World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:11, No:5, 2017

Secure Distance Bounding Protocol on Ultra-WideBand Based Mapping Code

Jamel Miri, Bechir Nsiri, Ridha Bouallegue

***Abstract*—**Ultra WidBand-IR physical layer technology has seen a great development during the last decade which makes it a promising candidate for short range wireless communications, as they bring considerable benefits in terms of connectivity and mobility. However, like all wireless communication they suffer from vulnerabilities in terms of security because of the open nature of the radio channel. To face these attacks, distance bounding protocols are the most popular counter measures. In this paper, we presented a protocol based on distance bounding to thread the most popular attacks: Distance Fraud, Mafia Fraud and Terrorist fraud. In our work, we study the way to adapt the best secure distance bounding protocols to mapping code of ultra-wideband (TH-UWB) radios. Indeed, to ameliorate the performances of the protocol in terms of security communication in TH-UWB, we combine the modified protocol to ultra-wideband impulse radio technology (IR-UWB). The security and the different merits of the protocols are analyzed.

***Keywords*—**Distance bounding, mapping code ultra-wideband, Terrorist Fraud.

I. Introduction

THE impulse radio UWB-IR (Ultra Wide Band Impulse Radio) is an interesting candidate for wireless networks at close range. From the world's radar and military research, the UWB-IR radio was adopted in the telecommunications world in the years 1990. Currently, the ultra-wideband impulse radio technology (UWB-IR) is a very relevant and promising solution for WSNs. Indeed, it's poised to find use in a broad range of consumer, enterprize, industrial and public safety applications [1].

In terms of standardization, UWB-IR technology was standardized as an alternative to ZigBee physical layer with the standard IEEE 802.15.4a-2007 [2]. It was also standardized in 2012 as a possible physical layer for BAN networks with the IEEE 802.15.6 standard [3]. On the academic and industrial level, interest in the UWB-IR radio has developed since 2002, regulation date of UWB systems by the agency FCC (Federal Communication Commission) [4].

The principle of the impulse radio based on the emission of very short pulses directly to baseband. This transmission principle allows to use simplified transmitter / receiver architectures with low cost. A remarkable feature of the UWB-IR radio is the wide bandwidth that can range from several hundred MHz to several GHz. This feature ensures a robustness in harsh propagation environments. Furthermore, this same feature provides a very fine time resolution for the localization in indoor environment. The structure of the UWB-IR symbol allows flexibility flow which is advantageous to diversify the applications.

The relay attack is carried in the physical layer and poses a great threat against the security of wireless communications introduced by Desmedt et al. [5]. Indeed, this attack requires few resources and does not require solving problems called "difficult". It is particularly effective against the authentication protocols and wireless secure location protocols (secure localization). Having presented the relay attack in these types of applications, the first solution to this threat is Distance Bounding (DB) protocols as called by Brand and Chaum (BC)[6]. The DB assumes a mechanism to measure the precise distance between two device radios. The IR-UWB technology is an ideal candidate for the implementation of distance bounding protocols. This has been recognized in several different proposals and work [7]-[9].

One of the interesting applications of UWB-IR technology is the location. In this sense, the IEEE 802.15.4a [2] provides an optional operating mode for localization. However, work has been published [10], [11] against attacks on dedicated location using the IR-UWB radio. The need to secure this mechanism becomes very important for the technology to be widely adopted. This point was mentioned as an important research direction in a review article on localization using UWB-IR technology [12].

In our work, we select the best DB protocol used in RFID systems having the highest quality of security evaluation called SKI. The SKI protocol consists in computing the resistance for every type of fraud, which is done by computing the probability for an adversary to successfully perform the considered fraud [13]. We adapt this protocol to the context of TH-UWB radios. In order to ameliorate the robustness and security communication between the different devices in UWB system, and to increase the resiliency to the noise and the active users in the same UWB, we combine the SKI and the mapping code protocol of UWB-IR.

This paper is organized as follows: The next section gives a brief review Distance Bounding protocols and the propriety of the best chosen protocol which can resist to three types of attacks. In Section III we introduced the mapping code protocol in UWB-IR . In Section IV, we describe the principle of the proposed Distance Bounding protocol with a secret mapping code and finally, the Section V evaluates and compares the security level of our protocol with existing Distance Bounding protocols implemented in UWB-IR system.

Jamel Miri is with the Innov'Com Laboratory, Sup'Com, ENIT, Tunisia (e-mail: jamel.miri@laposte.net).

