Distance Bounding Protocols on TH-UWB Link and their Analysis over Noisy Channels

Ahmed Benfarah, Benoit Miscopein, Jean-Marie Gorce, Cédric Lauradoux, Bernard Roux

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Distance Bounding Protocols on TH-UWB Link and their Analysis Over Noisy Channels

Ahmed Benfarah — Benoit Miscopein — Jean-Marie Gorce — Cédric Lauradoux — Bernard Roux

N° 7385

September 2010

Thème NUM

ISSN 0249-6399 ISRN INRIA/RR--7385--FR+ENG

INSTITUT NATIONAL
DE RECHERCHE
EN INFORMATIQUE
ET EN AUTOMATIQUE

INRIA

centre de recherche
GRENOBLE - RHÔNE-ALPES

Distance Bounding Protocols on TH-UWB Link and their Analysis Over Noisy Channels

Ahmed Benfarah *, Benoit Miscopein * , Jean-Marie Gorce †,
Cédric Lauradoux † , Bernard Roux ‡

Thème NUM — Systèmes numériques
Équipes-Projets SWING

Rapport de recherche n° 7385 — September 2010 — 29 pages

Abstract: Relay attacks represent nowadays a critical threat to authentication protocols. They can be thwarted by deploying distance bounding protocols on an UWB radio. Exploiting the characteristics of time-hopping UWB radios to enhance distance bounding protocols leads to two design strategies. The first one is based on a secret time-hopping code while the mapping code is public. The second strategy exploits a secret mapping code with a public time-hopping code. The merits of each strategy are established over noise-free and noisy channels as well as for different radio parameters.

Key-words: Relay attacks, distance bounding, UWB and time-hopping.

* Orange LABS, F-38240 Meylan, France
† Université de Lyon, INRIA, INSA-Lyon, CITI laboratory F-69621 Villeurbanne, France
‡ Université de Lyon, CNRS, INSA-Lyon, Institut Camille Jordan

Centre de recherche INRIA Grenoble – Rhône-Alpes
655, avenue de l'Europe, 38334 Montbonnot Saint Ismier
Téléphone : +33 4 76 61 52 00 — Télécopie +33 4 76 61 52 52

Résumé :

Mots-clés :

1 Introduction

Cooperative communications and the relay channel are two very active fields of information theory. Surprisingly, the problem of communication relaying has also been deeply studied over the last years by the security community: relaying messages is the basic mechanism to mount *man in the middle attacks* (MITMs). In practice, the simple act of relaying messages at the physical layer level is enough to break the most complex authentication protocols as shown by *Desmedt et al.* [1]. Since then, the so-called relay attacks have been demonstrated against various wireless technologies [2] [3] such as RFID [4], Bluethooth [5], and even smartcards [6]. Moreover, relay attacks can be used as a mean to implement more advanced attacks such as wormhole in wireless sensor networks (WSNs) [7].

Brands and Chaum proposed in [8] a first solution to relay attacks: *distance bounding protocols*. These protocols deal with the different variants of relay attacks, *i.e.* the mafia fraud, the terrorist fraud and the distance fraud. Fundamentally, a distance bounding protocol is a process between two parties, *i.e.* the verifier V and the prover P, that combines authentication and distance upper-bounding. An overview of the existing solutions as well as definitions are to be found in [9].

Ultra-wideband (UWB) communication is a promising candidate for the implementation of distance bounding protocols [10, 11]. An UWB system offers fine time resolution and synchronization which are critical to measure the time of flight to obtain distance or location [12]. Some recent works [13, 11] have discussed many issues on the implementation of a distance bounding protocol on an UWB radio.

This work presents two approaches to include distance bounding protocols on time-hopping UWB impulse radio (TH-UWB-IR or simply TH-UWB) in order to thwart the Mafia frauds. Some early results of this work are to be presented by the authors at Globecomm 2010 [14]. The main features of the TH-UWB radio are the time-hopping code and the mapping code. The first scheme proposed keeps the time-hopping code secret and the mapping code public. In the second scheme, the roles are swapped. The security and memory consumption of these protocols are analyzed and compared to existing distance bounding protocols for different modulation schemes, *i.e.* PPM and OOK. The security analysis is organized in two steps. The security of each protocol is assessed in a noise-free environment. Then, noise is considered. In the existing literature [15, 16, 11, 17], the noise is often modeled with the bit error rate (BER) independently from the radio technology. The proposed security analysis includes more radio parameters such as the modulation, the channel model or the receiver architecture. The benefits of adapting distance bounding protocols to the TH-UWB are established.

The paper is organized as follows. The next section describes the physical layer of the UWB link and presents the distance bounding protocols and more precisely the Hancke and Khun protocol [13]. In Section 3, a distance bounding protocol with a secret time-hopping code is introduced and analyzed. The impact of the modulation is also discussed. The Section 4 is devoted to the use of a secret mapping code. Finally, the Section 5 compares the results of this paper in terms of security and memory consumption to the state of the art.

2 Preliminaries

2.1 Time-Hopping UWB

UWB-IR (Ultra Wideband-Impulse Radio) is a transmission scheme which consists in the emission of very short temporal pulses with low duty cycle. These pulses occupy a broad spectrum in the order of GHz. Time-hopping in UWB systems provides the capacity of medium accessing [18]. It is also a way of smoothing the radiated spectrum to optimize the transmission power. The aim of this subsection is to detail the modeling of a TH-UWB radio.

2.1.1 Structure of a TH-UWB symbol

A TH-UWB symbol of duration T_s is composed of N_f frames each of duration T_f. The frame contains also N_c chips whose duration is T_c. The frame includes only one pulse associated to the information symbol. A pulse being very short, it does not occupy all the duration of the chip. A time-hopping code sequence S over $\mathbb{Z}/N_c\mathbb{Z}$ determines the chip occupied by the pulse in each frame.

The TH-UWB symbol contains redundancy: several pulses are transmitted per symbol. A mapping code C of length N_f corresponds the binary symbols 0 or 1 to their respective pulses modulation. A repetition mapping code is often used, *i.e.* the N_f pulses are similarly modulated [19]. However, other mapping codes are possible for instance the following code has been proposed in [20] ($N_f = 4$):

$$C = \begin{cases} 0,1,0,1 \text{ if the symbol is equal to 0,} \\ 1,0,1,0 \text{ if the symbol is equal to 1.} \end{cases} \quad (1)$$

Different modulation options have been suggested for UWB systems like BPSK, PPM and OOK. More details on modulations for UWB systems can be found in [21]. The PPM and OOK modulations are used in the following. A TH-UWB symbol is depicted for PPM (resp. OOK) in Fig. 1 (resp. Fig. 2). The expressions of the signal transmitted with PPM and OOK are:

$$s_{PPM}(t) = \sum_{k=-\infty}^{+\infty} \sum_{j=0}^{N_f-1} p\big(t - k.T_s - S_j(k).T_c - C_j(k).\delta\big), \quad (2)$$

$$s_{OOK}(t) = \sum_{k=-\infty}^{+\infty} \sum_{j=0}^{N_f-1} C_j(k) \cdot p\big(t - k.T_s - S_j(k).T_c\big), \quad (3)$$

where $p\big(t\big)$ is the pulse shape and δ is the delay introduced by PPM.

The protocols proposed in this paper are based on the parameters of the TH-UWB symbol: the time-hopping code S and the mapping code C.

2.1.2 Channel model

The received signal after passing through the channel can be modeled as:

$$r(t) = \sum_j A_j.s\big(t - \tau_j\big) + w(t), \quad (4)$$

where $s(t)$ is the signal transmitted for one of the two modulations. The A_j's denote the path amplitudes while the τ_j's denote their corresponding delays.

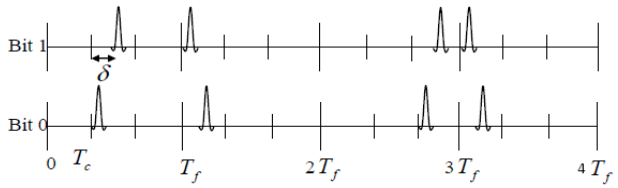

Figure 1: Structure of a TH-UWB symbol with $N_c = 3$, $N_f = 4$, PPM modulation and a mapping code like Equation 1.

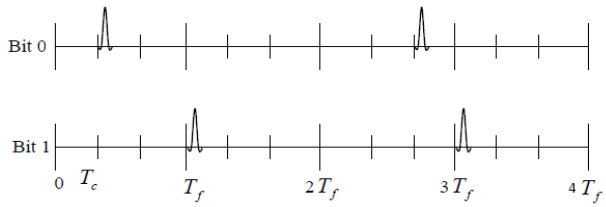

Figure 2: Structure of a TH-UWB symbol with $N_c = 3$, $N_f = 4$, OOK modulation and a mapping code like Equation 1.

A statistical channel model recommended by the IEEE 802.15.4a standard is adopted and particularly the CM1 model describing residential LOS (Line of sight) environment [22]. The frame duration T_f should be chosen such that the delay spread of the channel is much smaller than T_f. Thus, inter-pulses interferences can be neglected. The term $w(t)$ is a centered Gaussian random variable modeling the thermal noise whose two sided power spectral density is $N_0/2$.

