T_l + \gamma_0 \tag{2.7}$$

where k_γ describes the increase of the decay constant with delay.

The mean (over the cluster shadowing) mean (over the small-scale fading) energy (normalized to γ_l), of the lth cluster in general follows an exponential decay with

$$10\log(\Omega_l) = 10\log(exp(-T_l/\Gamma)) + M_{cluster} \tag{2.8}$$

where $M_{cluster}$ is a normally distributed variable with standard deviation $\sigma_{cluster}$ around it and Γ the inter cluster decay constant.

The above parameters give a complete description of the Power Delay Profile (PDP) to be estimated. Fig.2.5 shows the average power delay profile for 100 channel realizations. For the PDP, the rms delay spread characterizes dispersion and the majority of measurements campaigns available in literature use this parameter defined as

$$S_\tau = \sqrt{\frac{\int\limits_{-\infty}^{\infty} P(\tau)\tau^2\,d\tau}{\int\limits_{-\infty}^{\infty} P(\tau)\,d\tau} - \left(\frac{\int\limits_{-\infty}^{\infty} P(\tau)\,d\tau}{\int\limits_{-\infty}^{\infty} P(\tau)\,d\tau}\right)^2}\,. \tag{2.9}$$

Considering the focus on short range communications, mobility of the components can be seen as restricted. Therefore it can be assumed that the channel is constant over several milliseconds. In the remainder of the work it will always be worked with the line of sight office (CM 3) scenario of the IEEE 802.15.4a standard with the following parameters (see. Table 2.1) for the PDP. A realization of the Channel Impulse Response (CIR) is depicted in Fig.2.4.

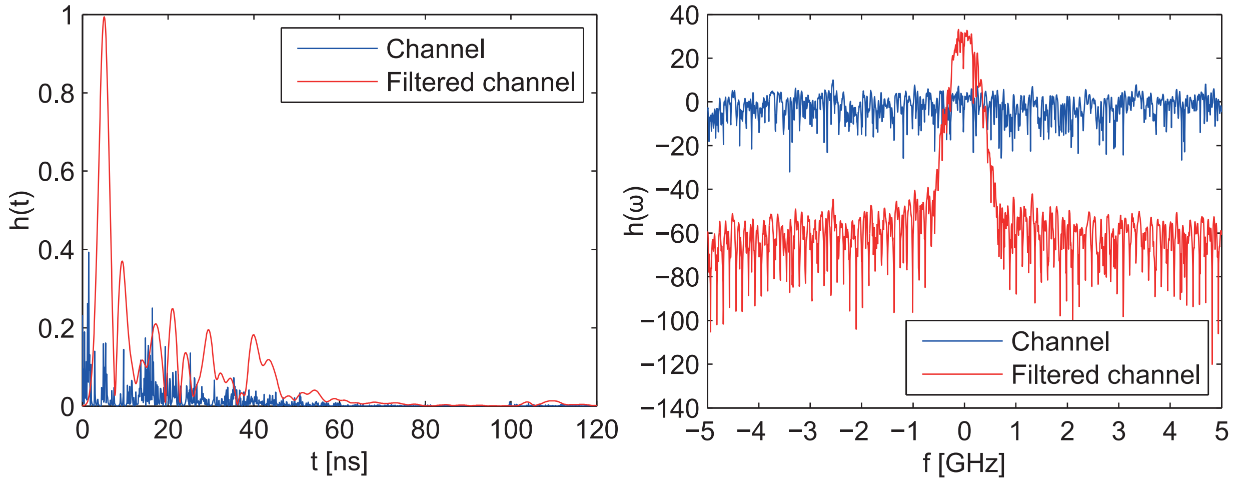


Figure 2.4.: CIR in time domain (left) and frequency domain (right)

After this the obtained CIR is filtered with the UWB pulse shape and then normalized to unit energy so that $||\tilde{g}(t)||^2 = 1$. For further characterizations of the channel model (including small scale fading) and an overview of the Saleh-Valenzuela model see [6][7].

$$\tilde{g}(t) = h(t) * \phi(t) = \sum_{i=0}^{L}\sum_{k=0}^{K} a_{k,l} e^{(j\varphi_{k,l})} \phi(t - T_L - \tau_{k,l}) \tag{2.10}$$

$$\tilde{g}(t) = \frac{g'(t)}{\sqrt{\sum\limits_{l=0}^{L}\sum\limits_{k=0}^{K} a_{k,l}^2}} \qquad \Rightarrow E_p = \sum_{l=0}^{L}\sum_{k=0}^{K} a_{k,l}^2 = 1$$

Power delay profile	Office LOS
$\bar{L}$	5.4
Λ [1/ns]	0.016
λ_1, λ_2 [1/ns], β	$0.19, 2.97, 0.0184$
Γ [ns]	14.6
k_γ	0
γ_0 [dB]	6.4
$\sigma_{cluster}$ [dB]	3

Table 2.1.: PDP parameters for the channel model

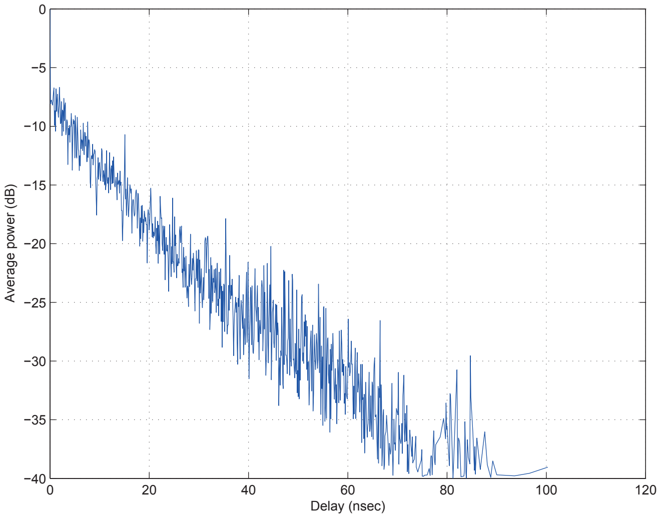


Figure 2.5.: Average Power Decay Profile over 100 channels

2.4. Distance Decreasing Relay Attack

For the current considerations it is focused on the distance decreasing relay attack. The attack is an external Physical Layer (PHY) attack against a secure ranging protocol. It is assumed that all the keys and nonces that are shared in the authentication process are unpredictable by the adversary. The relay attack focuses only on relaying and not on changing a whole Ranging Frame (RFRAME) during the Two Way Ranging (TWR) procedure. In literature the relay attack is also known as a man in the middle attack and is composed of an Adversarial Transmitter (ATX) and an Adversarial Receiver (ARX). In contrast the HTX is also defined as the honest verifier and HRX as the honest prover. The structure of the relay is depicted in Fig.2.6.

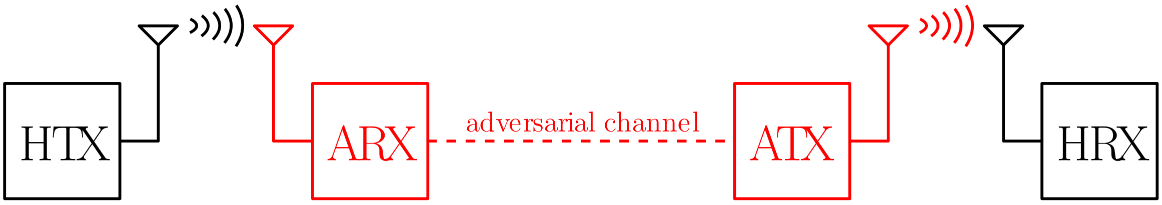


Figure 2.6.: Structure of the relay imposed by the attacker

The distance decreasing attacks were first introduced in [8]. These attacks can be mounted on the physical layer PHY of several communication systems and rely on two main principles:

ED

In the ED attack, ARX detects a PHY symbol of duration t_{dsym}, based only on the beginning part of this symbol $t_{ED} < t_{dsym}$, while still obtaining an acceptable BER. The attacker may not wait for the decision of which symbol has been received, concerning all the energy related to that symbol (see Fig.2.7(a)).

In contrast, a normal Energy detector wants to gather the whole energy spread by the channel, to achieve a considerable Signal to Noise Ratio (SNR). For this purpose, long integration windows T_{int} for non-coherent receivers are suggested by the IEEE 802.15.4a standard. This leads to a detection which is faster than that of a normal receiver because $T_{int} > t_{ED}$.

LC

In the LC attack, only the $(t_{dsym} - t_{LC})$-long-end-part of the symbol is modulated based on the intended value of the symbol (see Fig.2.7(b)). The attacker could send no energy for the initial time interval and then send a much stronger symbol during the final time interval reserved for the bit. This allows an ATX to delay the symbol decision to the latest possible moment by t_{LC}, where t_{LC} is the LC delay.

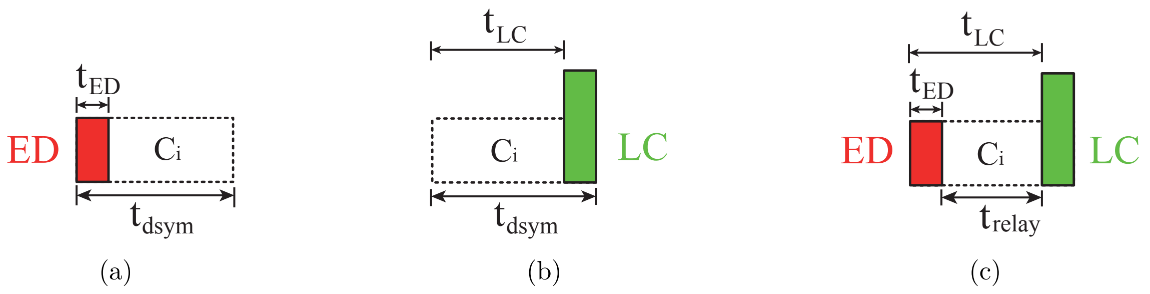


Figure 2.7.: ED on a symbol (a), LC on a symbol (b) and the resulting relay attack (c)

By combining the ED and LC attack the resulting relay time gain for the relay attack is given as $t_{relay} = t_{LC} - t_{ED}$ (see Fig.2.7(c)).

Figure 2.8 illustrates the main concept of the relay attack, where the green dashed line represents the maximum acceptance distance in the benign case. The attacker gains time when ARX detects the value of the challenge symbol (C_i) from HTX early on the symbol period (ED). Then ATX transmits a much stronger amplitude to HRX during the final time of the symbol interval (LC). The process is then repeated for the response symbol (R_i), with the difference that ARX and ATX swapping roles. This allows the attacker to extend the acceptance distance (radius) as shown in Fig.1.1.

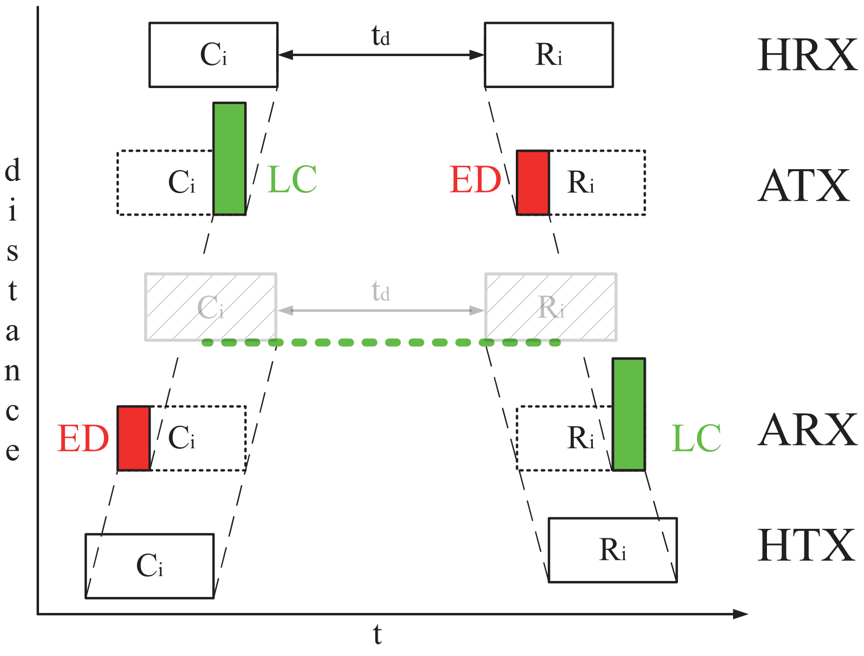


Figure 2.8.: Concept of the relay attack [8]

Further information on the distance decreasing attack can be found in [9].

2.5. Relay Attack adapted to the IEEE 802.15.4a

First it is noticed that Manuel Flury and Marcin Poturalski have adapted the idea of relay attacks on the standard; in this work it is referred to [10][11]. In the following Section we give a short introduction of how such an attack is mounted against the standard and derive the possible distance decrease an attacker is capable to achieve.

In the relay attack, the adversary relays a whole message between HTX and HRX, in such a way that HRX seems to be shifted back in time by $t_{trelay} = t_{LC} - t_{ED}$. To achieve such a relay attack it is essential that the whole packet (including the preamble and the payload part) is delayed in the right manner, so that the honest devices do not realize the fraudulent parties between them (see Fig.2.9).

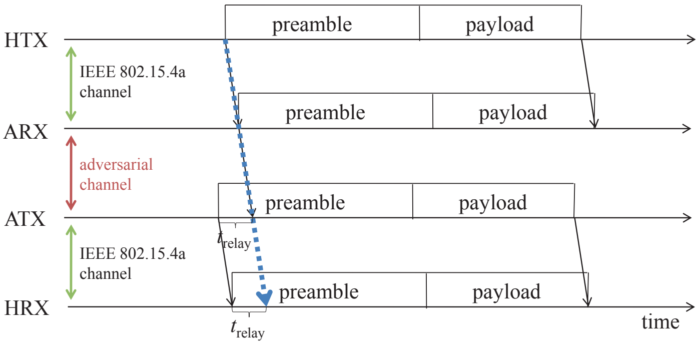


Figure 2.9.: Overview of the distance decreasing relay attack [11]

Therefore the measured distance between the honest devices is decreased by $c\, t_{relay}$. The time relay gain is of course the upper bound that an adversary can achieve theoretically, because there is to consider the processing delays of the attacker to decode the symbols. In the current investigations it is only focused on a single ranging message, because the other messages can be relayed in the same fashion.

2.5.1. Attack on the Preamble

Timing acquisition

For the adversary, timing acquisition is a very important step because it has to detect the presence of a Physical Protocol Data Unit (PPDU) on the wireless channel. This process also allows the receiver to determine the boundaries of an incoming symbol S_i (see Fig.2.10).

Upon timing acquisition ARX determines the time when receiving the first preamble symbol, which we call t_0. Furthermore it can be assumed that an adversary receiver is superior to a baseline receiver by using high-gain antennas and by moving very close to the honest devices and so forcing a LOS transmission. Therefore timing acquisition is determined in a few preamble cycles by correlating the incoming signal with the known preamble sequence. Meanwhile ATX remains silent until ARX signals that the timing acquisition was successful.

An honest receiver HRX does not count the incoming preamble symbols, it only needs enough symbols to synchronize correctly. When it is assumed that ATX is equipped with a superior set-up it also only needs a few preamble symbols to arrange this synchronization process; the remaining preamble symbols are always sufficient for HRX to synchronize, also assuming that ATX can move very closely to HRX for a better SNR.

Once timing acquisition is achieved ARX sends out signals to ATX which then switches to a transmission of a standard preamble. The delay τ to transmit the preamble to HTX depends on the whole relay time-gain and is chosen so that $T_{psym} - \tau = t_{relay}$.

This procedure is very essential for the attack because here the attacker begins to shift the PPDU by the time-gain t_{relay}. In most cases and also for this work the bottleneck of the attack is represented by the PSDU timings since the preamble symbols are much longer. Therefore the attacker has to choose t_{relay} dependent on the data symbols, because every section of the whole PPDU has to be shifted appropriately by the same time period to guarantee a successful processing of the whole ranging procedure.

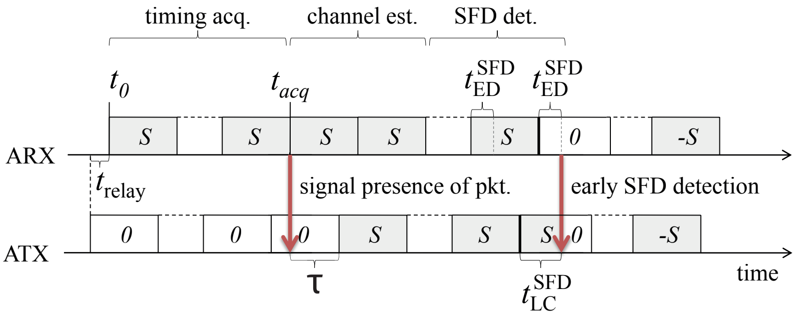


Figure 2.10.: Distance-decreasing relay attack on the preamble [11]

SFD early detection

The detection of the SFD is very crucial because it indicates the beginning of the data packet. The fact that the SFD sequence starts with a zero modulated preamble symbol favours the attacker, because he only has to implement a simple On-Off Keying (OOK) demodulation to detect the SFD prematurely. The maximal time to perform the detection depends on the series-connected zeros in the code sequence C_i and on the spreading length of the preamble symbol S_i.

ARX in the second stage performs early SFD detection and chooses an early SFD detection delay t_{ED}^{SFD}, by considering only the first portion of the symbol. Meanwhile ATX is always there sending the preamble symbols until ARX signals that the detection of the SFD was successful. Then ATX switches to transmitting of a standard compliant SFD, beginning from t_{LC}^{SFD} into the SFD (see Fig.2.10).

The late commit time t_{LC}^{SFD} is to be chosen appropriately, depending on the desired relay time gain $t_{relay} = t_{LC}^{SFD} - t_{ED}^{SFD}$. This determines the choice of τ, as $T_{psym} - \tau = (t_{LC}^{SFD} - t_{ED}^{SFD})$ mod T_{psym}. This in fact is the point where the attacker adjusts his shift. Assuming that in the LPRF mode a preamble symbol $T_{psym} = 3968ns$ long and the corresponding data symbol length $T_{dsym} = 1024ns$, the attacker has plenty of time to shift the packet to his favour.

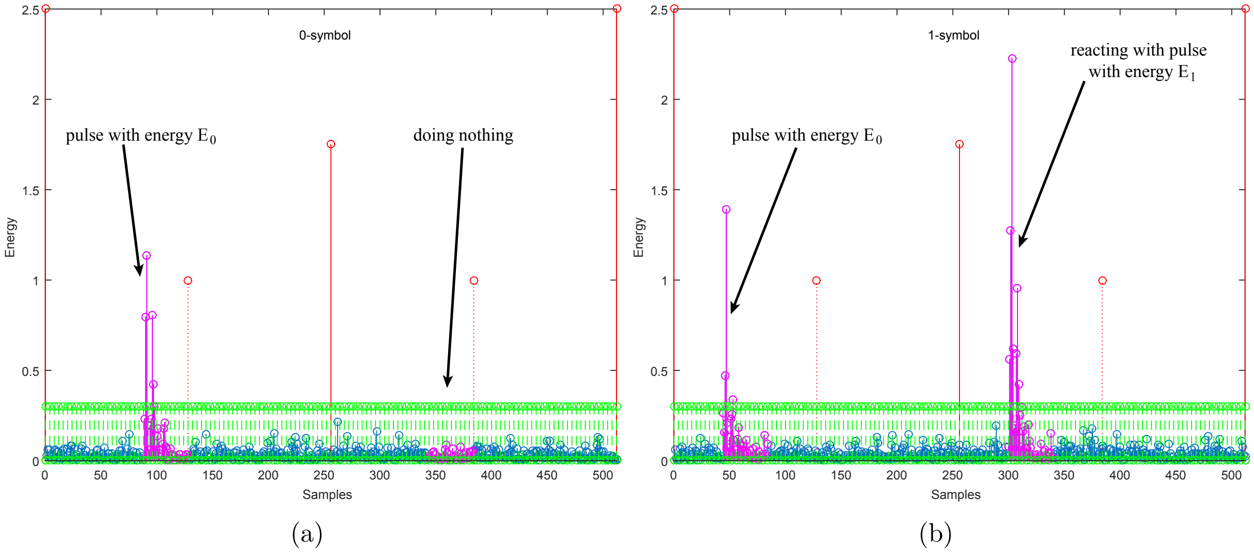
2.5.2. Attack on the Payload PSDU

When considering the Burst Position Modulation (BPM) modulation that is announced for non-coherent energy detectors in the standard, the symbol decision is always spread over a time of $T_{dsym}/2$. An adversary with a powerful setting can gain more time for relaying successfully than the half symbol duration, by mounting an ED and LC attack on every symbol.

For the mandatory LPRF mode, the attack on the payload is the bottleneck of the overall achieved relay time gain t_{relay}. The attack is always performed in the same manner. ARX performs an early detection attack with an early detection delay of $t_{ED}(g_{0,i}^{RX}) = t_{det}^{A}$, performing on-off keying demodulation on the first half of the symbol. Where $g_{0,i}^{RX}$ denotes the ith symbol decision of ARX and t_{det}^{A} is the detection time of ARX.

ARX implements a maximum likelihood hypothesis testing with a defined threshold for the signal and noise hypothesis, thus deciding only in the first half of the data symbol. With the early detection a detection time t_{det}^{A} can be achieved that is shorter than the normal T_{int} introduced by an honest receiver, whose integration window is adapted to the channel spread. After demodulating the symbol received from HTX, ARX signals the result to ATX.

Meanwhile ATX performs an LC attack and begins the transmission of a symbol $T_{dsym}/2$, before ARX signals the result based on the early detected symbol. The problem that ATX does not know what bit it should send to HRX is solved in a very simple way namely by always sending a pulse with energy E_0 in the first symbol half. Then ATX waits for the early detection result performed by ARX. Reacting on the received value from ARX it transmits a burst with higher energy $E_1 > E_0$, signaling a 1 to HRX or doing nothing (see Fig.2.11). For an honest receiver, this results in the same symbol, because it only compares the energies in the two blocks and decides accordingly.



(a)

(b)

Figure 2.11.: 0-symbol (a) and 1-symbol (b) under hostile influence of the relay attack

In that way an adversarial can simply exploit the BPM modulation of the standard and can achieve a late commit delay by at least $t_{LC}(g_{0,i}^{RX}) = T_{dsym}/2 + t_{PLC}$. Where t_{PLC} is the pulse late commit. Similarly to the normal LC described in Section 2.4, the pulse could be delayed to the latest moment, considering the integration window of HRX. For simplicity the time hopping positions are omitted, as they are the same for each symbol half. The relay time gain achieved with the whole relay attack is therefore given by $t_{relay} = t_{LC} - t_{ED}$. Fig.2.12 shows the upper bound of the relay attack on a single data symbol.

Comprising the relay time gain can be derived, achieved by an attacker against honest energy detector devices, operating in the LPRF mode of the standard ($T_{dsym} = 1024ns$) with

$$t_{relay} = t_{LC} - t_{ED} = \frac{T_{dsym}}{2} + t_{PLC} - t_{det}^{A} = 500ns \tag{2.11}$$

where $t_{PLC} = 0$ and $t_{det}^{A} = 12ns$. This corresponds to a distance decrease of $d_{relay} = 150m$. In Fig.2.12 the attack with an $t_{PLC} = 70ns$ is depicted, which results in a relay gain of $t_{relay} = 570ns$ and therefore a distance decrease of $d_{relay} = 171m$, which is near to the limits of feasibility.

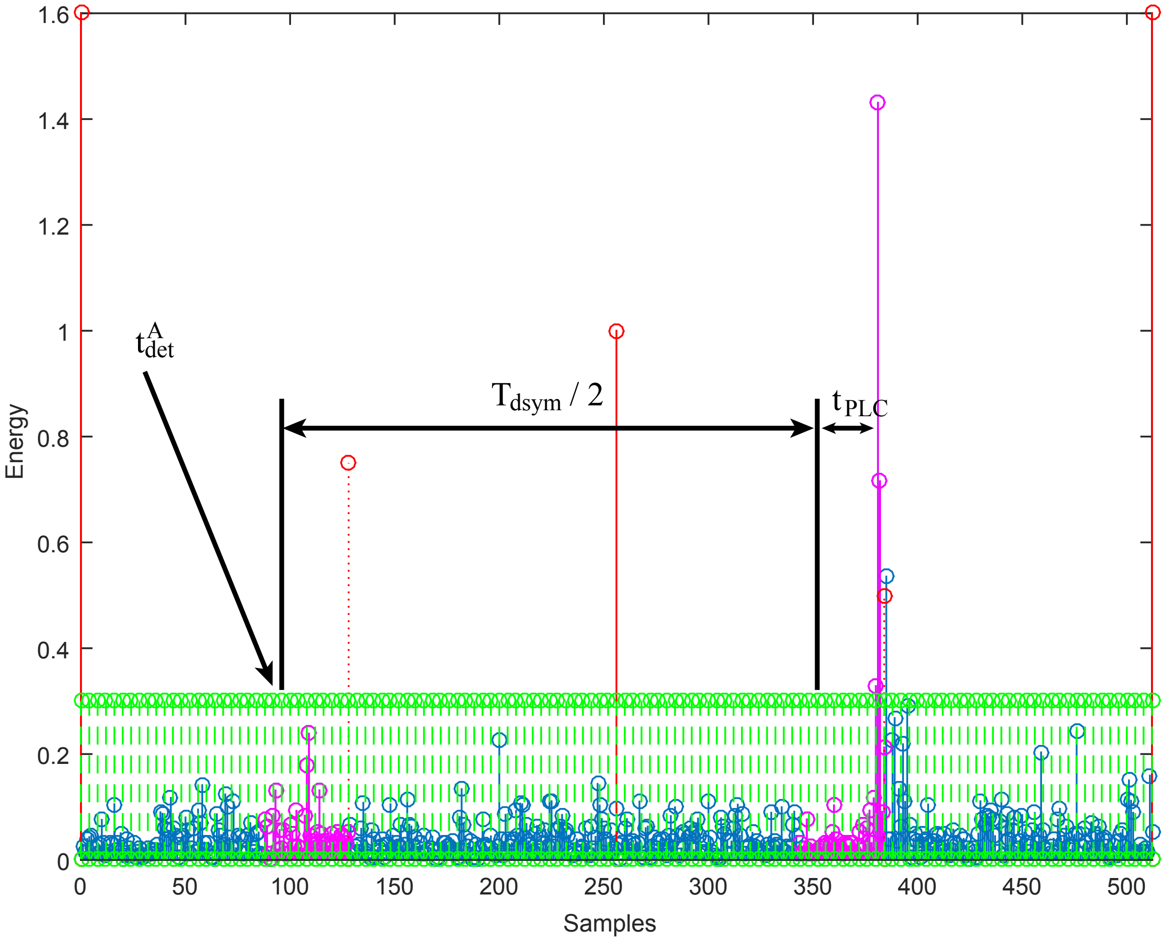


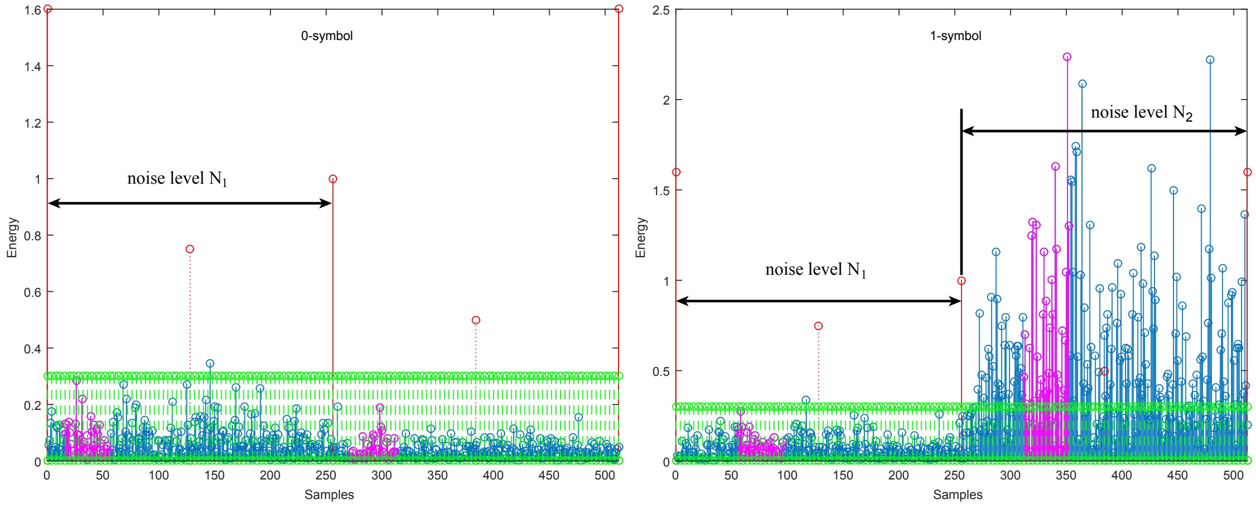
Figure 2.12.: Example of the manipulation boundaries on LPRF mode with $T_{int} = 80ns$

2.6. Attack with 2 different noise levels

The attacks discussed so far always assume that the hopping positions are public and therefore also known by the attacker. Of course, this is true when the honest devices operate with the parameters given by the standard but on the other side an encrypted spreading code increases the security level drastically. This encryption could be easily achieved by changing the binary sequence with which the Linear feedback shift Register (LFSR) is initialized. The attacker therefore can not determine the beginning of the slot in which the pulse is sent.

This problem can be solved in a very simple way, by sending in the symbol half always a fixed noise level N_1. Then ATX waits for the early detection result performed by ARX, who has only to check if the first symbol quarter contains the signal or only noise samples. Reacting on the received value from ARX it transmits a noise level with higher mean energy N_2, signaling a 1 to HTX or doing nothing.

The relay time gain achieved with this attack is determined by the length of the guard interval t_{guard} that is of course only a quarter of the symbol duration. Assuming that the devices operate in the LPRF mode this is always $t_{relay} = T_{dsym}/4 = 256ns$, which corresponds to a distance decrease of $d_{relay} \approx 77m$.



(a)

(b)

Figure 2.13.: 0-symbol (a) and 1-symbol (b) manipulated with 2 noise levels

This attack shows how easy it is to overcome an energy detector. An attacker can impose an arbitrarily signal and/or noise level to impose the decision on a honest device.

2.7. ED and LC attack on every symbol half

An attacker can also mount a ED and LC attack on every symbol half. Of course, this attack is not so efficient as the proposed relay attack in 2.4, although he has not to manipulate every first symbol half. The fact that the attacker has to react only on the symbol half that contains the signal samples makes it more difficult to detect the manipulation. Therefore we consider this attack as a good benchmark for the proposed countermeasure.