Bechir Nsiri is with the Sys'Com Laboratory, ENIT, Tunisia (e-mail: bechirnsiri@gmail.com).

Ridha Bouallegue is with the Innov'Com Laboratory, Sup'Com, Tunisia (e-mail: ridha.bouallegue@supcom.tn).

II. Distance Bounding Protocol

A first solution to the relay attack was provided by Brands and Chaum [6] with the distance bounding. The concept is to combine the authentication of the *Prover* and checking the distance to meet the definition of the entity authentication, wish is define as a process where one party is assured the identity of a second party involved in a protocol, and the second has actually participated [14]. Indeed, thanks to the distance verification mechanism, the *Verifier* can be said that the second part, the *Prover*, was really involved in the protocol. The property provided by checking the distance is an upper bound on the Euclidean distance between the two parts: establishing a neighborhood around the *Verifier* in which the *Prover* can authenticate successfully. The distance bounding protocol says sure if the *Verifier* rejects the *Prover* with overwhelming probability if it's not legitimate and / or it is not in the vicinity of the *Verifier*. The protocol says **ok** if the *Verifier* accepts the *Prover* when legitimate and in the neighborhood.

There are several techniques to estimate the distance between two devices [15]: GPS (*Global Positioning System*), RSSI (*Received Signal Strength Indication*), AoA (*Angle of Arrival*), RTT (*Round Trip Time*)... These Techniques have advantages and disadvantages in terms of accuracy and implementation. The author will detail some of these techniques. GPS is based on a set of satellites that provide a three-dimensional position. It achieves accuracies of a few meters in outdoor. However, the GPS system has certain limitations. Indeed, it runs in a degraded or no longer works in dense urban environments and indoors. In addition, a GPS receiver is a significant material cost for small embedded objects. GPS for civilian applications is vulnerable to certain attacks [16]. The technique $RSSI$ is disqualified from the security point of view as described in the preceding paragraph. The AoA technique examines the directions of the received signals to estimate the distance. This technique is still inadequate for security because the attacker can retransmit the signal from a different direction. The principle of RTT consists of measuring the time of return T_m between transmission of one bit c by the *Verifier* and the receipt of the response r sent by the *Prover*. The distance between the two parties may be deducted from T_m by (1).

$$d = c.\frac{T_m - T_d}{2} \tag{1}$$

where c is the propagation speed and T_d is the *Prover* processing time.

The Security distance measuring process requires the T_d delay is minimal. The implementation of the RTT technique requires at least a clock. This technique is very popular for embedded systems and this is the solution adopted by major distance bounding protocols. In DB protocol, the two parts the (*Prover* P and the *Verifier* V) need to share a common high-precision time. But in RTT, the *Prover* is no longer responsible for providing the security critical time measure and only the *Verifier* is require to maintain it. The distance between the *prover* and the *Verifier* is calculated according to the equation:

$$d = c(T_m - T_d)/2 \tag{2}$$

where T_m is the measured RTT and T_d is the *Prover* processing delay. The measured RTT (T_m) is defined as:

$$T_m = 2.T_p + T_d \tag{3}$$

The RTT based Distance Bounding protocol proposed by Hancke and Khan [5] is composed of two steps. In first step called $initialization\ phase$, the *Prover* and the *Verifier* compute a share state and in second phase, called $fast\ phase$, the RTT is measured several times and the authentication process is carried out. The Hancke and Khan protocol is described in Fig. 1.

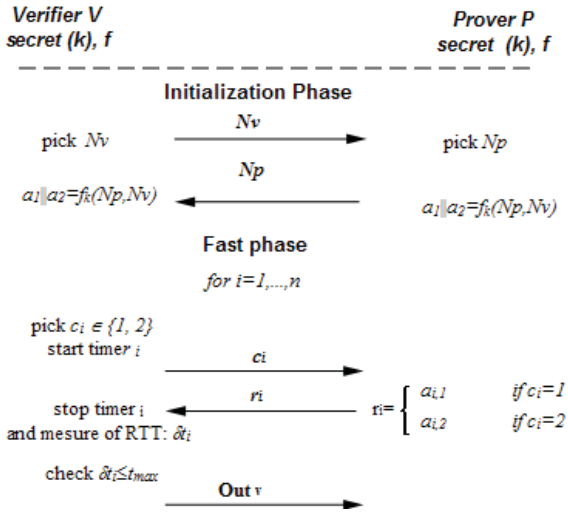

Fig. 1 Hancke and Kuhan Protocol

Many distance bounding protocols are designed every year and compared [2], [6], [17]-[20]. From different comparison methodology distance bounding protocol, the SKI provides the most appropriate protocol due to its resistance to attacks (distance fraud (D_f), mafia fraud (M_f) and terrorist fraud (T_f) from a fraudulent *Prover* and malicious third party [13]. The result of comparison of the different protocols is shown in Fig. 2 and described in Table I.