2.1.3 Receiver structure

Different receiver architectures have been proposed for UWB systems [23]. The non-coherent receiver, with low cost/consumption characteristics, is chosen in this paper. For a complete study of non-coherent receivers in UWB systems, see [24] [25]. The purpose of this paragraph is to give a model for the performance of a non-coherent receiver with the two modulations.

- **Synchronization:** Prior to data demodulation, a precise synchronization should be acquired between the transmitter and the receiver in order to detect the short pulses. Synchronization is acquired thanks to a packet preamble composed of unmodulated symbols with a predefined time-hopping code known to the receiver [26]. The latter compares temporal distances between the received pulses and those predicted by the predefined time-hopping code. Synchronization is declared when the TH sequence is fully identified [27]. Synchronization is a critical phase in UWB systems: the number of required pulses to acquire the synchronization is independent of the payload size. This implies that the energetic cost of synchronization becomes predominant in the consumption required for receiving a packet, when dealing with short packets.

- **Demodulation:** The demodulation scheme is depicted in Fig. 3 (resp. Fig. 4) for the PPM (resp. OOK). In both cases, the demodulator consists in a band-pass filter with bandwidth B, a quadratic detector coupled with an integrator whose integration time is T. A decision is taken by comparing the output of integrators in the two positions for the PPM demodulator. The OOK demodulator takes a decision by comparing the output of the integrator with a threshold ρ.

- **Error probability:** The performance of the two structures of reception has been studied analytically in [28] [29]. The chip error probabilities $P_{e,chip}$ for the two modulations are:

$$P_{e,chip,PPM} = \frac{1}{2^M} e^{-\frac{\mu(T)E_p}{2N_0}} \sum_{j=0}^{M-1} c_j \cdot \left(\frac{\mu(T)E_p}{2N_0}\right)^j, \tag{5}$$

$$\begin{aligned} P_{e,chip,OOK} = \frac{1}{2}\Big[1 - Q_M\Big(\sqrt{\frac{4\mu(T)E_p}{N_0}}, \sqrt{\frac{2\rho}{N_0}}\Big) \\ + e^{-\frac{\rho}{N_0}} \sum_{j=0}^{M-1} \frac{1}{j!}\Big(\frac{\rho}{N_0}\Big)^j\Big]. \end{aligned} \tag{6}$$

E_p refers to the mean pulse energy while $\mu(T)$ is referring to the proportion of energy collected in the integrator output. More details on the last term are left to the next paragraph. M is linked to the receiver parameters such that: $2M \cong (2.B.T + 1)$. $Q_M(a, b)$ is the generalized Marcum Q function of order M whose explicit expression can be found in [28]. Finally, the term c_j is defined by:

$$c_j = \frac{1}{j!} \sum_{k=j}^{M-1} 2^{-k} \cdot \binom{M+k-1}{k-j}.$$

It can be seen from Equation 6 that the performance of OOK receiver depends on the threshold ρ. The optimal threshold in the sense of the maximum likelihood criterion can be approximated by [29]:

$$\frac{\rho_{opt}}{N_0} \approx \frac{E}{2N_0} + M + \sqrt{M-1} \cdot \phi\left(\frac{2E}{N_0}\right),$$

where $E = \mu(T) \cdot E_p$ and ϕ is a tabulated function depending only on E/N_0. It has been shown in [28] that the performance of OOK receiver is slightly better than PPM receiver.

An upper-bound on the symbol error probability related to the chip error probability is given by [30]:

$$P_{es} \leq \sum_{j=t+1}^{N_f} \binom{N_f}{j} \cdot (P_{e,chip})^j \cdot (1 - P_{e,chip})^{N_f - j} \quad , \tag{7}$$

where $t = \left\lfloor \frac{N_f - 1}{2} \right\rfloor$ is the error correction capacity of the mapping code C.

- **Collected energy:** The pulse energy is dispersed among the paths and the amount of energy available in the integrator output is only a proportion of the pulse energy. The collected energy depends on the integration time and the multipath channel realization. *Dubouloz et al.* proposed in [31] a semi-analytical model to fit the statistics of $\mu(T)$. The model consists in:

$$\mu(T) = 1 - \exp\left(-\left(\frac{T + T_0}{\tau}\right)^{\alpha}\right), \quad T > 0, \tag{8}$$

where the parameters T_0, τ and α depend on the channel configuration. The parameters fitting the 802.15.4a CM1 channel model are: $T_0 = 10$, $\tau = 36.21$ and $\alpha = 1.27$ [31].

Finally, it should be noticed that the integration time influences the receiver performance. An optimal integration time exits but it is not the concern of this paper. A short fixed integration time is assumed.

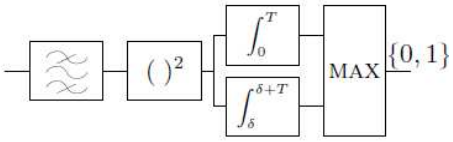

Figure 3: PPM demodulator.

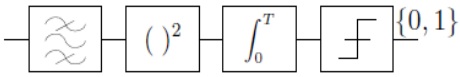

Figure 4: OOK demodulator.

2.2 Distance Bounding protocols

2.2.1 Basic concepts

Distance Bounding protocols have been introduced by Brands and Chaum [8] to mitigate certain classes of *man in the middle* (MITM) attack described by Desmedt et al. [1] and also known as *Mafia frauds*. The principle of the Mafia frauds includes two accomplices working together: the proxy verifier located in the radio range of the legitimate prover and the proxy prover located in the neighborhood of the verifier. The communication between the two accomplices may be wireless or a sophisticated wired link. The proxy prover forwards to her accomplice all the requests from the verifier. The accomplice (proxy verifier) sends them to the legitimate prover, receives its responses, which are forwarded to the verifier through the two accomplices.

A distance bounding protocol allows a *verifier V* to check that a legitimate user, *the prover P*, is within its *neighborhood*, *i.e.* the Euclidean distance between the verifier and the prover is upper bounded. It has two sides: a cryptographic side to authenticate the prover and a measurement side to bound the distance. The distance bounding protocol is said to be secure if the verifier rejects the prover with overwhelming probability when the prover is not legitimate and/or it is outside of the neighborhood. The verifier accepts the prover when the latter is legitimate and within the neighborhood. Many solutions are available to measure the distance between two radio devices: GPS, RTT, RSSI, AoA... The reader can consult [32] for more details on these techniques. For low cost embedded devices, the RTT (Round Trip Time) is the most popular

solution. The UWB technology is so far the most promising radio for the implementation of distance bounding protocols based on the measurement of RTT, (see [10, 11]) as UWB provides a very accurate synchronization between the verifier and the prover .

Most of the existing distance bounding protocols based on the RTT proposed in the literature [33, 15, 34] are variants of two fundamental solutions: the Brands and Chaum protocol [8] and the Hancke and Kuhn protocol [13].

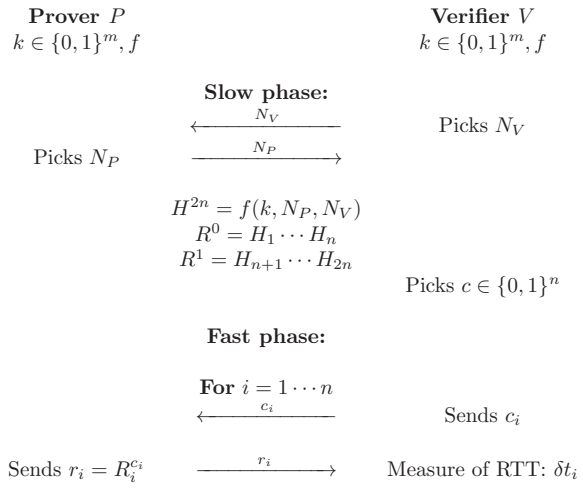

Figure 5: The Hancke and Kuhn protocol.

The latter protocol is depicted in Fig. 5. It is composed of two steps: the *slow phase* and the *fast phase*. The protocol requires that V and P agree on: (a) a shared secret key $k \in \{0,1\}^m$, (b) a pseudo-random function f, (c) a number of rounds n of the fast phase and (d) an upper-bound t_{max} for timing known to the verifier.

The slow phase begins as follow: the verifier picks a nonce N_V (number used once) and sends it to P. Reciprocally, the prover picks a nonce N_P and sends it to V. From the values N_P, N_V and the key k, P and V compute a shared state $H^{2n} = f(k, N_P, N_V)$ of length $2n$ bits. Then, V and P split H^{2n} into two registers of length n: $R^0 = H_1 \cdots H_n$ and $R^1 = H_{n+1} \cdots H_{2n}$ where $H_j, (1 \leq j \leq 2n)$ denotes the j^{th} bit of H^{2n}.

The fast phase consists in n rounds. In each round i $(1 \leq i \leq n)$, the verifier picks a random bit c_i (the challenge) and sends it to P. The prover responds with $r_i = R_i^{c_i}$ the i^{th} bit of the register R^{c_i}. The verifier computes in each round the RTT between sending c_i and receiving r_i denoted δt_i. The distance bounding protocol succeeds if all the responses r_i are correct and $\forall i, \delta t_i \leq t_{max}$.

In comparison, the Brands and Chaum protocol requires an additional phase because the distance checking and the authentication are two independent processes. The final slow phase in Brands and Chaum protocol is the verification of a signature algorithm used to complete the authentication.