An attacker can also switch to another demodulation scheme and using OOK with a fixed threshold, instead of BPM demodulation, so the detection time can be made arbitrarily short. Fig.2.14 illustrates the described ED attack using OOK for demodulation.

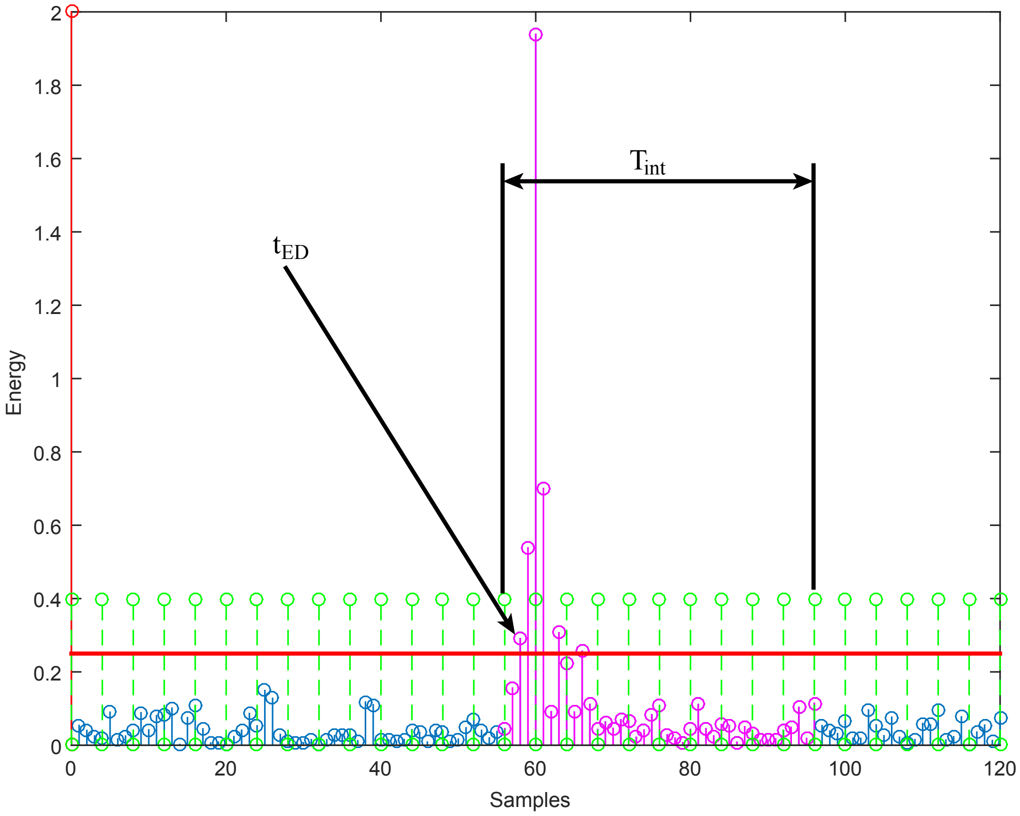


Figure 2.14.: ED with $t_{ED} = 6ns$ for the attacker and $T_{int} = 80ns$ for the honest receiver

Fig.2.15 illustrates the described LC attack, where the attacker needs only the last 5 samples $5\,T_s = 10ns$ to impose the decision to the honest receiver.

The achieved time gain of the distance decrease attack is given by $t_d = t_{LC} - t_{ED}$, of course it is strongly depending on the integration window T_{int} a honest device uses. Assuming that $t_{ED} = 6ns$ and $t_{LC} = 70ns$ the distance decrease is given as

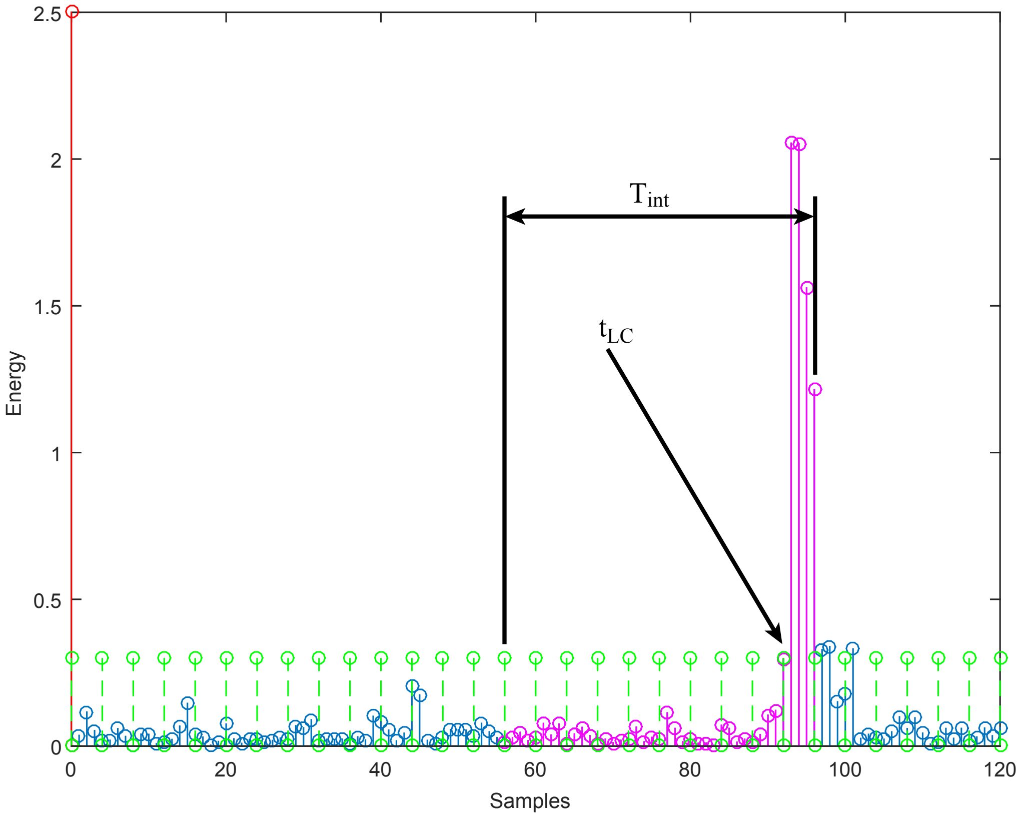


Figure 2.15.: LC with $t_{LC} = 70ns$ for the attacker and $T_{int} = 80ns$ for the honest receiver

$$t_d = t_{LC} - t_{ED} = 70ns - 6ns = 64ns \tag{2.12}$$

$$d_d = c\, t_d = 3 \cdot 10^8 \frac{m}{s} \cdot 64ns = 19.2m \tag{2.13}$$

2.8. Vulnerability of the IEEE 802.15.4a

In this Chapter a vulnerability of the standard that have been unveiled and published in [11] will be shortly indicated.

The vulnerability is given by the encoding process of the PSDU. The convolutional encoder generates both, the position bits g_0 for the BPM modulation and also the polarity bits g_1 for the BPSK modulation.

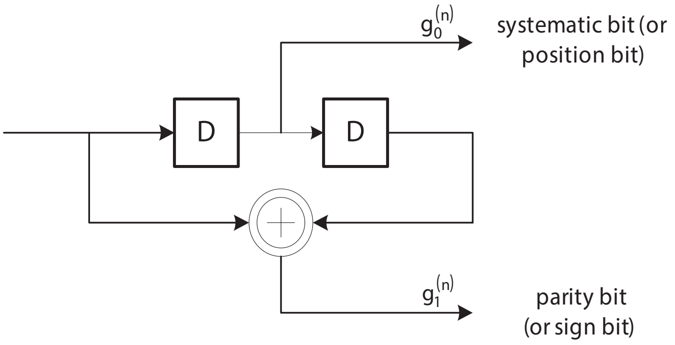


Figure 2.16.: Systematic convolutional encoder [12]

The inner convolutional encoder introduced by the standard and depicted in Fig.2.16 uses the rate $R = 1/2$ code with generator polynomials $g_0 = [0\,1\,0]_2$ and $g_1 = [1\,0\,1]_2$. Upon the transmission of each PPDU, the encoder shall be initialized to the all zero state. The problem considering the structure of the convolutional encoder is that the ith parity bit carries information about the $i + 1$th position bit and then it is

$$g_{1,i} = g_{0,i-1} \oplus g_{0,i+1} \tag{2.14}$$

where the operator $\oplus$ indicates a modulo two addition.

The polarity bits can only be decoded by a coherent receiver because by squaring the energy detector the phase information is lost. An attacker equipped with a coherent Rake receiver therefore can exploit this fact and has an advance in knowledge of 1 bit against an energy detector. The time-gain an attacker can achieve with this depends on the hopping and/or symbol position of the preceding symbol and is at least $T_{guard} = T_{dsym}/4$.

This stems from the fact that in the worst case the pulse in the preceding symbol can lie in the last hopping position T_{hop}^{MAX} of the second symbol half and is therefore given in the 1-symbol case (see Fig.2.17). This results in a ED delay of $t_{ED} = -T_{dsym}/2 + T_{hop}^{MAX} + t_{det}^{A}$. The LC is the same as for the standard attack and therefore the total relay time gain is given as

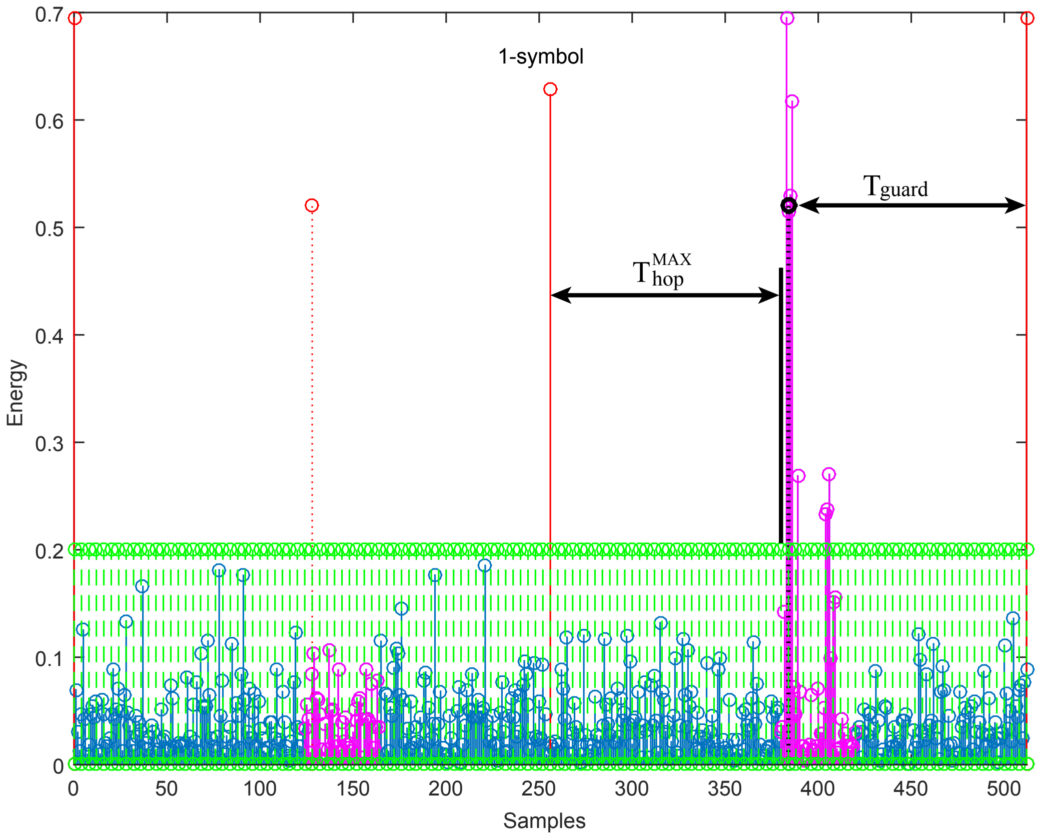


Figure 2.17.: Additional distance decrease if the adversary uses a coherent receiver

$$t_{relay} = t_{LC} - t_{ED} = \frac{T_{dsym}}{2} + t_{PLC} - \left(-\frac{T_{dsym}}{2} + T_{hop}^{MAX} + t_{det}^{A}\right) \tag{2.15}$$

$$= T_{dsym} + t_{PLC} - T_{hop}^{MAX} - t_{det}^{A} \approx 764ns \tag{2.16}$$

where $t_{PLC} = 0$ and $t_{det}^{A} = 12ns$. This corresponds to a distance decrease of $d_{relay} \approx 230m$.

2.9. Relay types and resulting distance decrease

Considering the assumption that an adversary equipped with a coherent Rake receiver can gather an additional relay time gain leads to further investigations on the different types of the relay and on the distance decrease they can achieve. In most cases HTX can be seen as the base station that has of course fewer restrictions in terms of complexity and power consumption. Therefore the case that at least one of the honest devices could be a Rake receiver must also be taken under consideration. The different types of relays that are relevant are shown in Fig.2.18. The first 2 relay types have already been discussed so far.

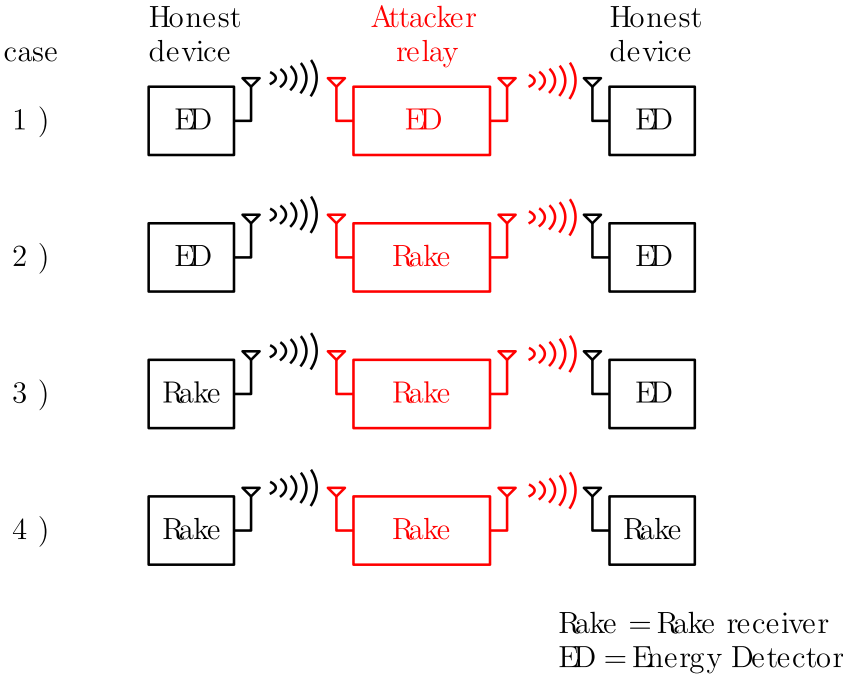


Figure 2.18.: Relevant relay set-ups

In the scenario Rake against Rake the attacker only can gain a relay time gain of $t_{relay} = t_{PLC} - t^{A}_{det}$. Since the honest receiver is also capable of decoding the parity bits $g_{1,i}$ the attacker hast to relay both bits correctly to avoid bit errors. The maximal achievable relay time gain is therefore given by the BPSK symbol duration, which is obtained by the channel spread. The attacker can achieve a time gain on a early detection of the symbol compared to the normal detection time $t_{relay} = t_{PLC} - t^{A}_{det} < t^{H}_{det}$ of the honest rake receiver.

Assuming the processing delays of the attacker and a detection time $t_{det} \approx 50ns$ introduced by honest rake receiver, this leaves only little margin for the adversary. Therefore it is assumed that in the best case for the attacker he can achieve a distance decrease in the order of $10m$.

Considering case 3 that is depicted in Fig.2.18 the adversary equipped with a Rake receiver competes against an energy detector on the forward path of the transmission but on the reply he encounters the honest rake receiver. The relay time gains discussed so far have always considered a symmetric relay set up. Therefore the distance decrease achieved against the energy detector has to be halved and is given by

$$d_{relay} = c\left(\frac{t_{relay}}{2}\right) = c\left(\frac{764ns}{2}\right) \approx 115m \tag{2.17}$$

assuming that the distance decrease against the Rake receiver is negligible.

The scenario Rake against energy detector is not taken into account because the adversary in this case has no chance to manipulate anything.

The achieved relay time gains and the resulting distance decrease for different relay set-ups are summarized in Table 2.2. It is assumed that the pulse late commit is fixed to $t_{PLC} = 0$ and the detection time of the adversary is given by $t^{A}_{det} = 12ns$.

case	relay time gain	distance decrease
1)	$\frac{T_{dsym}}{2} + t_{PLC} - t^{A}_{det}$	$150m$
2)	$T_{dsym} + t_{PLC} - T^{MAX}_{hop} - t^{A}_{det}$	$230m$
3)	$(T_{dsym} + t_{PLC} - T^{MAX}_{hop} - t^{A}_{det})/2$	$115m$
4)	$t_{PLC} - t^{A}_{det} < t^{H}_{det}$	$10m$

Table 2.2.: Summary of the distance decrease obtained by different relay set-ups

On more detailed information considering the effort an attacker has to make in terms of additional SNR, see [2].

3. Countermeasure Proposal

3.1. State of the Art

Private Ranging

The additional private ranging option, introduced by the standard and shortly described in Section 4.3, should avoid such attacks by the Dynamic Preamble Selection (DPS). Considering the relay attack, the private ranging mode makes the attack on the preamble slightly harder. Because each of the devices uses one out of eight preambles independently, the guessing probability reduces to 1/64, which makes guessing rather unnecessary. The adversarial can use eight parallel correlators to detect a packet on the channel. This can be done entirely in the digital domain and therefore involves only a little effort for the attacker that has only to choose the one with the highest correlation output. What additionally helps the adversary is the fact that these codes were designed to have minimum cross-correlation properties.

Except the minimal effort for the adversary, the private ranging mode uses the 127-chip ternary codes. The standard introduces these codes only with a Pulse Repetition Frequency (PRF) of $125MHz$ (referring to [12, p.70]), which means that every $8ns$ a preamble pulse is sent. This implies strong Inter Symbol Interference (ISI) when channel spreads of about $60ns$ are assumed. The private ranging mode therefore only seems to be designed for more sophisticated coherent receivers that are less susceptible to attacks anyway.

Switching to optional modes of the standard

Since the relay time gain depends directly of the symbol duration the simplest countermeasure is certainly to reduce the symbol duration and switch to a non-mandatory mode of the standard. Of course, this is a possible solution under certain circumstances, but the underlying problem remains unsolved. On the other side reducing the symbol duration to a level that makes relay attacks obsolete would introduce strong ISI, which degrades the performance of the system drastically.

Early Detection (ED) at HTX

This proposal deals with an ED at HTX where the receiver takes into account only the beginning part of the symbol. This ED can be achieved with OOK demodulation at the honest receiver. This countermeasure leaves an attacker nearly no chance for a distance decrease because the decision is always made in the first symbol half, which prevents a LC attack. Introducing this countermeasure would be in contrast with the BPM modulation scheme of the standard and the OOK demodulation would also degrade the system behaviour. For further information on this countermeasure see [11].

Security Enhanced Modulation (SEM)

SEM transmits a pulse in the first time slot independent of the transmit symbol. The pulse is scaled by $1/\sqrt{2}$ leading to an energy of $E_b/2$. Then in the second time slot, for the 0-symbol nothing is transmitted and for the 1-symbol the burst with energy E_b. This way, the first time slot does not allow to predict the overall signal in contrast to the BPM modulation scheme. However, the downside of SEM lies in the increased BER at the receiver. The energy difference of the symbol halves is reduced to $\pm E_b/2$, which leads to a loss of $3dB$ in the BER performance. For further information on this countermeasure see [13].

3.2. Overview

The proposals to mitigate relay attacks of course, are possible solutions under certain circumstances, but the underlying problem remains mainly unsolved.

Operating with the LPRF guarantees many advantages considering the complexity and the power consumption of e.g. RKS, and therefore it makes sense to rely on such a mandatory mode and to introduce only a few modifications to increase security aspects. The challenge therefore is to introduce a countermeasure that can achieve a very high security level by not changing the operating mode of the standard and by not introducing complex digital signal processing algorithms.

The general idea behind the countermeasure is to prevent the manipulation of the signal and noise levels in a data symbol. The attacker would have to modify the signal levels because he can react appropriately only in this way. The way such manipulations would be detected is with a very simple hypothesis test. The idea is to compare the decoded energies in each integration window for symbol s_0 and s_1 with the test statistics of the receiver. Due to the fact that the ranging process is performed anyway and this equals to a channel estimation, the energy within each symbol period containing the UWB pulse (or multiple pulses in a burst N_{cpb}) can be determined. It can also be assumed that every receiver makes some sort of noise estimation for adjusting the thresholds to detect the incoming packet.

Therefore it can be considered that the parameters for making such a hypothesis test can be estimated easily by every receiver and therefore the additional effort is only to save 2 energy values for every symbol in a packet and then to decide if a packet is manipulated or not. Knowing that the number of bits in a packet is restricted to 1016 data bits, the amount

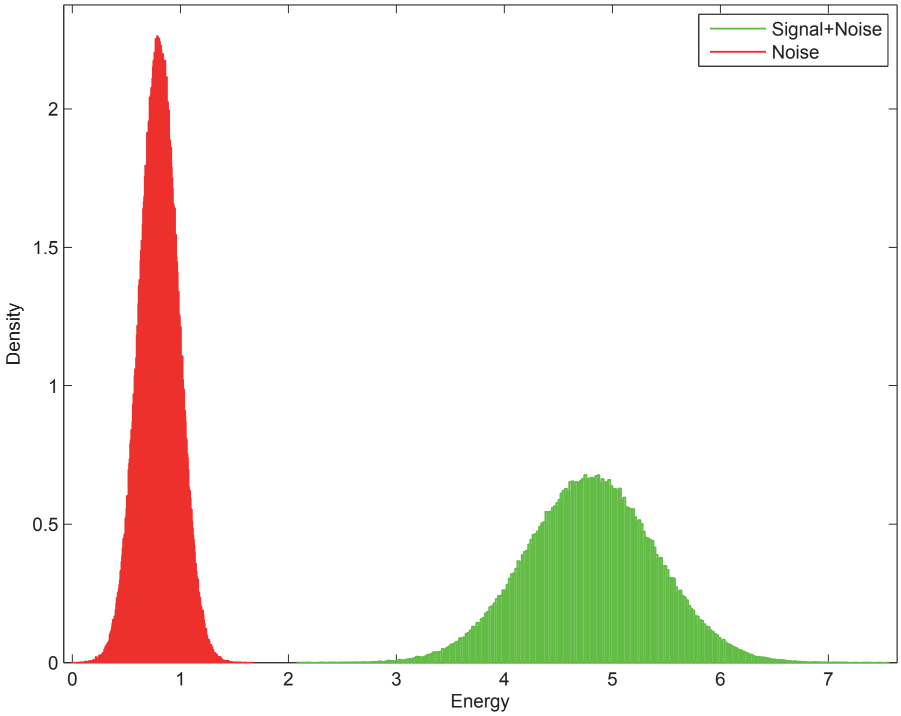


Figure 3.1.: Signal distribution for AWGN assumption with $E_b/N_0 = 20dB$

of accumulated energy values is quite manageable.

In Fig.3.1, we can see the *noise* and $signal + noise$ distributions of a given SNR. Testing against these distributions would not make much sense because it leaves too much space for manipulations, because the variance of both hypotheses is quite large. To counter this problem the mean of all demodulated symbols are simply taken in a whole packet (representing the sample size), to reduce the variance by N. This allows us to formulate a hypothesis that enables an evaluation whether the signals are found in the expected interval.

The assumptions made so far are very straight forward, but the fact that the standard uses N_{cpb} pulses in a burst that are spaced only by a chip period, leaves some problems. The BPM modulation scheme, in fact, introduces two fading effects that are superimposed. First, the random spreading codes lead to random Inter-Pulse-Interference (IPI), which increases the variance of the energies, referring to Section 4.1. Secondly, small scale variations of the channel impulse response must be considered. A closer evaluation of these effects is out of scope of this work. For further information see [14].

It has to be considered that the random spreading code has no influence on the signal mean. So we can suppose that the mean energy in every data packet is equivalent to the energy estimated in the preamble and then multiplied with the number of pulses per burst N_{cpb}. The derivation that leads to this assumption is stated in Appendix B.

3.3. Problem Statement

In this Section the test procedure for the hypothesis test is explained step by step on a more abstract way. For the detailed derivation of the signal and noise statistics and the channel estimation process the reader is directed to Appendix C.

Step 1: Parameter estimation, to define the 2 Hypotheses

The most important step for evaluating the test statistics is the channel estimation[1]. In this process the energy of the received pulse is estimated doing the preamble detection. This is achieved by first correlating the incoming signal with the known deterministic binary preamble sequence.

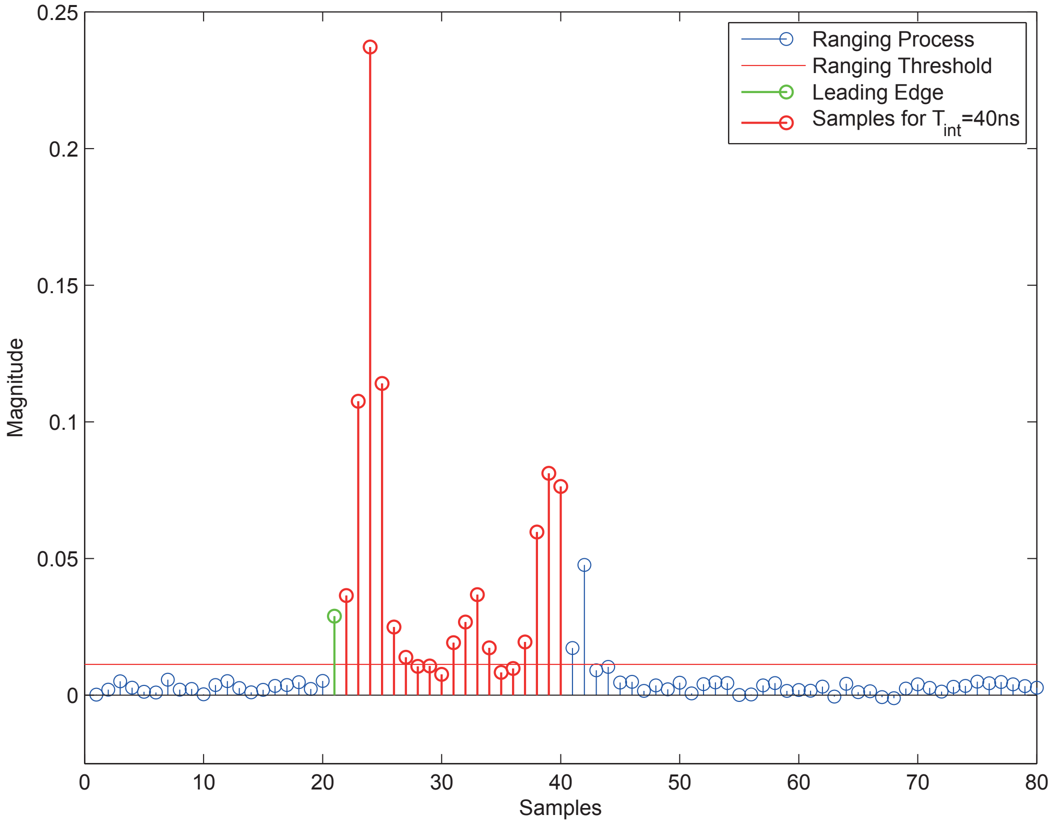


Figure 3.2.: Ranging Process with $T_{int} = 2ns$ and $E_b/N_0 = 20dB$

After this the obtained channel estimate is averaged over N_{sync} repetitions to minimize the variance introduced by the noise process. To achieve an adequate resolution of the channel estimate and even more importantly of a reliable leading edge detection, the integration

[1] By saying channel estimation, the squared and filtered CIR is meant that is equal to the power delay profile (PDP).

period (sampling period T_s) of the receiver should be in the range of the pulse duration ($T_{int} = T_s = 2ns$). Of course the samples of the estimate must be added up to achieve the same length that is used for the integration windows in the data demodulation process. For the leading edge detection a simple search back algorithm, stated also in Section 4.3 is applied.

The result of such a channel estimate is depicted in Fig.3.2 , where the red points are samples that are taken into consideration for the energy estimate E_{est} to establish the signal hypothesis. Of course, also the data part is corrupted by noise and a mean and variance to describe the amplitude distributions can be defined.

Finally, a very general form for the 2 hypotheses can be stated as

$$H_0 : \quad x[n] = w[n] \tag{3.1}$$

$$H_1 : \quad x[n] = s[n] + w[n]. \tag{3.2}$$

Where Equation 3.1 represents the only *noise* case and Equation, 3.2 is the *signal* + *noise* case.

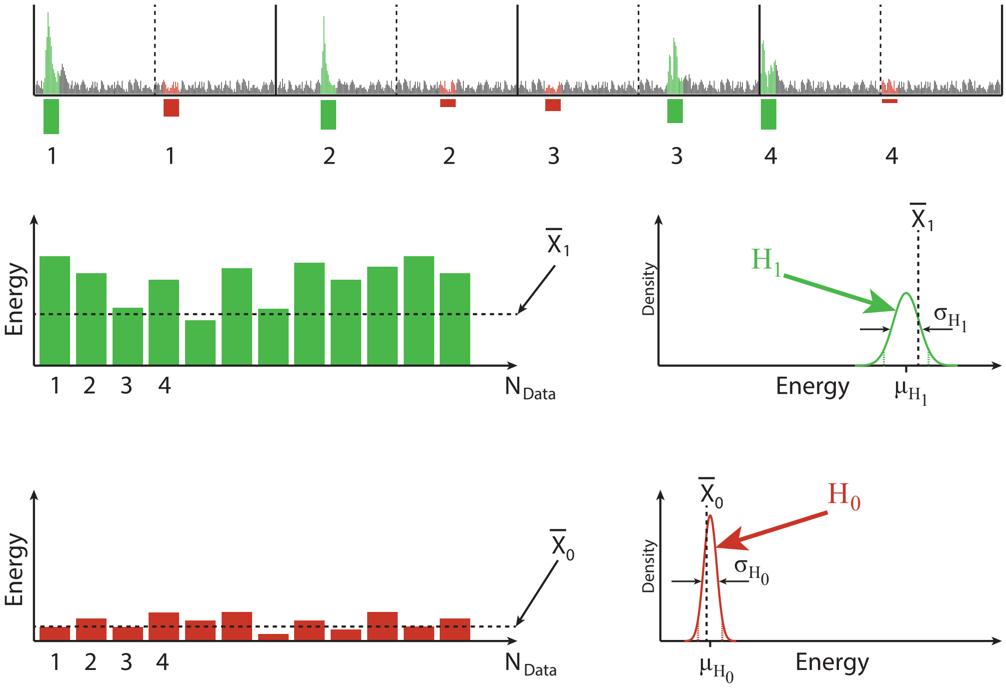


Figure 3.3.: Procedure of the countermeasure

The *noise* hypothesis H_0 depends on the noise PSD N_0 at the input, the bandwidth of the bandpass filter B and the integration time T_{int} introduced by the receiver.

