SRTTU

Journal of Electrical and Computer Engineering Innovations

JECEI, Vol. 2, No. 2, 2014

Regular Paper

Security Analysis of the Distance Bounding Protocol Proposed by Jannati and Falahati

Fatemeh Baghernejad[1], Nasour Bagheri[1,*], and Masoumeh Safkhani[i2]

[1]Faculty of Electrical Engineering, Shahid Rajaee Teacher Training University, Tehran, Iran

[2]Faculty of Computer Engineering, Shahid Rajaee Teacher Training University, Tehran, Iran

*Corresponding Author' Information: NBagheri@srttu.edu

ARTICLE INFO

ARTICLE HISTORY:
Received 15 Jun 2014
Revised 24 July 2014
Accepted 12 August 2014

KEYWORDS:
RFID
Distance bounding protocol
Man-In-The-Middle (MITM)

ABSTRACT

In this paper, the security of a distance bounding protocol is analyzed which has been recently proposed by Jannati and Falahati (so-called JF). We prove that an adversary can recover key bits of JF protocol with probability of "1" while the complexity of attack is "2n" runs of protocol. In addition, we propose an improved protocol and prove that the improved protocol is resistant to mafia fraud attack, distance fraud attack and key recovery attack.

1. INTRODUCTION

Radio Frequency Identification (RFID) is a kind of technology that can be used in applications such as access control, electronic passports, public transportation, payment, ticketing etc.

Security and privacy are two most critical concerns of RFID technology. Authentication protocols and distance bounding protocols have been proposed in order to increase the security level and preserve the tag's privacy. Distance bounding protocols enable a verifier to establish an upper bound on the physical distance to an untrusted prover [1]. Some distance bounding protocols are proposed in recent years [2]-[10]. Various attacks have been proposed and considered in these distance bounding protocols. Some of the most commonly considered attacks are: impersonation fraud, distance fraud, mafia fraud, terrorist fraud, and distance hijacking attack. Mafia fraud and terrorist fraud are considered as relay attacks. Relay attacks occur when a legitimate reader thinks that it communicates with a legitimate tag which is supplanted by an adversary and legitimate tag thinks that it communicates with a legitimate reader which is supplanted by an adversary (Fig. 1). In the following, we briefly introduce each of these attacks:

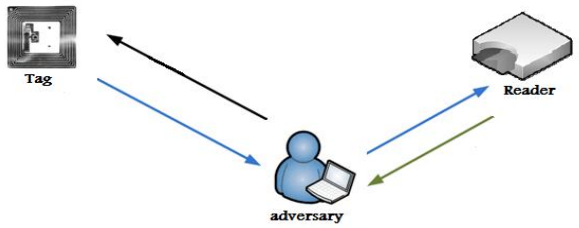

Figure 1: Relay attack

Impersonation fraud: In impersonation fraud, the adversary impersonates the legitimate tag or the legitimate reader.

Distance fraud: In distance fraud a dishonest prover claims that he is at a different distance than he really is.

Mafia fraud: In mafia fraud, both the reader and the tag are honest. However, the tag is outside the neighborhood. In this fraud, an adversary performs his attack using a Man-In-The-Middle (MITM) between the reader and the tag.

Terrorist fraud: In terrorist fraud, a dishonest tag is located outside the neighborhood helping an adversary perform his attack using a MITM between the reader and a dishonest tag [11].

Distance hijacking attack: In distance hijacking attack a dishonest prover exploits honest parties to convince the verifier that he is at the honest parties distance [12].

Hancke and Kuhn's protocol: In 2005, Hancke and Kuhn proposed a new distance bounding protocol (HK protocol) [4]. Their protocol consists of a single slow phase and a fast phase. As depicted in Fig. 2, in the slow phase the tag and the reader exchange nonces, both the reader and the tag compute a 2n-bit value H=h(K, NR, NT) which is split in two n-bit registers v_0 and v_1. In this protocol, the reader checks both the authentication and the distance in the fast phase, the reader sends challenge C_i and the tag replies $R_i=v_i^{C_i}$, where *i* is the *i*th bit of the register v^{Ci}. At last, the reader checks whether the received responses and Δt_s are valid.