TABLE I
Distance Bounding Protocols Resistance to Attacks

Protocols	$P(M_f)$	$P(D_f)$	$P(D_f)$
BC	$(1/2)^n$	$(1/2)^n$	1
HK	$(3/4)^n$	$(3/4)^n$	1
SK	$(1/2)^n$	$(3/4)^n$	$(3/4)^n$
SKI	$(t+1/2t)^n$	$< (3/4)^n$	$(2t-2/2t)^n$

t is the size of the messages exchanged in the RTT fast phase.

In our paper, we consider a two identical capability UWB devices used by the *Prover* and *Verifier*. The chosen distance bounding protocol is based on the work of SKI protocol due to its resistance to the most popular attacks. The SKI protocol is described in [21], [22] and Fig. 3 shows how this protocol works.

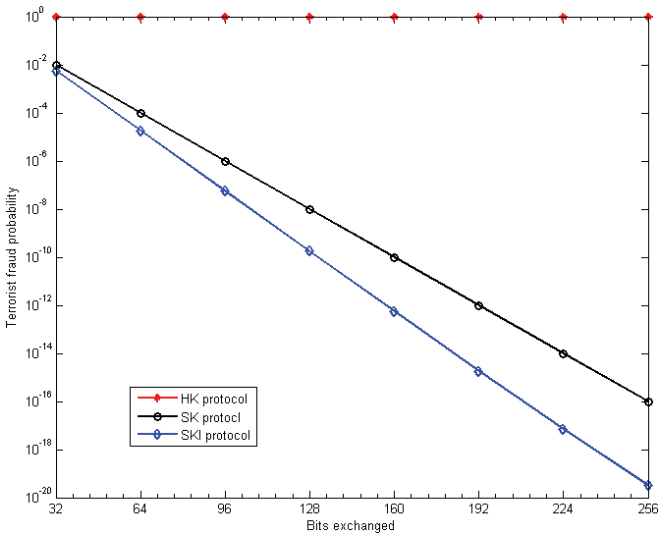

Fig. 2 Terrorist Fraud (T_f) Resistance of Protocols HK, SK and SKI

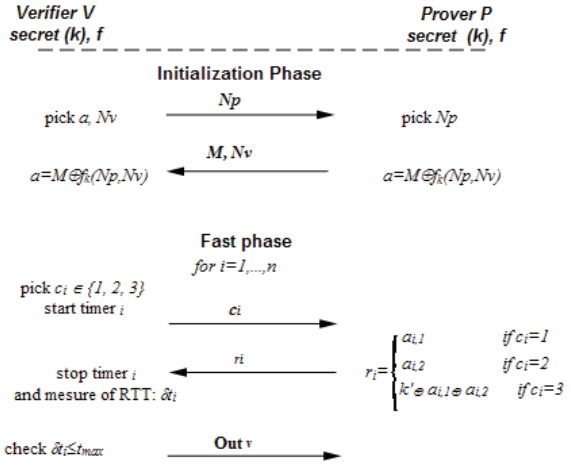

Fig. 3 SKI Protocol

III. Proposed Distance Bounding Protocol

For UWB distance bounding protocols, many researches are proposed in order to ameliorate the sensibility to thwart the most popular attacks. Reference [23] proposed the protocol B based on the HK and it is called **Secret Mapping Code Protocol** (SMCP), where the mapping code is the secret part of the proposed scheme. The protocol SMCP is described in Fig. 4.

The proposed distance bounding protocol can resist to two attacks (Distance Fraud and Mafia Fraud), but not to terrorist fraud because the core of these protocols follows the principle of HK. To fix this problem, our proposed protocol has a goal to resist to these three attacks (D_f, M_f, and T_f). In our paper, we proposed a new protocol what is based on SKI protocol used in RFID systems. This choice is not arbitrary but is due to the power of SKI to resist to these three attacks. We called MCSKI (Mapping Code SKI). It is a combination of the SKI protocol and Mapping Code.