The *signal* + *noise* hypothesis H_1 depends on the signal energy E_b which determines the signal-by-signal term and the noise-only term as in hypothesis H_0. The squaring operation of the receiver introduces also an additional signal-by-noise cross term. The derivation of each term is described in detail in Equation C.2.

The channel estimation E_{est} that is needed to estimate the energy E_b introduced by the signal is also affected by noise; although it is minimized by the averaging process, it has to be taken into consideration for the hypotheses. Therefore mean and variance for the noise in the channel estimation are defined as $\mu_{est,noise}$ and $\sigma^2_{est,noise}$.

And in a more explicit way including the statistical parameters derived in Appendix C, there is

$$H_0: \quad \mu_{H_0} = N_0 T_{int} B \qquad \sigma^2_{H_0} = N_0^2 T_{int} B \tag{3.3}$$

$$H_1: \quad \mu_{H_1} = N_0 T_{int} B + E_{est} \qquad \sigma^2_{H_1} = N_0^2 T_{int} B + 2 E_{est} N_0. \tag{3.4}$$

Coming to this point the first step of the countermeasure is completed by gathering the parameter necessary to define the 2 hypotheses.

Step 2: Estimation of the mean energy over N_{data} symbols

The second step is to derive the mean of the energy, decoded in every symbol half of the N_{data} symbols that were transmitted in a packet, by

$$\bar{X}_0 = \frac{1}{N_{data}} \sum_{i=0}^{N_{data}-1} w_0[n] \tag{3.5}$$

$$\bar{X}_1 = \frac{1}{N_{data}} \sum_{i=0}^{N_{data}-1} s[n] + w_1[n]. \tag{3.6}$$

where $w_1[n]$ includes also the signal by noise term introduced by the energy detector. Therefore there is a sample for every decoded symbol for the *noise* only and the *signal* + *noise*, with which the sample mean can be computed to compare with the proper hypothesis. T_{int} here represents the integration window for the data symbols, or equally sums up N samples of T_s, with T_s being the sampling interval of the energy detector. This process is illustrated in Fig.3.3.

Step 3: Finalize the decision

In a final step the decision boundaries must be stated to decide if it is dealt with a standard signal (the mean energy derived from step 2 lies inside the interval) or a manipulated once (the mean energy derived from step 2 lies outside the interval). Depending on the security level achieved, a confidence interval in which the sample mean should lie can then be defined to consider it not manipulated.

Choosing this interval too small naturally leaves a higher rate of false alarms P_{fa}. False alarms for current considerations are when the hypothesis is rejected and it is dealt with a manipulated signal, when in fact the hypothesis is true and there is no manipulation. In literature this is also known as a Type 1 error, referring to [15].

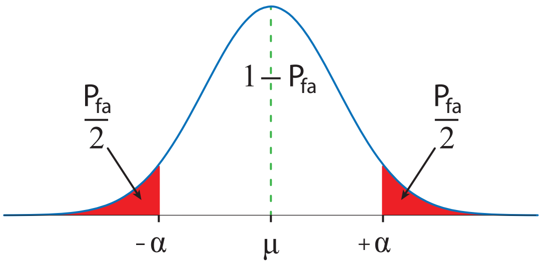


Figure 3.4.: Hypothesis with confidence intervals

By defining a certain P_{fa}, the upper and lower threshold in which the sample mean should lie can then be derived for each hypothesis as

$$P_{fa} = P\{-\alpha > \bar{X} > \alpha; H\} \tag{3.7}$$

$$= \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{-\alpha} e^{-\frac{1}{2}t^2}\, dt + \frac{1}{\sqrt{2\pi}} \int_{\alpha}^{\infty} e^{-\frac{1}{2}t^2}\, dt \tag{3.8}$$

$$= 1 - Q(-\alpha) + Q(\alpha) \tag{3.9}$$

and since $Q(-x) = 1 - Q(x)$ there is

$$P_{fa} = 2\, Q(\alpha). \tag{3.10}$$

By standardizing the hypothesis parameter with $Z = \left(\frac{X-\mu}{\sigma}\right)$, there is

$$P_{fa_0} = 2\, Q_0 \left(\frac{\alpha_0 - \mu_{H_0}}{\sqrt{\frac{\sigma^2_{H_0}}{N}}} \right) \qquad P_{fa_1} = 2\, Q_1 \left(\frac{\alpha_1 - (\mu_{H_1} - \mu_{est,noise})}{\sqrt{\frac{\sigma^2_{H_1}}{N} + \sigma^2_{est,noise}}} \right). \tag{3.11}$$

Then the thresholds can be computed by taking the inverse of the Q-function and solve the equation as

$$\alpha_0 = Q_0^{-1} \left(\frac{P_{fa_0}}{2} \right) \sqrt{\frac{\sigma^2_{H_0}}{N}} + \mu_{H_0} \tag{3.12}$$

$$\alpha_1 = Q_1^{-1} \left(\frac{P_{fa_1}}{2} \right) \sqrt{\frac{\sigma^2_{H_1}}{N} + \sigma^2_{est,noise}} + (\mu_{H_1} + \mu_{est,noise})\,. \tag{3.13}$$

For a probability of false alarm $P_{fa} = 0.05 = 5\%$, we obtain a probability for each tail of $\frac{P_{fa}}{2} = 0.025 = 2.5\%$ and therefore a probability of detection $P_D = (1 - P_{fa}) = 0.95 = 95\%$. Fig. 3.4 illustrates the method of defining a confidence interval on a hypothesis. The limits for the upper and lower boundaries, where $\bar{X}$ should lie can be computed as

$$\mu_{H_0} - \alpha_0 \sqrt{\frac{\sigma^2_{H_0}}{N}} < \bar{X}_0 < \mu_{H_0} + \alpha_0 \sqrt{\frac{\sigma^2_{H_0}}{N}} \tag{3.14}$$

$$(\mu_{H_1} - \mu_{est,noise}) - \alpha_1 \sqrt{\frac{\sigma^2_{H_1}}{N} + \sigma^2_{est,noise}} < \bar{X}_1 < (\mu_{H_1} - \mu_{est,noise}) + \alpha_1 \sqrt{\frac{\sigma^2_{H_1}}{N} + \sigma^2_{est,noise}}. \tag{3.15}$$

Fig.3.5 shows an example of the countermeasure for a given channel realization with $N_{data} = 399$ and $E_b/N_0 = 16dB$. The two sample means fit into the given confidence intervals of the estimated hypotheses and no manipulation is detected.

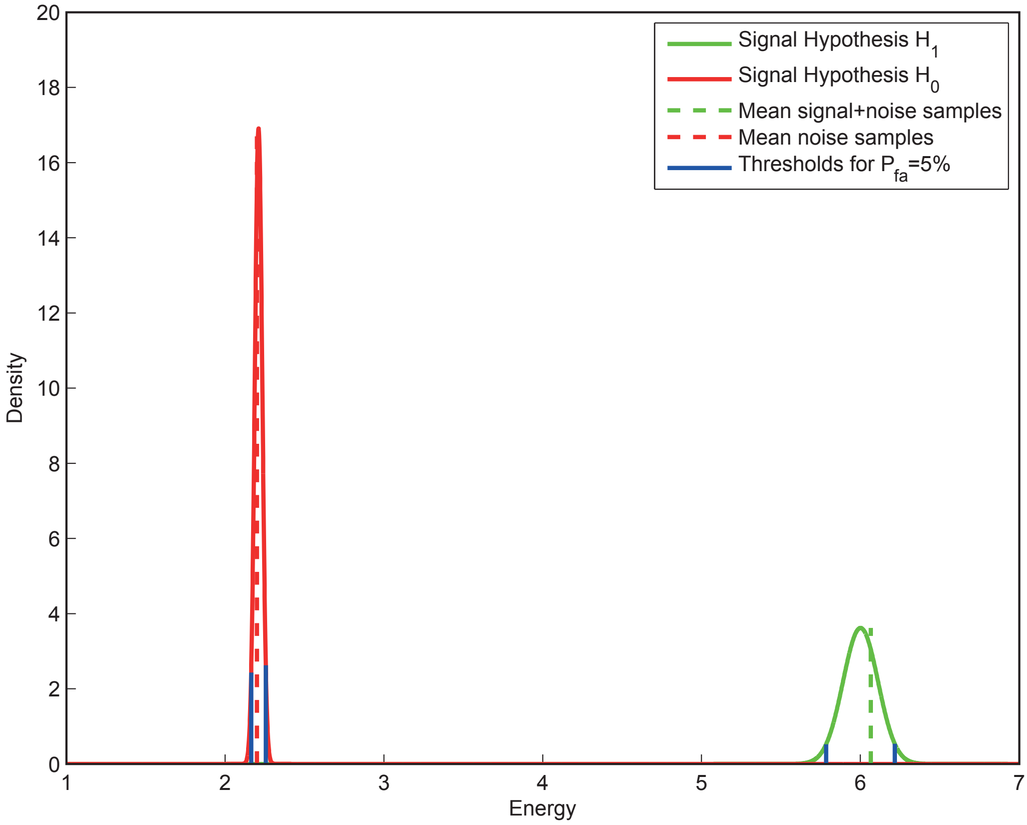


Figure 3.5.: Countermeasure for a single channel realization

4. Statistical Analysis

4.1. Test Statistics

Analysis BER vs. Probability of detection

The test statistic that determines the performance of an attacker is given by the BER that he obtains by manipulating the transmitted symbols (bits) at a certain SNR. Whereas the countermeasure is benchmarked on the probability of detection at a certain SNR.

BER Analysis

A commonly used method for deriving the BER of the energy detector is the Gaussian Approximation which is used in many communication systems [16]. This method makes use of the Central Limit Theorem (CLT) Approach, which says that the sum of N i.i.d random variables with finite mean and variance approaches a normal distribution when N is large enough. In other words, when the time bandwidth product $2TW$ of the χ^2-distribution is large enough, it can be assumed Gaussian within a certain confidence interval, see Fig.C.3.

Due to non-coherent detection, the phase information of the signal is lost and therefore the performance obtained of a binary antipodal signal is changed. The energy detector makes its symbol wise decision depending on the difference of accumulated energy in the two symbol halfs (see Fig.4.1) as

$$y[n] = y_1[n] - y_2[n] = \int\limits_{nT_{int}}^{(n+1)T_{int}} r^2(t)\,dt - \int\limits_{(n+\frac{T_{dsym}}{2})T_{int}}^{(n+\frac{T_{dsym}}{2}+1)T_{int}} r^2(t)\,dt. \tag{4.1}$$

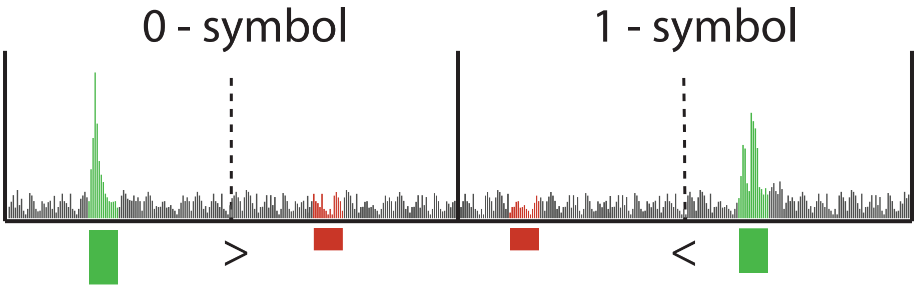


Figure 4.1.: Symbol wise decision of the energy detector

For simplicity, it is assumed that the pulse is transmitted in the first symbol half and in the second symbol half there are the noise only samples, which is defined as the zero symbol s_0. Assuming there is no ISI the mean value and variance of the approximated Gaussian variables are (referencing to Section C)

$$y_1 \sim \mathcal{N}(E_b + N_0 T_{int} B, N_0^2 T_{int} B + 2E_b N_0) \tag{4.2}$$

$$y_2 \sim \mathcal{N}(N_0 T_{int} B, N_0^2 T_{int} B). \tag{4.3}$$

Considering that $y = y_1 - y_2$, the density function for the zero symbol s_0 can be defined as

$$y \mid s_0 \sim \mathcal{N}(E_b, 2N_0^2 T_{int} B + 2E_b N_0) \tag{4.4}$$

$$f(y \mid s_0) = \frac{1}{\sqrt{2\pi\sigma_v^2}} e^{-(y-E_b)^2/2\sigma_v^2}. \tag{4.5}$$

where σ_v^2 is the variance of the normal distribution given in equation 4.4.
Vice versa if the pulse is transmitted in the second half

$$y_1 \sim \mathcal{N}(N_0 T_{int} B, N_0^2 T_{int} B) \tag{4.6}$$

$$y_2 \sim \mathcal{N}(E_b + N_0 T_{int} B, N_0^2 T_{int} B + 2E_b N_0) \tag{4.7}$$

and for the symbol s_1 there is

$$y \mid s_1 \sim \mathcal{N}(-E_b, 2N_0^2 T_{int} B + 2E_b N_0) \tag{4.8}$$

$$f(y \mid s_1) = \frac{1}{\sqrt{2\pi\sigma_v^2}} e^{-(y+E_b)^2/2\sigma_v^2}. \tag{4.9}$$

In the 2-PPM modulation scheme one symbol equals one bit and therefore the BER can be computed as

$$P_e = P(s_0, y < \gamma) + P(s_1, y > \gamma) \tag{4.10}$$

$$= P(e \mid s_0)P(s_0) + P(e \mid s_1)P(s_1) \tag{4.11}$$

$$= P(s_0) \int\limits_{-\infty}^{\gamma} \frac{1}{\sqrt{2\pi}\sigma_0} e^{-\frac{(y-\mu_O)^2}{2\sigma_0^2}}\, dy \;+\; P(s_1) \int\limits_{\gamma}^{-\infty} \frac{1}{\sqrt{2\pi}\sigma_1} e^{-\frac{(y-\mu_1)^2}{2\sigma_1^2}}\, dy \tag{4.12}$$

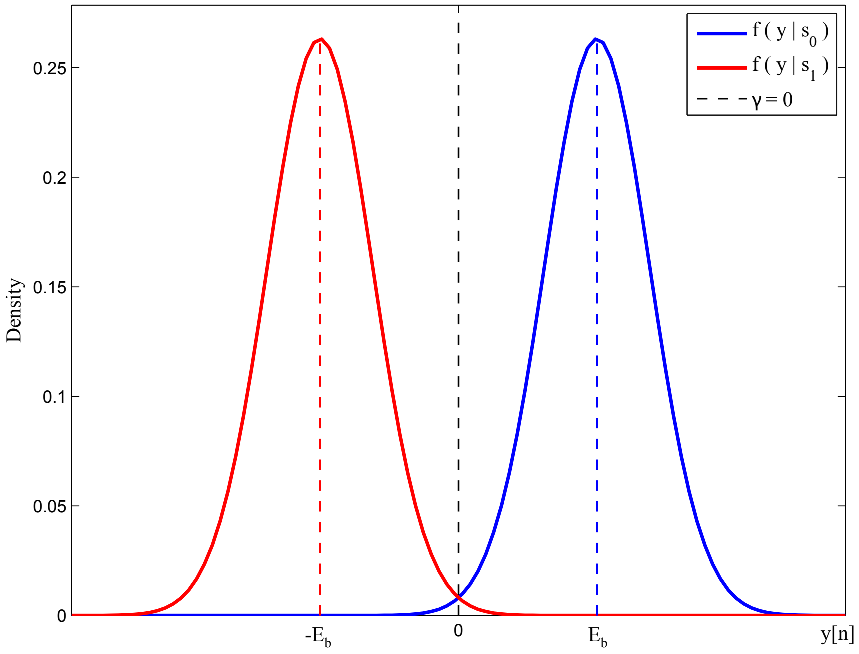


Figure 4.2.: Conditional PDF of two symbols $E_b/N_0 = 15dB$

where γ is the decision threshold. Substituting the mean value and variance

$$\mu_0 = E_b \qquad \sigma_0^2 = 2N_0^2 T_{int} B + 2E_b N_0 \tag{4.13}$$

$$\mu_1 = -E_b \qquad \sigma_1^2 = 2N_0^2 T_{int} B + 2E_b N_0 \tag{4.14}$$

$$P_e = P(s_0)\, Q\left(\frac{E_b - \gamma}{\sqrt{2N_0^2 T_{int} B + 2E_b N_0}}\right) + P(s_1)\, Q\left(\frac{E_b + \gamma}{\sqrt{2N_0^2 T_{int} B + 2E_b N_0}}\right) \tag{4.15}$$

is obtained.

The optimum MAP detector bases its decision on the posterior probability metrics represented as

$$PM(y, s_m) = f(y \mid s_m) P(s_m) \qquad m = 0, 1. \tag{4.16}$$

If $PM(y, s_0) > PM(y, s_1)$, s_0 is selected as the transmitted symbol, otherwise s_1. Therefore the decision rule may be expressed as

$$\frac{PM(y, s_0)}{PM(y, s_1)} \overset{s_0}{\underset{s_1}{\gtrless}} \tag{4.17}$$

$$\frac{P(s_0)}{P(s_1)} e^{\frac{(y+E_b)^2-(y-E_b)^2}{\sqrt{2N_0^2T_{int}B+2E_bN_0}}} \gtrless 1 \tag{4.18}$$

$$\frac{(y^2 + 2E_{by} + E_b^2 - y^2 + 2E_{by} - E_b^2)}{\sqrt{2N_0^2T_{int}B + 2E_bN_0}} \gtrless \ln\left(\frac{P(s_0)}{P(s_1)}\right) \tag{4.19}$$

$$y \overset{s_0}{\underset{s_1}{\gtrless}} \frac{\sqrt{2N_0^2T_{int} + 2E_bN_0}}{4E_b} \ln\left(\frac{P(s_0)}{P(s_1)}\right) = \gamma. \tag{4.20}$$

For the symbol encoding process, with equally likely symbols $P(s_0) = P(s_1) = 1/2$ and given integration window, there is for the bit error rate

$$P_e = Q\left(\frac{E_b}{\sqrt{2N_0^2T_{int}B + 2E_bN_0}}\right) \tag{4.21}$$

and the optimal threshold with $\gamma = 0$. For more detailed information see [17].

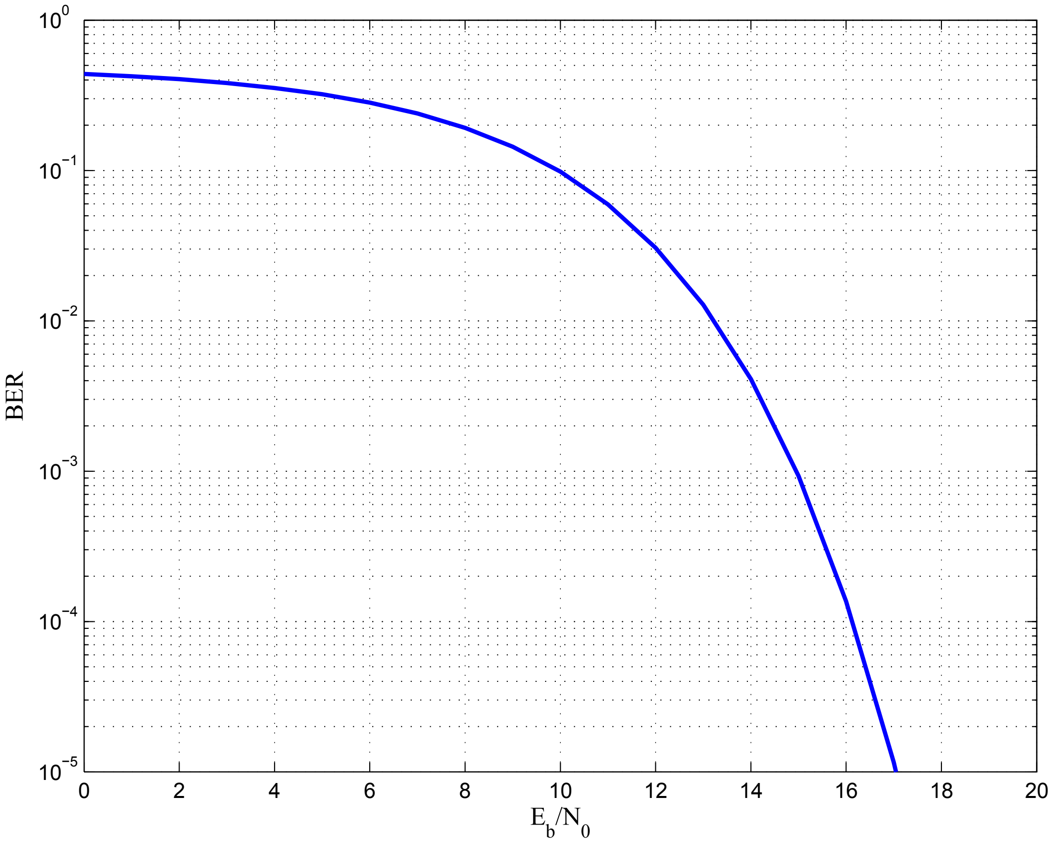


Figure 4.3.: BER for $T_{int} = 40ns$ and $B = 500MHz$

Probability of detection

The test statistics that determines the performance of the countermeasure is defined as the probability of detection at a certain SNR. The simulations where always made over N_{sim} different channel realizations for every SNR. When no manipulation is given the probability should converge to the predefined P_{fa}. Of course, this can only be assumed at higher SNR regions, where the BER is almost zero. This is obvious, because any bit error leads to an exchange of an energy sample in the respective symbol that then distorts the mean value and induces a wrong decision considering the hypothesis. An exemplary outcome of such a simulation is depicted in Fig.4.4. The green line shows the percentage of simulated channel realizations, where the accumulated sample mean from the data symbols $\bar{X}_1$ does not lie in the interval defined by the $signal + noise$ hypothesis H_1 and the given P_{fa}. Therefore the red line shows the percentage of simulated channel realizations, where the accumulated sample mean from the data symbols $\bar{X}_0$ does not lie in the interval defined by the *noise* hypothesis H_0 and the given P_{fa}.

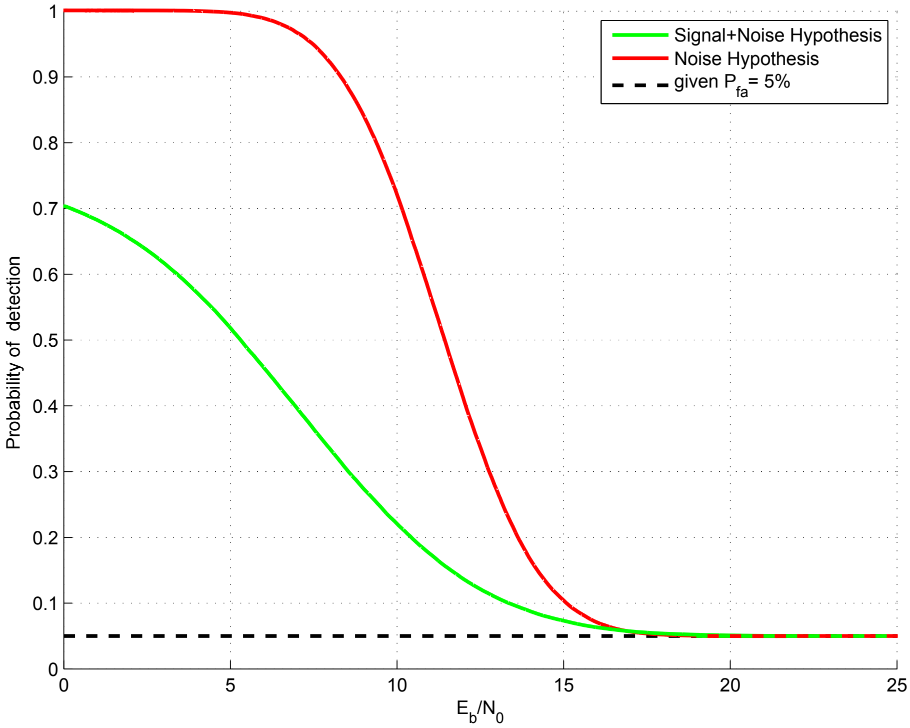


Figure 4.4.: Exemplary outcome of the countermeasure for the benign case

A manipulation is given when the attacker modifies the signal levels to his favour. In this case the countermeasure should detect the manipulated packets independent of the given channel realization and the probability of detection should converge to 1 or 100%.

4.2. Channel Estimation Process

The ranging process is the most important part for the current considerations, because the main part of the statistics are established on the channel estimate. In this Section only a short review is given on how the channel is estimated; for a deeper look into this topic, see [18][19].

In the previous Section the receiver steps have been described in detail, starting by the filter and ending with the integration over a short time interval T_{int}, that defines the sampling period T_s. Naturally, the integration time for the preamble part and the data part need not to be the same as a greater integration time leads to less operations at the receiver. For the statistics this results only by summing up independent identical distributed samples, and therefore in a multiplication by N depending on the samples that the integration window contains.

More crucial is the fact that the integration time affects the ranging resolution and the Mean Average Error (MAE) that is greater or equal to $T_i/\sqrt{12}$. This fact forces to very short integration periods to achieve an accurate range estimate.

After integration, the energy samples $y[n]$ were correlated with a reference symbol $\tilde{c}[n]$ and then averaged over N_{sync} symbols. The reference symbol $\tilde{c}[n]$ is obtained by spreading the used preamble code C_i introduced by the transmitter. Since it is operated with a non-coherent receiver the preamble code C_i first has to be converted to a binary code $\tilde{C_i} = 2|C_i|-1$ and than spread as

$$\tilde{c} = \tilde{C_i} \otimes \delta_L[n]. \tag{4.22}$$

For simplicity it is assumed that the chip period T_c is identical to the integration period T_{int}, otherwise the spreading factor has to be computed as LT_c/T_{int}. The 2 preamble sequences and their cross correlation are illustrated in Fig.4.5.

Correlation

In Section C the statistics for the different terms an energy detector imposes on the received signal have already been derived. From the correlation stage the PDP estimate of the channel should by achieved to determine the leading edge, which is needed for the Ranging Marker (RMARKER) and finally for the computation of the TOF and the distance between 2 RDEVs. Considering 4.5 it can be seen that the cross-correlation is only non-zero for a delay of zero. Therefore in the sum over $N_{pcode}L$ chips, only N_{pcode} are relevant, because the symbol spreading introduces only zeros that give no signal contributions. The output of the correlator stage is then given by

$$g[m] = \sum_{n=0}^{(N_{pcode}L)-1} \tilde{C_n} y[n-m] \qquad \Rightarrow \qquad g[m] = \sum_{n=0}^{N_{pcode}-1} \tilde{C_n} y[n-m]. \tag{4.23}$$

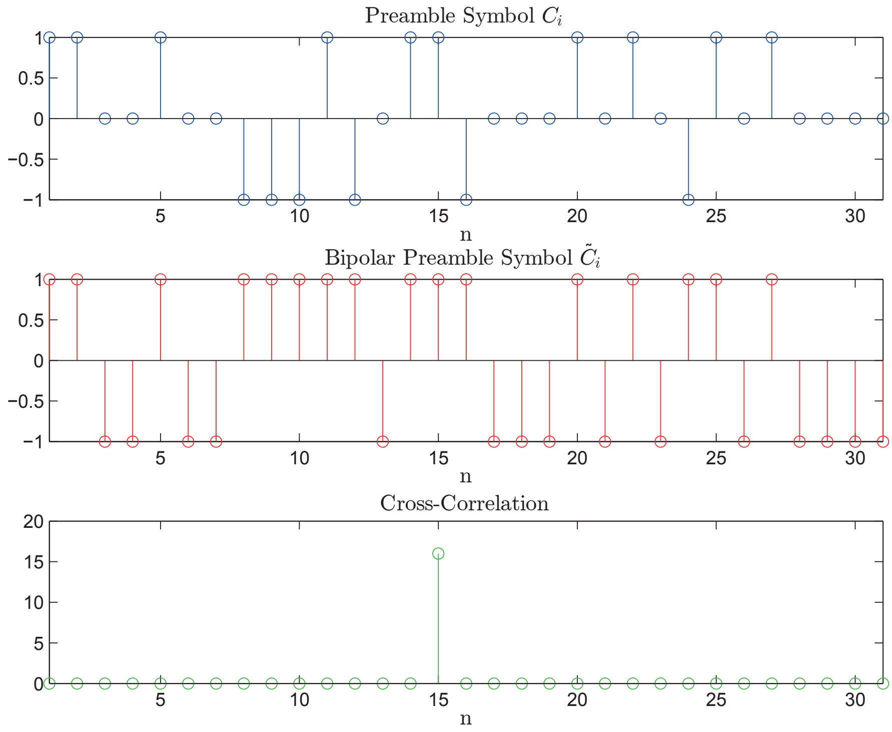


Figure 4.5.: Code sequences and their cross-correlation used by an energy detector

Signal by Signal Term

During transmission every pulse in the preamble sequence C_i is convolved with the CIR. This fact makes it obvious that when the CIR is longer than the introduced spreading length (LT_c for LPRF $128ns$), the CIRs will overlap and IPI is introduced. This work does not deal with these effects and no IPI is assumed; the interested reader is referred to [18].