2.2.2 Strategies of attack

The adversary can choose between different strategies for executing her Mafia fraud. The strategies depend if the adversary asks or not the prover and the moment she asks it. One strategy may be more useful to the attacker than others depending on the distance bounding protocol and on which class it belongs to.

- *No-ask strategy:* The adversary relays the initial slow phase between the legitimate prover and the verifier. After that, the adversary tries to complete the protocol by herself. This strategy can not be strictly considered as a form of Mafia fraud. But, it is interesting to study the security of distance bounding protocols against this type of attack. The probability of success against the Hancke and Kuhn protocol with this strategy of attack is:
$$P_{na,HK} = \left(\frac{1}{2}\right)^n. \tag{9}$$
- *Pre-ask strategy:* The adversary relays the initial slow phase. Then, before executing the fast phase with the verifier, the proxy verifier starts the fast phase with the legitimate prover by querying it with false challenges. After that, the proxy prover starts the fast phase now with the verifier by exploiting the responses in her possession. If the protocol is not finished, the adversary relays the final slow phase. With this strategy of attack, the adversary can retrieve one register among two in the Hancke and Kuhn protocol and the probability of success is:
$$P_{pa,HK} = \left(\frac{3}{4}\right)^n. \tag{10}$$

The other possibility of attack is the *post-ask strategy*. The adversary executes the fast phase with the verifier without asking the prover. After that, she queries the legitimate prover with the right challenges just extracted in the aim of obtaining the signature of the last phase. This strategy of attack finds application only for the Brands and Chaum's class of protocols.

In this paper, two distance bounding protocols (protocol A and protocol B) are introduced on a TH-UWB radio using PPM and OOK modulations. The verifier and the prover are two UWB devices with identical capabilities. The core of our protocols follows the principle of the Hancke and Kuhn's protocol. A preliminary version of this work was accepted at Globecomm 2010 [14]. These early results have been completed to provide an in-depth analysis of our distance bounding protocols. The major new aspects treated by this article are briefly summarized here. First, the protocol A using secret time-hopping codes has been generalized for a variable number of listening slots and for different modulations. Second, the analysis over noisy channel is more realistic for both protocols as a complete UWB link has been considered. Finally, the memory cost has been explored to provide a fair comparison with the state of the art.

3 Protocol A: secret TH codes

The main idea of protocol A is to adapt the Hancke and Khun protocol to a TH-UWB radio by using secret shared time-hopping codes between V and P. The principle of the protocol is detailed and then analyzed.

3.1 Description of the protocol

The protocol is described in Fig. 6. It is assumed that synchronization is performed between the verifier and the legitimate prover prior to the start of the protocol and that it is maintained. In practice, radio transceivers own an electronic circuit responsible for synchronization tracking. Moreover, the mapping code used by the verifier and the prover is the one given in Equation 1. In what follows, the specifications of the protocol are mentioned.

3.1.1 Protocol requirements

P and V share a secret key k. They can both compute a pseudo-random function f and they have an access to a random number generator. The pseudo-random function can be implemented with a cryptographic hash function such as SHA-256. V and P share also a parameter $N' \in \{1, \cdots, N_c - 1\}$. The verifier sets a timing upper-bound t_{max}.

3.1.2 Initialization phase

The prover picks a nonce N_P and sends it to V. Reciprocally, the verifier picks a nonce N_V and sends it to P. From the values N_V, N_P and the key k, V and P compute a share state $H = f(k, N_P, N_V)$. H is a bit string of length $2n(p.N_f + 1)$ where n is the number of rounds in the fast phase and $p = \log_2 N_c$. For an ease of implementation, the number of chips N_c is always a power of two. H is split into four parts:

- The time-hopping code S^V of the verifier of length $n.p.N_f$ bits. It defines the $n.N_f$ time slots used by the verifier to transmit its pulses. For $1 \leq i \leq n$, the bit string S_i^V of length $p.N_f$ bits determines the sequence of integers over $\mathbb{Z}/N_c\mathbb{Z}$ corresponding to time slots used to emit the i^{th} symbol.
- The time-hopping code S^P of the prover which defines the time slots used for transmitting the symbols of the prover.
- A first register R^0 containing n bits.
- A second register R^1 which contains also n bits.

In addition, the verifier and the prover pick an n-bit random vector c and z. The prover also picks randomly an $n.p.N_f$-bit vector q. This vector is decomposed into a sequence q_i of n symbols with $p.N_f$ bits as S_i^P and S_i^V.

The protocol requires also for both verifier and prover $(n \cdot N_f)$ random binary words of length $(N_c - 1)$ and weight N'. The purpose of these binary words is to determine the additional listening slots in each frame, besides the time slot allocated to receive the answer. The additional slots are used to detect an attack.

3.1.3 Fast phase

The fast phase consists in n rounds. In each frame of a round, both V and P activate their radio in N' time slots selected from the binary word of length $(N_c - 1)$. Thus, they can detect an attack if they notice an activity in these time slots. The fast phase starts by sending a challenge bit c_i to P. Each

challenge is sent according to the public mapping code in time slots defined by S_i^V. If the prover receives the pulses in the time slots predicted, it replies with $r_i = R_i^{c_i}$ the i^{th} bit of the register R^{c_i} with the time-hopping sequence S_i^P. Otherwise (P detects at least one pulse in the wrong time slot), the prover notifies an attack and reacts by replying from the vector z with the symbol q_i. Reciprocally, the verifier also assumes an attack if it receives an impulse not in the time slot predicted and stops the protocol. Unless an attack is detected, the verifier computes in each round the RTT, denoted δt_i, between sending c_i and receiving r_i. This RTT measure is linked to the time of flight so a distance upper-bound between V and P can be deduced.

3.1.4 Verification

The protocol succeeds if all the responses r_i sent by the prover are correct and $\forall i, \delta t_i \leq t_{max}$.

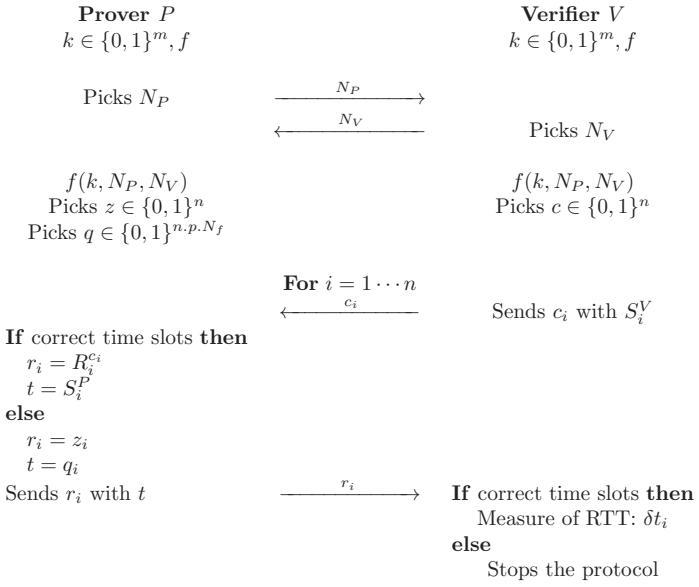

Figure 6: Protocol A: secret TH codes.

3.2 Security analysis over noise-free channels

A detailed security analysis of protocol A for the no-ask and pre-ask strategies of attack is given. In this subsection, the security is analyzed in an idealistic case with noise-free channel. The analysis is considered for the two modulation options: PPM and OOK. Indeed, the security is different with OOK because chips 0 and 1 are not symmetric.

3.2.1 PPM Modulation

No-ask strategy - The adversary responds to the challenges of the verifier with random bits $\hat{r_i}$. The response bit is transmitted with its corresponding public mapping code. Specifically, the adversary emits in each frame x pulses

at different time slots, $x \in \{1, \cdots, N_c - N'\}$. To compute the adversary success probability, it is helpful to define the following events at the i^{th} round:

- A_i the event that $\hat{r_i} = R_i^{c_i}$,
- B_i the event that the adversary emits one pulse among x in the true time slot S_i^P in each frame,
- C_i the event that the adversary emits x pulses in time slots that are not detected by V in each frame.

The adversary succeeds her attack at the i^{th} round if the event (A_i and B_i and C_i) is realized. The probability for this event is:

$$\begin{aligned} P(A_i \text{ and } B_i \text{ and } C_i) &= P(A_i) \cdot P(B_i \text{ and } C_i) \\ &= P(A_i) \cdot P(C_i|B_i) \cdot P(B_i) \\ &= \frac{1}{2}. \left[\frac{\binom{N_c-(1+N')}{x-1}}{\binom{N_c-1}{x-1}} \cdot \frac{x}{N_c} \right]^{N_f} \end{aligned}$$

Let denote $Y = x.\binom{N_c-(1+N')}{x-1}/N_c.\binom{N_c-1}{x-1}$. Assuming that the success probability at each round is independent, the total success probability against protocol A with the no-ask strategy is given by:

$$P_{na,PPM,A} = \left(\frac{Y^{N_f}}{2} \right)^n . \tag{11}$$

It is interesting for the adversary to choose the optimal number of pulses x_{opt} to transmit in order to maximize her probability of success. The problem of optimization in $\mathbb{N}$ turns into:

$$x_{opt} = \arg \max_{1 \leq x \leq N_c - N'} Y \quad . \tag{12}$$

The value x_{opt} that maximizes the success probability is:

$$x_{opt} = \left\lceil \frac{N_c - N'}{N' + 1} \right\rceil . \tag{13}$$

It should be noticed that when $N' \geq N_c/2$, the optimal value is $x_{opt} = 1$. Moreover, considering values of N' greater than $N_c/2$ does not improve the security.