In our proposition, we assume that the synchronization is performed initially between the *Verifier* (V) and the legitimate

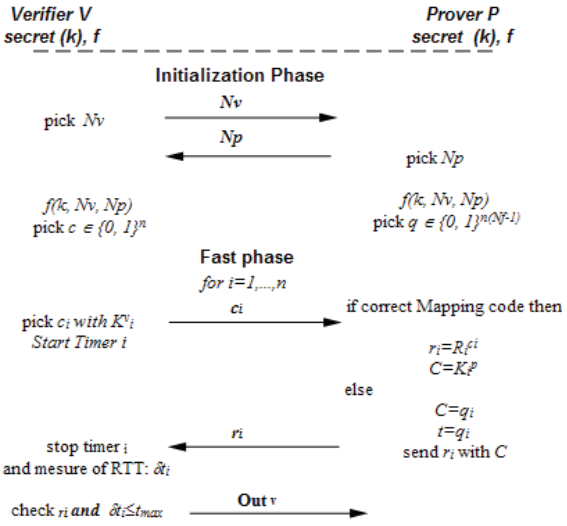

Fig. 4 Secret Mapping Code Protocol (SMCP)

Prover (P) before the distance bounding protocol begins. The synchronization will be maintained during the protocol execution. During our transmission, the **mapping code will be secret** and the Time Hopping code is public. The full function of the protocol is described in Fig. 5.

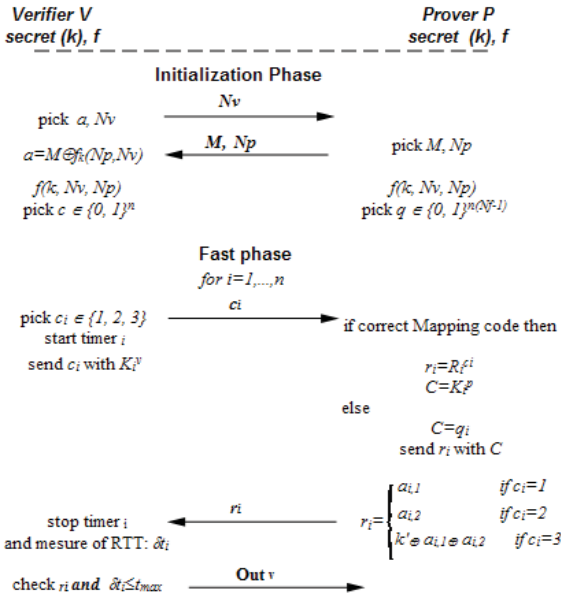

Fig. 5 Mapping Code SKI (MCSKI)

A. Protocol Requirements

In our protocol, P and V share secret key $K\epsilon\ \{0,1\}^m$ using a secret sharing schemes named "Leakage scheme". The protocol should leak one bit of the secret key each time a malicious user provides the adversary with all vectors required for authentication. A linear function $L_\mu\ (K)\epsilon\ \{0,1\}^n$ as defined as $L_\mu\ (K)$ = ($\mu.K\ \mu.K\ \ldots\ \mu.K$). In which $K\epsilon\ \{0,1\}^s$ and $\mu.K$ is the inner product of μ and K. For each μ, $L_\mu\ (K)$ contains only one bit of information about the key

K. For this case SKI resist to terrorist fraud. Let K' be the output of leakage scheme functionK'= $\mu.K$.

The relationship between a random vector a and K' is a linear function as in $F(c_i, a_i, K')$. The F function is defined in SKI protocol which means the *Prover* and the *Verifier* agrees on the three vectors on a random vector called a and the leakage scheme output K'. The F scheme is defined in (4).

$$\begin{aligned} F(1, a_i, K) &= a_{1,i} \\ F(2, a_i, K) &= a_{2,i} \\ F(3, a_i, K) &= a_{1,i} \oplus a_{2,i} \oplus K' \end{aligned} \tag{4}$$

The protocol is divided to three steps: the Initialization phase, fast phase and the verification of the RTT measurement and authentication. The mapping code used in UWB systems to provide redundancy and correct transmission errors. In the MCSKI protocol, the mapping code will be operated in addition to its primary functionality to enhance security. Indeed, *V* and *P* will be able to detect an attack if the word of the received code is a Hamming distance exceeds a certain threshold of the expected code word. Where, The Hamming distance between two binary codewords of the same length is defined by the Hamming weight of the result of the logic operation XOR between the bit words.