Because of the squaring and integration process the mean in every output sample is the average energy that the signal contains in this interval. Squaring the preamble sequence leads to $\sum_{n=0}^{N_{pcode}-1} {C_n}^2 = \frac{N_{pcode}+1}{2} = N_N$, because al non-zero elements than become positive. Comparing the squared preamble sequence C_i with the bipolar reference $\tilde{C}_i$, it is noted that the positive patterns are equal. When these two sequences overlap perfectly the output of the correlator is the sum of the active elements N_N, multiplied with average energy represented by each sample and then resulting in the PDP estimate. Since the variance introduced by the deterministic signal term is zero the correlation process does not change anything and therefore there is

$$E\{y_{ss}[n]\} = E_p N_N \qquad var\{y_{ss}[n]\} = 0. \tag{4.24}$$

Signal by Noise Term

The expected value of the signal to noise term remains zero, because the noise term is zero mean and the correlation does not change this fact. For correctness, it must be stated that also this term contains the CIR and can therefore also be affected by IPI. The noise contributions are added up by every squared active code element and then multiplied with the average signal energy per sample, see equation 4.24. Therefore the mean and variance are defined as

$$E\{y_{sv}[n]\} = 0 \qquad var\{y_{sv}[n]\} = 2N_0 E_p N_N. \tag{4.25}$$

Noise by Noise Term

The bipolar sequence is $\tilde{C_n} \in \{1, -1\}$ and therefore different noise samples can be summed up, which can be assumed independent. An other property of the bipolar sequences is that they always have one positive pulse more than a negative. This means that the sum $\sum_{n=0}^{N_{pcode}-1} \tilde{C_n} = 1$ and that the correlation process does not change the mean of the noise distribution. For the variance this changes because squaring the bipolar code sequence leads to $\sum_{n=0}^{N_{pcode}-1} \tilde{C_n}^2 = N_{pcode}$

$$E\{y_{vv}[n]\} = N_0 T_{int} B \qquad var\{y_{vv}[n]\} = N_0^2 T_{int} B N_{pcode}. \tag{4.26}$$

Averaging

After correlating the despread symbols can be averaged over the N_{sync} repetition, to achieve an additional processing gain. This method reduces the noise variance relative to the signal energy, which enables a better PDP estimation. Considering obtaining $N_{pcode}L$ samples from the correlation process, there is

$$\bar{g}[n] = \sum_{q=0}^{(N_{sync}-1)} g[n + qN_{pcode}L]. \tag{4.27}$$

This leads to an averaging over the whole preamble symbol length $T_{psym} = N_{code}LT_c = 3968ns$ for LPRF. Averaging can be considered as a summation of N_{sync} independent χ^2-distributed Random Variables (RVs). Combining this assumption with the result from the correlation, the mean and variance are

$$E\{y_{ss}[n]\} = E_p N_N N_{sync} \qquad var\{y_{ss}[n]\} = 0 \tag{4.28}$$

$$E\{y_{sv}[n]\} = 0 \qquad var\{y_{sv}[n]\} = 2N_0 E_p N_N N_{sync} \tag{4.29}$$

$$E\{y_{vv}[n]\} = N_0 T_{int} B N_{sync} \qquad var\{y_{vv}[n]\} = N_0^2 T_{int} B N_{pcode} N_{sync}. \tag{4.30}$$

Normalizing

Following the statement in Section C.1, that the pulse energy at transmitter and receiver site is unity, the mean and variances must be normalized to guarantee a correct notation and therefore divide by $N_N N_{sync}$.

$$E\{y_{ss}[n]\} = E_p \qquad var\{y_{ss}[n]\} = 0 \tag{4.31}$$

$$E\{y_{sv}[n]\} = 0 \qquad var\{y_{sv}[n]\} = \frac{2N_0E_p}{N_N N_{sync}} \tag{4.32}$$

$$E\{y_{vv}[n]\} = \frac{N_0 T_{int} B}{N_N} \qquad var\{y_{vv}[n]\} = \frac{N_0^2 T_{int} B N_{pcode}}{N_N^2 N_{sync}} \tag{4.33}$$

At this point it is again referred to the CLT and assumed that after the correlation and average process the χ^2-distributed RVs can be seen as approximately Gaussian. This assumption simplifies the threshold derivation for synchronization and ranging, as the Q-function could be used.

4.3. Ranging

After all the effort to gather the PDP estimate, it has finally come to the leading edge detection. The leading edge is essential for the ranging process but also for fine synchronization considering the data demodulation. For the countermeasure this point is of course the most crucial one, because not aligning perfectly would distort the statistical assumption. Only a brief overview of the used ranging algorithm is given; for beyond considerations see [19].

The ranging algorithm applied in this work is a simple search back algorithm. Starting from the maximum in the PDP, also known as the strongest peak sample in $g[k]$, with the index k_{max}. Then a search back window ω_{SB} is defined that locates the first sample that exceeds a certain threshold γ_{toa} (Fig.4.6).

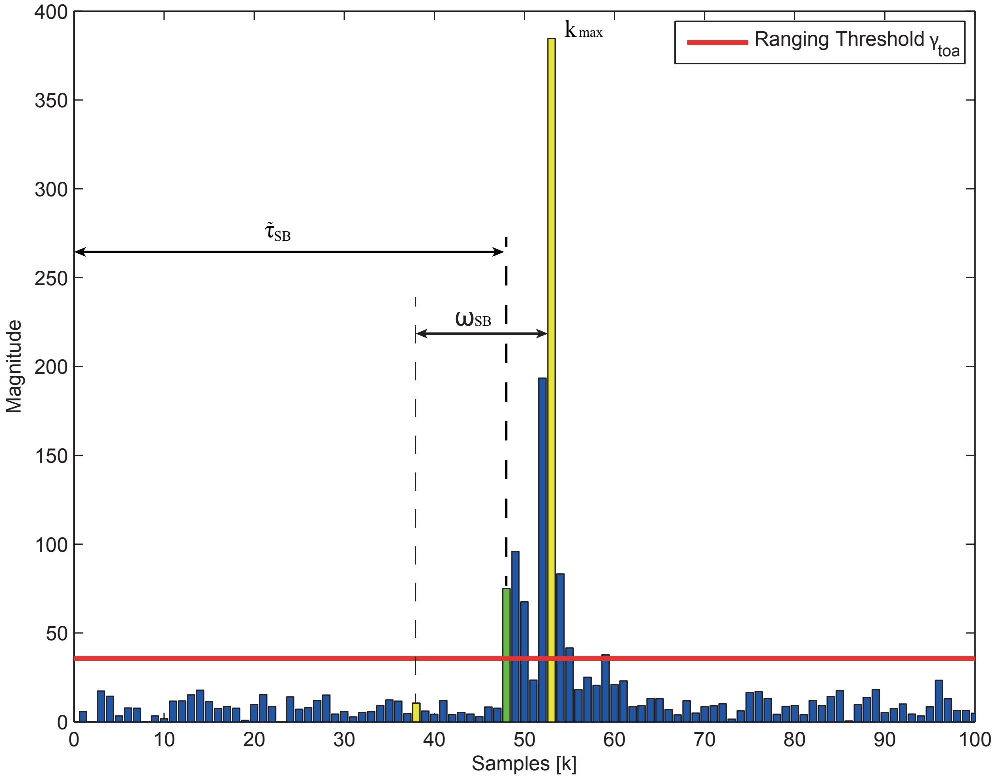


Figure 4.6.: TOA estimate for $T_{int} = 2ns$, $E_b/N_0 = 15dB$ and $\omega_{SB} = 30ns$

Mathematically this can be described as

$$\hat{\tau}_{SB} = min\left(k \in \{k_{max}, k_{max} - 1, ..., k_{max} - \omega_{SB}\} | g_k > \gamma_{toa}\right) T_{int} + \frac{T_{int}}{2}. \tag{4.34}$$

The threshold γ_{toa} can be chosen for a fixed probability of false alarm P_{fa}, that a noise sample exceeds the threshold, considering the noise statistics derived in 4.2 as

$$P_{fa} = P(g[k] > \gamma_{toa}) = Q\left(\frac{\gamma_{toa} - \mu_{vv}}{\sigma_{vv}}\right). \tag{4.35}$$

In the receiver design the threshold is fixed to a P_{fa} of 10^{-10} and therefore the threshold can be calculated as

$$\gamma_{toa} = \sigma_{vv}\, Q^{-1}(P_{fa}) + \mu_{vv} \tag{4.36}$$

$$= \sqrt{N_0^2 T_{int} B N_{pcode} N_{sync}}\, Q^{-1}(P_{fa}) + N_0 T_{int} B N_{sync} \tag{4.37}$$

4.3.1. Simulation and Results

In order to check the accuracy of the implemented ranging algorithm, the range estimate was simulated over a 100 channel realizations from the (CM3) scenario of the standard. In the simulations the integration time was fixed to $T_{int} = 2ns$ and the length of the search back window to $\omega_{SB} = 40ns$. The ranging threshold used is stated in equation 4.26 and therefore changes depending on the SNR. The ranging accuracy is measured in term of the MAE which can be calculated as

$$\text{MAE} = \frac{1}{N_{sim}} \sum_{n=0}^{N_{sim}-1} |\hat{\tau}[n] - \tau[n]|. \tag{4.38}$$

This formula compares the estimated TOA $\hat{\tau}[n]$ with the exact TOA $\tau[n]$, for each simulated channel.

Fig.4.7 shows the results obtained for the MAE, considering a LOS scenario and an integration time of T_{int}. Reaching a certain SNR $E_b/N_0 \approx 17dB$ the implemented algorithm performs very well and constantly and leads to an accurate range estimate. Fig.4.8 shows the probability that the MAE is less than $1m$.

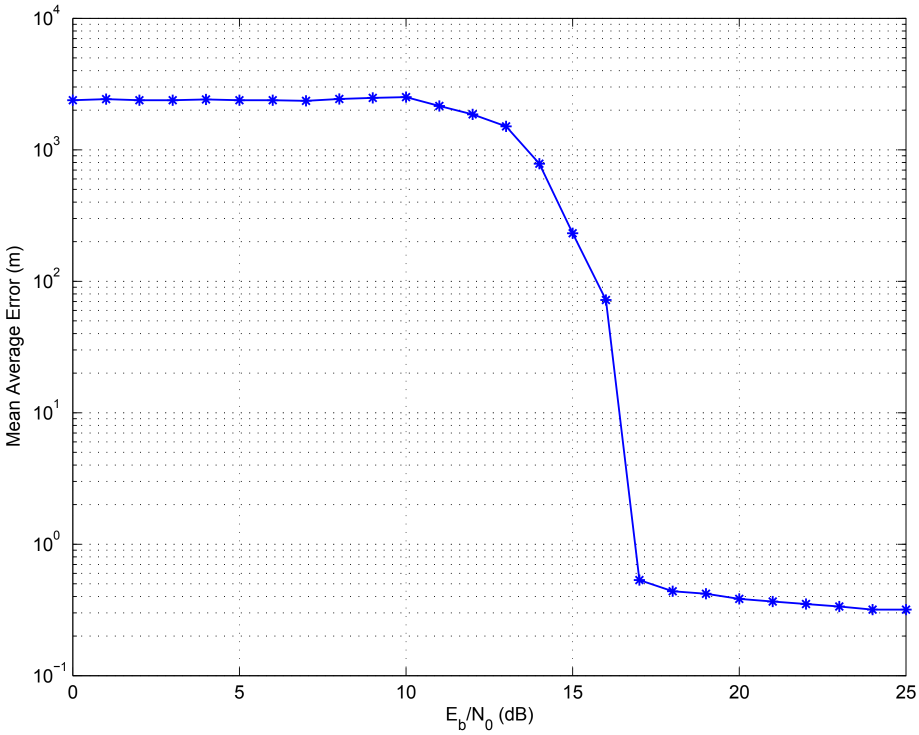


Figure 4.7.: MAE for (CM3) LOS

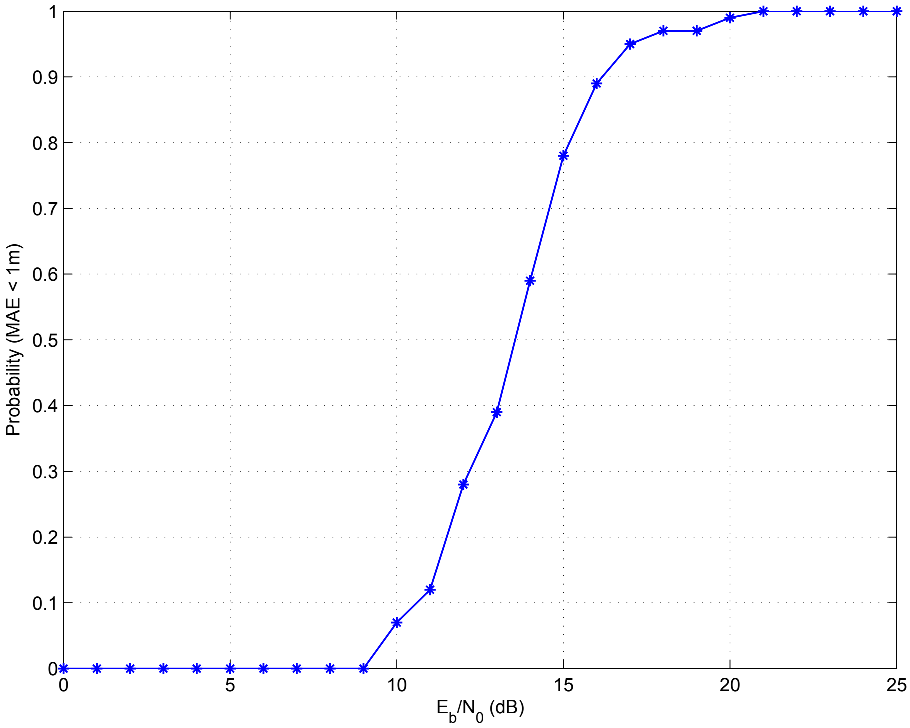


Figure 4.8.: MAE less than $1m$ for (CM3) LOS

4.4. Synchronization

Although the synchronization in the following simulations is assumed as perfect, it has to be evaluated how the algorithm performs with the reduced preamble symbols of the attacker.

For the investigation a baseline algorithm is used that is split in two main parts: signal detection and timing acquisition. During the signal detection the presence of a signal is given if one sample of the correlation output introduced by the channel estimation exceeds the threshold.

The threshold is given by fixing the false alarm rate $P_{fa,det} = 10^{-8}$ and considering the already derived noise statistics for the correlation process in equation 4.26 as,

$$\gamma_{det} = \sigma_{vv}\, Q^{-1}(P_{fa}) + \mu_{vv} = \sqrt{N_0^2 T_{int} B N_{pcode}}\, Q^{-1}(P_{fa}) + N_0 T_{int} B. \tag{4.39}$$

When a signal is detected in the ith correlation block, containing $N_{pcode}L$ samples (assuming that the chip period equals the sampling period of the energy detector), the highest correlation output sample is searched, given with the index m_i^{max}, for the ith block.

Then, in the timing acquisition part it is verified, that in $N = 4$ consecutive blocks the index does not differ by more then $8ns$, to ensure that the maxima stems from the same preamble pulse.

Synchronization is declared if the timing acquisition process succeeds, otherwise synchronization fails. For further interests and more complex algorithms see [10].

This baseline algorithm works very well (see Fig.4.9) because the fine synchronisation is achieved anyway by the TOA estimation within the channel estimation process.

The reduced number of preamble symbols introduced by the attacker does not affect the synchronization process. In most cases timing acquisition is achieved within 10 preamble blocks. This leaves enough space for the attacker to achieve the signal detection and also to shift the following preamble symbols.

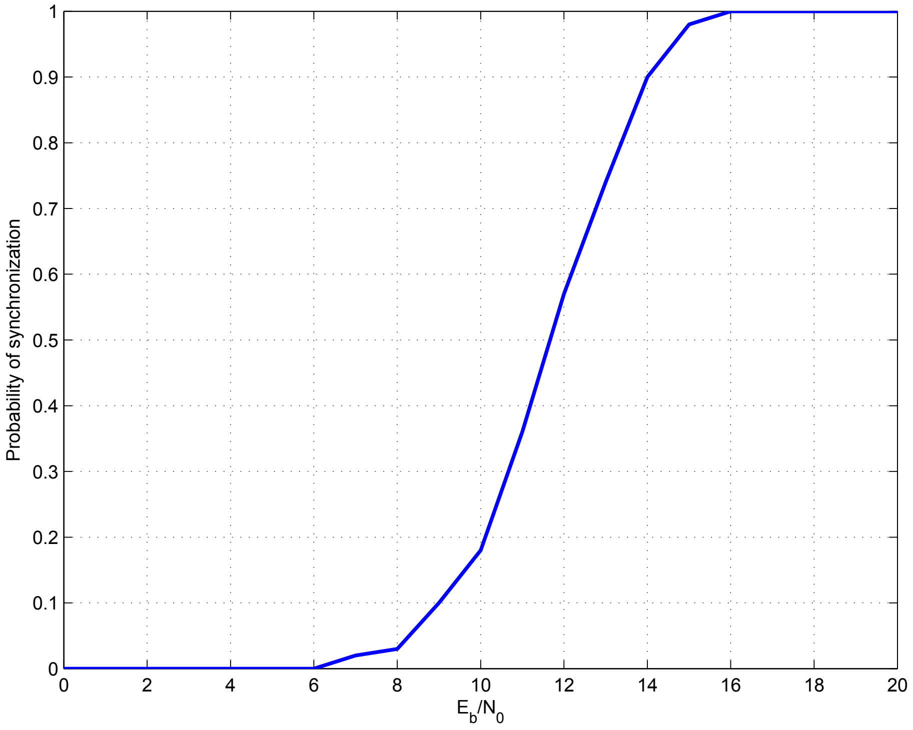


Figure 4.9.: Probability of synchronization

5. Simulation and Results

5.1. Overview

To simulate the relay attacks and the countermeasure proposed, an IEEE standard conform transmitter was implemented in MATLAB. The transmitter includes all the standard specific encoding operations as, Reed Solomon and convolutional encoding and operates on a sampling rate of $f_s = 10\,GHz$. With the sampling interval $T_s = 1/f_s$, the continuous time integral is approximated as

$$\int g^2(t)\,dt \approx \sum_n g^2(T_s n)T_s. \tag{5.1}$$

For the investigation it was focused only on the LPRF mode of the standard with the parameters defined in Section 2.3 and more precisely in Table 2.1. In the IEEE standard the mandatory LPRF mode is described by the channel number 3.

The ranging packet conveyed between the RDEVs is simulated with a random bit string of $N_{data} = 399$ bits. Also the hopping positions and the random spreading sequence were implemented with a LFSR, defined by the standard.

Throughout the whole work and also in this Chapter the SNR was defined for the AWGN model as

$$\gamma = \frac{E_b}{E\{|v|^2\}} = \frac{N_{cpb}E_p}{N_0} \tag{5.2}$$

where the energy per bit is $E_b = N_{cpb}E_p$. E_p is the pulse energy spread by the channel and then normalized as described in Equation 2.10.

The input filter applied in the simulation is a nearly ideal low pass filter that simplifies the derivation of the noise terms. Considering the SNR this changes almost nothing, because the main energy of the pulse is concentrated inside the bandwidth of the filter.

The simulations were always made under the assumption that the attacker does not introduce any additional processing delays. It is feasible to keep these delays in the order of nanoseconds. For more detailed information see [2].

5.2. Evaluation of the Test Statistics

The most important thing is to check that the implemented receiver works properly. In Section 4.1 the test statistics for the AWGN model has already been derived. Now the receiver simulation is compared to the χ^2 test statistics to evaluate the correctness of the implementation. For a detailed derivation of the χ^2 statistics and the resulting BER see [20]. For comparing the results, the IEEE 802.15.4a compliant transmitter is modified so that only a single pulse per symbol is sent. Sending only one pulse per symbol prevents inter-pulse interference caused by the time-dispersive channel and the random code sequence. This leads to a better comparison between the Chi-square test statistics and the simulation. Of course, this single pulse has the same mean energy as the 4 pulses used from the standard in the LPRF mode. Fig.5.1 shows the result of the comparison of the simulated and analytical values.

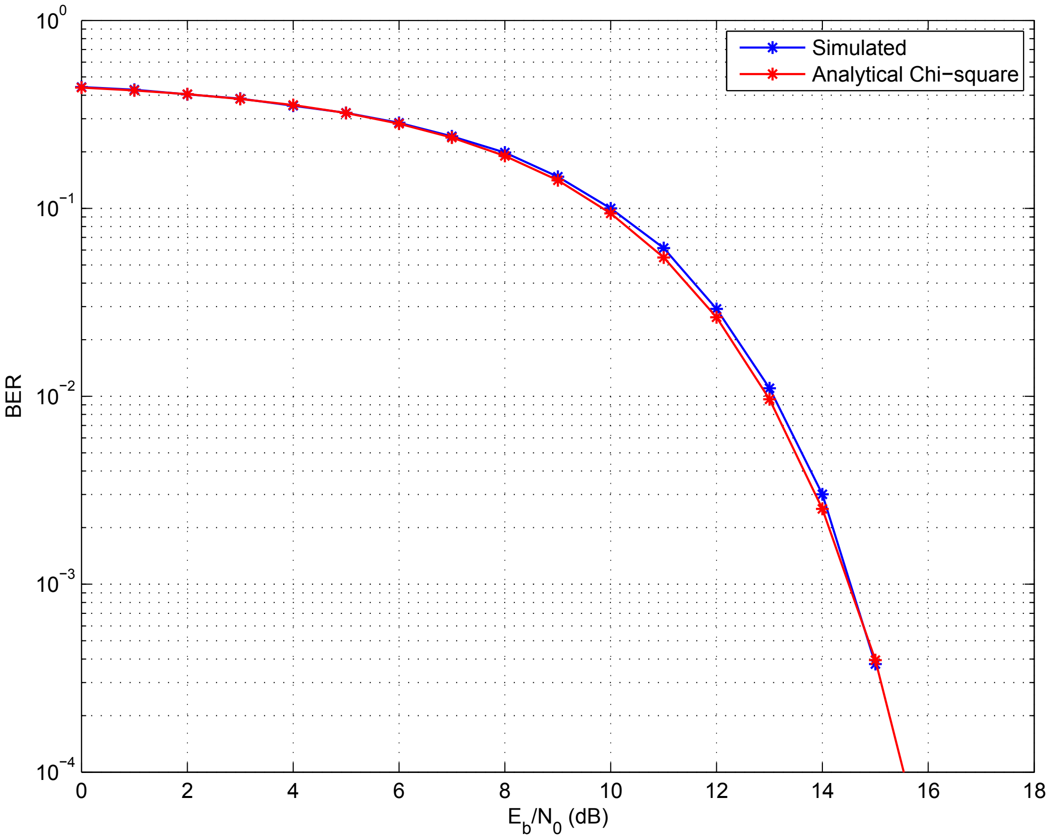


Figure 5.1.: Comparison of analytical (χ^2) and simulated BER

The resulting BER curves fit very well together so that it can be assumed that the receiver works properly. Of course, this has little to do with the final implementation of the standard conform receiver, but in this way it can be shown step by step how it comes to deviations introduced by adding up N_{cpb} pulses to a burst.

The next thing to evaluate is the deviation of the Chi-square test statistics to the AWGN

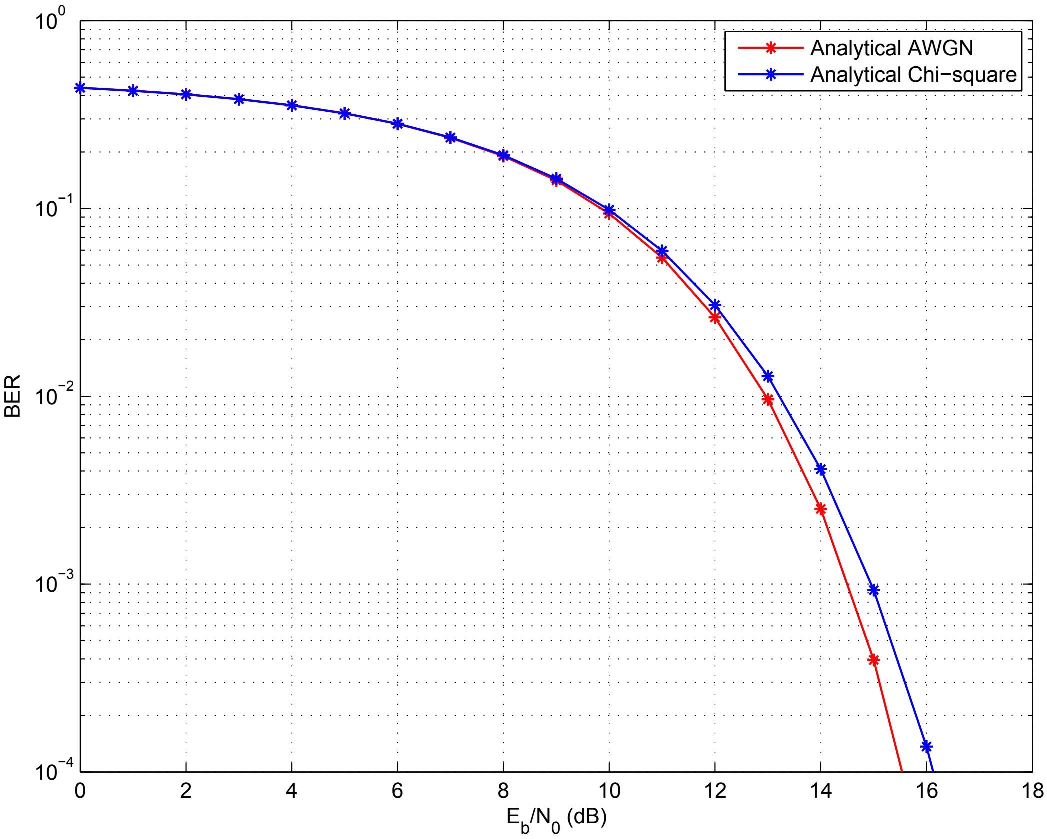


Figure 5.2.: Comparison of analytical (χ^2) and analytical AWGN BER

approximation introduced in Section 4.1. Many references, including [21] state that a χ^2-distributed RV with more than 40 degrees of freedoms can be approximated by a Gaussian RV with a confidence better than 5%. As $2\,T_{int}B = 40$ this condition is exactly fulfilled and we can act on the previous assumption. Fig.5.2 shows the difference between the true distribution and the AWGN model.

The results confirm that the Gaussian approximation is a really god fit for the statistics of the energy detector implemented.

Finally, the IEEE 802.15.4a compliant receiver is considered. To assemble N_{cpb} pulses to a burst, of course, is advantageous considering the spectral spreading of the energy. In terms of satisfying the UWB regulations in different countries, this is an effective tool, but it introduces also a degradation of the statistical behaviour of the signal. For further consideration on this more complex topic see [14].

Fig.5.3 shows the well apparent deviation that were introduced by the fading and the interference between pulses, caused by the delay spread of the channel. Statistically this can be seen as an increase of the variance between the demodulated symbols. In the early times of the simulations, this fact has introduced reasonable doubts on the accuracy of my implementation and on the statistical behaviour of the model.

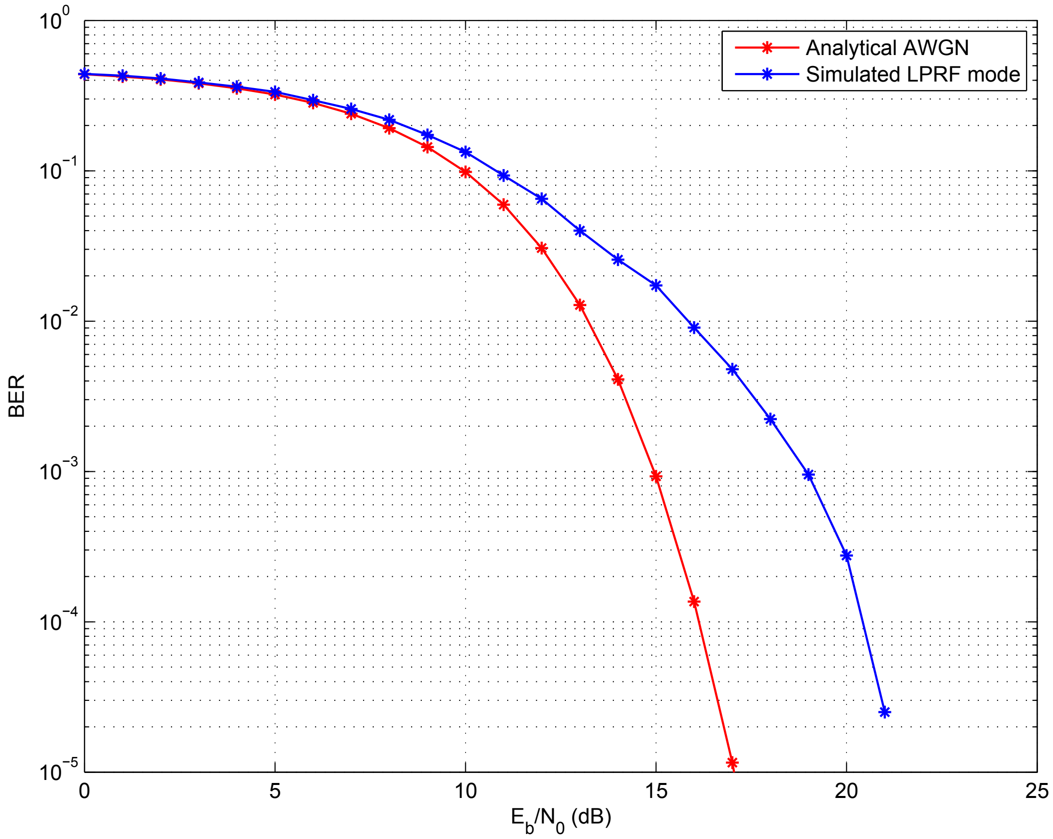


Figure 5.3.: BER of the AWGN model and the LPRF mode of the standard

The code-induced fading caused by the random spreading code can be efficiently reduced by forward error correction, which enables the usage of a Reed Solomon (RS) encoder. With this coding gain the performance of the receiver should be increased. For an attacker this error correction means a facilitation of his work because he does not have to worry about single bit errors he might introduce.

Fig.5.4 shows how the RS encoder supports the receiver and increases its performance dealing with bit errors. The achieved coding gain is approximately $2dB$ at a $BER = 10^{-4}$, concerning the 399 data bits conveyed in the simulation. This result is also approved from other references and for further information, dealing with the structure of the RS encoder see [12, p.78].