Pre-ask strategy - During the attack, the adversary queries P with challenges $\hat{c_i}$ chosen randomly. She emits in each frame x pulses, $x \in \{1, \cdots, N_c - N'\}$ in random time slots. After receiving the answers r_i from P, the adversary now executes the protocol with V. She answers to V challenges with $\hat{r_i} = r_i$ emitted in same time slots as received. So, in each frame, the adversary responds with only one pulse. In addition to the events already introduced, the following events are defined at the i^{th} round :

- E_i the event that $\hat{c_i} = c_i$,
- F_i the event that the adversary emits one pulse among x in the true time slot S_i^V in each frame,
- G_i the event that the adversary emits x pulses in time slots that are not detected by P in each frame.

The attack succeeds at the i^{th} round if the event $(A_i \text{ and } B_i)$ is realized with $x = 1$. The probability of this event $P(A_i \text{ and } B_i) = P(A_i) \cdot P(B_i)$ is computed:

$$\begin{aligned} P(A_i) &= P(A_i|(E_i \text{ and } F_i \text{ and } G_i)) \cdot P(E_i \text{ and } F_i \text{ and } G_i) \\ &+ P(A_i|\overline{E_i \text{ and } F_i \text{ and } G_i}) \cdot P(\overline{E_i \text{ and } F_i \text{ and } G_i}) \\ &= 1 \cdot \frac{Y^{N_f}}{2} + \frac{1}{2} \cdot (1 - \frac{Y^{N_f}}{2}) \end{aligned}$$

$$\begin{aligned} P(B_i) &= P(B_i|(F_i \text{ and } G_i)) \cdot P(F_i \text{ and } G_i) \\ &+ P(B_i|\overline{F_i \text{ and } G_i}) \cdot P(\overline{F_i \text{ and } G_i}) \\ &= 1 \cdot Y^{N_f} + \frac{1}{N_c^{N_f}} \cdot (1 - Y^{N_f}) \end{aligned}$$

Therefore, the probability of success against protocol A with the PPM modulation is given by:

$$P_{pa,PPM,A} = \left([\frac{(N_c^{N_f} - 1).Y^{N_f} + 1}{N_c^{N_f}}] \cdot [\frac{2 + Y^{N_f}}{4}] \right)^n . \tag{14}$$

The adversary searches the number of pulses to emit for maximizing her probability of success. The equivalent optimization problem turns into maximizing an increasing function of Y so the solution is the same as previously given by Equation 13.

Comparing strategies - The security of protocol A is fixed by the $\max(P_{na,PPM,A}, P_{pa,PPM,A})$. To determine the best strategy for the adversary, the ratio $P_{pa,PPM,A}/P_{na,PPM,A}$ is computed:

$$\frac{P_{pa,PPM,A}}{P_{na,PPM,A}} = \left(\frac{2(N_c \cdot Y)^{N_f} + \dots}{2(N_c \cdot Y)^{N_f}} \right)^n \geq 1.$$

Thus, the pre-ask strategy is better for the adversary.

The Fig. 7 depicts the impact of N' on the success probability for $n = 15$. The probability of success decreases rapidly for $1 \leq N' < N_c/2$ and becomes constant from $N' \geq N_c/2$ as noticed previously.

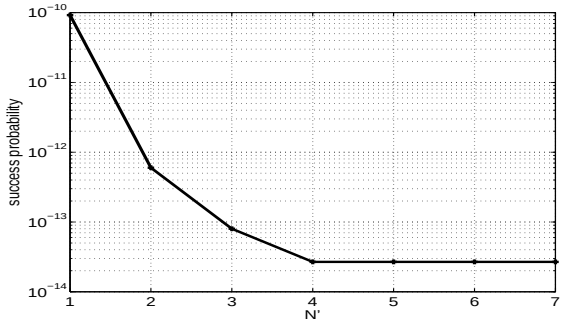

Figure 7: Adversary success probability of protocol A as a function of N' with PPM modulation, $N_c = 8$ and $N_f = 1$.

3.2.2 OOK Modulation

With the PPM modulation, the adversary is detected when she emits in the wrong time slots. However, with OOK modulation, the adversary is detected if she emits in the wrong time slots if and only if the chip is 1. Therefore, the security differs with OOK. The mapping code C used in protocol A is like Equation 1, so the same number of pulses is transmitted for symbols 0 and 1 which equals $N_f/2$. The probability of success is computed just with the pre-ask strategy as demonstrated that it is better for the adversary.

In comparison to the previous computation of PPM, the following values are modified:

$$P(F_i \text{ and } G_i) = Y^{N_f/2},$$

$$P(B_i) = \frac{(N_c^{N_f/2} - 1)U^{N_f/2} + 1}{N_c^{N_f/2}},$$

where $U = \binom{N_c - N'}{x} / \binom{N_c}{x}$. The event B_i becomes independent of the event F_i because the prover is not susceptible to detect an attack when it does not receive a pulse in the predicted time slot. Finally, the probability of success with OOK modulation is given by:

$$P_{pa,OOK,A} = \left(\left[\frac{(N_c^{\frac{N_f}{2}} - 1).U^{\frac{N_f}{2}} + 1}{N_c^{\frac{N_f}{2}}} \right] \cdot \left[\frac{2 + Y^{\frac{N_f}{2}}}{4} \right] \right)^n . \tag{15}$$

The number of pulses that the adversary should emit for maximizing her probability of success is similar to previously. The loss in security level with OOK modulation compared to PPM depends on the parameters of the protocol. In Fig. 8, the security level of protocol A with respectively PPM and OOK modulations is given with parameters $N_c = 8, N_f = 2$ and $N' = 3$. At the same security level, the number of rounds necessary with OOK is approximately 2.76 higher than the number of rounds necessary with PPM.

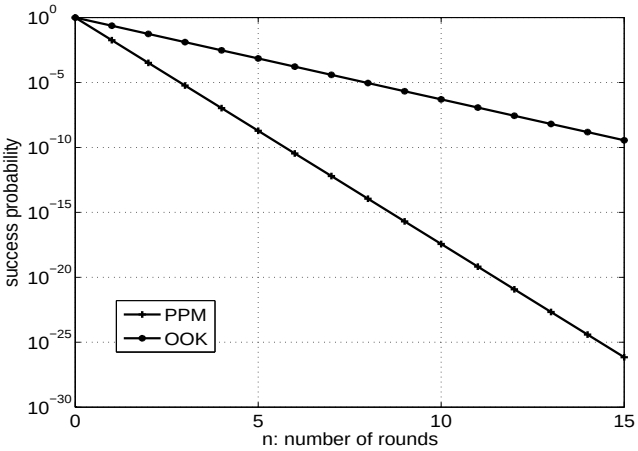

Figure 8: Comparison of security performance of protocol A between PPM and OOK modulations, $N_c = 8, N_f = 2$ and $N' = 3$.

3.3 Security analysis over noisy channels

In the noise-free channel, all responses sent by the prover must be correctly received for succeeding the protocol. However, in practical systems, some responses may be erroneous due to noise. The protocol must be modified for a noisy environment by tolerating ℓ errors in the verification phase. The number of tolerated errors ℓ is an important security parameter, since raising ℓ decreases the probability of false rejection but at the same time increases the probability of false accept. The security of protocol A is discussed with the channel model described in Subsection 2.1.

3.3.1 Probability of false rejection

The probability of false rejection is defined by the probability that the verifier rejects a legitimate prover in absence of an attacker. This occurs when more than ℓ errors appear. For computing this probability, the following events are defined:

- H_i the event that the received $r_i \neq R_i^{c_i}$,
- I_i the event that c_i is correctly received,
- J_i the event that $r_i = R_i^{c_i}$.

The probability that a response is erroneous at the i^{th} round corresponds to $\varepsilon_A = P(H_i)$. The probability of this event is:

$$\begin{aligned}\varepsilon_A &= P(H_i|J_i) \cdot P(J_i) + P(H_i|\bar{J}_i) \cdot P(\bar{J}_i) \\ &= P_{es} \cdot P(J_i) + (1 - P_{es}) \cdot (1 - P(J_i)),\end{aligned}$$

$$\begin{aligned}P(J_i) &= P(J_i|I_i) \cdot P(I_i) + P(J_i|\bar{I}_i) \cdot P(\bar{I}_i) \\ &= 1 \cdot (1 - P_{es}) + \frac{1}{2} \cdot P_{es},\end{aligned}$$

where P_{es} is the symbol error probability which depends on the choice of modulation and is given by Equation 7 taken with equality. In this computation, the symbol error probability is assumed the same for the two links $V \rightleftharpoons P$, since both V and P have the same capabilities. The result is:

$$\varepsilon_A = \frac{3}{2} \cdot P_{es} - (P_{es})^2.$$

Finally, the probabilty of false rejection $P_{FR,A}$ is given by:

$$P_{FR,A} = \sum_{i=\ell+1}^{n} \binom{n}{i} \cdot \varepsilon_A^i \cdot (1 - \varepsilon_A)^{n-i}. \tag{16}$$

The number of tolerated errors is chosen to be adapted to the symbol error probability by the relation:

$$\ell = \lceil \varepsilon_A.n \rceil \quad . \tag{17}$$

This choice requires that the verifier knows the symbol error rate of the link.