Munilla and Peinado's protocol: In 2008, Munilla and Peinado [8] proposed a new distance bounding protocol (MP protocol) to improve the security level of Hancke and Kuhn's protocol. In their protocol, the challenges are divided into two categories, full challenge and void challenge. As depicted in Fig. 3, at first the tag and the reader exchange nonces, they both compute a 3n-bit sequence, $P||v0||v1$, using a pseudorandom function. In the fast bit exchange, if $P_i=1$ the reader sends a random challenge bit, where *i* is the *i*th bit of the register P. Upon reception of the challenge, the tag sends the corresponding response. The protocol ends with a message to verify that no adversary has been detected. However, the main disadvantage of their protocol is using three (physical) states which is difficult to implement.

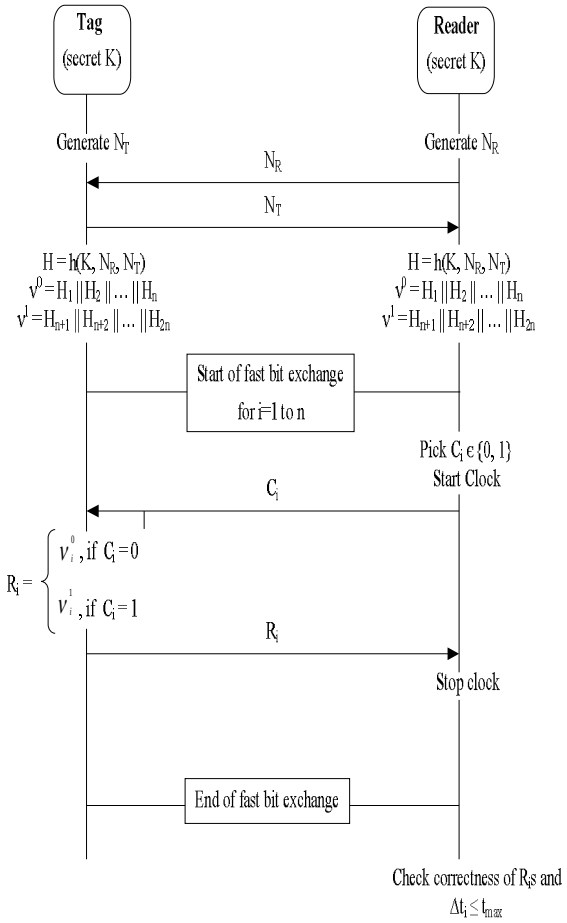

Figure 2: Hancke and Kuhn's protocol

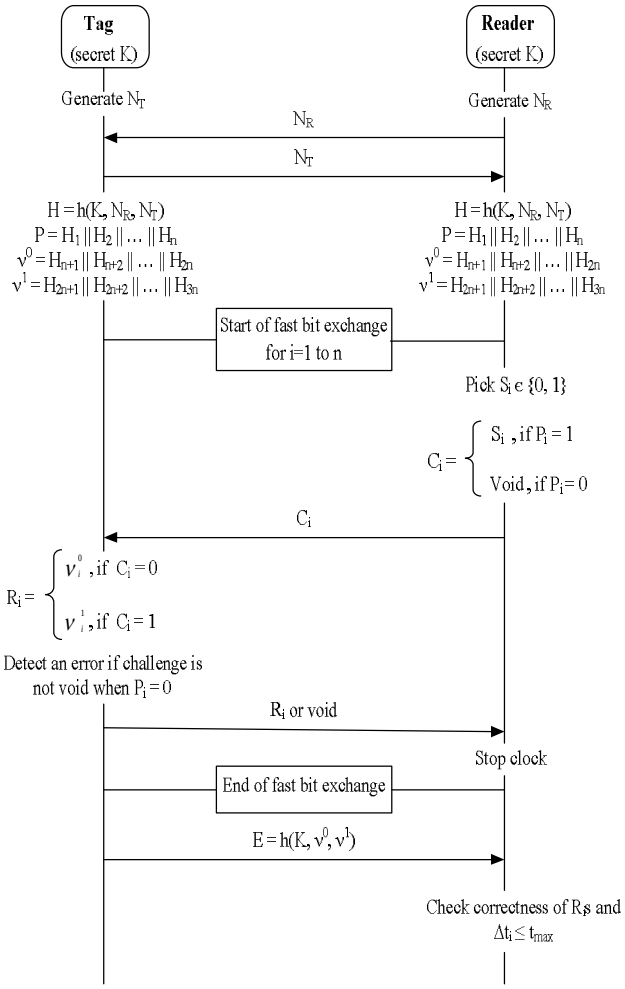

Figure 3: Munilla and Peinado's protocol

Kim and Avoine's protocol: Kim and Avoine in [13] proposed two distance bounding protocols, KA1 and KA2, based on binary mixed challenges. Compared to Munilla and Peinado's protocol [8], they do not use three physical states and confirmation message in their protocols which improves the efficiency of their protocols. In Kim and Avoine's protocol, the challenges from the reader to the tag in the fast-bit exchange are divided into two categories, the random challenges and the predefined challenges. In KA1 and KA2, at each round, the reader forwards only a predefined challenge bit or a random challenge bit to the tag and KA2 requires half the memory required by KA1 and increases the resistance against mafia fraud attack. For more details, the reader to the original work is referred.