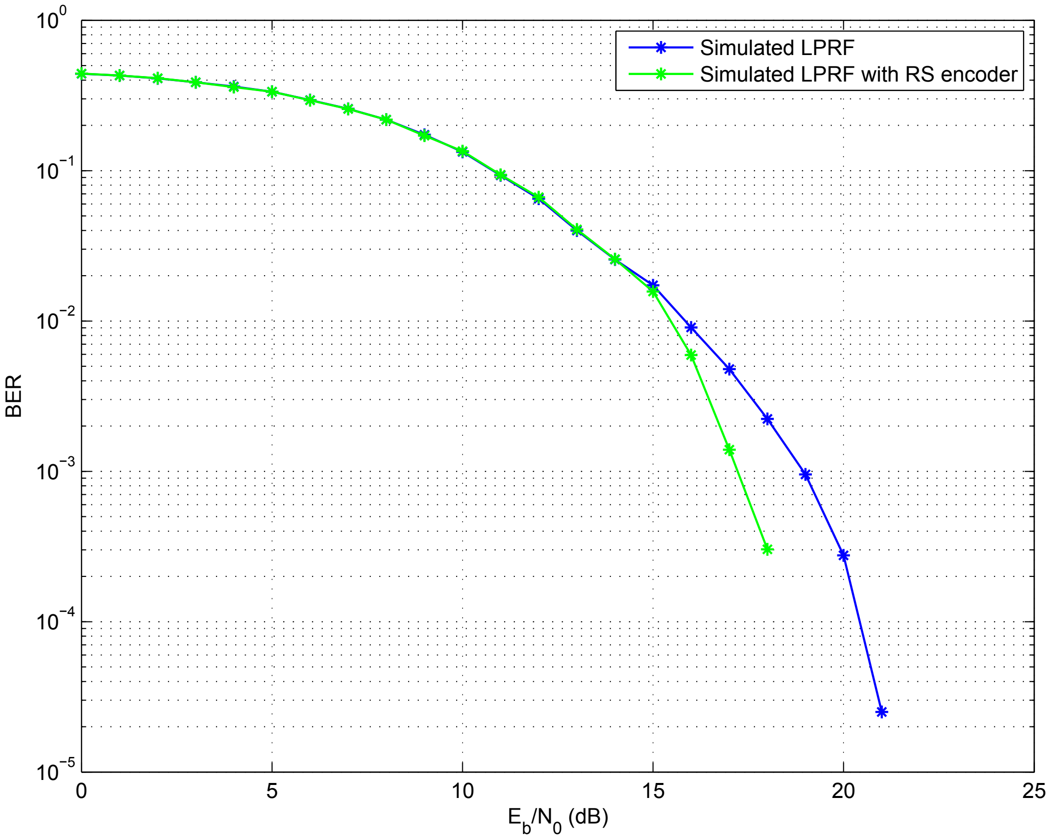


Figure 5.4.: BER of LPRF mode with and without the RS encoder

5.3. Evaluation of the Hypothesis

One of the most crucial things to evaluate, considering the countermeasure, are the derived noise-statistic parameters for the hypothesis. For this purpose a entire ranging packet was simulated with a fixed channel realization and a fixed SNR $= 20dB$, with $N_{sim} = 1000$ independent noise realizations.

In the remainder of this Section the noise statistics of the channel estimation process and the data demodulation process are derived separately. Even if they arise from the same noise process the levels are different due to the correlation and averaging at the preamble side. Then a comparison between simulated and analytical values shows the obtained deviations. Finally, the analytical values are brought together to describe the hypotheses for the countermeasure.

Noise "Channel Estimation"

In Section 3.3 the noise terms have been stated introduced by the channel estimation process as $\mu_{est,noise}$ and $\sigma^2_{est,noise}$. Then in Section 4.2 the parameters for the noise and for the signal and noise term (see equation 4.31) have been derived. By combining the terms are

$$\mu_{est,noise} = \underbrace{\left(\frac{N_0 T_{int} B}{N_N}\right)}_{=y_{vv}} N_{cpb} \tag{5.3}$$

$$var_{est,noise} = \left(\underbrace{\frac{N_0^2 T_{int} B N_{pcode}}{N_N^2 N_{sync}}}_{=y_{vv}} + \underbrace{\frac{2N_0 E_p}{N_N N_{sync}}}_{=y_{sv}} \right) N_{cpb}^2. \tag{5.4}$$

E_p is the mean of the estimated energy over the $N_{sim} = 1000$ realizations

$$E_p = \frac{1}{N_{sim}} \sum_{n=0}^{N_{sim}-1} E_p[n] \tag{5.5}$$

with a given integration window of $T_{int} = 40ns$.

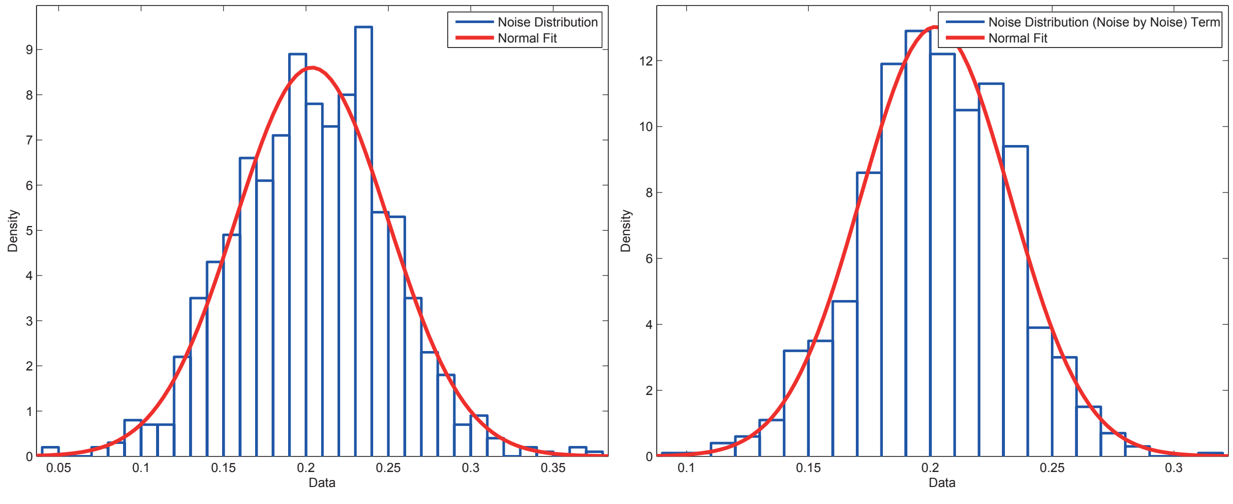
Fig.5.5(a) shows the distribution of the whole noise process, whereas 5.5(b) shows the distribution of the noise by noise term introduced by the estimation process. It can be seen that the simulated values agree very well with the analytical values obtained from Equations 5.3 and 5.4.

Taking the difference of the mean and the variance of the two distributions, then leads to the signal-by-noise term. At a fixed SNR $= 20dB$ the variance introduced from the signal by noise term, is twice the variance from the noise-by-noise term. Knowing that the receiver operates only accurately at higher SNRs the implication of this term is absolutely important to state the hypothesis. Therefore the signal-by-noise term can not be omitted, because at higher SNR regions, where the receiver operates correctly it gains the upper hand considering the noise statistics.

Finally, it can be said that the derivations fit perfectly to the simulated data and the AWGN model works very accurately. A comparison of the simulated and analytical values are listed in Table 5.1.

	Simulated	**Analytical**	**Deviation in dB**
$\mu_{est,noise}$	$0,2$	$0,2036$	$-0,077$
$\sigma_{est,noise}$	$4,6368\text{E}{-2}$	$4,6690\text{E}{-2}$	$-0,03$
$\sigma_{est,noise_{vv}}$	$3,0631\text{E}{-2}$	$3,1124\text{E}{-2}$	$-0,069$
$\sigma_{est,noise_{sv}}$	$3,4816\text{E}{-2}$	$3,4818\text{E}{-2}$	$-1,79\text{E}{-4}$
μ_{data}	$0,8$	$0,7967$	$0,0179$
σ_{data}	$2,8998\text{E}{-2}$	$2,9293\text{E}{-2}$	$-0,044$
$\sigma_{data_{vv}}$	$8,4563\text{E}{-3}$	$8,9555\text{E}{-3}$	$-0,249$
$\sigma_{data_{sv}}$	$2,7737\text{E}{-2}$	$2,7890\text{E}{-2}$	$0,0238$

Table 5.1.: Comparison between simulated and analytical values



(a)

(b)

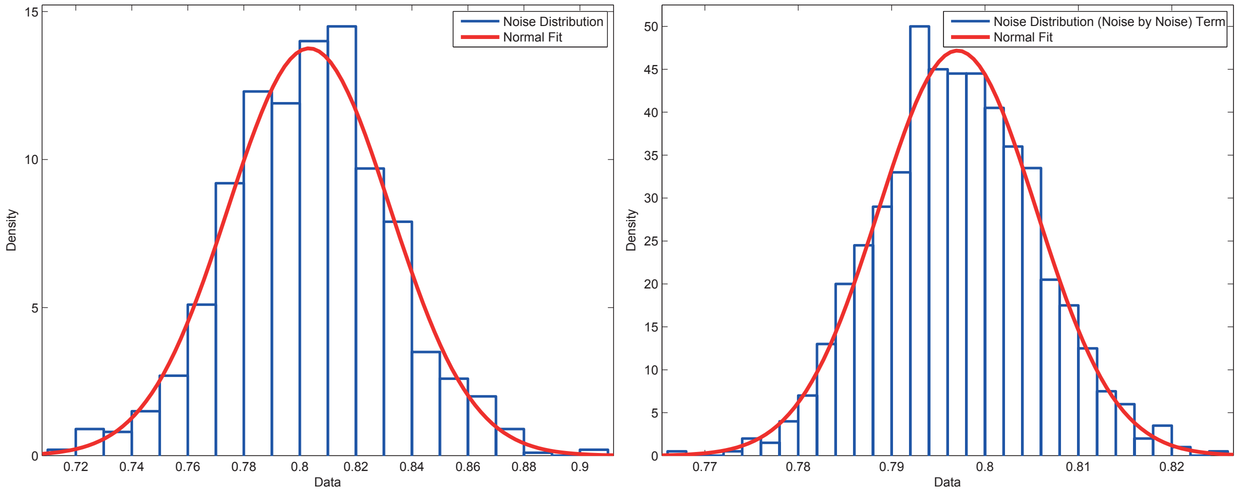
Figure 5.5.: Noise distributions for the whole channel estimation process (a) and for the Noise by Noise term (b)

Noise "Data Symbols"

The noise introduced in the data part of the receiver is described by quations (C.25) and (C.27). Finally the variance is only to divide by the number of bits in the data packet $N_{data} = 399$ and is therefore given as

$$\mu_{data} = \underbrace{N_0 T_{int} B}_{=y_{vv}} \qquad \sigma^2_{data} = \underbrace{\frac{N_0^2 T_{int} B}{N_{data}}}_{=y_{vv}} + \underbrace{\frac{2E_p N_0}{N_{data}}}_{=y_{sv}} . \tag{5.6}$$

Fig.5.6(a) shows the distribution of the whole noise process, whereas 5.6(b) shows the distribution of the noise by noise term introduced in the demodulation process of the data symbols.



(a)

(b)

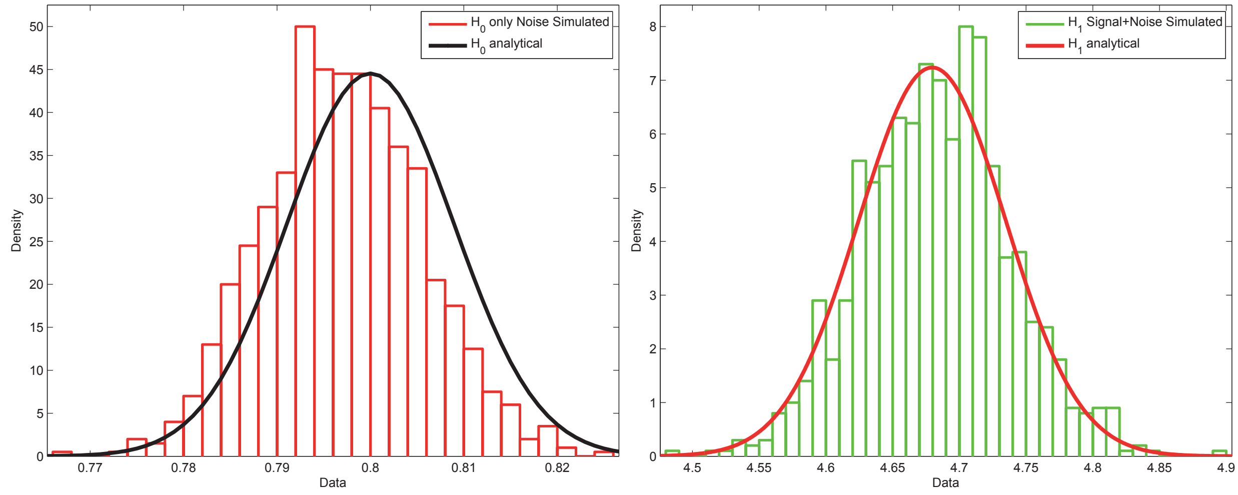
Figure 5.6.: Noise distributions for the data part (a) and for the Noise by Noise term (b)

Also for the data part the signal by noise term dominates. More interesting is the fact that the noise distortion from the channel estimate is higher than the noise introduced from the data part (see Table 5.1).

The noise by noise term is already the final hypothesis for the noise-only symbol parts as

$$H_0 : \qquad \mu_{H_0} = N_0 T_{int} B \qquad \sigma^2_{H_0} = \frac{N_0^2 T_{int} B}{N_{data}} . \tag{5.7}$$

The noise hypothesis resulting from the simulation is depicted in Fig.5.7(a). The accuracy of the noise-only hypothesis depends on the noise level at receiver side and this, it can be assumed, is achieved in the right fashion.



(a)

(b)

Figure 5.7.: Noise hypothesis H_0(a) and signal + noise hypothesis H_1(b)

For the signal hypothesis the mean of the noise of the channel estimation must finally be subtracted from the signal mean and then add up the noise mean introduced by the data part as

$$H_1 : \mu_{H_1} = E_p - (\mu_{est,noise}) + N_0 T_{int} B = E_p - \left(\frac{N_0 T_{int} B}{N_N} N_{cpb} \right) + N_0 T_{int} B. \qquad (5.8)$$

The variances are added up as

$$H_1 : \sigma^2_{H_1} = var_{est,noise} + \frac{N_0^2 T_{int} B + 2 E_{est} N_0}{N_{data}} \qquad (5.9)$$

$$= \left(\frac{N_0^2 T_{int} B N_{pcode}}{N_N^2 N_{sync}} + \frac{2 N_0 E_p}{N_N N_{sync}} \right) N_{cpb}^2 + \frac{N_0^2 T_{int} B + 2 E_{est} N_0}{N_{data}}. \qquad (5.10)$$

The signal+noise hypothesis resulting from the simulation is depicted in Fig.5.7(b).

5.4. Simulation of different Attack Scenarios

Every simulation is first determined in terms of the BER. Then it is evaluated how the countermeasure performs over $N_{sym} = 100$ channel realizations with a fixed $P_{fa} = 5\%$ for every simulation. This P_{fa} is motivated on the fact that a repetition after every twentieth ranging process, due to a false alarm is acceptable for the consumer. Additionally the different attack scenarios are shown on symbol base and with a fixed SNR.

Simulation of the benign case with 1 pulse per symbol

In the last Section the accuracy of the derivations have been reviewed. Before the proposed method is tested under hostile action, it has to be verified how it performs under "normal" conditions, to ensure a proper functionality. For this purpose first the performance operating only with one pulse per symbol is evaluated, to have a good comparison for the deviations introduced by the random spreading code of the standard.

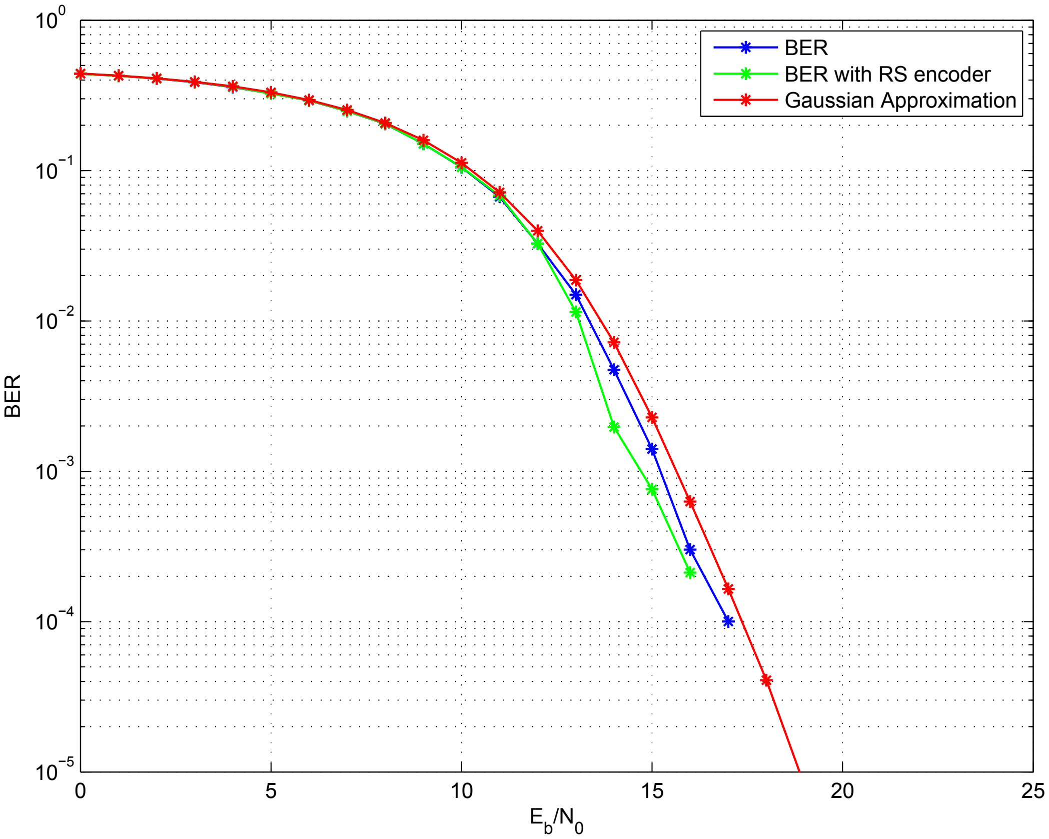


Figure 5.8.: BER for simulation with 1 pulse per symbol

The BER in Fig.5.8 shows us that the receiver operates accurately from an SNR $\approx 17dB$. Fig.5.9 shows the probability of detection. It can be seen that the countermeasure works as expected: In higher SNR regions, where no more bit errors occur the probability locks

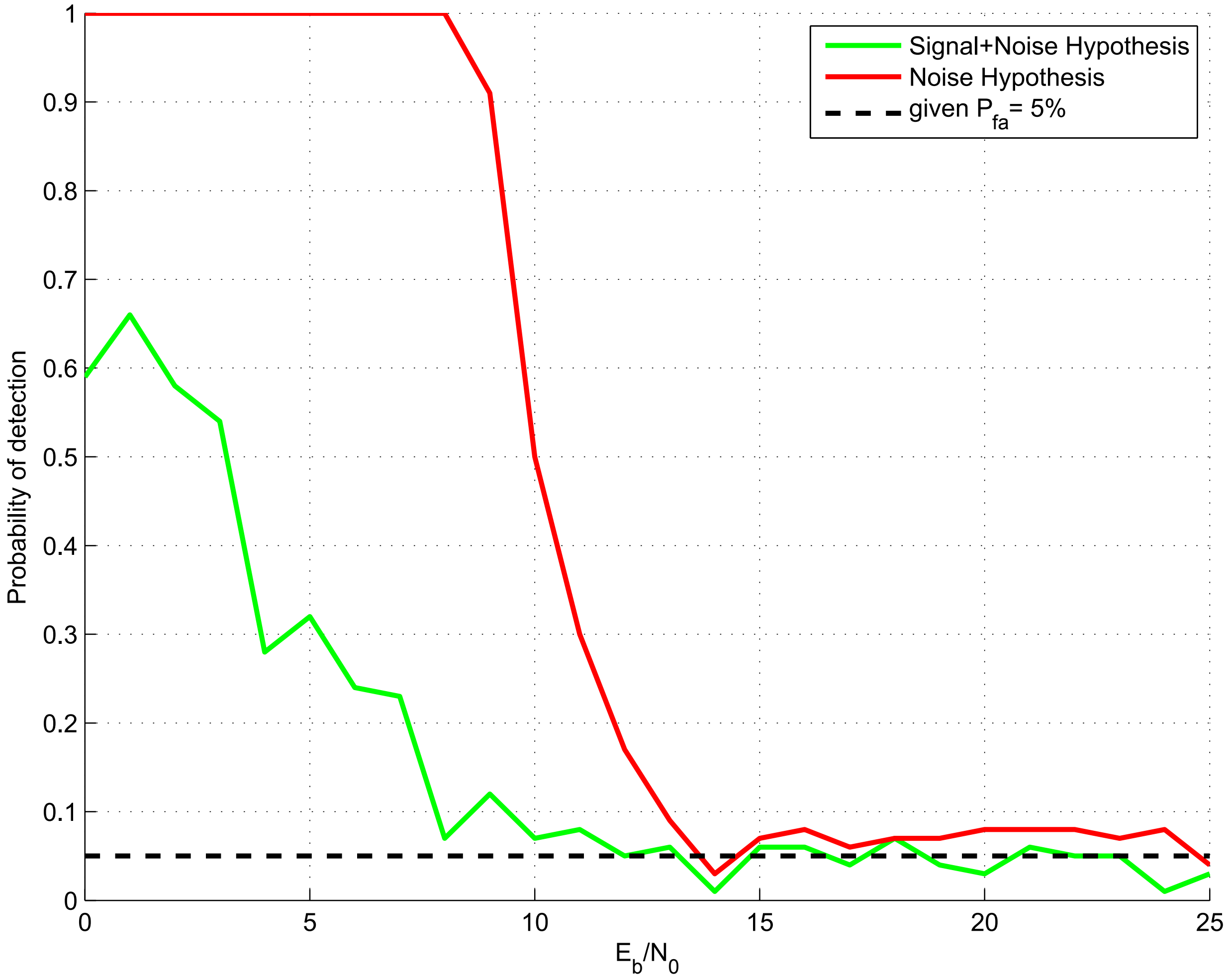


Figure 5.9.: Probability of detection a for benign case

into the given P_{fa} of 5%. Of course, some fluctuations around the expected value (P_{fa}) are obtained, which can be accounted on the limited number of simulations and on the simplified assumptions. The countermeasure introduces a very tight energy window that complicates attacks very effectively. This fact is illustrated very well in Fig.5.10, where the single hypothesis are depicted for a given $E_b/N_0 = 20dB$. Every single green $signal + noise$ hypothesis represents a single channel realization. Logically, the same applies for the red $noise$ hypothesis, which can not be distinguish because they lie to close to each other. The large spreading of the $signal + noise$ hypothesis over the energy domain is caused by the different delay spreads introduced by the channel model, which leads to different energy estimates over the integration interval T_{int} for every channel.

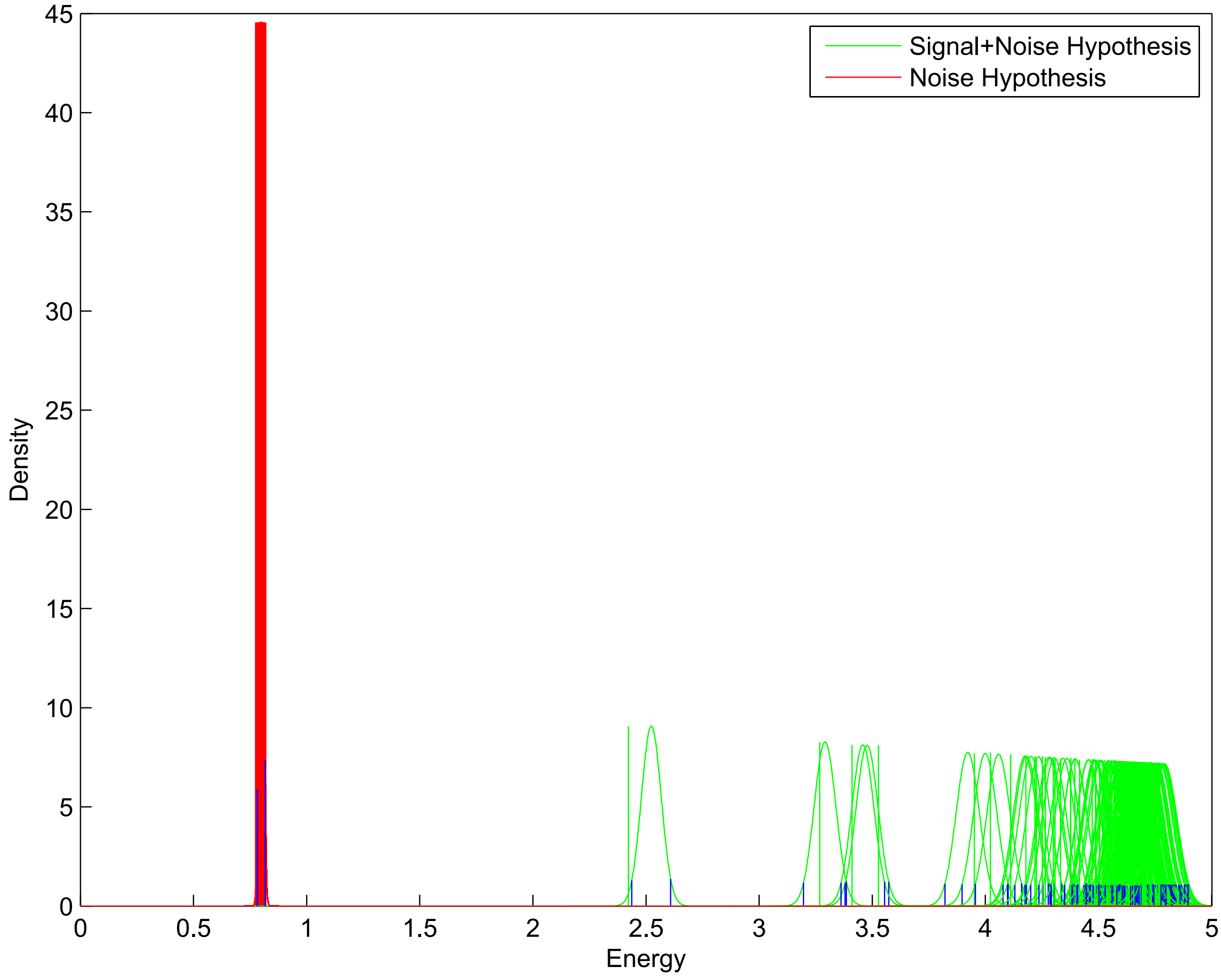


Figure 5.10.: Hypotheses for $E_b/N_0 = 20dB$

Simulation of the benign case with the LPRF mode

As known from the evaluation of the test statistic in Section 5.2, the signal energy varies from symbol to symbol. This is caused by the random spreading code that introduces interference between pulses of each chip and thus leads to problems in the accuracy of the countermeasure. Fig.5.11 shows the BER for the simulation and the given deviations from the Gaussian approximation.

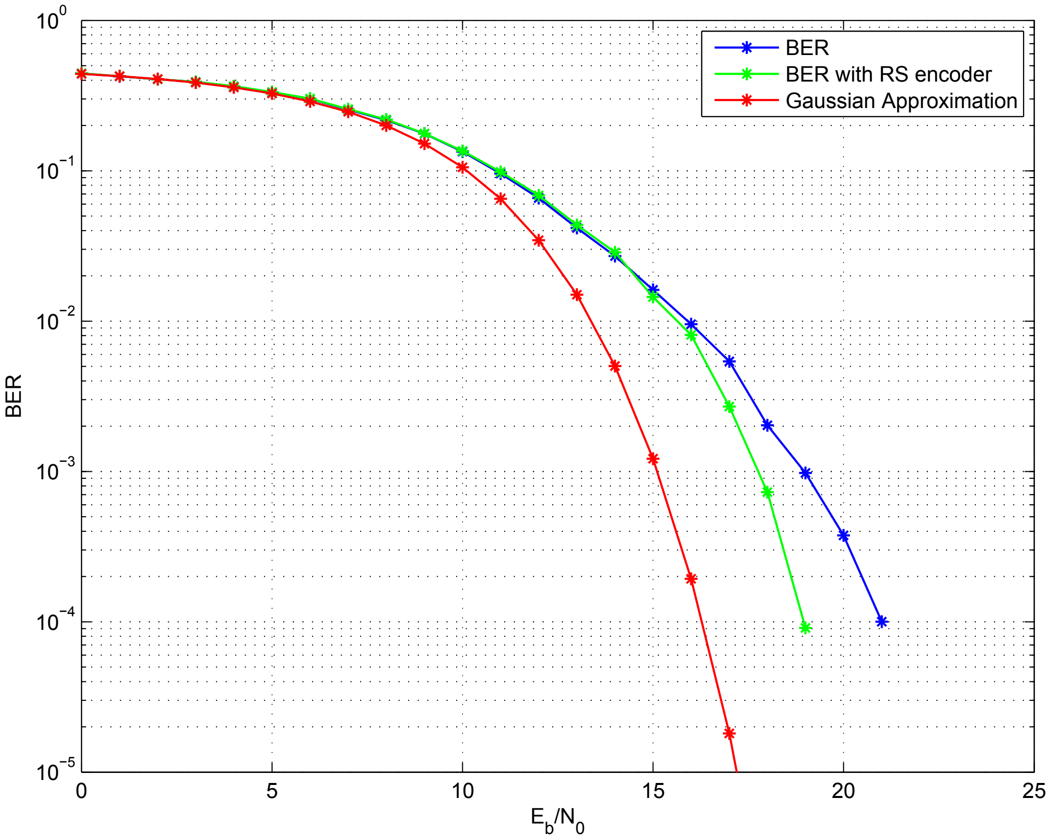


Figure 5.11.: BERs for the LPRF mode

The probability of manipulation for the 2 hypotheses is depicted in Fig.5.12. The noise hypothesis performs very well and locks to the given P_{fa} at higher SNR, as expected. Unfortunately this is not true for the signal and P_{fa} can be set lower for the signal and noise hypothesis, but this only leads to a greater acceptance of a potential attack. One way to counter this problem, is to incorporate the statistics of these fading effects, given by the spreading code and the radio channel, as proposed in [14].