The Fig. 9 describes the probability of false rejection for the two modulations as a function of the signal-to-noise ratio E_p/N_0 with a fixed number of rounds $n = 25$. The parameters of the TH-UWB link taken for studying the probability

of false rejection are: $T = 2$ ns, $B = 1.5$ GHz and $N_f = 8$. For $E_p/N_0 < 12$ dB, the probability of false rejection is almost constant and not satisfying from the security point of view. For $E_p/N_0 \geq 12$ dB, the probability of false rejection decreases rapidly with E_p/N_0. Moreover, the probability of false rejection is better with OOK than with PPM. This result is in concordance with the fact that the performance of OOK non-coherent receiver is slightly better than PPM receiver.

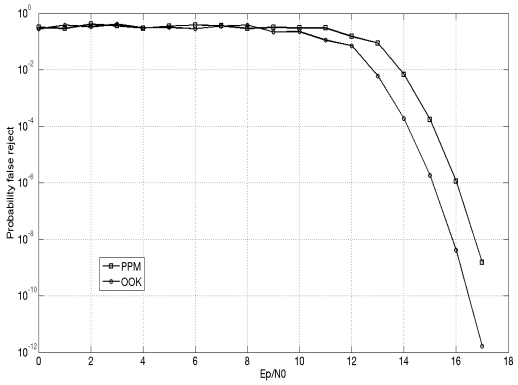

Figure 9: Probability of false rejection of protocol A with PPM and OOK modulations, $T = 2$ ns, $B = 1.5$ GHz and $N_f = 8$.

3.3.2 Probability of false accept

The fact that V tolerates some errors changes the adversary's probability of success: *i.e.* the probability of false accept. Now, the adversary needs to succeed in only $(n-j)$ rounds, $0 \leq j \leq \ell$, and the event ($\bar{A}_i$ and B_i) must be realized in j rounds. Thus, the probability of false accept for the two modulations is given by:

$$P_{FA,A} = \sum_{j=0}^{\ell} \binom{n}{j} \cdot X_A^{n-j} \cdot Z_A^j \quad . \tag{18}$$

X_A corresponds to the probability of success in a round for the two modulations already computed while Z_A corresponds to $P(\bar{A}_i$ and $B_i)$:

$$Z_{PPM,A} = \left(\frac{(N_c^{N_f} - 1).Y^{N_f} + 1}{N_c^{N_f}}\right) \cdot \left(\frac{2 - Y^{N_f}}{4}\right),$$

$$Z_{OOK,A} = \left(\frac{(N_c^{N_f/2} - 1).U^{N_f/2} + 1}{N_c^{N_f/2}}\right) \cdot \left(\frac{2 - Y^{N_f/2}}{4}\right).$$

The computation is established for the worst case situation of the noise resilient protocol A consisting of an adversary capable of setting channels without errors.

The Table 1 gives the probability of false accept for different values of the signal-to-noise-ratio. The parameters for protocol A are $N_c = 4$, $N_f = 2$, $N' = 2$ and $n = 15$. The probability of false accept depends on E_p/N_0 via

the number of tolerated errors yet given by Equation 17. The behavior of the probability of false accept is different according to which interval belongs E_p/N_0. In fact, the probability of false accept is variable in the range $E_p/N_0 <$ 16.5 dB for PPM modulation and in the range $E_p/N_0 <$ 15.5 dB for OOK modulation. Otherwise, the probability of false accept becomes constant and minimal. The signal-to-noise ratio required to achieve this minimal value is less with OOK compared to PPM but the security level of the protocol is greatly increased compared to PPM. The choice of the number of tolerated errors given by Equation 17 guarantees that the probability of false accept becomes minimal and independent of E_p/N_0 if the latter is above a certain value. But, this constant security level can not achieve the security level of the noise-free channel.

E_p/N_0 [dB]	$P_{FA,PPM,A}$	$P_{FA,OOK,A}$
5	$1.5 \cdot 10^{-14}$	$8.1 \cdot 10^{-4}$
8	$1.3 \cdot 10^{-14}$	$7.3 \cdot 10^{-4}$
11	$9.6 \cdot 10^{-15}$	$4.2 \cdot 10^{-4}$
14	$1.3 \cdot 10^{-15}$	$4.5 \cdot 10^{-5}$
17	10^{-17}	$2 \cdot 10^{-6}$
18	10^{-17}	$2 \cdot 10^{-6}$
∞ (without noise)	$8.54 \cdot 10^{-19}$	$1.55 \cdot 10^{-7}$

Table 1: Probability of false accept function of the signal-to-noise ratio, $N_c = 4$, $N_f = N' = 2$ and $n = 15$.

4 Protocol B: secret mapping codes

In the previous section, the time-hopping code was kept unknown to the adversary while the mapping code was public. It is quite logical to study the security performance of a scheme in which the time-hopping code is public and the mapping code is unknown to the adversary.

4.1 Description of the protocol

Let consider the following encoding/decoding strategy: the encoder has to send 0 or 1 message. It chooses randomly N_f bits to obtain a codeword y. If the most significant bit of y is set to one, y is associated to 1 or 0 otherwise. The encoder sends y or $\overline{y}$. To achieve a successful decoding, the decoder needs to be synchronized with the encoder to know the value of y. If the received symbol is at distance $\Delta \leq \lfloor \frac{N_f - 1}{2} \rfloor$ of y (resp. $\overline{y}$), the decoding is successful otherwise it errs. To transmit n bits, the encoder and the decoder need to draw $N_f \cdot n$ random bits. The goal of Δ is to offer a trade-off between error correction and security. Taking $\Delta = 0$ is more beneficial to security while taking $\Delta \geq 1$ is more beneficial to error correction.

In fact, the strategy just described consists in using the cosets of a repetition code of length N_f and dimension 1. The encoder and the decoder are encoding/decoding with a known coset of the repetition code. One element of each coset is associated to 0 and the other to 1. For instance, the cosets used by the

encoder and the decoder are for $N_f = 4$: $K_1 = \{0000, 1111\}$, $K_2 = \{0001, 1110\}$, $K_3 = \{0010, 1101\}$, $K_4 = \{0011, 1100\}$, $K_5 = \{0100, 1011\}$, $K_6 = \{0101, 1010\}$, $K_7 = \{0110, 1001\}$, $K_8 = \{0111, 1000\}$. To transit n bits, the encoder and the decoder need to draw $(N_f - 1) \cdot n$ random bits while storing in memory $N_f 2^{N_f - 1}$ bits for the cosets. If $N_f 2^{N_f - 1}$ is negligible compared to n, almost n bits can be saved compared to the previous strategy.

The protocol B is depicted in Fig. 10. Its requirements are the same as protocol A with the addition of the cosets.

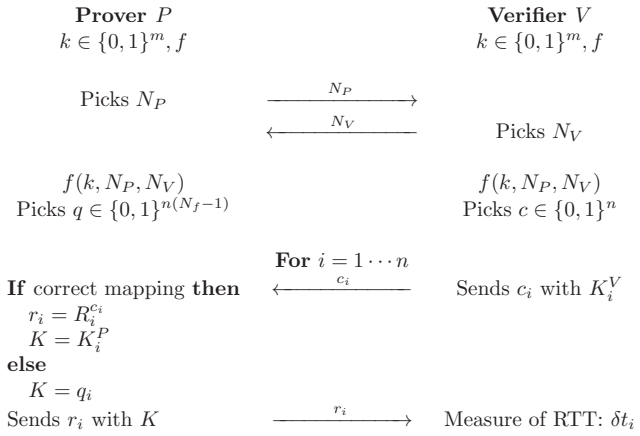

Figure 10: Protocol B: secret mapping codes.

4.1.1 Initialization phase

The prover and the verifier exchange the nonces N_P and N_V. Then, they both compute the share state $H = f(k, N_P, N_V)$ which is split into four parts:

- The register K^V of length $n.(N_f - 1)$ bits. It defines the successive cosets K_i^V used by the verifier at each round i.
- In the same vain, the register K^P of length $n.(N_f - 1)$ bits defines the cosets K_i^P used by the prover.
- A register R^0 containing n bits.
- A register R^1 which contains also n bits.

In addition, the verifier and the prover pick respectively an n-bit random vector c and an $n.(N_f - 1)$-bit vector q. This vector q has the same purpose than K^V and K^P but it will be used in case of incorrect challenge.

4.1.2 Fast phase

During each round $i \in \{1, \cdots, n\}$, the verifier sends a challenge bit c_i to the prover. This challenge bit is transformed into a codeword from the coset K_i^V. The prover decodes the received challenge with respect to K_i^V. If the decoding is successful, *i.e.* the received challenge is at Hamming distance Δ from one of the two words of the coset, the prover responds with $r_i = R_i^{c_i}$ the i^{th} bit

of the register R^{c_i}. This answer bit is transformed into a codeword from the coset K_i^P. Otherwise if the decoding errs, the prover detects an attack and responds randomly. This random answer is coded with respect to a mapping code extracted from q. The verifier computes in each round the RTT δt_i.

4.1.3 Verification

The protocol succeeds if the verifier decodes successfully the answers received from the prover and if $\forall i, \delta t_i \leq t_{max}$.