Jannati and Falahati's protocol: To enhance the security level for KA1 and KA2, Jannati and Falahati proposed a new distance bounding protocol, called JF, which utilizes both predefined and random challenge bits at each round [14] and claimed that their protocol obtains the desirable attackers' success probabilities, with minimum system memory requirement and minimum number of rounds compared with other distance bounding protocols. However, we prove that JF protocol is actually insecure by presenting key recovery attack.

TABLE 1
COMPARISON OF THE MENTIONED DISTANCE BOUNDING PROTOCOLS

Protocol	Distance fraud	Mafia fraud	Terrorist fraud
HK	$\left(\frac{3}{4}\right)^n$ [15]	$\left(\frac{3}{4}\right)^n$ [16]	1 [16]
MP	$\left(\frac{3}{4}\right)^n$ [15]	$\left(\frac{3}{5}\right)^n$ [16]	1 [15]
KA	$\left(\frac{7}{8}\right)^n$ [15]	$\left(\frac{1}{2}\right)^n$ [16]	1 [15]
JF	$\left(\frac{3}{4}\right)^n$	1	1
Improved protocol (in this paper)	$\left(\frac{3}{4}\right)^n$	$\left(\frac{3}{4}\right)^n \times \left(\frac{1}{2}\right)^n + \left(\frac{1}{2}\right)^{n-1} \times (1-\left(\frac{3}{4}\right)^n)$	1

The success probabilities of distance fraud attack, mafia fraud attack and terrorist fraud attack in the mentioned protocols are compared in Table 1.

Paper Organization: The rest of the paper is organized by introducing the notations in section 2. We describe JF protocol in section 3. After that,

security analysis is expressed in section 4. Improved version of JF protocol is proposed in section 5. Security analysis of the improved protocol is presented in section 6. Finally, the conclusion is given in section 7.

2. NOTATIONS

We use the following notations to describe JF protocol, which have also been used in [14].

TABLE 2
NOTATION

Notation	Description
K	Secret key shared between the tag T and the reader R
$F(.)$	Public pseudorandom function
N_T	Random number generated by the tag
N_R	Random number generated by the reader
$\oplus$	Exclusive-OR operator (XOR)
$\|\|$	Concatenation operator

In addition, JF protocol [14] is parameterized by the bit length 2n of Q and the bit length n of D and a.