The *Prover* and the *Verifier* use codebook to encoding and decoding with a side information. The codebook consists in the cosets of an $(N_f, 1, d)$ reputation code. For example let consider the $(4, 1, 4)$. The 2^{N_f-1} cosets of the code are defined in Table II.

TABLE II
COSETS OF THE CODE $(4, 1, 4)$

Number of coset	cosets
K_1	00001111
K_2	00011110
K_3	00101101
K_4	00111100
K_5	01001011
K_6	01011010
K_7	01101001
K_8	01111000

The Hamming distance between codewords of each coset is $d = 4$. For each bit transmitted during the protocol, a coset is chosen to define how the 0 and the 1 are encoded. For instance, 0 can coded with minimum of the coset. The MCSKI have the same requirements as the protocol A (SMCP) [23] with addition of the codebook.

B. Initialization Phase

The *Prover* and the *Verifier* exchange N_P and N_V . Then, they both compute the share state H = $f(k, N_P, N_V)$ of length $2.N_f.n$ bits. Let consider $N_f = 4$, the length of H is $8n$ which is split into five registers:

- The register C^V of length $3n$ defines the sequence C_i^V of cosets used during the protocol by the *Verifier*: $C^V = \underbrace{H_1, H_2, H_3}_{C_1^V}, \underbrace{H_4, H_5, H_6}_{C_2^V}, ..., \underbrace{H_{3n-2}, H_{3n-1}, H_{3n}}_{C_n^V}.$
- The register C^P of length $3n$ defines the sequence C_i^P of cosets used during the protocol by the *Prover*: $C^V = \underbrace{H_{3n+1}, H_{3n+2}, H_{3n+3}}_{C_1^P}, ..., \underbrace{H_{6n-2}, H_{6n-1}, H_{6n}}_{C_n^P}.$
- A register $R^0 = H_{6n+1}...H_{7n}$ containing n bits.
- A register $R^1 = H_{7n+1}...H_{8n}$ containing n bits.
- A register R^2 = $R^0 \oplus R^1 \oplus K'$.

In addition, the *Verifier* and the *Prover* pick respectively an $n - bit$ random vector c and $3n - bit$ vector q. The vector q has the same purpose than C^V and C^P. It is composed of symbols of 3 bits.

C. Fast Phase

For each round i, $1 \leq i \leq n$, the *Verifier* sends a challenge bit c_i coded with a word form the coset C_i^V to P. The *Prover* checks that the challenge corresponds to a word from the coset C_i^V: the *Prover* computes the Hamming distance between the mapping code of received challenge and the two words from the coset C_i^V. If this Hamming distance$\leq \Delta$, then the *Prover* responds with $r_i = R_i^{ci}$ coded from the coset C_i^P. Δ must be chosen such that:

$$\Delta \preceq \lfloor \frac{d-1}{2} \rfloor \tag{5}$$

So, in our example $\Delta \leq 1$. The interest of Δ is to make a tradeoff between security and resiliency to noise. Taking $\Delta = 0$ is more beneficial to security while taking Δ such as (5) with equality is more beneficial to error correction. If the Hamming distance condition is not satisfied, the *Prover* detects an attack and responds with a random mapping form the vector q. The *Verifier* computes the RTT in each round.

D. Verification Phase

The protocol succeeds if all responses r_i are distant at most with Δ from the codeword of coset C_i^P and $\forall i$, $\delta t_i \leq t_{max}$ where t_{max} is an upper-bound.

IV. PERFORMANCES ANALYSIS

For simulating and comparing our Distance Bounding protocol MCSKI with protocol SMCP [23] where the best strategy for the adversary is the pre-asking strategy. But how can we compute this attack for the our protocol MCSKI?

In this section, we provide the security analysis of protocol MCSKI with no noise, $i.e$ $\Delta = 0$. The adversary queries the *Prover* with challenge $\widehat{c_i}$ encoded randomly from all the combinations. Then, the adversary obtains the encoded form of r_i from the *Prover*. Here, the time-hopping (TH) sequences are predefined and public, so the adversary knows in which time slots it should transmit the pulses. In this section, Our protocol MCSKI belongs to the class of SKI. Thus, the security analysis was performed with the no-asking strategy and by pre-asking strategy.