4.2 Security analysis over noise-free channels

In the protocol B, the time-hopping code is public meaning that the adversary knows when the information is transmitted. Therefore, the security of protocol B is independent of the type of modulation and either PPM or OOK can be assumed. In a first time, it is assumed that no noise is tolerated, $\Delta = 0$.

No-ask strategy - The adversary attempts to answer to the verifier challenges with randomly chosen mapping codes. The following events are defined:

- $K_i(\Delta)$ the event that the mapping code of $\hat{r_i}$ is at an Hamming distance less than Δ from the mapping code of the correct answer $r_i = R_i^{c_i}$.

The probability of success with the no-ask strategy in the i^{th} round corresponds to $P(K_i(0)) = 1/2^{N_f}$. Thus, the probability of success with this strategy of attack is given by:

$$P_{na,B} = \left(\frac{1}{2^{N_f}}\right)^n. \tag{19}$$

Pre-ask strategy - The adversary queries the prover with challenges sent with randomly chosen mapping codes. For computing the probability of success with this strategy of attack, the following event is defined:

- $L_i(\Delta)$ the event that $\hat{c_i}$ is sent with a mapping code distant at most Δ from one of the two codewords of the coset K_i^V.

The probability of success in the i^{th} round corresponds to the probability of event $K_i(0)$:

$$\begin{aligned} P(K_i(0)) &= P(K_i(0)|L_i(0)) \cdot P(L_i(0)) \\ &\quad + P(K_i(0)|\overline{L_i(0)}) \cdot P(\overline{L_i(0)}) \\ &= \frac{3}{4} \cdot \frac{1}{2^{N_f-1}} + \frac{1}{2^{N_f}} \cdot (1 - \frac{1}{2^{N_f-1}}). \end{aligned}$$

Thus, the probability of success with the pre-ask strategy is:

$$P_{pa,B} = \left(\frac{1}{2^{N_f}} \cdot (\frac{5}{2} - \frac{1}{2^{N_f-1}})\right)^n. \tag{20}$$

4.3 Security analysis over noisy channels

As for protocol A, the probability of false rejection and the probability of false accept are computed using the channel model described in Subsection 2.1.

4.3.1 Probability of false rejection

The following event is introduced:

- M_i the event that the received mapping code of r_i is at Hamming distance $> \Delta$ from the mapping code of $R_i^{c_i}$.

The i^{th} round fails if the event M_i is realized. To compute $\varepsilon_B = P(M_i)$, this complete system of events is defined at the i^{th} round:

- $N_{i,1}$ the event that a codeword is received with a number of erroneous chips $\leq \Delta$,
- $N_{i,2}$ the event that a codeword is received with a number of erroneous chips strictly including between Δ and $N_f - \Delta$,
- $N_{i,3}$ the event that a codeword is received with a number of erroneous chips $\geq N_f - \Delta$.

$$\begin{aligned}\varepsilon_B &= P(M_i|N_{i,1}) \cdot P(N_{i,1}) + P(M_i|N_{i,2}) \cdot P(N_{i,2}) \\ &\quad + P(M_i|N_{i,3}) \cdot P(N_{i,3}) \\ &= P_{es} \cdot Q_1 + \frac{1 - \sum_{j=0}^{\Delta} \binom{N_f}{j}}{2^{N_f}} \cdot Q_2 \\ &\quad + \frac{Q_3}{2} \cdot \big(P_{es} + Q_1 + Q_2\big),\end{aligned}$$

where P_{es} is the symbol error probability of the link for the two modulations yet given by Equation 7 except that now t the error correction capacity for protocol B equals Δ. The terms Q_1, Q_2 and Q_3 are defined such that:

$$Q_1 = P(N_{i,1}) = \sum_{j=0}^{\Delta} \binom{N_f}{j} . (P_{e,chip})^j . (1 - P_{e,chip})^{N_f - j},$$

$$Q_3 = P(N_{i,3}) = \sum_{j=N_f-\Delta}^{N_f} \binom{N_f}{j} . (P_{e,chip})^j . (1 - P_{e,chip})^{N_f - j},$$

$$Q_2 = 1 - \big(Q_1 + Q_3\big),$$

where $P_{e,chip}$ refers to the chip error probability of the two modulations. Thus, the probability of false rejection is given by:

$$P_{FR,B} = \sum_{i=\ell+1}^{n} \binom{n}{i} \cdot \varepsilon_B^i \cdot (1 - \varepsilon_B)^{n-i} \quad . \tag{21}$$

The number of tolerated errors chosen is such that:

$$\ell = \lceil \varepsilon_B . n \rceil \quad . \tag{22}$$

Fig. 11 depicts the probability of false rejection of protocols A and B as a function of the signal-to-noise ratio. Parameters of the TH-UWB link are the same as previously, PPM modulation is considered and $n = 25$. Protocol B is studied with the two following limit cases $\Delta = 0$ with no error correction and $\Delta = 3$ corresponding to a maximal error correction capacity. The probabilities of false rejection of protocols A and B ($\Delta = 3$) are very close. This can be

explained by the fact that both have the same error correction capacity. The probability of false rejection of protocol B with $\Delta = 3$ (resp. $\Delta = 0$) becomes a decreasing function from $E_p/N_0 = 12$ dB (resp. $E_p/N_0 = 18$ dB). To guarantee a probability of false rejection of 10^{-6}, the signal-to-noise ratio required is of about 15.5 dB for $\Delta = 3$ and about 21.5 dB for $\Delta = 0$. This result points out that taking $\Delta = 0$ and so exploiting the mapping code only for security purposes introduces a loss of about 6 dB.

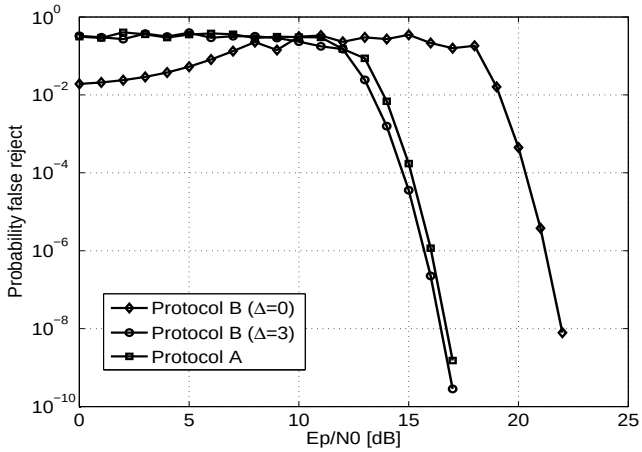

Figure 11: Probability of false rejection of protocol B with $N_f = 8$, $T = 2$ ns, $B = 1.5$ GHz and PPM modulation.

4.3.2 Probability of false accept

Tolerating some erroneous responses changes the success probability of the attack. The strategy of attack considered here is the pre-ask strategy. Now, the adversary needs to succeed in only $(n-j)$ rounds, $j \in \{0, \cdots, \ell\}$, and the event $P_i(\Delta)$ must be realized in j rounds. The event $P_i(\Delta)$ is defined by:

- $P_i(\Delta)$ the event that the mapping code of $\hat{r_i}$ is at Hamming distance less than Δ from the wrong codeword of the coset K_i^P.

The probability of false accept of protocol B is given by:

$$P_{FA,B} = \sum_{j=0}^{\ell} \binom{n}{j} \cdot X_B^{n-j} \cdot Z_B^j, \tag{23}$$

where:

$$X_B = P(K_i(\Delta)) = \frac{\sum_{k=0}^{\Delta} \binom{N_f}{k}}{2^{N_f}} \cdot \left(\frac{5}{2} - \frac{\sum_{k=0}^{\Delta} \binom{N_f}{k}}{2^{N_f-1}}\right),$$

$$Z_B = P(P_i(\Delta)) = \frac{\sum_{k=0}^{\Delta} \binom{N_f}{k}}{2^{N_f}} \cdot \left(\frac{3}{2} - \frac{\sum_{k=0}^{\Delta} \binom{N_f}{k}}{2^{N_f-1}}\right).$$

The probability of false accept depends on E_p/N_0 via the number of tolerated errors given by Equation 22. The parameters of the TH-UWB link are the same as previously. Two values of Δ are considered here, $\Delta = 3$ and an intermediate value $\Delta = 2$. The conclusion from Fig. 12 is that the probability of false accept

decreases with E_p/N_0 until achieving a constant and minimal value. This value is reached with $E_p/N_0 = 12$ dB, $\Delta = 3$ and $E_p/N_0 = 13.5$ dB, $\Delta = 2$. The security level with $\Delta = 3$ is not sufficient and considering $\Delta = 2$ instead of $\Delta = 3$ improves greatly the security and reduces little the robustness. Moreover, protocol B with $\Delta = 2$ guarantees a certain security level for low E_p/N_0. The only drawback compared to $\Delta = 3$ consists in the fact that it reaches the minimal probability value with a loss of 1.5 dB in the signal-to-noise ratio. The choice $\Delta = 2$ offers a good tradeoff between security and robustness.