3. THE JF PROTOCOL

Recently Jannati and Falahati have proposed a new distance bounding protocol, called JF, based on mutual utilization of binary predefined and random challenges [14]. In this section we describe JF protocol as follows.

A. Detailed Description of JF Protocol

JF protocol, which is depicted in Fig. 4, runs as below:

Step 1 The reader selects a random number N_R and sends it to the tag.

Step 2 The tag selects a random number N_T and sends it to the reader.

Step 3 The reader and the tag compute $Q = F(K \,||\, N_R \,||\, N_T)$.

$$D=Q_1||Q_2||\ ...||Q_n \quad (1)$$

$$a=Q_{n+1}||Q_{n+2}||...||Q_{2n} \quad (2)$$

Step 4 The fast bit exchange is started. At each round i:

- The reader selects $W_i = D_i$ as a predefined challenge bit and selects a random bit C_i as a random challenge bit, then it sends W_i and C_i to the tag and starts a clock.
- Once the tag received W_i and C_i, it checks correctness of W_i. If $W_i = D_i$ the tag sends a_i to the reader when $C_i = 0$ and sends $a_i \oplus K_i$ when $C_i = 1$, otherwise the tag detects an error and sends random bits to all the next challenge bits sent by the reader.
- Once the reader received response bit r_i, the reader stops the clock and stores the delay time Δt_i.

Step 5 After completion of the fast bit exchange the reader checks correctness of r_i and Δt_i. If r_i is incorrect or $\Delta t_i > \Delta t_{max}$ the reader rejects the tag as invalid.

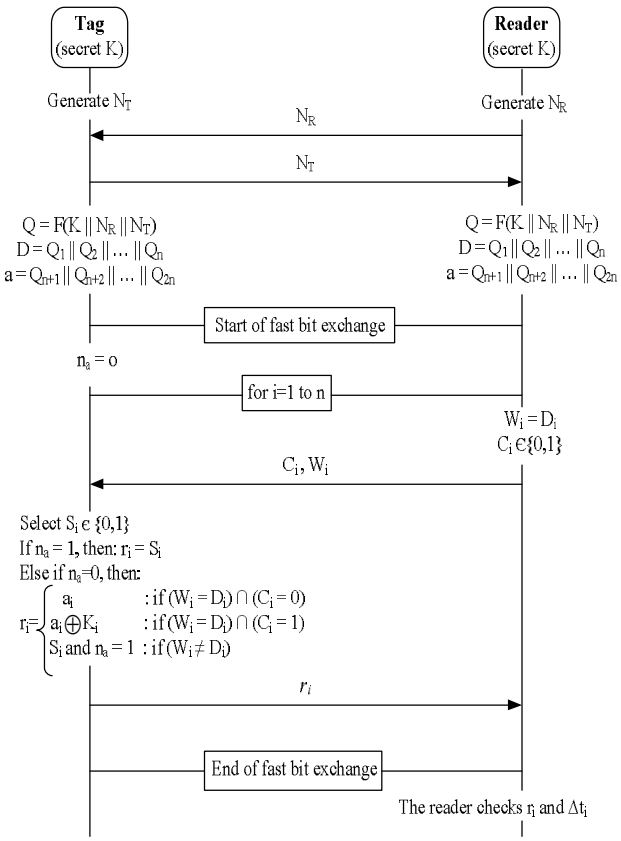

Figure 4: JF protocol

4. SECURITY ANALYSIS

In this section, we describe how JF protocol is vulnerable against key recovery attack.

A. Key recovery attack

In key recovery attack, the adversary would be able to retrieve key bits and given the secret key, any other attack would be possible to apply to the protocol. In this section, we describe the vulnerability of JF protocol against key recovery attack. In our attack the adversary, that is a man in the middle adversary, works as below (see Fig. 5).