No-asking strategy: The adversary attempts to answer to the *Verifier* challenges with randomly chosen mapping code. The adversary tries to meet the challenges of V alone. He does not know the codes mapping of responses, so the adversary

chooses randomly mapping codes. He succeeded his attack in the round *i* if the chosen mapping code is the code expected by V. Let define E_i the event that the mapping code of $\widehat{r}_i$ is at an Hamming distance less than Δ from the mapping code of the correct answer r_i. The probability of success with this strategy in the round i corresponds to $P(E_i) = \frac{1}{2^{N_f}}$. Thus the probability of success with no-asking strategy of attack for the protocol SMCP [23] and our protocol MCSKI are given in Table III.

TABLE III
PROBABILITY OF SUCCESS WITH NO-ASKING STRATEGY

Protocols	P_{na}
SMCP	$(1/2^{N_f})^n$
CMSKI	$(1/3^{N_f})^n$

Pre-asking strategy: The adversary queries the *Prover* with a challenge $\widehat{c_i}$ encoded randomly from all the combinations. Then, the adversary obtains the encoded form of r_i from the *Prover*. Let define G_i the event that the Hamming distance between the mapping code of c_i and one of the two words of coset C_i^v is less than Δ. The adversary succeeds its attack at round i^{th} if the event E_i is realized. We compute the probability of this event: $P(E_i) = P(E_i|G_i).P(G_i) + P(E_i|\bar{G}_i).P(\bar{G}_i)$ Thus the probability of success with **pre-asking strategy** of attack for the protocol SMCP [23] and our protocol MCSKI are given in Table IV.

TABLE IV
PROBABILITY OF SUCCESS WITH PRE-ASKING STRATEGY

Protocols	P_{pa}
SMCP	$(1/2^{N_f}).(5/2 - 1/2^{Nf-1})^n$
CMSKI	$(1/3^{N_f}).(5/2 - 1/3^{Nf-1})^n$

The security of the protocol is defined by the max (P_{na}, P_{pa}). In the both cases $P_{pa}/P_{na} \geq 1$. A against, the best strategy for the adversary is the pre-asking strategy.

In the case of noise free communication $\Delta = 0$, the we compare the probabilities of success of the pre-asking strategy for protocols HK, SKI, SMCP and our protocol MCSKI. From the obtained results (Fig. 6) we can see that the proposed protocol enhances the HK and the SMCP protocols we obtained a probability of success than less the value obtained using the two protocols. To evaluate the proposed protocol in terms of security, we compare all of them when $N_f = 4$, $N_c = 2$, $p = 2^{Nf} = 16$ the obtained results in terms of probability of success vs. Number of round.

Fig. 6 represents the probability that the adversary succeeds to attack the three protocols: HK, SMCP and the proposed protocol MCSKI. We can see that the proposed protocol which is a combination of mapping code and the SKI protocol achieved the best results and the performance enhancement almost then $1/3$ of the required number of rounds as compared with SMCP.

V. CONCLUSION

In this paper, we evaluate and compare the performance of three protocols: Hancke and Khun (HK) [5], Secure Mapping Code Protocol (SCMP) [8] and our protocol Mapping Code SKI (MCSKI). MCSKI is a combination of two protocols: SKI and mapping code protocol. Our work consists in implementing the protocol in TH-UWB system and comparing the performances of these protocols in terms of probability that the adversary can succeed to attack the system. In the second part, we compare the probability of success for different round number.

From the obtained results, it is clear that MCSKI can achieve the highest security level as compared with HK and SMCP protocols proposed in [23]. Theses results are obtained due to the propriety security of the SKI which can resist to three types of attacks: Distance fraud, mafia fraud and terrorist fraud. The combination of the SKI protocol and Mapping Code protocol increases the security level of the protocol which outperforms the HK and SMCP protocols. Further work will investigate the importance of our protocol if it used in network UWB-IR radio.