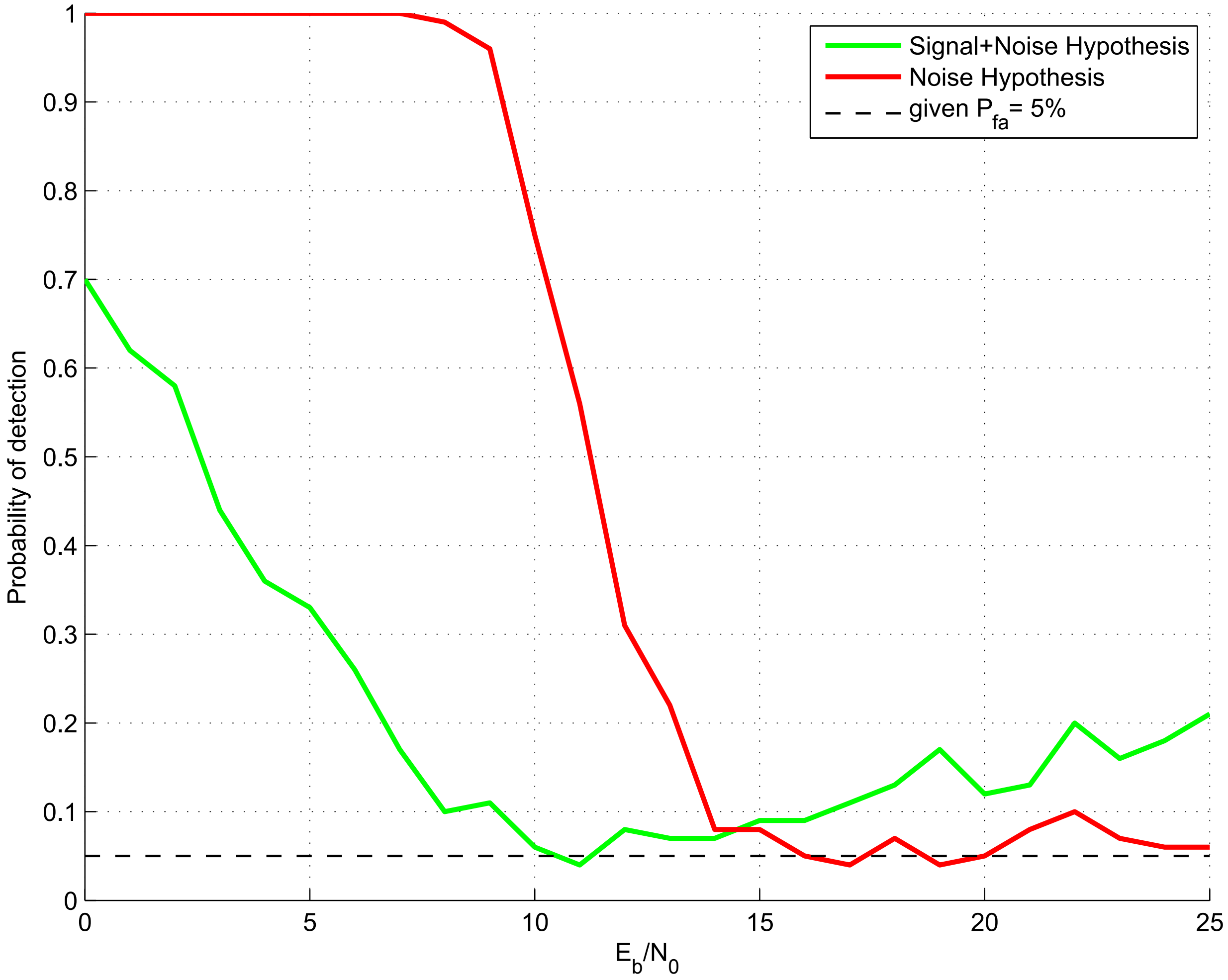


Figure 5.12.: Probability of detection, LPRF $T_{int} = 40ns$

The other way is to increase the integration window for the data demodulation process. A short integration window leads to a greater deviation of the energy given from the channel estimate, due to the cut off on higher energy samples. Longer integration windows perform much better with the delay spread introduced by the channel and this leads to a better accuracy for the energy given by the channel estimate. Therefore a new simulation by doubling the window to $T_{int} = 80ns$ and using the same 100 channel realizations were performed. The outcome of the simulation is depicted in Fig.5.13, where it can be noticed that the signal + noise hypothesis performs much better that in the simulation with the shorter integration window.

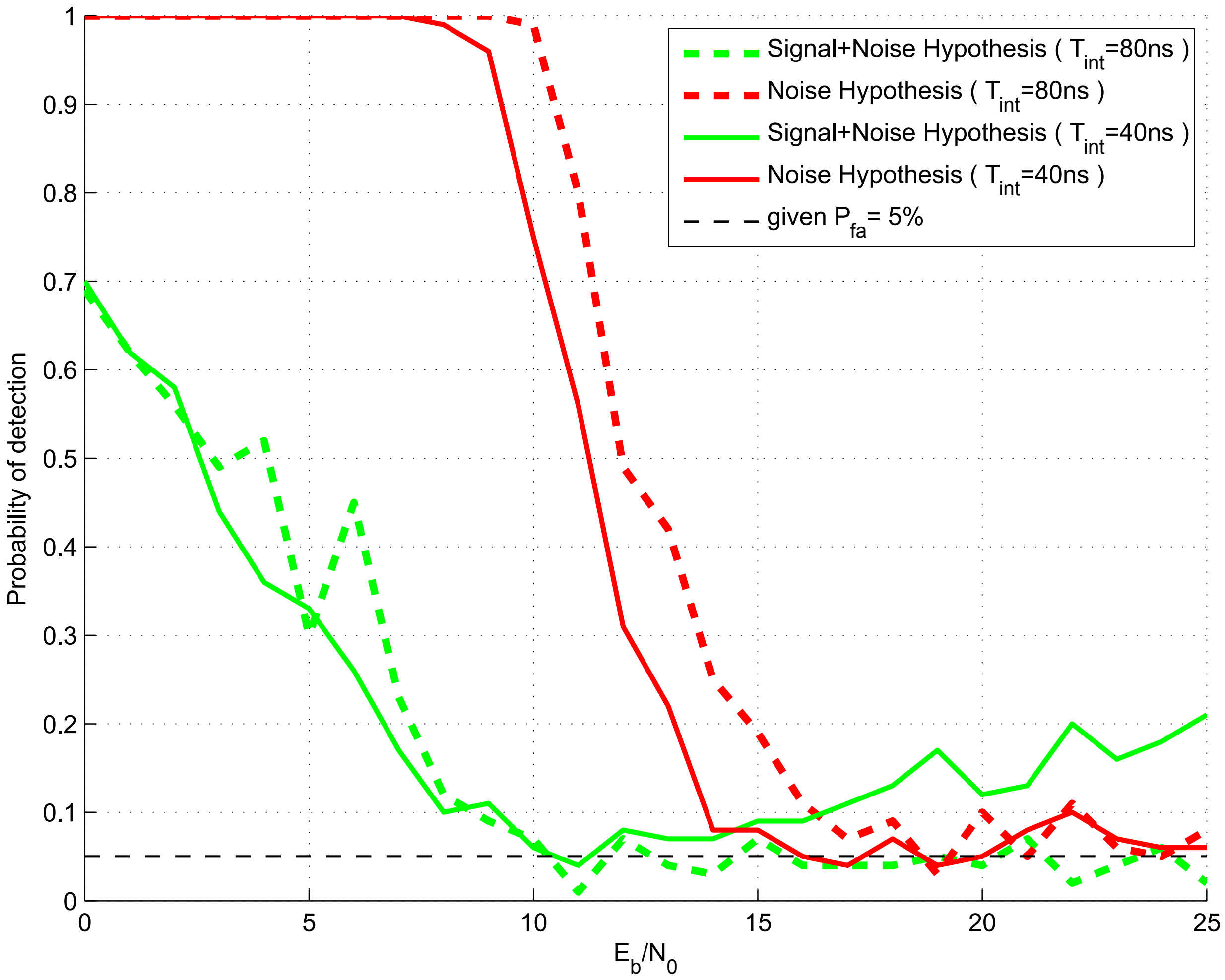
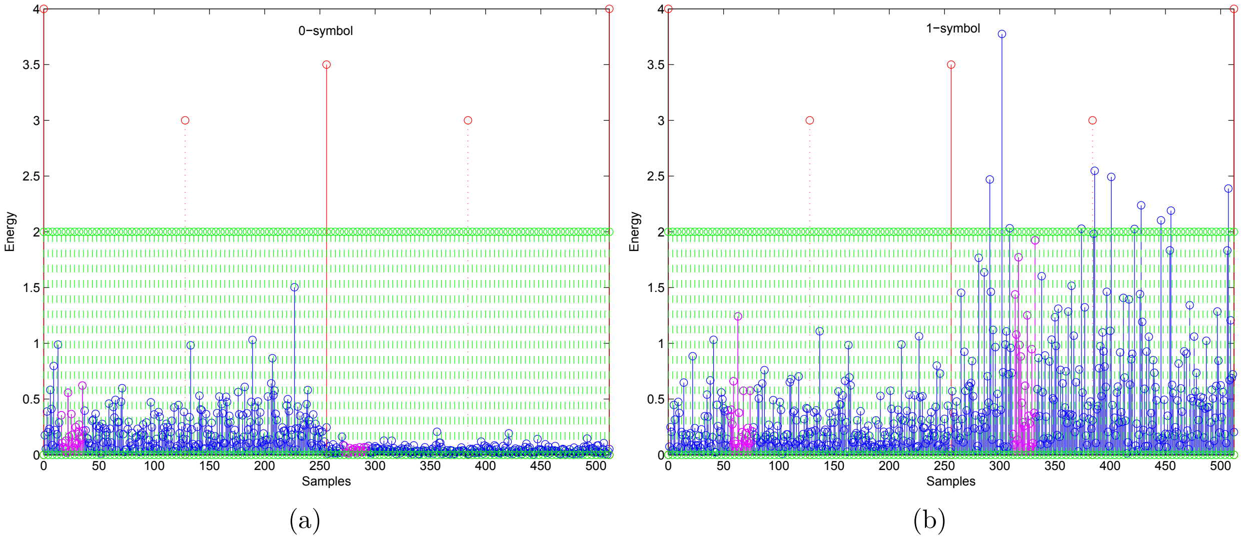


Figure 5.13.: Probability of detection, LPRF $T_{int} = 80ns$

Simulation of the simplest attack with 2 noise levels

This has lead to the point to evaluate the countermeasure against different attack scenarios. The simplest way to overcome an energy detector is to send two different noise levels to manipulate the symbol decision. This attack is explained in detail in Section 2.6.

Of course, this attack is not the most efficient in terms of achieving the highest relay distance. However this attack also works when the hopping sequence is unknown for the attacker and obtains a relay gain of at least the guard interval. In terms of the LPRF mode of the standard this is almost $T_{guard} = 256ns$, which corresponds to a distance decrease of $76m$.



(a)

(b)

Figure 5.14.: 0-symbol (a) and 1-symbol (b) under hostile influence (noise attack)

It is assumed that the preamble part is sent with the given pulse shape, so the considerations of the SNR do not change and the channel can be estimated properly. Fig.5.14 illustrates the attack for a 0-symbol (a) and a 1-symbol (b). The noise levels are fixed, so that the mean energy of the 2 noise levels equals the average signal energy of the previous simulations. The signal energy for the symbols is given as

$$E_s = \frac{1}{2}E_0 + \frac{1}{2}E_1 \qquad\qquad E_1 = E_0(1+\gamma) \tag{5.11}$$

where $\gamma = 3$ defines the proportion between the 2 noise levels E_0 and E_1.

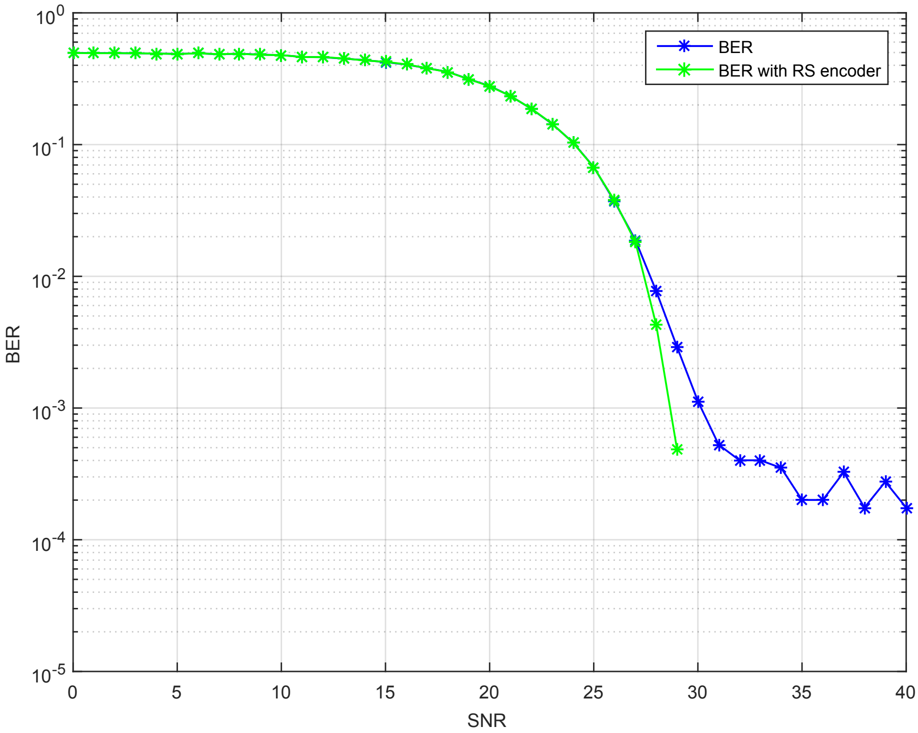


Figure 5.15.: BER for the noise attack

Then the SNR is calculated as

$$P_s = \frac{1}{2}\sigma_s^2 \frac{N_{sample}}{2} + \frac{1}{2}\sigma_s^2(1+\gamma)\frac{N_{sample}}{2} \tag{5.12}$$

$$= \frac{1}{4}\sigma_s^2(2+\gamma)N_{sample} \tag{5.13}$$

$$P_n = \sigma_n^2 \tag{5.14}$$

$$SNR = \frac{P_s}{P_n} = \left(\frac{1}{2} + \frac{\gamma}{4}\right)\frac{\sigma_s^2}{\sigma_n^2} \tag{5.15}$$

where σ_s^2 is the variance of the signal (here assumed as noise level) and σ_n^2 is the variance of the thermal noise.

The BER of the attack (see Fig.5.15) looks very strange compared to the previous. Considering the normal BER it is recognized that the attack introduces a permanent error floor, also in high SNR regions. This error floor is caused by the proportion $\gamma = 3$ between the 2 noise levels E_0 and E_1. In summary it can be said that the RS decoder facilitates the attack by correcting the introduced bit errors.

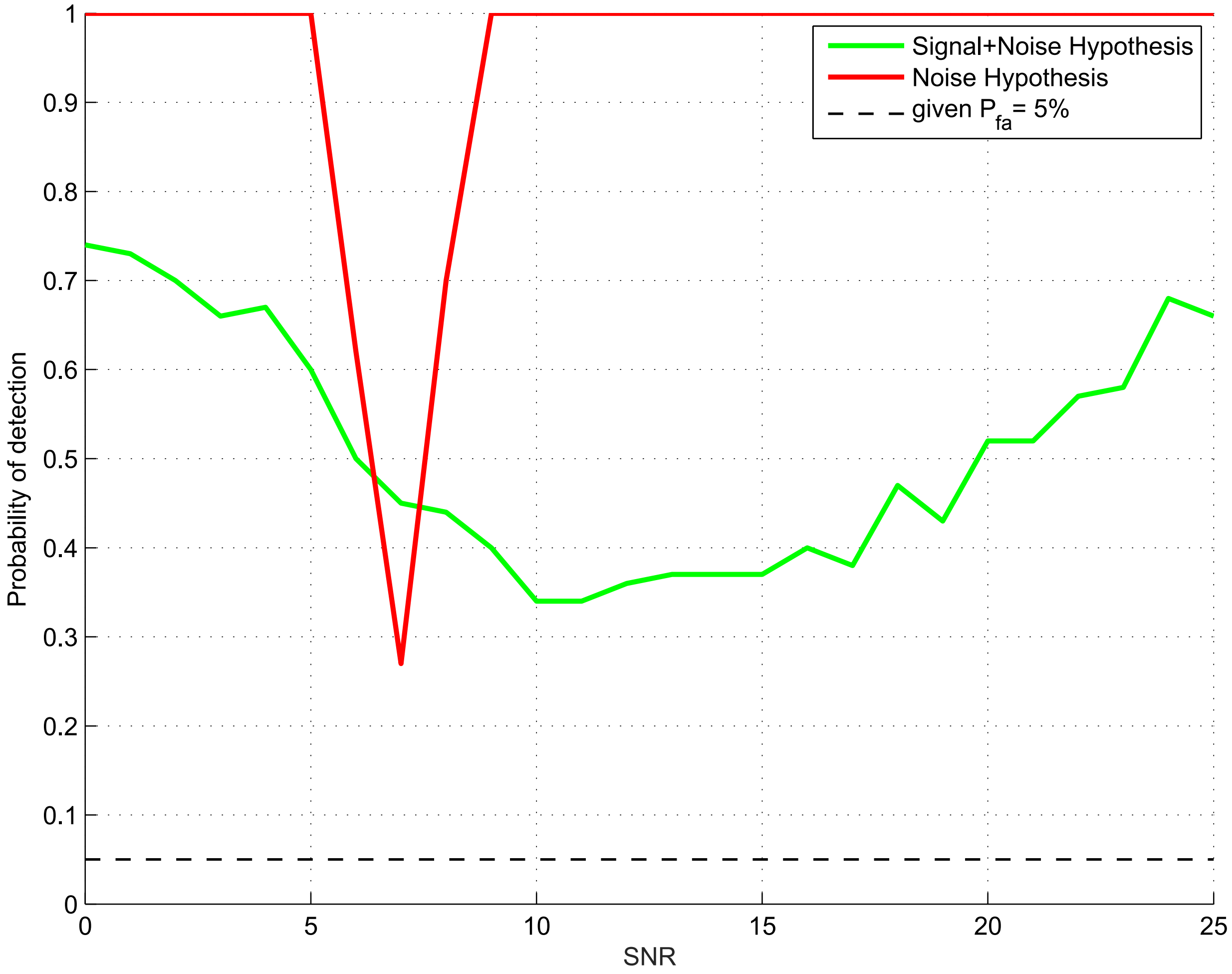
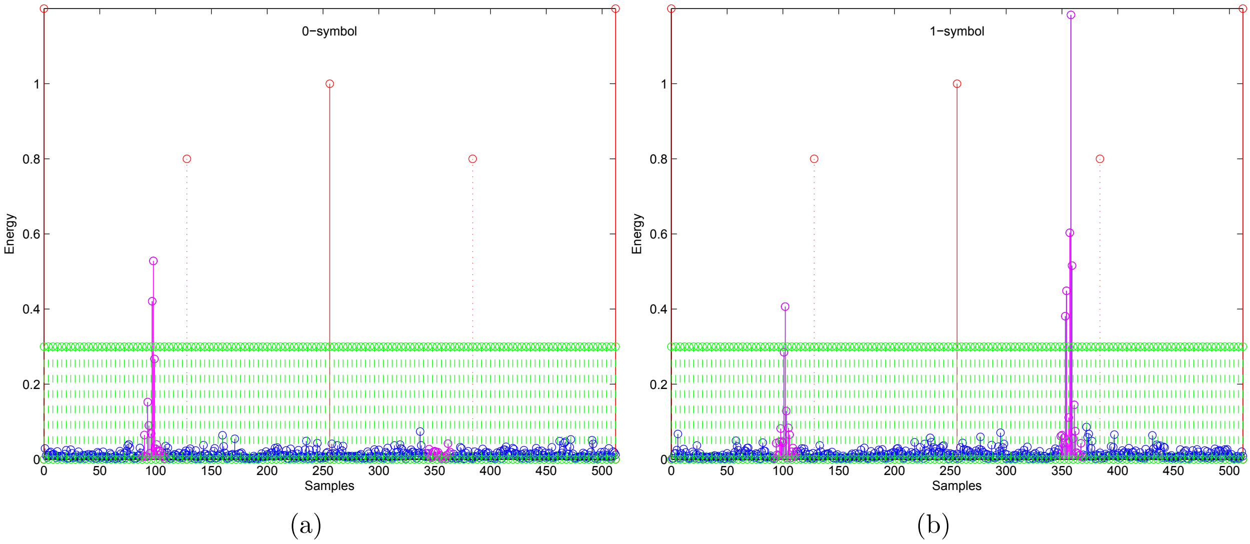


Figure 5.16.: Probability of detection (noise attack)

Looking at the performance of the countermeasure, depicted in Fig.5.16, gives confidence, because the manipulation could be detected very well. The manipulation of the noise level is detected without exception in the error-less SNR regions. The detection of the manipulated signal level is very poor. This comes from the fact that the mean energy of the 2 noise levels is chosen so that it is equal to the average signal energy introduced by the 4 pulses with $N_{cpb}E_p$. Of course, this is the worst case for the countermeasure, but it can be assumed that an attacker can estimate the SNR of the receiver. This allows him to adjust the noise levels for the attack and to force this scenario.

Simulation of the introduced Relay Attack

The next attack referred to is the one proposed in Section 2.5. The attack is achieved by sending in the first symbol half always a pulse with energy E_0 and then reacting in the second symbol half with a pulse of higher energy E_1, or by just doing nothing. Fig.5.17 shows the attack in the symbol domain. The energy E_1 is assumed to be equal to the energy introduced by the N_{cpb} pulses, whereas the energy E_0 is unity, for 1 pulse.



(a)

(b)

Figure 5.17.: 0-symbol (a) and 1-symbol (b) under hostile influence (relay attack)

Assuming that the attacker knows the hopping positions introduced by the LFSR, this attack is highly effective and achieves a relay gain of at least $T_{dsym}/2 = 512ns$, which corresponds to a distance decrease of $153m$.

In the BER depicted in Fig.5.18 it can be seen that the attack is very effective. The increased BER is to be accounted on the decreased energy distance for E_0 to the noise level and also between the 2 pulses.

Considering the outcome of the countermeasure (see Fig.5.19, it can be determined that signal and noise hypotheses do not behave as intended. Using the same energy as in the simulation of the benign case with 1 pulse per symbol, depicted in 5.8 the probability of detecting the manipulation differs. Logically, this is because the section where the signal should be is determined by both pulse energies and so the mean energy depends on the number of the transmitted ones and zeros. The same applies for the noise only section, which is determined by the real noise and the energy of the single pulse. Obviously this also holds for the noise attack previously treated. So the attacker almost has no chance to mount an attack that can not be detected by the countermeasure.

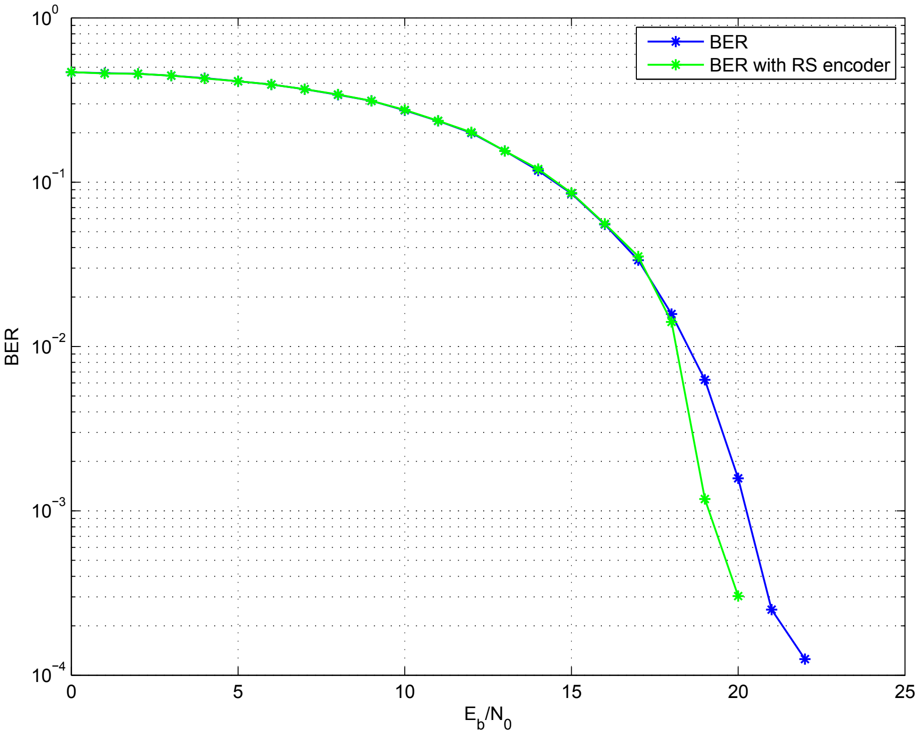


Figure 5.18.: BER for the relay attack

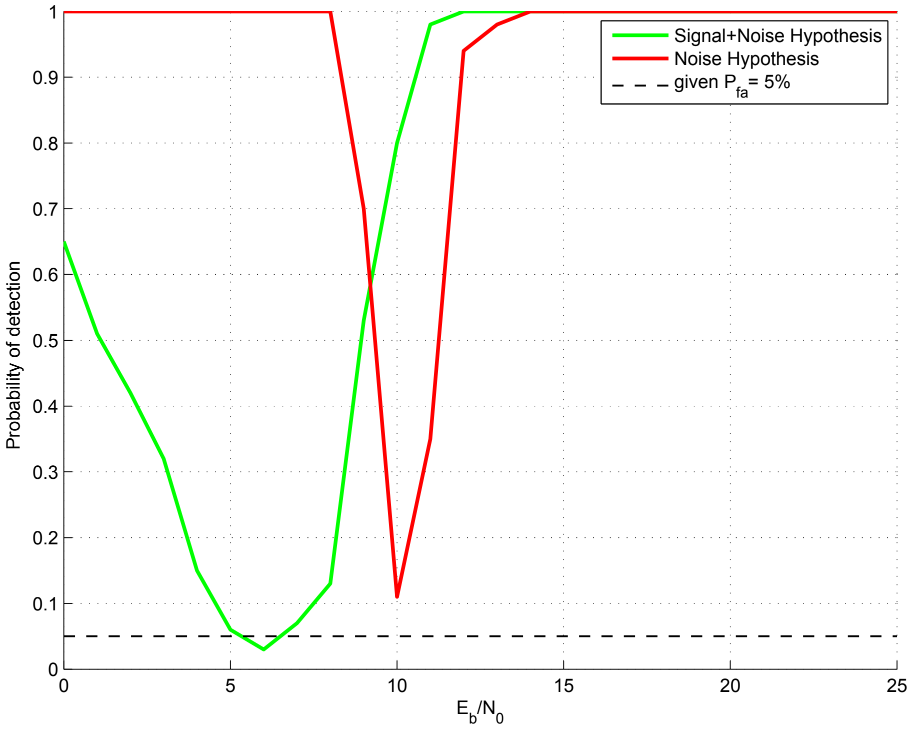
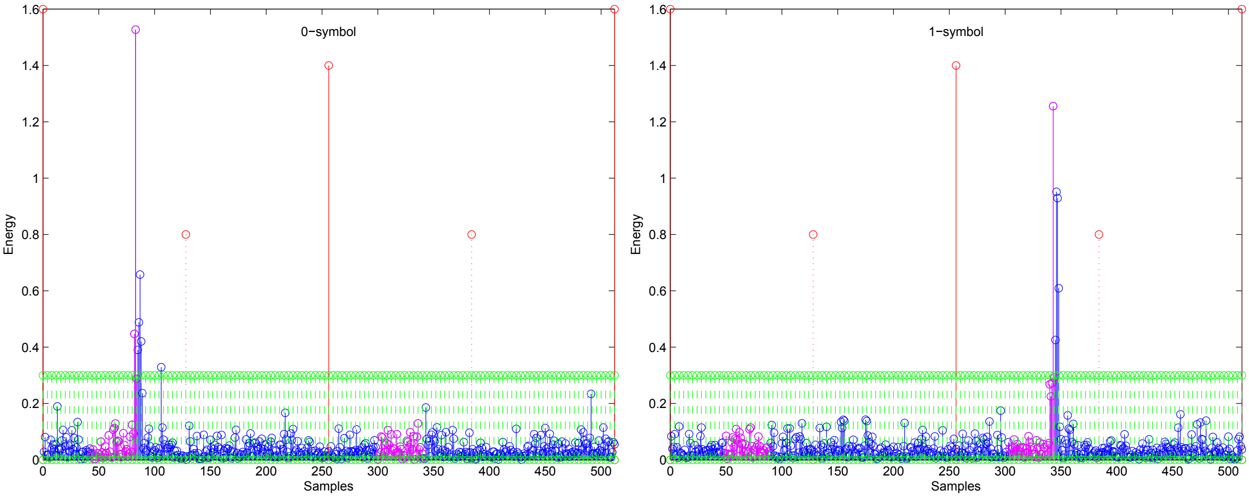


Figure 5.19.: Probability of detection (relay attack)

ED and LC attack on every symbol half

Considering that the countermeasure only works accurately when the integration window is in the region of the delay spread induced by the channel (see Fig.5.13), this opens the door for a normal ED and LC attack on every symbol half (described in Section 2.4). An attacker therefore can mount an ED, considering only the first $10ns$ of the signal and then delaying the pulse to the latest moment. In the current simulation the LC is fixed to $t_{LC} = 70ns$ so that the attacker has 5 samples or $10ns$ to manipulate the symbol on the long-end part. The achieved relay gain is therefore $t_{relay} = t_{LC} - t_{ED} = 70ns - 10ns = 60ns \approx 18m$, assuming that the honest devices uses an integration window $T_{int} = 80ns$. Fig.5.20 illustrates how such an attack is mounted on symbol basis.



(a)

(b)

Figure 5.20.: 0-symbol (a) and 1-symbol (b) under hostile influence (ED and LC attack)

Of course, this attack can only be achieved when the attacker knows the hopping positions of the honest devices, but dealing with LPRF mode of the standard, they are given anyway.

Because of the LC the attacker, of course, needs a higher SNR for not introducing any bit errors. Comparing the BER in Fig.5.21 with Fig.5.1 the attacker almost needs a $9dB$ higher SNR to achieve a successful transmission.

Looking at Fig.5.22 it can be seen that the noise hypothesis could not detect the manipulation; this is obvious because the noise level is not manipulated at all. The manipulation of the signal level is detected exceptionless at higher SNR regions, so that the attacker is forced to guess the proper signal energy, which is very unlikely.