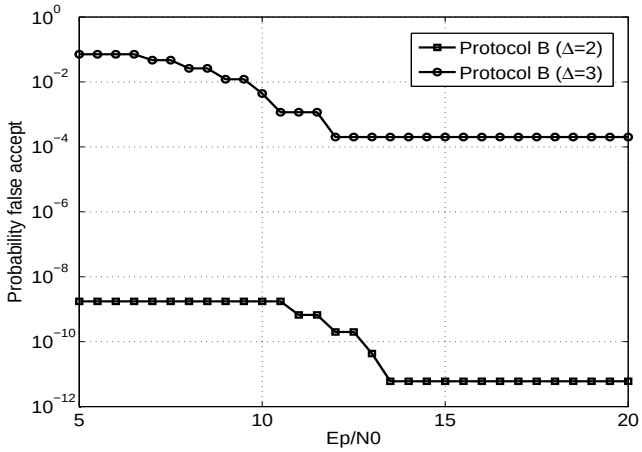

Figure 12: Probability of false accept of protocol B over noisy channels, $N_f = 8$.

5 Comparison with different distance bounding protocols

In this section, figure of merits of protocols A and B are compared to the standard protocol of Hancke and Khun and one variant the MUSE-pHK [35]. The considered metrics are the security performance and the memory consumption.

5.1 Security performance comparison

5.1.1 Noise-free channels

Table 2 resumes the success probabilities against protocol A (PPM), protocol B, the Hancke and Khun protocol [13] and the MUSE-pHK protocol [35]. In Fig. 13, the curves of the success probabilities are plotted with the following values: protocol A ($N_c = 8$, $N_f = 1$ and $N' \in \{1, 4\}$), protocol B ($N_f = 3$, $\Delta = 0$) and $p = 8$. These parameters are chosen to ensure fair comparison. Clearly, protocol A offers the best security level and outperforms the MUSE-8HK for all values of N'. Protocol B offers a security level slightly less than MUSE-8HK. The counterpart of the security performance of protocol A compared to protocol B is the additional energy consumption required for activating radio in some time slots.

Protocol	P
HK	$\left(3/4\right)^n$
MUSE-pHK	$\left((2.p-1)/p^2\right)^n$
A (PPM)	$\left(\left[\frac{(N_c^{N_f}-1).Y^{N_f}+1}{N_c^{N_f}}\right] \cdot \left[\frac{2+Y^{N_f}}{4}\right]\right)^n$
B	$\left(\frac{1}{2^{N_f}} \cdot (\frac{5}{2} - \frac{1}{2^{N_f-1}})\right)^n$

Table 2: Security comparison of distance bounding protocols.

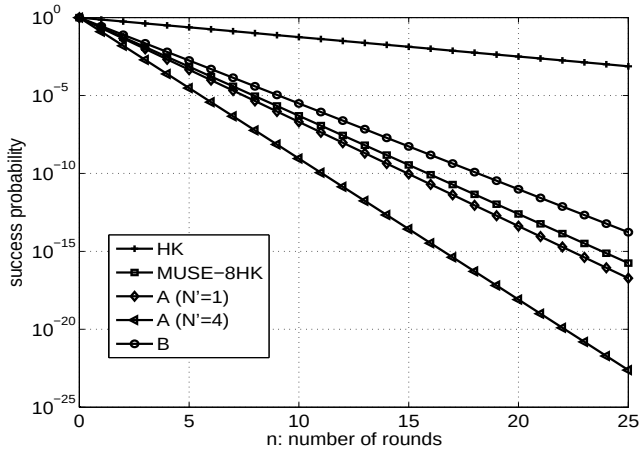

Figure 13: Security comparison of distance bounding protocols: A (PPM, $N_c = 8$, $N_f = 1$), B ($N_f = 3$, $\Delta = 0$) and MUSE-pHK ($p = 8$).

5.1.2 Noisy channels

The resiliency of protocols A and B to noise is compared to the HK and MUSE-pHK protocols. Table 3 shows the probabilities of false accept already computed as a function of ℓ. Parameters of protocol A are: $N_c = 8$, $N_f = 1$, $N' = 1$ and PPM modulation is used. In HK and MUSE-pHK protocols, error correction is not considered. Thus, to simply draw fair conditions of comparison, Δ is set to 0 and N_f equals 3 for protocol B. The number of rounds n is fixed to 25 for all the protocols. The conclusion to be drawn is that protocol A offers the best security level in presence of errors even with a minimal value $N' = 1$. Protocol B, in contrast to the case of noise-free channel, can outperform the MUSE-8HK protocol in relatively heavy noisy environment (number of tolerated errors $\ell \geq 3$).

5.2 Memory consumption comparison

The initial phase of protocols A and B requires the use of registers to store bit elements necessary for the execution of the protocol. Table 4 presents the memory consumption in term of the number of bits stored by each protocol. The comparison is first made on the base of a fixed common number of rounds n. For parameters chosen to ensure fair comparison between A, B and MUSE-

ℓ	HK	MUSE-8HK	A (PPM)	B
5	$3.78 \cdot 10^{-1}$	$3.76 \cdot 10^{-9}$	$3 \cdot 10^{-13}$	$7.62 \cdot 10^{-11}$
4	$2.13 \cdot 10^{-1}$	$2.7 \cdot 10^{-10}$	10^{-13}	$2.81 \cdot 10^{-11}$
3	$9.62 \cdot 10^{-2}$	$1.74 \cdot 10^{-11}$	$2 \cdot 10^{-14}$	$8.47 \cdot 10^{-12}$
2	$3.21 \cdot 10^{-2}$	$5.81 \cdot 10^{-13}$	$3.5 \cdot 10^{-15}$	$1.81 \cdot 10^{-12}$
1	$7 \cdot 10^{-3}$	$1.46 \cdot 10^{-14}$	$4 \cdot 10^{-16}$	$2.51 \cdot 10^{-13}$

Table 3: Security comparison of distance bounding protocols in noisy channels, A ($N_c = 8$, $N_f = 1$, $N' = 1$) and B ($N_f = 3$, $\Delta = 0$).

pHK protocols, the memory consumption is minimal for protocol B. Protocol A guarantees a lower memory consumption than MUSE-pHK for $N_c = p \geq 8$.

Protocols	Memory consumption
HK	$2.n$
MUSE-pHK	$n.p. \log_2 p$
A	$n.(3.N_f. \log_2 N_c + 3 + N_f.(N_c - 1))$
B	$n.(3.N_f - 1)$

Table 4: Memory consumption comparison for different distance bounding protocols.

The memory consumption comparison can be made also on the base of a fixed common security level. In fact, n intervenes in the memory consumption and the number of rounds required for a certain security level is not the same for the different protocols. Thus, Table 5 depicts the memory consumption for a fixed security level. Parameters of protocol A (resp. protocol B) are $N_c = 4$, $N' = 2$ and $N_f = 1$ (resp. $N_f = 2$ and $\Delta = 0$). Based on Table 5, the HK protocol is placed in first position. The protocol B is placed in second position, followed by protocol A and finally MUSE-4HK protocol. The first position of HK protocol hides the drawback that n is large and therefore the long runtime of this protocol. The benefits of our proposed protocols is that protocol B insures the same security level than MUSE-4HK with less memory consumption. Regarding protocol A, the memory consumption and also the number of rounds become less important than MUSE-4HK protocol, in contrast to the comparison based on a fixed n.

6 Conclusion

Distance bounding protocols can greatly benefit from being integrated into the physical layer of a radio system. This has been shown in this paper for the TH-UWB radio. This technology offers two opportunities to enhance the security of distance bounding protocols: secret time-hopping codes and/or secret mapping codes. The impact of each strategy has been studied and it appears that secret time-hopping codes are to be favored over secret mapping codes from a security point of view.

	HK		MUSE-4HK		A (PPM)		B	
Probability	Memory	Rounds	Memory	Rounds	Memory	Rounds	Memory	Rounds
$8.14 \cdot 10^{-7}$	98	49	136	17	120	10	105	21
$7.35 \cdot 10^{-10}$	148	74	208	26	180	15	155	31
$6.63 \cdot 10^{-13}$	196	98	272	34	240	20	205	41
$5.99 \cdot 10^{-16}$	244	122	344	43	300	25	255	51

Table 5: Memory consumption comparison of different protocols for a fixed security level, protocol A ($N_c = 4$, $N_f = 1$, $N' = 2$) and protocol B ($N_f = 2$, $\Delta = 0$)

The security of the proposed strategies A and B has been analyzed in noise-free and noisy cases. The analysis takes into account the parameters of the TH-UWB link : PPM and OOK modulations for the transmitter, the IEEE 802.15.4a CM1 multipath model for the channel and a non-coherent structure for the receiver. The results in the noisy case have permitted to determine the signal-to-noise ratios required to satisfy security constraints. Moreover, the comparison of our proposed protocols to the state of the art has affirmed that protocol A offers the best security level in both noise-free and noisy channels. Protocol B guarantees a security level better than MUSE-pHK [35] in a noisy environment. Furthermore, it offers a good trade-off between security and memory consumption compared to [35]. Further work will investigate the resiliency of our protocols to the other types of relay attacks: the terrorist and the distance frauds.

References

[1] Yvo Desmedt, Claude Goutier, and Samy Bengio. Special Uses and Abuses of the Fiat-Shamir Passport Protocol. In *Advances in Cryptology – CRYPTO'87*, Lecture Notes in Computer Science 293, pages 21–39, Santa Barbara, California, USA, 1988. Springer-Verlag.