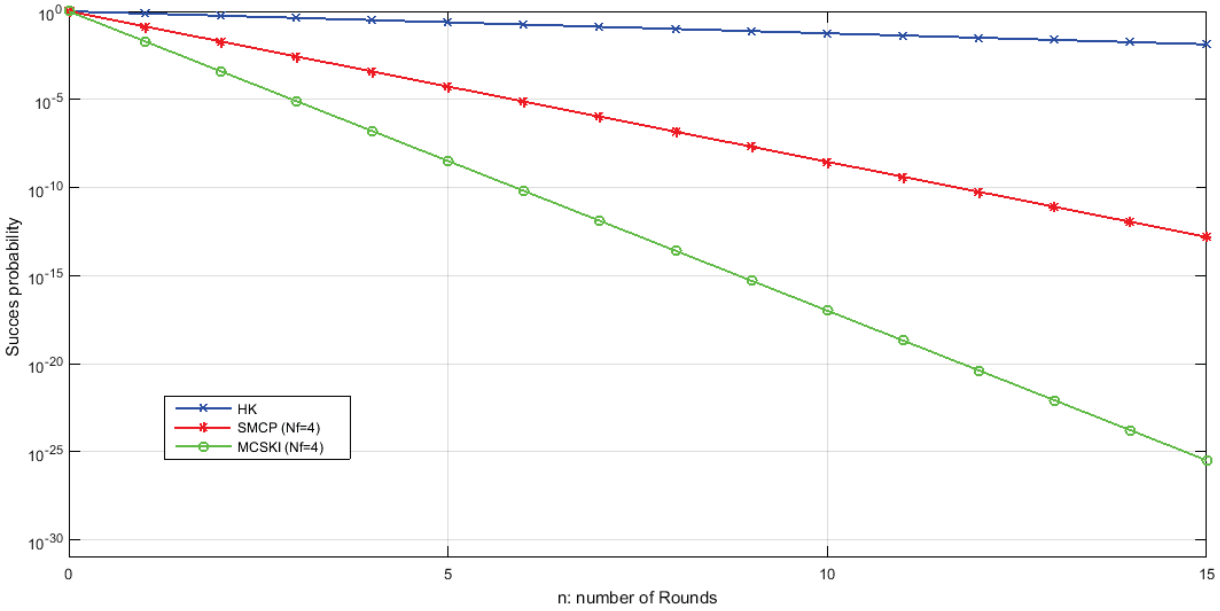

Fig. 6 Adversary success probability against protocols HK, SMCP, and MCSKI with $N_s = 8$, $N_f = 4$

REFERENCES

[1] Phillips, Kevin, "System Simulations of DSTRD and TH-PPM for Ultra Wide Band (UWB) Wireless Communications" (2006). All Volumes (2001-2008), Paper 70.

[2] IEEE. 802.15.4a: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Personal Area Networks (LR-WPANs)-Amendment 1: Add Alternate PHYs, August 2007.

[3] IEEE Standard for Local and Metropolitan Area Networks-Part 15.6: Wireless Body Area Networks, February 2012.

[4] "FCC. First Report and Order Regarding UWB Transmission," Federal Communication Commission, Washington, Technical Report ET Docket D.C. 20554, February 2002.

[5] Y. Desmedt, C. Goutier, and S. Bengio, "Special Uses and Abuses of the Fiat-Shamir Passport Protocol," in Advances in Cryptology- CRYPTO'87, ser.Lecture Notes in Computer Science 293. Santa Barbara, California, USA: Springer-Verlag, 1988, pp.21-39.

[6] S. Brands and D. Chaum, "Distance-Bounding Protocols," in Advances in Cryptology-EUROCRYPT'93, ser. Lecture Notes in Computer Science765. Springer-Verlag, 1993, pp.344-359.

[7] G. Hancke and M. Kuhn, "An RFID Distance Bounding Protocol," in Conference on Security and Privacy for Emerging Areas in Communication Networks-Secure-Comm 2005. Athens, Greece : IEEE Computer Society, December 2005, pp. 67-73.

[8] N. O. Tippenhauer and S.Capkun, "ID-Based Secure Distance Bounding and Localization," in European Symposium on Research in Computer Security-ESORICS 2009, ser. Lecture Notes in Computer Science 5789. Saint Malo, France: Springer Verlag, September 2009, pp. 621-636.

[9] M. Kuhn, H. 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.

[10] M. Flury, M. Poturalski, P. Papadimitratos, J.-P. Hubaux, and J.-Y. LeBoudec, "Effectiveness of Distance-decreasing Attacks Against Impulse Radio Ranging," in 3rd ACM Conference on Wireless Network Security (WiSec'10), Hoboken, NJ, USA, March 2010.

[11] M. Poturalski, "Secure Neighbor Discovery and Ranging in Wireless Networks," Ph.D. dissertation, Ecole Polytechnique Federale de Lausanne, 2011.