1. The reader generates N_R and sends it to the tag.
2. The tag generates N_T and sends it to the reader.
3. Both the reader and the tag compute Q, D and a as follows:
   $Q = F(K \,||\, N_R \,||\, N_T)$
   $D=Q_1||Q_2||\ ...||Q_n$

$a=Q_{n+1}||Q_{n+2}||...||Q_{2n}$

4. The reader sends predefined challenge bit $W_i = D_i$ and a random bit C_i to the tag which is supplanted by the adversary.
5. In this step the adversary does as follows:
   - blocks C_i and W_i,
   - sends random bit r'_i as a response to the reader,
   - sends $\overline{C_i} = C_i \oplus 1$ and W_i to the tag.
6. According to the random challenge bit $\overline{C_i}$, the tag chooses $r_i=a_i$ if $\overline{C_i}=0$ and chooses $r_i=a_i \oplus K_i$ if $\overline{C_i} = 1$. Then, the tag sends it to the reader which is supplanted by the adversary.
7. The adversary does not block other challenge bits and allows the legitimate reader and the tag communicates with each other.

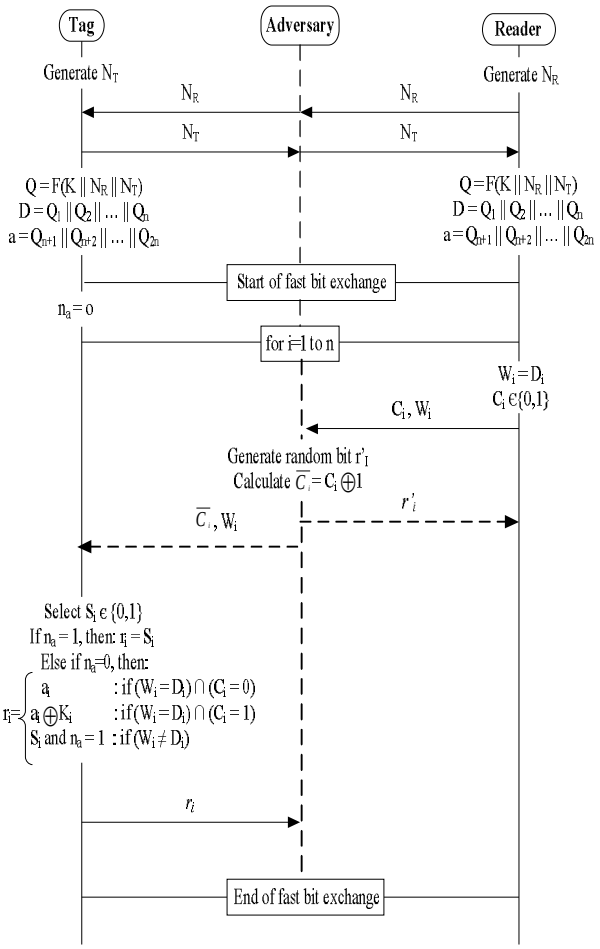

Figure 5: Our key recovery attack against JF protocol

If the reader rejects the adversary, the adversary understands that r'_i and corresponding response to the challenge bit C_i are not equal, therefore he obtains the value of $a_i \oplus K_i$ and a_i and if the reader accepts the adversary, the adversary understands that r'_i and corresponding response to the challenge bit C_i are equal and he obtains the value of $a_i \oplus K_i$ and a_i too. To obtain every key bit, the adversary needs two runs of protocol but they are not complete runs of protocol and the values of Q, D and a are the same in both of them.

As above mentioned, the adversary can obtain both a_i and $a_i \oplus K_i$ for each round; hence the adversary can make a simple calculation to find the ith bit of the key K. By repeating this strategy for i = 1,..., n, the adversary would be able to deduce the bits of the secret key K.

Hence, the adversary would be able to deduce the bits of the secret key K with probability of "1" and the complexity of "2n" runs of protocol.

We explain the key recovery attack with a numerical example (see Table 3). In the table 3, the reader, the tag and the adversary are denoted by R, T and A, respectively.

For example in highlighted row, the reader sends W_i and C_i = 1 to the tag. However, the adversary blocks this message. The adversary sends random bit r'_i = 1

to the reader as a response bit and sends W_i and $\overline{C_i}$= 0 to the tag.