[2] Jolyon Clulow, Gerhard P. Hancke, Markus G. Kuhn, and Tyler Moore. So Near and Yet So Far: Distance-Bounding Attacks in Wireless Networks. In *Security and Privacy in Ad-Hoc and Sensor Networks, Third European Workshop - ESAS 2006*, Lecture Notes in Computer Science 4357, pages 83–97. Springer Verlag, 2006.

[3] L. Francis, G.P. Hancke, K.E. Mayes, and K. Markantonakis. Practical NFC Peer-to-Peer Relay Attack using Mobile Phones. In *Workshop on RFID Security - RFIDSec 2010*, Istanbul, Turkey, June 2010.

[4] Gerhard Hancke. A Practical Relay Attack on ISO 14443 Proximity Cards. Manuscript, February 2005.

[5] Albert Levi, Erhan Çetintas, Murat Aydos, Çetin Kaya Koç, and M. Ufuk Çaglayan. Relay Attacks on Bluetooth Authentication and Solutions. In *International Symposium Computer and Information Sciences - ISCIS 2004*,

Lecture Notes in Computer Science 3280, pages 278–288. Springer Verlag, 2004.

[6] Saar Drimer and Steven J. Murdoch. Keep your enemies close: distance bounding against smartcard relay attacks. In *16th USENIX Security Symposium*, pages 1–16. USENIX Association, 2007.

[7] Srdjan Capkun and Jean-Pierre Hubaux. Secure Positioning in Wireless Networks. *IEEE Journal on Selected Areas in Communications: Special Issue on Security in Wireless Ad Hoc Networks*, 24(2):221–232, 2006.

[8] Stefan Brands and David Chaum. Distance-Bounding Protocols. In *Advances in Cryptology – EUROCRYPT'93*, Lecture Notes in Computer Science 765, pages 344–359. Springer-Verlag, 1993.

[9] Gildas Avoine, Muhammed Bingol, Suleyman Kardars, Cédric Lauradoux, and Benjamin Martin. A Framework for Analyzing RFID Distance Bounding Protocols. *Journal of Computer Security - Special Issue on RFID System Security*, 2010.

[10] Nils Ole Tippenhauer and Srdjan Capkun. ID-Based Secure Distance Bounding and Localization. In *European Symposium on Research in Computer Security - ESORICS 2009*, Lecture Notes in Computer Science 5789, pages 621–636. Springer Verlag, 2009.

[11] Marc Kuhn, Heinrich Luecken, and N O. Tippenhauer. UWB Impulse Radio Based Distance Bounding. In *7th Workshop on Positioning, Navigation and Communication 2010 (WPNC'10)*, Dresden, Germany, March 2010.

[12] Robert J. Fontana and Steven J. Gunderson. Ultra-Wideband Precision Asset Location System. In *IEEE Conference on Ultra Wideband Systems 2002*, pages 147–150. IEEE, 2002.

[13] Gerhard Hancke and Markus Kuhn. An RFID Distance Bounding Protocol. In *Conference on Security and Privacy for Emerging Areas in Communication Networks – SecureComm 2005*, pages 67–73. IEEE Computer Society, 2005.

[14] A. Benfarah, B. Miscopein, J. M. Gorce, C. Lauradoux, and B. Roux. Distance Bounding Protocols on TH-UWB Radios. In *The Proceedings of the 2010 IEEE Global Telecommunications Conference (GLOBECOMM 2010)*, page to be appeared, December 2010.

[15] Jorge Munilla and Alberto Peinado. Distance bounding protocols for RFID enhanced by using void-challenges and analysis in noisy channels. *Wireless Communications and Mobile Computing*, 8(9):1227–1232, 2008.

[16] Dave Singelée and Bart Preneel. Distance Bounding in Noisy Environments. In *European Workshop on Security and Privacy in Ad-Hoc and Sensor Networks (ESAS), Springer-Verlag LNCS 4572*, pages 101–115, 2007.

[17] A. Mitrokotsa, C. Dimitrakakis, P. Peris-Lopez, and J. C. Hernandez-Castro. Reid et al.'s distance bounding protocol and mafia fraud attacks over noisy channels. *Comm. Letters.*, 14(2):121–123, 2010.

[18] R. A. Scholtz. Multiple Access with Time Hopping Impulse Modulation -Invited Paper. In *Proc. IEEE MILCOM Conf.*, pages 447–450, Bedford, 1993.

[19] M. Z. Win and R. A. Scholtz. Impluse radio : how it works. *IEEE Communications Letters*, 2:36–38, Feb 1998.

[20] *France Telecom R&D proposal for IEEE 802.15.4a Task Group*, 2005.

[21] I. Guvenc and H. Arslan. On the Modulation Options of UWB Systems. In *Proc. IEEE MILCOM '03*, pages 892–897, October 2003.

[22] A. F. Molisch, K. Balakrishnan, D. Cassioli, C.-C Chong, S. Emami, A. Fort, J. Karedal, J. Kunisch, H. Schantz, U. Schuster, and K. Siwiak. IEEE 802.15.4a channel model- final report. Technical Report ET Document IEEE 802.15-04-0662-02-004a, IEEE 802.15.4a Channel Sub-Committee, 2005.

[23] Giuseppe Durisi and Sergio Benedetto. Comparison between Coherent and Noncoherent Receivers for UWB Communications. *EURASIP J. Appl. Signal Process.*, 2005:359–368, 2005.

[24] Y. Souilmi and R. Knopp. Challenges in UWB signalling for adhoc networking. In *DIMACS Workshop on Signal Processing for Wireless Transmission*, oct 2002.

[25] M. Weisenhorn and W. Hirt. Robust Noncoherent Receiver Exploiting UWB Channel Properties. In *UWBST04*, pages 156–160, Kyoto, Japan, May 2004.

[26] Y. Ying, M. Ghogho, and A. Swami. Code-Assisted Synchronization for UWB-IR Systems: Algorithms and Analysis. *IEEE Transactions on Signal Processing*, 56(10):5169–5180, October 2008.

[27] B. Miscopein and J. Schwoerer. Low complexity synchronization algorithm for non-coherent UWB-IR receivers. In *Vehicular Technology Conference 2007 VTC2007-Spring IEEE 65th*, pages 2344–2348, Dublin, April 2007.

[28] P.A. Humblet and M. Azizoglu. On the Bit Error Rate of Lightwave Systems with Optical Amplifiers. *Journal of Lightwave Technology*, 9(11), November 1991.

[29] S. Paquelet, L-M. Aubert, and B. Uguen. An Impulse Radio Asynchronous Transceiver for High Data Rates. In *proceedings of joint UWBST & IWUWBS*, Kyoto, Japan, 2004.

[30] J. G. Proakis. *Digital Communications*. Mc Graw-Hill International Editions, third edition, 1995.

[31] S. Dubouloz, B. Denis, S. de Rivaz, and L. Ouvry. Performance Analysis of LDR UWB Non-Coherent Receivers in Multipath Environments. In *IEEE International Conference on Ultra-Wideband*, pages 491–496, September 2005.

[32] J. Bachrach and C. Taylor. *Handbook of Sensor Networks*, chapter Localization in Sensor Networks. Wiley, 2005.

[33] Gildas Avoine and Aslan Tchamkerten. An Efficient Distance Bounding RFID Authentication Protocol: Balancing False-acceptance Rate and Memory Requirement. In *Information Security Conference-ISC'09*, volume 5735 of *Lecture Notes in Computer Science*. Springer Verlag, 2009.

[34] Jason Reid, Juan Gonzalez Neito, Tee Tang, and Bouchra Senadji. Detecting Relay Attacks with Timing-Based Protocols. In *Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security-ASIACCS'07*, pages 204–213, March 2007.

[35] Gildas Avoine, Christian Floerkemeier, and Benjamin Martin. RFID Distance Bounding Multistate Enhancement. In *Progress in Cryptology - INDOCRYPT 2009*, Lecture Notes in Computer Science 5922, pages 290–307. Springer Verlag, 2009.

Contents

Centre de recherche INRIA Grenoble – Rhône-Alpes
655, avenue de l'Europe - 38334 Montbonnot Saint-Ismier (France)

Centre de recherche INRIA Bordeaux – Sud Ouest : Domaine Universitaire - 351, cours de la Libération - 33405 Talence Cedex
Centre de recherche INRIA Lille – Nord Europe : Parc Scientifique de la Haute Borne - 40, avenue Halley - 59650 Villeneuve d'Ascq
Centre de recherche INRIA Nancy – Grand Est : LORIA, Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - BP 101 - 54602 Villers-lès-Nancy Cedex
Centre de recherche INRIA Paris – Rocquencourt : Domaine de Voluceau - Rocquencourt - BP 105 - 78153 Le Chesnay Cedex
Centre de recherche INRIA Rennes – Bretagne Atlantique : IRISA, Campus universitaire de Beaulieu - 35042 Rennes Cedex
Centre de recherche INRIA Saclay – Île-de-France : Parc Orsay Université - ZAC des Vignes : 4, rue Jacques Monod - 91893 Orsay Cedex
Centre de recherche INRIA Sophia Antipolis – Méditerranée : 2004, route des Lucioles - BP 93 - 06902 Sophia Antipolis Cedex

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt, BP 105 - 78153 Le Chesnay Cedex (France)
http://www.inria.fr
ISSN 0249-6399