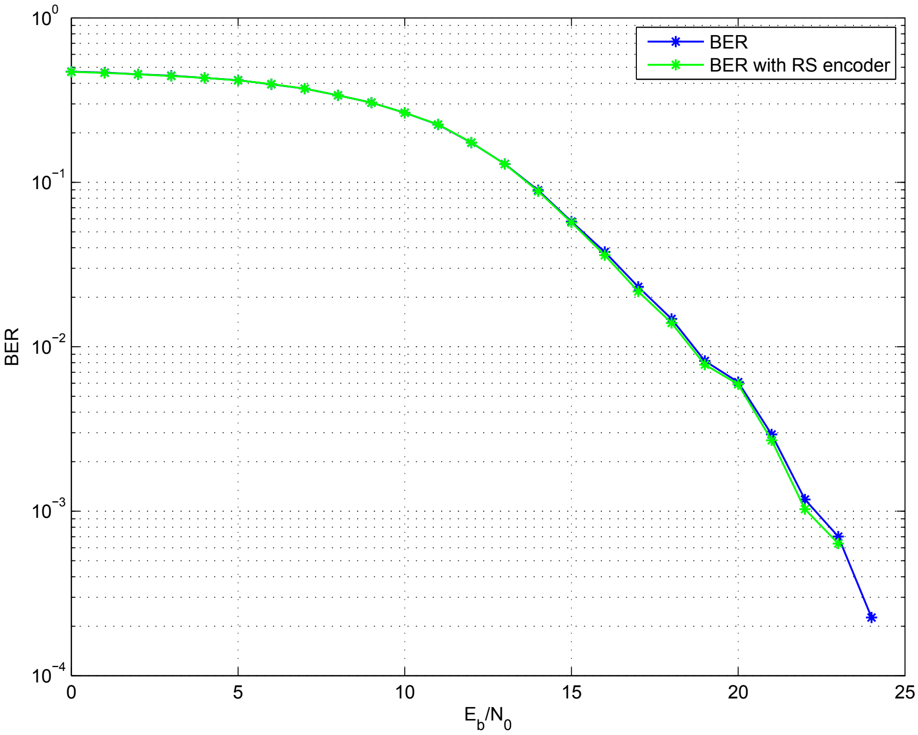


Figure 5.21.: BER for ED and LC attack

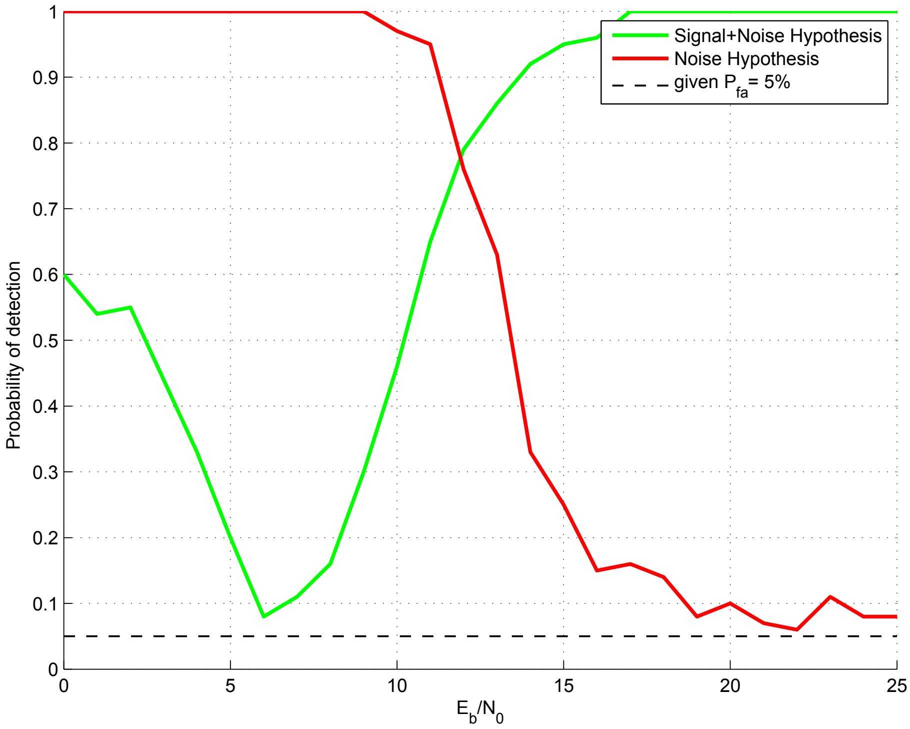


Figure 5.22.: Probability of detection (ED and LC attack)

6. Discussion

In the first Chapters of this work, it is shown that relay attacks against the standard are quite possible. Well matched they achieve a very effective distance manipulation and circumvent any cryptographic effort. The vulnerability introduced by the convolutional encoder has to be patched anyway or can also be eliminated totally considering a non-coherent system.

Following, a simple countermeasure is presented for preventing relay attacks mounted against an energy detector. The approach is based on a hypothesis test of the signal and the noise characteristics, induced by the channel and the receiver.

The derivations of the noise statistics fit very well with the simulations carried out. In contrast, the signal statistics deviate for shorter integration periods and thus lead to inaccuracies in the performance of the countermeasure. Knowing that the random spreading code of the standard produces a superimposed fading effects, the integration window has to be increased for a better estimation of the mean signal level.

Based on the simplicity and therefore the power consumption, the introduced countermeasure leaves anyway a higher security level, because without it an attacker can manipulate the signal levels arbitrarily.

Concerning the simulations the proposed countermeasure works very well and gives an attacker almost no chance to manipulate the signal level, without being detected. Therefore the countermeasure could also be used for warning the consumer that someone has tried to mount an attack against his system.

For further work, it would be interesting to test the countermeasure on CIRs obtained from a measurement campaign and naturally also to carry out further simulations with e.g. the Non-Line Of Sight (NLOS) scenario of the standard (CM4).

A. IEEE 802.15.4a Standard

A.1. Overview

The IEEE 802.15.4a - 2007 Standard is an amendment of the IEEE 802.15.4 Standard (formally called IEEE 802.15.4-2006), specifying the additional alternate PHYs, added to the original standard. The IEEE 802.15 Low Rate (LR) Alternative PHY Task Group (TG4a) for Wireless Personal Area Networks (WPANs), was tasked to amend the 802.15 standard to provide alternate PHY standards that would allow a precision ranging capability with an accuracy in the scale of 1 meter and low power usage within the scope of WPAN.

IEEE 802.15.4a specifies two additional PHYs using UWB and Chirp Spread Spectrum (CSS). For UWB devices, there are three independent bands: the sub-gigahertz band (250-750 MHz), the low band (3.1-5 GHz), and the high band (6-10.6 GHz).

The specifications for UWB LR-WPAN devices also incorporate a number of optional enhancements to improve performance, reduce power consumption, or enhance coexistence characteristics. The most important enhancements is to provide the capability of UWB-LR-WPAN devices to operate under a wider range of radio frequency (RF) channel conditions, while still providing robust performance and precision ranging. Combined with advances in low-cost and low-power process technology, they enable the implementation of LR-WPAN devices that provide enhanced resistance to multipath fading for robust performance in ranging and with very low transmit power.

Furthermore, a common signaling scheme is used to support both coherent and non-coherent receivers. The modulation combines both BPSK and PPM, where each symbol is composed of a burst of UWB pulses. This burst of randomly coded pulses is used to increase the SNR. Aside from that it changes also the statistical behaviour, due to the superimpositions of the fading pulses over the UWB channel.

A.2. Physical Layer of the IEEE 802.15.4a

A.2.1. UWB Frame Format

The format of the UWB frame consists of three major parts: The Synchronization Header SHR preamble, the Physical Header (PHR), and the Physical Service Data Unit PSDU, as shown in Fig.A.1.

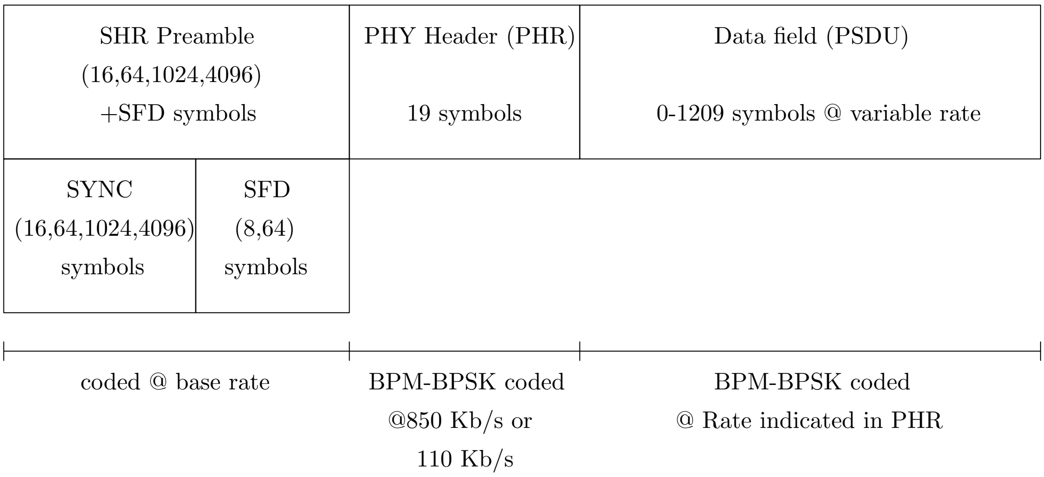


Figure A.1.: UWB frame format

A.2.2. SHR Preamble

The SHR Preamble is added before the PHR, to support receiver algorithms related to Automatic Gain Control (AGC) setting, timing acquisition, coarse and fine frequency recovery, packet and frame synchronization, channel estimation, and leading edge signal tracking for ranging. The SHR preamble depicted in Fig.A.2, can further be divided into the SYNC sequence and the SFD.

In the standard four different lengths for the SYNC field are mandatory with $N_{sync} \in \{16, 64, 1024, 4096\}$ symbols. Mathematically the SYNC part can be expressed by the repetition operation as

$$N_i = \delta_N[n] \otimes S_i \tag{A.1}$$

$$\delta_N[n] = \begin{cases} 1 & n = 0, ..., N_{sync} - 1 \\ 0 & elsewhere. \end{cases} \tag{A.2}$$

The length of the SYNC is a function of the multipath channel, the SNR of the link, and the capability of the receiving PHY. Due to the Figure of Merits (FOM) the length will be

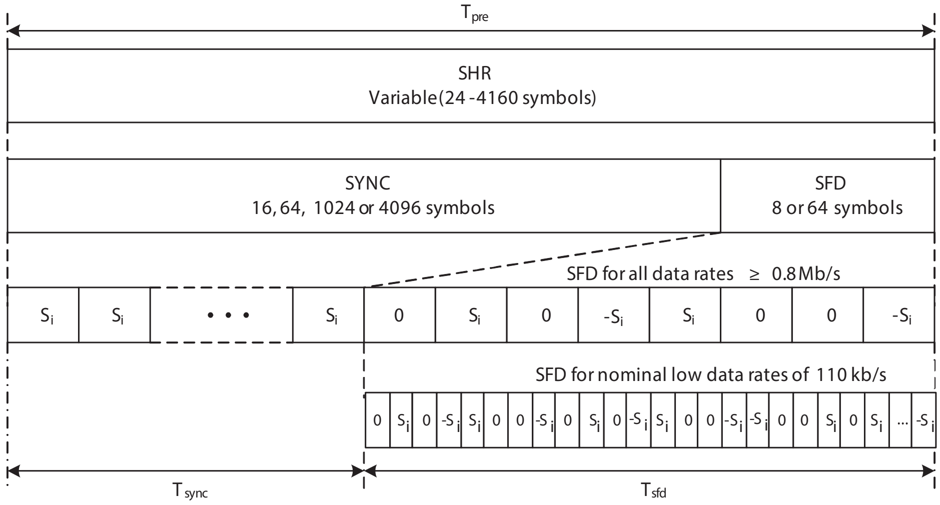

T pre
SHR
Variable(24 -4160 symbols)
SYNC
16, 64, 1024 or 4096 symbols
SFD
8 or 64 symbols
SFD for all data rates ≥ 0.8 Mb/s
Si Si • • • Si 0 Si 0 -Si Si 0 0 -Si
SFD for nominal low data rates of 110 kb/s
0 Si 0 -Si Si 0 0 -Si 0 Si 0 -Si Si 0 0 -Si -Si 0 0 Si 0 Si ... -Si
T sync
T sfd

Figure A.2.: SHR preamble structure [12]

adjusted during transmission or ranging. The longer lengths are preferred for non-coherent receivers to help them improve the SNR, to obtain a reasonably accurate TOA estimate. Each preamble symbol S_i is a sequence of code symbols C_i, drawn from a ternary alphabet and therefore called Ternary Preamble Sequence (TPS) $C_i \in \{-1, 0, 1\}$. Those are selected for use in the UWB PHY because of their periodic autocorrelation properties. The standard defines 24 of these sequences where the first 8 codes are $N_{pcode} = 31$ in length and the remaining 16 are $N_{pcode} = 127$ in length. In each code, $N_N = \frac{N_{pcode}+1}{2}$ elements are non-zero (wich corresponds to the number of pulses in each preamble Symbol S_i). Every code symbol C_i, is then spread by the delta function δ_L of length L. Valid spreading factors L for the TPS are 16 and 64 (Fig.A.3). Using the fact that each symbol has the same number of chips, $N_c = N_{pcode}\, L$ is also correct. The spreading operation, where C_i is extended to the preamble symbol duration is mathematically described as,

$$S_i = C_i \otimes \delta_L[n] \tag{A.3}$$

$$\delta_N[n] = \begin{cases} 1 & n = 0 \\ 0 & n = 1, 2..., L-1 \end{cases} \tag{A.4}$$

where the operator $\otimes$ indicates a Kronecker product.

The duration of one Preamble Symbol S_i is $T_{psym} = N_c T_c = 3968ns$, where T_c is the duration of a chip. Throughout the simulations and the remainder of this work, it is assumed that $T_c = 2ns$, which corresponds to a signal or pulse bandwidth of $B = 500MHz$. Regarding the preceding derivations the length of the whole SYNC field $T_{sync} = N_{sync} N_c$ can be finally defined, which is essential for channel estimation and ranging and has an important function in further considerations.

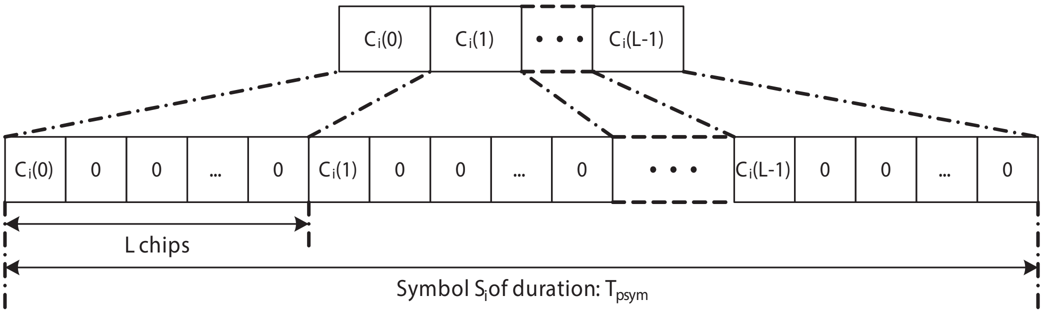


Figure A.3.: Construction of Symbol S_i from Code C_i [12]

Assuming that $\phi(t)$ is the pulse shape of a single UWB pulse, the signal transmitted in the SYNC part is defined by

$$s_{sync,i}(t) = \sqrt{2E_p} \sum_{n=0}^{N_c N_{sync}-1} N_i[n]\, \phi(t - nT_c). \tag{A.5}$$

The features of the ternary sequences are such that their periodic autocorrelation function generated by coherent or non-coherent receivers has no side lobes. Therefore, the PDP is achieved, when the autocorrelation overlaps completely.

The SYNC field is then followed by the SFD with the length $N_{sfd} \in \{8, 64\}$ symbols S_i, modulated by two different sequences A. The short SFD supports the default and medium data rates, while the optional long SFD stands for the nominal low data rate of $110\,kb/s$, see Fig.A.2. The SFD is essential in order to find the start of the data transmission. If the end of the SFD is not detected correctly, the rest of the data packet will be demodulated incorrectly and the transmission fails. The short sequence SFD is depicted completely in Fig.A.2. In contrast to the SHR in the SFD only half of the symbols are active; this fact will be very advantageous for attackers, which can be seen later on in Chapter 2.

The spreading process can be described mathematically as the Kronecker product of the sequence A with the ternary symbol S_i, as

$$M_i = A \otimes S_i \tag{A.6}$$

$$s_{sfd,i}(t) = \sqrt{2E_p} \sum_{m=0}^{N_c N_{sfd}-1} A_i[m]\, \phi(t - mT_c). \tag{A.7}$$

And for the whole SHR preamble the transmitted signal is given by

$$s_{pre}(t) = \sqrt{2E_p} \left\{ \sum_{n=0}^{N_c N_{sync}-1} N_i[n]\, \phi(t - nT_c) + \sum_{m=0}^{N_c N_{sfd}-1} A_i[m]\, \phi(t - mT_c - T_{sync}) \right\}. \tag{A.8}$$

A.2.3. PSDU (Data field)

PHR

The PHR, which consist of 19 bits and conveys information necessary for a successful decoding of the packet at the receiver, shall be added in front of the data field. The PHR contains information about the data rate, used to transmit the following PSDU, the duration of the current frame's preamble and the length of the payload frame. The most important bit is the Ranging Packet Bit (RNG), that makes the current frame to an RFRAME and is intended for ranging. For current considerations the PHR bits are only additional PSDU bits, since they are coded with the same method as the PSDU.

PSDU

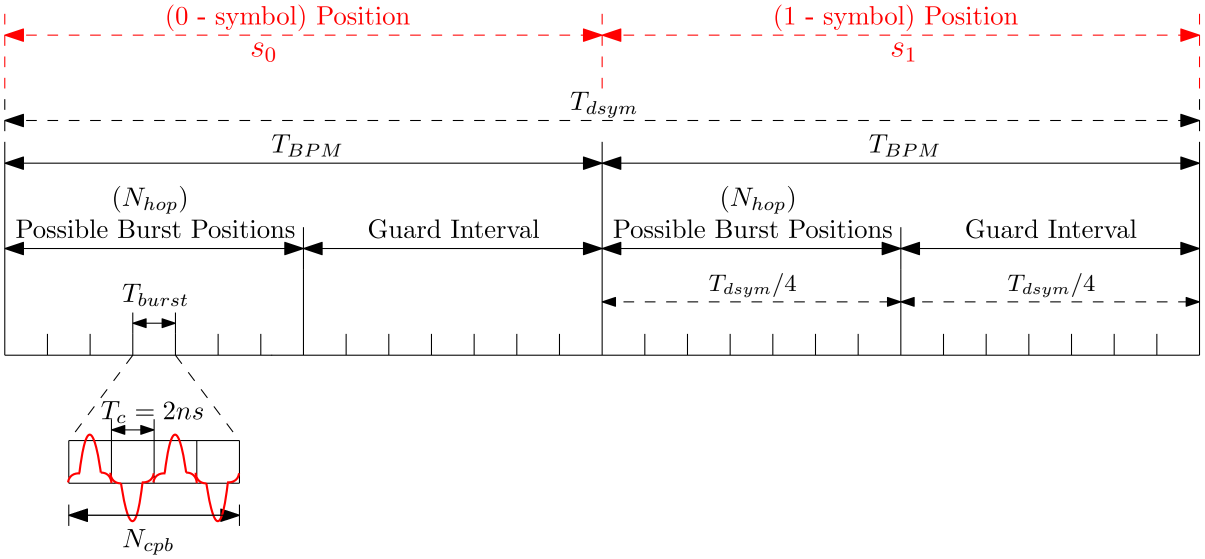


Figure A.4.: Symbol structure of BPM-BPSK

The Data field is the last component of the PPDU and follows the BPM-BPSK modulation scheme. A UWB symbol is capable of carrying two bits of information. One bit determines the position of a burst of pulses while an additional bit is used to modulate the phase (polarity) of the same burst. This modulation scheme enables the application of both non-coherent and coherent receiver; however, the phase can only be decoded by a coherent receiver, due to its perfect synchronization.

Each symbol consists of an integer number of chips N_c, each with duration T_c. The chip duration T_c is derived from the PRF$= 499,2MHz \approx 500MHz$ and is therefore approximately $2ns$. The overall symbol duration is given by $T_{dsym} = N_c T_c$. For BPM the whole symbol is divided into two BPM intervals $T_{BPM} = T_{dsym}/2$.

If the burst is in the first half, the symbol is considered as a 0-symbol s_0 and therefore modulates a zero bit. In contrast, if the burst is located in the second half the symbol is called a 1-symbol s_1 and is therefore a modulated one bit. Each symbol half is also followed by a guard interval of the same length $T_{guard} = T_{dsym}/2$, to mitigate the ISI, introduced by the channel spread, see Fig.A.4.

Each burst is formed by grouping N_{cpb} consecutive pulses and has a duration $T_{burst} = N_{cpb}T_c$. Additional, the polarity of the pulses $\beta \in \{-1, 1\}$ are used to indicate a second bit of information, modulated with the time-varying spreading code from the LFSR. The Total Number of burst durations per symbol is given by $N_{hop} = T_{dsym}/T_{burst}$.

The fact that the burst duration is typically much shorter than the symbol duration, enables multi user access in form of time hopping. When the scrambling code is unknown to the attacker this time hopping can guarantee also additional security against attacks. The number of possible burst positions in a data symbol is given by $N_{hop} = N_{burst}/4$.

Finally, the transmitted waveform during the ith payload symbol can be defined as

$$s_{data,i}(t) = \sqrt{2E_p}\left\{(1-2g_{1,i})\sum_{n=0}^{N_{cpb}-1}(1-2_{s_{n+iN_{cpb}}})\phi(t-g_{0,i}T_{BPM}-iT_{burst}-nT_c)\right\} \quad (A.9)$$

where N_{cpb} is the number of Chips per Burst, $g_{0,i}$ represents the burst position and $g_{1,i}$ the burst polarity, of the ith symbol. $(1-2s_{n+iN_{cpb}})$ is the scrambling sequence derived from the LFSR and iT_{burst} indicates the hopping position within the ith symbol interval.

The whole data field is encoded as follows (Fig.A.5):

- Encode PSDU using systematic Reed-Solomon $RS_6(63, 55)$ block code
- Encode the output of the Reed-Solomon block code using a systematic convolutional encoder
- Spread and modulate the encoded block using BPM-BPSK modulation

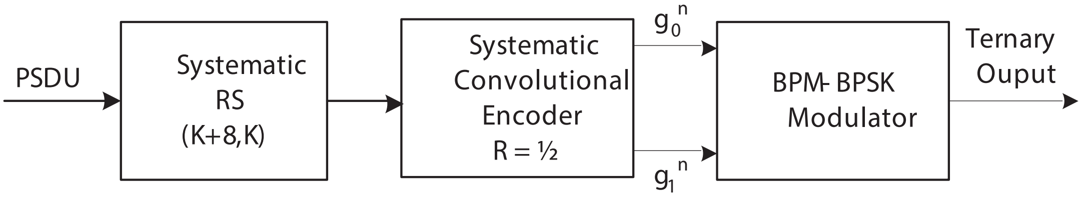


Figure A.5.: Data field encoding process [12]

Throughout the remainder of the work the mandatory LPRF mode is applied. This mode is ideal in terms of dealing with low complexity non-coherent energy detectors. The different timing parameters are shown in Table A.1, for the data frame and in Table A.2 for the SHR preamble part.

Data Symbol Structure					
N_{hop}	N_{cpb}	T_{chip}	# Chips per Symbol	T_{burst}	T_{dsym}
32	4	$2ns$	512	$8ns$	$1024ns$

Table A.1.: LPRF Data timing parameters

Preamble Symbol Structure							
T_{psym}	T_{sync}	T_{sfd}	T_{pre}	N_{sfd}	N_{pcode}	N_{sync}	L
$3968ns$	$254\mu s$	$31.8\mu s$	$285.8\mu s$	8	31	64	64

Table A.2.: LPRF Preamble timing parameters

A.3. Ranging in the IEEE 802.15.4a

Ranging is an optional capability of the standard that has also additional options within. Ranging capability is achieved through support of a number of specific PHY capabilities as well as defined Media Acess Control (MAC) behaviours and protocols. The key protocol focused on, also the mandatory ranging protocol in the standard, is the two-way frame exchange. This protocol relies on the time of flight measurement and is shown in Fig.A.6.

UWB devices that have implemented optional ranging support are called ranging-capable devices RDEVs. UWB PHYs have a bit in the PHR called ranging bit, which is set by the transmitting PHY for frames used in ranging. This bit serves to signal the receiver that this particular frame is intended for ranging and this frame is therefore called a RFRAME.

The critical instant in a RFRAME is the first pulse of the PHR. This pulse is called ranging marker RMARKER. The RMARKER is the most important time instance in the TWR-protocol, because it starts and stops the counter in the receiver who determines T_{ta}^{B} and also in the transmitter for computing T_{round}^{A}. The counter start value therefore represents the TOA of the first pulse of the first symbol of the PHR.

For a full ranging-process the following steps are required. First, a RFRAME is sent from the Verifier to the Prover. A ranging counter start value is captured in the originating device upon the RMARKER departure from the Verifier, and a ranging counter start value is captured in the responding device upon RMARKER arrival at the Prover. At the end of the first frame transmission the counters are running in both devices.

For the second frame transmission the Prover sends an RFRAME as acknowledgment to the Verifier. A ranging counter stop value is captured in the Prover upon RMARKER departure from the Prover and a counter stop value is captured in the Verifier upon RMARKER arrival at the Verifier. Therefore, the Verifier measures the total Round Trip Time (RTT) and the Prover measures the time it takes to reply to the Verifier T_{ta}^{B}. The RTT $= T_{round}^{A}$, the time of flight T_t and therefore also the distance can be computed by the Verifier as

$$T_{round}^{A} = 2\,T_t + T_{ta}^{B} \tag{A.10}$$

$$T_t = \frac{T_{round}^{A} - T_{ta}^{B}}{2} \tag{A.11}$$

$$d = c\,T_t. \tag{A.12}$$

In addition to the two-way ranging the IEEE 802.15.4a standard includes also a private ranging set-up, a time-stamp report and a Symmetric Double Sided (SDS) TWR-protocol.

The private set-up is defined for the initialization of the whole ranging process. In this stage the two devices authenticate each other by exchanging nonces that are unpredictable to an adversary. Once authentication is complete, the TWR can begin, as discussed in the previous part. When the TWR process is successful, every RDEV should have two counter values saved for the computation of the time of flight. The standard for this purpose has specified a time-stamp report that contains five parameters that characterize a single range

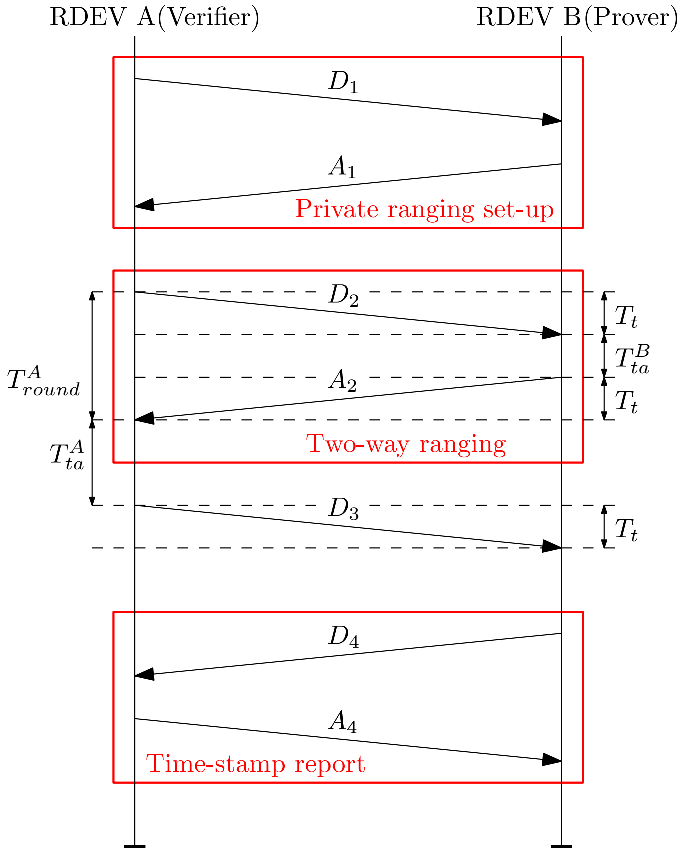


Figure A.6.: Ranging protocol supportet by the IEEE 802.15.4a [22]

measurement: ranging counter start value, ranging counter stop value, two numbers that characterize the crystal and FOM. There is a total of 16 octets in a time-stamp report. These values are generated by the PHY as a set and are not split apart during subsequent data handling. The SDS-protocol allows to reduce the effect of the finite crystal tolerances e_A and e_B, by an additional D_3 illustrated in Fig.A.6. This results in a considerable smaller error margin than in the normal TWR-protocol, the difference is given by

$$\hat{T}_t^{SDS} \approx T_t + \frac{1}{4}\delta(e_A - e_B) \tag{A.13}$$

$$\hat{T}_t^{TWR} \approx T_t + \frac{1}{2}\delta(e_A - e_B). \tag{A.14}$$

Further information about the ranging in IEEE 802.15.4a can be found in[22].

A.3.1. Private Ranging Mode

The private ranging is an optional mode for enhancing the integrity of ranging traffic. The first effective thing that an application can do is encrypting the time stamp reports and so to prevent hostile devices from learning the range information. There is no problem doing this because the exchange of the time stamp report is done in a non-time-critical phase.

Even if the time reports are encrypted, a hostile device can monitor traffic and listen for preambles, which makes it easier to disrupt the ranging traffic between two honest devices. For this reason the standard offers the Dynamic preamble selection DPS, to make attacks more difficult to mount against the ranging protocol.

This countermeasure is effective against the following attacks:

- **Snooper attack**: A hostile device listens to ranging messages and tries to determine the position of the RDEVs.
- **Impostor attack**: A hostile device transmits a conventional RFRAME and tries to confuse the honest devices in terms of timing acquisition.
- **Jamming attack**: A hostile device jams during transmission of the RFRAMEs, to thwart timing acquisition and ranging of the honest device.