[12] D. Dardari, A. Conti, U. Ferner, A. Giorgetti, and M. Z. Win, "Ranging with ultrawide bandwidth signals in multipath environments," Proceedings IEEE, vol. 97, no. 2, pp. 404-426, 2009.

[13] Gildas Avoine. Sjouke Mauw, Rolando Trujillo-Rasua "Comparing Distance Bounding Protocols: a Critical Mission Supported by Decision Theory," Preprint submitted to Elsevier March 17, 2015.

[14] A. J. Menezes, P. C. Oorschot, and S. Vanstone, Handbook of Applied Cryptography. CRC Press, 1997.

[15] J. Bachrach and C. Taylor, Handbook of Sensor Networks. Wiley, 2005, ch. Localization in Sensor Networks.

[16] S. Capkun and J.-P. Hubaux,"Secure Positioning in Wireless Networks," IEEE Journal on Selected Areas in Communications : Special Issue on Security in Wireless AdHoc Networks, vol. 24, no. 2, pp. 221-232, February 2006.

[17] Tu, Y. J., Piramuthu, S., "RFID Distance Bounding Protocols," In First International EURASIP Workshop on RFID Technology. Vienna, Austria (September 2007).

[18] Rasmussen, K. B., Capkun, S., "Realization of RF Distance Bounding," In Proceedings of the 19th USENIX Security Symposium. Aug 2010 pp. 389-402.

[19] Munilla, J., Ortiz, A., Peinado, A. "Distance bounding protocols with voidchallenges for RFID" 2006, printed handout at the Workshop on RFID Security (RFIDSec).

[20] Bussard, L., Bagga, W. "Distance-Bounding Proof of Knowledge to Avoid Real-Time Attacks," in Proceedings of 20th International Conference on Security and Privacy in the Age of Ubiquitous Computing, May 2005, pp. 223-238.

[21] I. Boureanu, A. Mitrokotsa, and S. Vaudenay, "Secure and lightweight distance-bounding," in Lightweight Cryptography for Security and Privacy, ed : Springer,2013, pp. 97-113

[22] C. H. Kim, G. Avoine, F. Koeune, F.-X. Standaert, O. Pereira. The Swiss-Knife RFID Distance Bounding Protocol. In Information Security and Cryptology ICISC'08, Seoul, Korea, Lecture Notes in Computer Science 5461, Springer-Verlag, 2009. pp. 98-115,

[23] Benfarah, Ahmed and Miscopein, Benoit and Gorce, Jean-Marie and Lauradoux, Cédric and Roux, Bernard "Distance Bounding Protocols on TH-UWB Link and their Analysis over Noisy Channels" inria-00519064 - RR-7385- 2010, pp. 28.

Jamel Miri was born in Sidi Bouzid, Tunisia, on May 1970. He Received the Dipl.- Engi. degree in Telecommunication engineering in 2001 from Sup'Com . Currently he is a Ph.D. student at the School of Engineering of Tunis (ENIT). The research works are realized Research Laboratory Innov'COM / Sup'Com. His principal research interests lie in the fields of Wireless Ad Hoc and Sensor Networks, Embedded and RFID Systems, focusing on identification, modeling and mitigation of network security vulnerabilities, and analysis of network performance such as UWB, WSNs and Ad'Hoc technology.

Bechir Nsiri was born in Boussalem, Tunisia, on August 1983. From September 2011 until now, he teaches in Higher Institute of Applied Science and Technology Mateur, Tunisia. He received his master degree and Ph.D. in telecommunication specialty from the National School of Engineering in Tunis

(ENIT) in Tunisia in 2011. The research works are realized in Department Sys'COM laboratory in ENIT. His principal research interests lie in the fields of Wireless and Radio Mobile Telecommunications engineering such as MIMO OFDM technology and scheduling in radio network planning in LTE system.

Ridha Bouallegue was born in Tunis, Tunisia. He received the M.S degree in Telecommunications in 1990, the Ph.D. degree in Telecommunications in 1994, and the Habilitation a Diriger des Recherches (HDR) degree in Telecommunications in 2003, all from the National Engineer School of Tunis (ENIT), Tunisia. He is currently Professor in the National Engineer School of Tunis (ENIT) and Director of Research Laboratory Innov'COM / Sup'Com. His current research interests include mobile and satellite communications, Access technique, intelligent signal processing, CDMA, MIMO, OFDM and UWB system.