TABLE 3
NUMERICAL EXAMPLE OF KEY RECOVERY ATTACK

C_i	a_i	K_i	$R \xrightarrow{C_i} A$	$A \xrightarrow{\overline{C_i}} T$	$A \xrightarrow{r'_i} R$	$T \xrightarrow{r_i} A$
0	0	0	0	1	0	0
0	0	1	0	1	1	1
0	1	0	0	1	0	1
0	1	1	0	1	1	0
1	0	0	1	0	0	0
1	0	1	1	0	1	0
1	1	0	1	0	0	1
1	1	1	1	0	1	1

According to $\overline{C_i}$ the tag sends $r_i = a_i = 0$ as a response bit to the adversary, for finding *i*th key bit the adversary just blocks W_i and C_i and does not interfere on other challenge bits. According to exchanged bits, the reader accepts the tag. Hence, the adversary can understand that $a_i \oplus K_i = 1$, he knows the value of $r_i = a_i = 0$. Therefore, the adversary can understand that $K_i = 1$.

5. IMPROVEMENT OF JF PROTOCOL

In this section, we introduce a modified version of JF protocol such that it withstands the presented attack; the proposed protocol is shown in Fig. 6. In this protocol we assume that $Q=F(K||N_R||N_T) = D||a||b$ such that:

- Q: 3-n bit sequence,
- D, a, b: n-bit sequence.

The revised protocol accomplishes as follows:

Step 1: The reader generates N_R and sends it to the tag.

Step 2: The tag generates N_T and sends it to the reader.

Step 3: Both the reader and the tag compute $Q=F(K||N_R||N_T) = D||a||b$ such that:

$D=Q_1||Q_2|| \ldots ||Q_n$

$a=Q_{n+1}||Q_{n+2}||\ldots||Q_{2n}$

$b= Q_{2n+1}||Q_{2n+2}||\ldots||Q_{3n}$

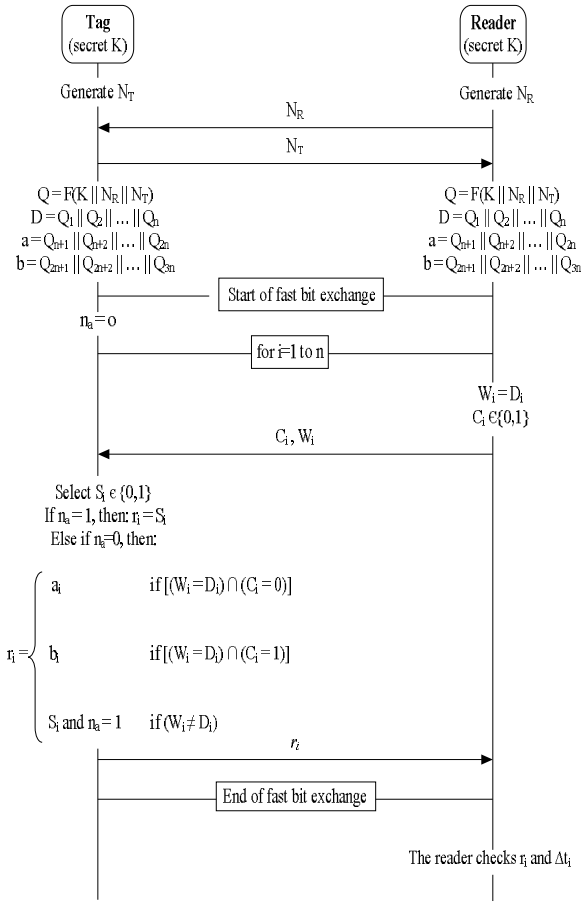

Figure 6: The proposed scheme

Step 4 : The fast bit exchange is started. At each round *i*:

- The reader selects $W_i = D_i$ as a predefined challenge bit and selects a random bit C_i as a random challenge bit, then it sends W_i and C_i to the tag and starts a clock.
- Upon reception of W_i and C_i, the tag checks correctness of W_i. If $W_i = D_i$ and $C_i = 0$, the tag sends back a_i to the reader as a response bit and else if $W_i = D_i$ and $C_i = 1$, the tag sends

back b_i to the reader as a response bit, otherwise if $W_i \neq D_i$ it detects an error and sends random bits to all the next challenge bits sent by the reader.