The private ranging mode can be divided in two steps:

Authentication Phase

The originator RDEV A, sends a so-called Range Authentication Packet (RAP) to the target RDEV B. This phase is shown as D_1 in Fig.A.6, where the two devices authenticate each other and convey in its encrypted payload the identifiers of the two 127-chips preamble symbols (DPS_{TX}, DPS_{RX}), that will be used in the RFRAMEs D_2, A_2. If RDEV B finds RDEV A authentic, it may reply with an acknowledge A_1 .The DPS were chosen randomly out of the eight predefined codes and they should be varied for each ranging process to deal with replay attacks. Finally, there are no retries allowed with these preambles so that ”jam and spoof the retry” attack will also be defeated.

Ranging Phase

The ranging phase is equal to the normal TWR, RDEV A transmits RFRAME D_2 that uses DPS_{TX} and RDEV B returns an acknowledge A_2 that uses DPS_{RX}. This leads to a probability of 1/8 for a malicious device of picking the right preamble in both sides of the transmission. After these two steps, the honest devices exchange the encrypted time stamp report D_4 and acknowledgment A_4 that completes the private ranging protocol.

B. Signal Mean

The following derivation shows that the mean energy in every data packet is independent from the random spreading code sequence. The countermeasure proposed in Section 3.3 bases on these assumption. The CIR is presented in every single data symbol. Assuming that the integration window collects the whole energy spread by the channel there is

$$h = \int\limits_{0}^{T_{int}} |g(t)|^2 \, dt \tag{B.1}$$

where $g(t)$ is the CIR filtered with the UWB pulse shape $g(t) = h(t) * \phi(t)$.

Next the channel is convolved with the random spreading sequence, generated in the LFSR as

$$h'_n = \int\limits_{0}^{T_{int}} |g(t) * c_n(t)|^2 \, dt = \int\limits_{0}^{T_{int}} \int\limits_{-\infty}^{+\infty} g(\lambda) c_n(t-\lambda) \, d\lambda \left[\int\limits_{-\infty}^{+\infty} g(\mu) c_n(t-\mu) \, d\mu \right]^* dt. \tag{B.2}$$

The spreading code is described as Dirac sequence $c_n(t) = \sum\limits_{i} d_i \, \delta(t - iT_c)$, where $d_i \in \{\pm 1\}$.

Then the mean energy of the channel for the nth code realization is given as

$$\bar{h} = E_c\{h'_n\} \widehat{=} E_c \left\{ \int\limits_{0}^{T_{int}} \int\limits_{-\infty}^{+\infty} \int\limits_{-\infty}^{+\infty} g(\lambda) c_n(t-\lambda) g^*(\mu) c_n^*(t-\mu) \, d\lambda \, d\mu \, dt \right\} \tag{B.3}$$

$$= \int\limits_{0}^{T_{int}} \int\limits_{-\infty}^{+\infty} \int\limits_{-\infty}^{+\infty} g(\lambda) \, g^*(\mu) \; \underbrace{E_c\{(t-\lambda) c_n^*(t-\mu)\}}_{=I} \, d\lambda \, d\mu \, dt. \tag{B.4}$$

By applying $c_n(t) = \sum\limits_{i=1}^{N_{cpb}} d_i \, \delta(t - iT_c)$ and $c_n(t) = \sum\limits_{j=1}^{N_{cpb}} d_j^* \, \delta(t - jT_c)$ for the complex conjugate on I in equation B.4, there is

$$I = E \left\{ \sum_{i=1}^{N_{cpb}} d_i \, \delta(t - \lambda - iT_c) \sum_{j=1}^{N_{cpb}} d_j^* \, \delta(t - \mu - jT_c) \right\} \tag{B.5}$$

for $(\lambda + iT_c) = (\mu + jT_c)$

$$I = \sum_{i=1}^{N_{cpb}} \sum_{j=1}^{N_{cpb}} E\{d_i\, d_j^*\}\, \delta(t - \lambda - iT_c)\, \delta(\lambda + iT_c - \mu - jT_c) \tag{B.6}$$

$$\tag{B.7}$$

for $i = j$

$$I = \sum_{i=1}^{N_{cpb}} \underbrace{E\{|d_i^2|\}}_{=1}\, \delta(t - \lambda - iT_c)\, \delta(\lambda - \mu) \tag{B.8}$$

since $E\{d_i\, d_j^*\} = 0$ for $i \neq j$.

Applying the result in equation B.8 on B.4 there is

$$= \sum_{i=1}^{N_{cpb}} \int_0^{T_{int}} \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} g(\lambda)\, g^*(\mu)\, \delta(t - \lambda - iT_c)\, \delta(\lambda - \mu)\, d\lambda\, d\mu\, dt \tag{B.9}$$

$$= \sum_{i=1}^{N_{cpb}} \int_0^{T_{int}} \int_{-\infty}^{+\infty} g(\lambda)\, g^*(\lambda)\, \delta(t - \lambda - iT_c)\; d\lambda\, dt \tag{B.10}$$

$$= \sum_{i=1}^{N_{cpb}} \underbrace{\int_0^{T_{int}} |g(t - iT_c)|^2\, dt}_{\widehat{=}\, h} \tag{B.11}$$

$$\widehat{=}\, N_{cpb}\, h. \tag{B.12}$$

Assuming that $\bar{h} = \frac{1}{N} \sum_{n=1}^{N} h'_n = 1$ and for the LPRF mode $N_{cpb} = 4$ a mean energy of 4 is achieved.

C. Signal and Noise Statistics

Considering the receiver architecture given in Fig.2.1, the statistical behavior of the sampled discrete signal has to be derived as follows:

$$r(t) = \sqrt{2}\Re\{[g(t) + v(t)]e^{j\omega_c t}\} \tag{C.1}$$

The received bandpass signal $r(t)$ that is fed into the energy detector is given by the real value of the complex baseband signals $g(t)$ and $v(t)$ and modulated by a carrier with frequency $\omega_c = 2\pi f_c$.

$$y[n] = \int\limits_{nT_{int}}^{(n+1)T_{int}} r^2(t)\,dt = \int\limits_{nT_{int}}^{(n+1)T_{int}} \left[\sqrt{2}\Re\{[g(t) + v(t)]e^{j\omega_c t}\}\right]^2 dt \tag{C.2}$$

$$= 2\int\limits_{nT_{int}}^{(n+1)T_{int}} \{[g_r(t) + v_r(t)]\cos(\omega_c t) - [g_i(t) + v_i(t)]\sin(\omega_c t)\}^2\,dt \tag{C.3}$$

$$\begin{aligned} = 2\int\limits_{nT_{int}}^{(n+1)T_{int}} & [g_r(t) + v_r(t)]^2 \underbrace{\cos^2(\omega_c t)}_{=\frac{1}{2}} \\ & - 2[g_r(t) + v_r(t)]\underbrace{\cos(\omega_c t)}_{=0}[g_i(t) + v_i(t)]\underbrace{\sin(\omega_c t)}_{=0} \\ & + [g_r(t) + v_r(t)]^2 \underbrace{\sin^2(\omega_c t)}_{=\frac{1}{2}}\,dt \end{aligned} \tag{C.4}$$

$$= 2\int\limits_{nT_{int}}^{(n+1)T_{int}} \frac{1}{2}[g_r(t) + v_r(t)]^2 + \frac{1}{2}[g_i(t) + v_i(t)]^2\,dt \tag{C.5}$$

$$= \int\limits_{nT_{int}}^{(n+1)T_{int}} [g_r(t) + v_r(t)]^2 + [g_i(t) + v_i(t)]^2\,dt \tag{C.6}$$

$$= \int\limits_{nT_{int}}^{(n+1)T_{int}} |[g(t) + v(t)]|^2\,dt \tag{C.7}$$

$$= \int\limits_{nT_{int}}^{(n+1)T_{int}} \underbrace{|g(t)|^2}_{y_{ss}} + \underbrace{|v(t)|^2}_{y_{vv}} + \underbrace{2|g_r(t)v_r(t) + g_i(t)v_i(t)|}_{y_{sv}}\,dt. \tag{C.8}$$

The squaring operation of the receiver generates 3 terms, which are the signal-by-signal term y_{ss}, the noise-by-noise term y_{vv} and the signal-by-noise cross term y_{sv}. In the following Sections these terms are described in more detail, as they are essential for the calculation of the hypotheses.

C.1. Signal by Signal Term

Considering that the integration time equals the delay spread of the channel and the fact that the transmitted pulse energy is normalized to one, the received pulse energy is unity. The mean represents the accumulated signal energy in each integration interval as

$$y_{ss}[n] = \int\limits_{nT_{int}}^{(n+1)T_{int}} |g(t)|^2 \, dt = E_p. \tag{C.9}$$

Due to the deterministic nature of $g(t)$, the expectation $E\{y_{ss}[n]\} = y_{ss}[n]$ and the variance $var\{y_{ss}[n]\} = 0$.

C.2. Noise by Noise Term

Considering the $w(t)$ is AWGN with the two-sided power spectral density of N_0, the real and imaginary parts are $w_{r,i}(t)$ each having a two sided PSD of $N_0/2$.

$$y_{vv}[n] = \int\limits_{nT_{int}}^{(n+1)T_{int}} |v(t)|^2 \, dt \tag{C.10}$$

$$E\left\{w_{r,i}(t)\, w_{r,i}(t-\tau)\right\} = \frac{N_0}{2}\delta(\tau) \tag{C.11}$$

Filtering

To reduce the accumulated noise in the receiver the first stage is to apply a band pass filter. The filter used for this purpose is a matched filter, which means that the impulse response is the reversed pulse shape $\phi(-t)$. This filter is optimal, in terms of maximizing the SNR. The filtered noise signal $v(t)$ is shown in Fig.C.1 and described as

$$v(t) = w(t) * \phi(-t). \tag{C.12}$$

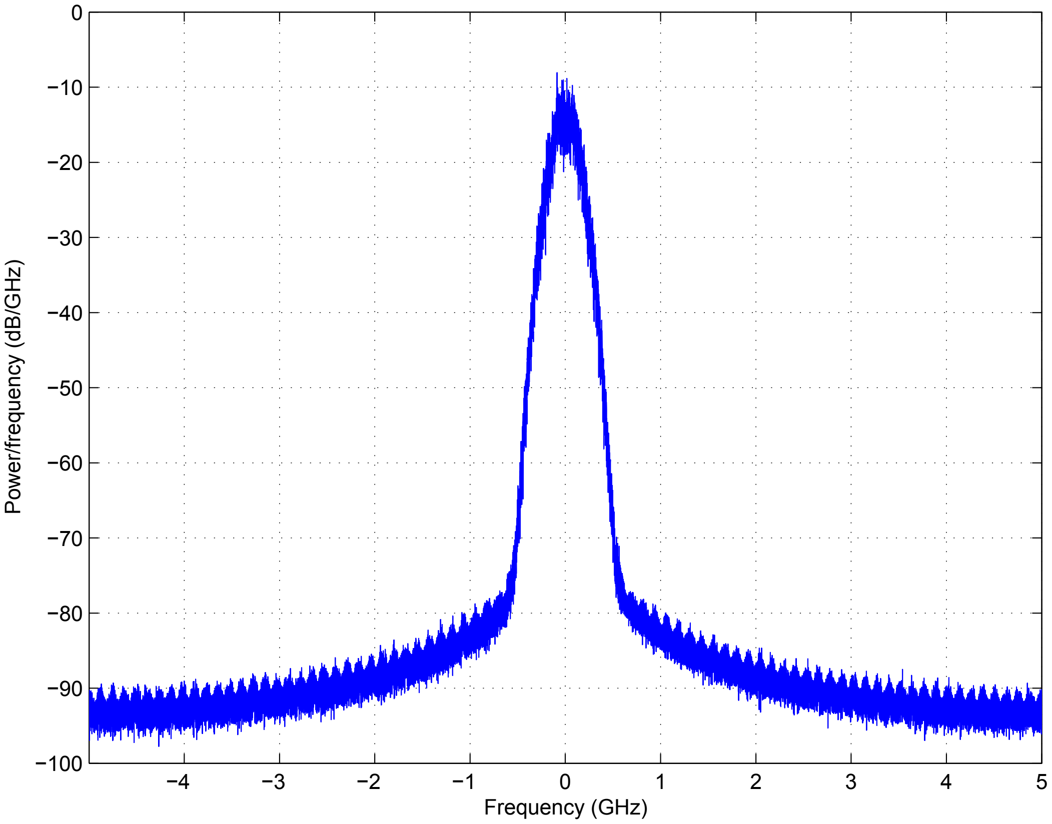


Figure C.1.: Filtered Noise $E_b/N_0 = 20dB$

The filtering process changes the Amplitude distribution depending on the bandwidth ($B = 1/T_p$) of the filter[2]. The real and imaginary part of the filtered noise are normal distributed according to

$$v_r(t) \sim \mathcal{N}\left(0, \frac{N_0 B}{2}\right) \qquad v_i(t) \sim \mathcal{N}\left(0, \frac{N_0 B}{2}\right). \tag{C.13}$$

Squaring

The next step in the receiver architecture is the square-law device. This component increases the signal bandwidth and changes the amplitude of the distribution of the noise samples. Consequently, the distribution of the noise samples changes; from a Gaussian

[2] For the Simulations, the filter is considered as an ideal low-pass filter, with a flat frequency response between $f \pm \frac{B}{2}$, because the matched filter changes the noise distribution, which complicates further derivations

distribution with zero mean for the real and imaginary part to a Chi-Square distribution with 2 degrees of freedom as

$$\chi_2^2 \sim Z_1^2 + Z_2^2 \qquad Z_n \sim \mathcal{N}(0,1) \tag{C.14}$$

$$E\{\chi_n^2\} = n = 2 \qquad var\{\chi_n^2\} = 2n = 4. \tag{C.15}$$

By substituting $Z_i = \left(\frac{X_i - \mu}{\sigma}\right)^2$ with $\mu = 0$ and $\sigma^2 = \frac{N_0 B}{2}$, there is

$$E\{\chi_n^2\} = n = 2\sigma^2 = \frac{2N_0 B}{2} = N_0 B \tag{C.16}$$

$$var\{\chi_n^2\} = 2n = 4(\sigma^2)^2) = \frac{4N_0^2 B^2}{4} = N_0^2 B^2$$
$$. \tag{C.17}$$

Therefore $v^2(t) \sim \{\chi_2^2\}$ with $\mu = N_0 B$ and $\sigma^2 = N_0^2 B^2$.

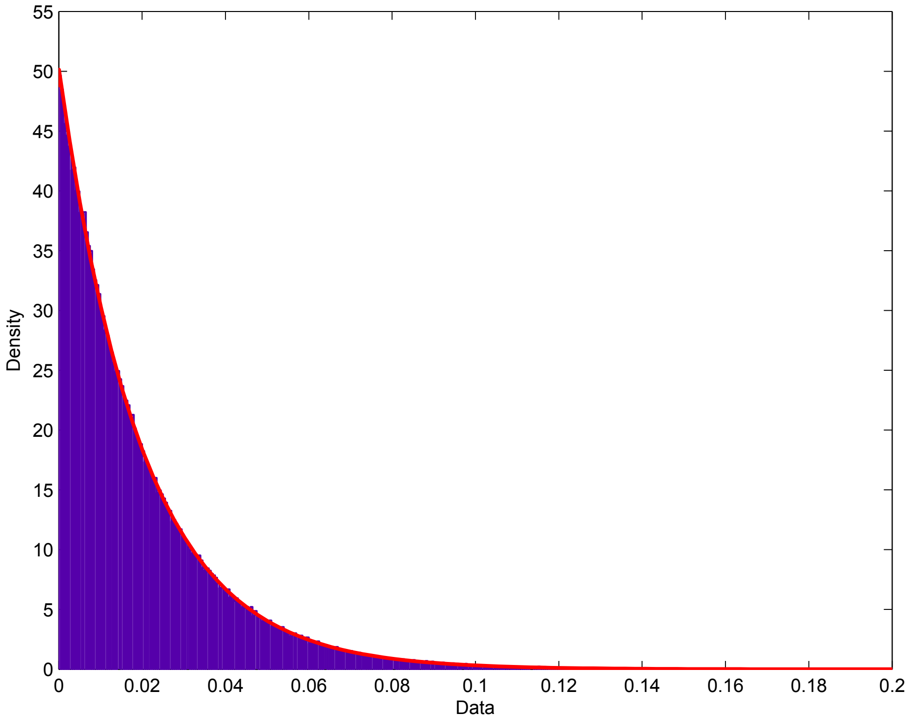


Figure C.2.: Squared noise distribution $E_b/N_0 = 20dB$.

Integration

Up to this point, the statistic fits perfectly with the simulation. The integration device is also known as low pass or moving average filter. In the time domain, the filter has rectangular impulse response, averaging over the length of $T_{int}/T_p = 2T_{int}B$ noise samples. For the noise samples the integration process is given by (following the reference [16])

$$y[n] = \int_{nT_{int}}^{(n+1)T_{int}} v^2(t)\,dt \approx T_p \sum_{i=1}^{\frac{T_{int}}{T_p}} v^2[i] \approx \frac{1}{B} \sum_{i=1}^{2T_{int}B} v^2[i]. \tag{C.18}$$

The Amplitude distribution changes into a Chi-square distribution with $2T_{int}B$ degrees of freedom. The mean and the variance of the distribution can be calculated by using the summation and scaling properties of the distribution.

$$y_{vv}[n] \sim \chi^2_{2T_{int}B} \text{ with } \mu = \frac{N_0BT_{int}B}{B} = N_0BT_{int} \text{ and } \sigma^2 = \frac{N_0^2B^2T_{int}B}{B^2} = N_0^2T_{int}B$$

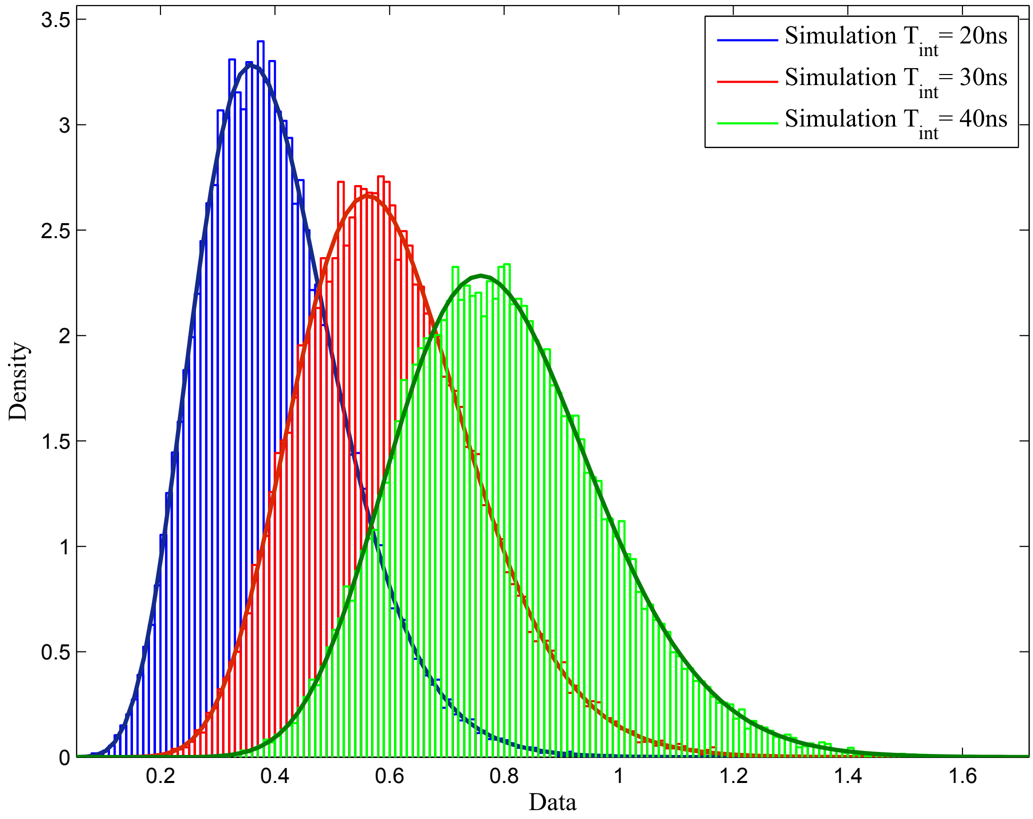


Figure C.3.: Noise distributions for different integration windows $B = 500MHz$.

The derivation for the integration process expressed above is a good approximation for large time bandwidth products ($T_{int}B$).

C.3 shows the simulated noise distributions for different integration intervals. The difference of the analytical chi-square fits and the simulated distributions reduces with increasing integration intervals.

Looking at the noise distribution, it can be observed that with increasing integration intervals the shape tends to be more and more Gaussian.

C.3. Signal by Noise Term

$$y_{sv}[n] = \int\limits_{nT_{int}}^{(n+1)T_{int}} 2|g_r(t)v_r(t) + g_i(t)v_i(t)|\,dt \tag{C.19}$$

The expected value of the signal by noise Term is zero because each of the noise terms is a zero mean Gaussian random process and they are independent of each other. Therefore there is no new contribution to the previously computed terms, in the expected value $E\{y_{sv}[n]\} = 0$.

$$E\{y_{sv}[n]\} = 2\underbrace{E\{g_r(t)v_r(t)\}}_{=0} + 2\underbrace{E\{g_i(t)v_i(t)\}}_{=0} = 0 \tag{C.20}$$

It follows for the variance $y_{sv}[n] = E\{y_{sv}^2[n]\}$

$$var\{y_{sv}[n]\} = 4\left(E\{g_r(t)g_r(t)\}E\{v_r(t)v_r(t)\}\right) + 4\left(E\{g_i(t)g_i(t)\}E\{v_i(t)v_i(t)\}\right) \tag{C.21}$$

$$= 4g_r^2(t)E\{v_r(t)v_r(t)\} + 4g_i^2(t)E\{v_i(t)v_i(t)\}. \tag{C.22}$$

The expectation of the 2 noise terms could be seen as the autocorrelation at $\tau = 0$, which equals to the spectral power of the filtered noise and thus to the variance of the real and imaginary parts $var\{v_{i,q}(t)\} = \frac{N_0 B}{2}$. Therefore the equation simplifies to

$$var\{y_{sv}[n]\} = 4g_r^2(t)\frac{N_0 B}{2} + 4g_i^2(t)\frac{N_0 B}{2} = 2g_r^2(t)N_0 B + 2g_i^2(t)N_0 B. \tag{C.23}$$

Assuming that the bandwidth of the filter is equal to the bandwidth of the pulse shape, there is

$$var\{y_{sv}[n]\} = 2(g_r^2(t) + g_i^2(t))N_0 \approx 2E_p N_0. \tag{C.24}$$

Finally, all the means and variances to complete the statistical model can be added up. The expected value of $y[n]$ is given by

Order k	Moment $E(X^k)$
0	1
1	μ
2	$\mu^2 + \sigma^2$
3	$\mu^3 + 3\mu\sigma^2$
4	$\mu^4 + 6\mu^2\sigma^2 + 3\sigma^4$

Table C.1.: Moments of a normal distributed RV

$$E\{y[n]\} = E\{y_{ss}[n]\} + E\{y_{sv}[n]\} + E\{y_{ss}[n]\} \tag{C.25}$$

$$= N_0 T_{int} B + E_p \tag{C.26}$$

and the variance is computed as

$$var\{y[n]\} = var\{y_{ss}[n]\} + var\{y_{sv}[n]\} + var\{y_{vv}[n]\} \tag{C.27}$$

$$+ 2covar\{y_{ss}[n], y_{vv}[n]\} + 2covar\{y_{ss}[n], y_{sv}[n]\} + 2covar\{y_{vv}[n], y_{sv}[n]\} \tag{C.28}$$

$$= N_0^2 T_{int} B + 2E_p N_0. \tag{C.29}$$

A simpler way to achieve this result (proposed in [23]), is given by introducing the moments of $E(x^2)$, see Table C.1.

The mean and the variance are given as

$$E(x^2) = \mu^2 + \sigma^2 \tag{C.30}$$

$$var(x^2) = E(x^2)^2 - E^2(x^2) = E(x^4) - E^2(x^2) \tag{C.31}$$

$$= (\mu^4 + 6\mu^2\sigma^2 + 3\sigma^4) - (\mu^4 + 2\mu^2\sigma^2 + \sigma^4) \tag{C.32}$$

$$= 4\mu^2\sigma^2 + 2\sigma^4. \tag{C.33}$$

By using $x_r^2 \sim \mathcal{N}(g_r, \frac{N_0 B}{2})$ and $x_i^2 \sim \mathcal{N}(g_i, \frac{N_0 B}{2})$, there is

$$E(x^2) = (g_r + g_i)^2 + N_0 B \tag{C.34}$$

$$var(x^2) = 2(g_r + g_i)^2 N_0 + N_0^2 B^2. \tag{C.35}$$

Due to the scaling properties introduced by the integration process see equation C.18, the same result is achieved as

$$E(x^2) = E_p + N_0 T_{int} B \tag{C.36}$$

$$var(x^2) = 2E_p N_0 + N_0^2 T_{int} B. \tag{C.37}$$

List of Figures

List of Tables

Bibliography

[1] Capkun, Srdjan ; Danev, Boris ; Francillon, Aurélien: Relay attacks on passive keyless entry and start systems in modern cars, Eidgenössische Technische Hochschule Zürich, Department of Computer Science, 2011

[2] Flury, Manuel ; Poturalski, Marcin ; Papadimitratos, Panos ; Hubaux, Jean-Pierre ; Le Boudec, Jean-Yves: Effectiveness of Distance-decreasing Attacks Against Impulse Radio Ranging. In: *Proceedings of the Third ACM Conference on Wireless Network Security*. New York, NY, USA : ACM, 2010 (WiSec '10). – ISBN 978–1–60558–923–7, S. 117–128

[3] Flury, Manuel: *Interference Robustness and Security of Impulse-Radio Ultra-Wide Band Networks*. Suisse, ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE, Doctoral Thesis, 2010

[4] Brands, Stefan ; Chaum, David: Distance-Bounding Protocols. In: Helleseth, Tor (Hrsg.): *Advances in Cryptology — EUROCRYPT '93* Bd. 765. Springer Berlin Heidelberg, 1994. – ISBN 978–3–540–57600–6, S. 344–359

[5] Gigl, Thomas ; Preishuber-Pfluegl, Josef ; Arnitz, Daniel ; Witrisal, Klaus: Experimental characterization of ranging in IEEE802.15.4a using a coherent reference receiver. In: *2009 IEEE 20th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2009)*, S. 92–96

[6] Andreas F. Molisch ; Kannan Balakrishnan ; Chia-chin Chong ; Shahriar Emami ; Andrew Fort ; Johan Karedal ; Juergen Kunisch ; Hans Schantz ; Ulrich Schuster ; Kai Siwiak: IEEE 802.15.4a channel model - final report. In: *Converging: Technology, work and learning.*, 2004

[7] Molisch, Andreas F.: *Wireless communications*. Chichester : Wiley, 2007. – ISBN 0–470–84888–X

[8] Hancke, Gerhard P. ; Kuhn, Markus G.: Attacks on Time-of-flight Distance Bounding Channels. In: *Proceedings of the First ACM Conference on Wireless Network Security*. New York, NY, USA : ACM, 2008 (WiSec '08). – ISBN 978–1–59593–814–5, S. 194–202

[9] Clulow, Jolyon ; Hancke, Gerhard P. ; Kuhn, Markus G. ; Moore, Tyler: So Near and Yet So Far: Distance-Bounding Attacks in Wireless Networks. In: *Computer Laboratory, University of Cambridge* Bd. 4357, S. 83–97

[10] Flury, Manuel ; Merz, Ruben ; Le Boudec, Jean-Yves: Robust non-coherent timing acquisition in IEEE 802.15.4a IR-UWB networks. In: *2009 IEEE 20th International Symposium on Personal, Indoor and Mobile Radio Communications - (PIMRC 2009)*, S. 1642–1646

[11] Poturalski, Marcin ; Flury, Manuel ; Papadimitratos, Panos ; Hubaux, Jean-Pierre ; Le Boudec, Jean-Yves: Distance Bounding with IEEE 802.15.4a: Attacks and Countermeasures. In: *IEEE Transactions on Wireless Communications* 10 (2011), Nr. 4, S. 1334–1344. – ISSN 1536–1276

[12] IEEE: *Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirement Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs).* 2007

[13] Kuhn, Marc ; Luecken, Heinrich ; Tippenhauer, Nils O.: UWB impulse radio based distance bounding. In: *2010 7th Workshop on Positioning, Navigation and Communication (WPNC)*, S. 28–37

[14] Witrisal, Klaus: Statistical Analysis of the IEEE 802.15.4a UWB PHY over Multipath Channels. In: *Wireless Communications and Networking Conference, 2008. WCNC 2008. IEEE*, 2008, S. 130–135

[15] Kay, Steven M.: *Prentice Hall signal processing series.* Bd. / Steven M. Kay ; Vol. 1: *Estimation theory.* 19. print. Upper Saddle River, NJ : Prentice Hall PTR, 2011. – ISBN 0133457117

[16] Urkowitz, Harry: Energy detection of unknown deterministic signals. In: *Proceedings of the IEEE* 55 (1967), April, Nr. 4, S. 523–531

[17] Witrisal, K. ; Leus, G. ; Janssen, G.J.M. ; Pausini, M. ; Troesch, F. ; Zasowski, T. ; Romme, J.: Noncoherent ultra-wideband systems. In: *Signal Processing Magazine, IEEE* 26 (2009), July, Nr. 4, S. 48–66

[18] Thomas Gigl: *Low-Complexity Localization using Standard-Compliant UWB Signals.* Austria, Graz University of Technology, Doctoral Thesis, 01.12.2010

[19] Bernhard Geiger: *Enhanced Accuracy Channel Estimation and Ranging for Energy Detectors.* Austria, Graz University of Technology, Master's Thesis, 01.10.2009

[20] Gishkori, Shahzad ; Leus, Geert ; Delic, Hakan: Energy Detection of Wideband and Ultra-Wideband PPM. In: *GLOBECOM 2010 - 2010 IEEE Global Communications Conference*, S. 1–5

[21] Dubouloz, S. ; Denis, B. ; Rivaz, S. d. ; Ouvry, L.: Performance Analysis of LDR UWB Non-Coherent Receivers in Multipath Environments. In: *2005 IEEE International Conference on Ultra-Wideband*, 05-08 Sept. 2005, S. 491–496

[22] Sahinoglu, Zafer ; Gezici, Sinan: Ranging in the IEEE 802.15.4a Standard. In: *WAMICON 2006.* Mitsubishi Electric Research Laboratories, S. 1–5

[23] Kay, Steven M.: *Prentice Hall signal processing series.* Bd. / Steven M. Kay ; Vol. 2: *Detection theory.* 15. print. Upper Saddle River, NJ : Prentice Hall PTR, 2011. – ISBN 0–13–504135–X