- Once the reader received the response bit r_i the reader stops the clock and stores the delay time Δt_i.

Step 5: At the end, the reader checks correctness of r_i and Δt_i. If r_i is incorrect or $\Delta t_i > \Delta t_{max}$ the reader rejects the tag as invalid.

6. Security Analysis of the Improved Protocol

The main idea in the improved protocol is prevention of data leaks. Hence, due to the weakness of an Exclusive-OR operation we don't use of it. Also the same data should not be used for challenges, so we were forced to use 3*n*-bit sequence *Q* and two *n*-bit sequences *a* and *b*.

Mafia Fraud Attack In this attack the adversary is a man in the middle adversary. He guesses two random bits W_i and C_i and queries the tag before it starts the fast phase with the reader. If $W_i$is correct according to the C_i the tag sends response bit r_i to the adversary, when the reader starts the fast phase the adversary supplants the tag, if W_i and C_i are guessed correctly he sends correct response, otherwise he must guess the response bit and sends it to the reader. Detailed calculations of the success probability of this attack against the improved protocol is similar to which is calculated in [14]. According to the calculations performed in [14], the success probability of this attack is:

$$P=\left(\frac{3}{4}\right)^n \times \left(\frac{1}{2}\right)^n + \left(\frac{1}{2}\right)^{n-1} \times \left(1-\left(\frac{3}{4}\right)^n\right) \quad (3)$$

Distance Fraud Attack In distance fraud attack, a dishonest tag sends its response bit before the dishonest tag receives the challenge bit. For performing distance fraud attack in the improved protocol, if a_i and b_i are the same the dishonest tag can sends correct response otherwise it must guess the response. Therefore the success probability of this attack is $\left(\frac{3}{4}\right)^n$.

Key Recovery Attack: In the improved protocol the key is not used directly or in a XOR operation, therefore the adversary cannot deduce the key from challenge bits or response bits. Therefore the improved protocol is resistant to key recovery attack.

7. Conclusion

In this paper, we have analyzed the security of a distance bounding protocol which has been recently proposed by Jannati and Falahati. We proved that an adversary can recover key bits in this protocol with probability of "1" and complexity of "2n" runs of protocol. Finally, we proposed an improved protocol and proved that the improved protocol provides suitable resistance against mafia fraud attack, distance fraud attack and key recovery attack.

References

[1] J.-P. Aumasson, A. Mitrokotsa, and P. Peris-Lopez, "A Note on a Privacy- Preserving Distance-Bounding Protocol," In S. Qing, W. Susilo, G. Wang, and D. Liu, editors, *ICICS*, *volume 7043 of Lecture Notes in Computer Science*, pp. 78-92. Springer, 2011.

[2] G. Avoine and A. Tchamkerten, "An Efficient Distance Bounding RFID Authentication Protocol: Balancing False-Acceptance Rate and Memory Requirement," In P. Samarati, M. Yung, F. Martinelli, and C. A. Ardagna, editors, *ISC*, volume 5735 of *Lecture Notes in Computer Science*, pp. 250-261. Springer, 2009.

[3] S. Brands and D. Chaum, "Distance-Bounding Protocols," In T. Helleseth, editor, *EUROCRYPT*, volume 765 of *Lecture Notes in Computer Science*, pp. 344-359. Springer, 1993.

[4] G. P. Hancke and M. G. Kuhn, "An RFID Distance Bounding Protocol," In SecureComm, pp. 67-73. *IEEE*, 2005.

[5] S. Kardas, M. S. Kiraz, M. A. Bingöl, and H. Demirci, "A Novel RFID Distance Bounding Protocol Based on Physically Unclonable Functions," In A. Juels and C. Paar, editors, *RFIDSec*, volume 7055 of *Lecture Notes in Computer Science*, pp. 78-93. Springer, 2011.

[6] C. H. Kim and G. Avoine, "RFID distance bounding protocol with mixed challenges to prevent relay attacks," *IACR Cryptology ePrint Archive*, 2009:310, 2009.

[7] A. Mitrokotsa, C. Onete, and S. Vaudenay, "Mafia fraud attack against the R Distance-Bounding Protocol," In *RFID-TA*, pp. 74-79. IEEE, 2012.

[8] J. Munilla and A. Peinado, "Distance bounding protocols for RFID enhanced by using void-challenges and analysis in noisy channels," *Wireless Communications and Mobile Computing*, 8(9), pp.1227-1232, 2008.

[9] P. Peris-Lopez, A. Orfila, E. Palomar, and J. C. Hernandez-Castro, "A secure distance-based RFID identification protocol with an off-line backend database," *Personal and Ubiquitous Computing*, 16(3), pp.351-365, 2012.

[10] A. Yang, Y. Zhuang, and D. S. Wong, "An Efficient Single-Slow-Phase Mutually Authenticated RFID Distance Bounding Protocol with Tag Privacy," In T. W. Chim and T. H. Yuen, editors, *ICICS*, volume 7618 of *Lecture Notes in Computer Science*, pp. 285-292. Springer, 2012.

[11] G. Avoine, M. A. Bingöl, S. Kardas, C. Lauradoux, and B. Martin, "A framework for analyzing RFID distance bounding protocols," *Journal of Computer Security*, 19(2), pp.289-317, 2011.

[12] C. J. F. Cremers, K. B. Rasmussen, and S. Capkun, "Distance Hijacking Attacks on Distance Bounding Protocols," In *NDSS*. The Internet Society, 2012.

[13] C. H. Kim and G. Avoine, "RFID Distance Bounding Protocols with Mixed Challenges," *IEEE Transactions on Wireless Communications*, 10(5), pp.1618-1626, 2011.

[14] H. Jannati and A. Falahati, "Mutual Implementation of Predefined and Random Challenges over RFID Distance Bounding Protocol," 9th*International ISC Conference on Information Security and Cryptology*, 2012

[15] A. Ö. Gürel, A. Arslan, and M. Akgün, "Non-uniform Stepping Approach to RFID Distance Bounding Problem," In J. García-Alfaro, G. Navarro- Arribas, A. R. Cavalli, and J. Leneutre, editors, *DPM/SETOP*, volume 6514 of *Lecture Notes in Computer Science*, pp. 64-78. Springer, 2010.

[16] C. H. Kim, G. Avoine, F. Koeune, F.-X. Standaert, and O. Pereira,"The Swiss-Knife RFID Distance Bounding Protocol," In P. J. Lee and J. H. Cheon, editors, *ICISC*, volume 5461 of *Lecture Notes in Computer Science*, pp. 98-115. Springer, 2008.

BIOGRAPHIES

Fatemeh Baghernejad received her B.Sc. degree in Electronic Engineering from Faculty of Electrical Engineering of Dr. Shariaty Teacher Training University and her M.Sc. degree in Electronic Engineering from Faculty of Electrical Engineering, Shahid Rajaee Teacher Training University (SRTTU), Tehran, Iran, in 2011 and 2013, respectively. Her research interests include RFID security and CDMA.

Nasour Bagheri is a lecturer at Electrical Engineering Faculty of Shahid Rajaee Teacher Training University, Tehran, Iran. He is the author of over 50 articles in information security and cryptology. Homepage of the author is available at: http://n-bagheri.srttu.ir.

Masoumeh Safkhani received her Ph.D. degree from Electrical Engineering department of Iran University of Science and Technology (IUST). She is the author of 10 articles in cryptology. Her current research interest includes RFID security.