An Efficient Single-Slow-Phase Mutually Authenticated RFID Distance Bounding Protocol with Tag Privacy

Anjia Yang, Yunhui Zhuang, and Duncan S. Wong

Department of Computer Science,
City University of Hong Kong, Hong Kong, China
{ayang3,yhzhuang2}@student.cityu.edu.hk, duncan@cityu.edu.hk

Abstract. Among the RFID distance bounding protocols in the literature, besides defending against various attacks such as impersonation, distance fraud, Mafia attack, terrorist attack, and distance hijacking, some also support mutual authentication and tag privacy protection. Due to the requirements of being lightweight, low-cost, and efficient, it is the common objective to design new RFID distance bounding protocols which require fewer message flows and less complex cryptographic operations, while maintaining or enhancing the security and privacy of the protocols. In this paper, we propose a new RFID distance bounding protocol which achieves mutual authentication, supports the untraceability of the tags, and resists all the attacks above by having only one slow transmission phase, and is more efficient and energy-saving when compared with other protocols' two slow phases. The new protocol requires the tag to evaluate a PRF function for two times only, rather than three times as in one of the most efficient mutually authenticated RFID distance bounding protocols currently available, for example, the Swiss-Knife protocol.

Keywords: RFID, Distance Bounding, Privacy, Mutual Authentication.

1 Introduction

RFID (Radio Frequency Identification) is a technology that has been widely used in our daily life. An RFID tag is a simple chip equipped with an antenna, which allows the tag to communicate with a reader. The reader needs to determine whether the tag is valid and within a legitimate distance which we call *a neighbor area* by using a distance bounding protocol. As an identification method, better than the bar code, an RFID chip makes it possible to identify non-line-of-sight objects using wireless communication technology. Nowadays, RFID chips have already been deployed in many big supermarkets such as Wal-Mart. They have also been increasingly applied to track goods or even animals and so forth. In addition, another important application of RFID is proximity-based authentication, such as the student card for entering a library, the payWave -enabled visa card for payment, and the electronic passport.

T.W. Chim and T.H. Yuen (Eds.): ICICS 2012, LNCS 7618, pp. 285–292, 2012.
© Springer-Verlag Berlin Heidelberg 2012

There have been a handful of RFID distance bounding protocols proposed recently [1–7]. Among them, various attacks have been proposed and considered in their security analysis. Five of the most commonly considered attacks are: Impersonation fraud [1], Distance fraud [1], Mafia fraud [9], Terrorist fraud [9], and Distance hijacking attack [10]. In this paper, we only consider the distance hijacking attacks in single-protocol environment defined in [10]. To mitigate Mafia fraud attack, Brands and Chaum [1] presented the first distance bounding protocol in 1993. In 2005, Hancke and Kuhn proposed a simple and efficient distance bounding protocol [2], but it cannot prevent terrorist fraud attacks. Subsequently there're some other protocols proposed. However, they either cannot prevent terrorist attacks [3–5, 7], or are not quite efficient [6]. In 2011, Avoine et al. prevented a general method to defeat terrorist frauds [8]. They made a conclusion that at least a $(3, 3)$ threshold secret-sharing scheme should be used to resist terrorist frauds. Our distance bounding protocol is based on this paper.

Besides the security issue, another critical concern of RFID technology is privacy. We mainly consider the tag's privacy which suffers from traceability, which means that the adversary can distinguish whether it's the target tag that is communicating with a reader. Actually, in order to preserve the tag's privacy, many methods have been proposed [6, 11–15]. One of the most well-known methods is hash-chain based schemes [13–15], however, all of them suffer from the *de-synchronization attack* by Juels and Weis [16]. What's more, only in [6] the tag's privacy issue is considered in a distance bounding protocol.

Finally, the efficiency of a distance bounding protocol is an important concern of RFID technology, due to the tag's limited computation and storage capacities. Among the previous distance bounding protocols, only [6] has the expected properties at the same time: resistant to terrorist fraud attacks, protecting the tag's privacy, achieving mutual authentication. Nevertheless, there're four slow transmission flows in this protocol and the tag needs to compute the time-consuming pseudo-random function(PRF) for three times; what's more, the reader exhaustively searches for the tag's ID from its local database at each protocol run, which again reduces the efficiency. Therefore we need to design a secure efficient distance bounding protocol which protects the tag's privacy as well.

Contribution. We propose a new efficient RFID distance bounding protocol which achieves mutual authentication and resists all the current attacks with only single slow phase. Our protocol also preserves tag's privacy with untraceability efficiently, which can prevent the de-synchronization attack as well.

Table 1 shows a comparison between our scheme and the previous schemes. From the second column to the fourth column, we show the adversary's success probability of launching Mafia frauds, terrorist frauds and distance hijacking attacks respectively to these selected protocols. The fifth column indicates whether those protocols protect the tag's privacy, and the sixth column gives the reader's cost of providing the service of tag's privacy protection. The next column represents whether these protocols support mutual authentication. In the eighth

column, we give the cost of the tag needed in each protocol, where we measure the cost as the number of computation of pseudo-random function (PRF), hash function ($Hash$), commitment ($com.$), symmetric key encryption ($Enc.$) and signature ($sig.$). The last column displays how many flows needed in slow phases in each protocol. Taking the limited space into account, we don't put the impersonation frauds or distance frauds in Table 1 since these two attacks are easy to be prevented and all of the protocols are resistant to them.

Table 1. Comparison of distance bounding protocols

	Maf.	Terr.	Hij.	Pri.	Pri.-cost of reader	MA	Comp. of tag	No. of flows in slow phase
BC [1]	$(\frac{1}{2})^n$	NO	1	NO	-	NO	$1com.+1sig.$	2
HK [2]	$(\frac{3}{4})^n$	NO	$(\frac{1}{2})^n$	NO	-	NO	$1PRF$	2
MP [3]	$(\frac{1}{2})^n$	NO	$(\frac{1}{2})^n$	NO	-	NO	$2Hash$	3
KA [7]	$\approx(\frac{1}{2})^n$	NO	$(\frac{1}{2})^n$	NO	-	NO	$1PRF$	2
Reid et al. [5]	$(\frac{3}{4})^n$	$(\frac{3}{4})^n$	$(\frac{1}{2})^n$	NO	-	NO	$1PRF+1Enc.$	2
Swiss-knife [6]	$(\frac{1}{2})^n$	$(\frac{3}{4})^n$	$(\frac{1}{2})^n$	YES	$O(n)PRF$	YES	$3PRF$	4
Our scheme	$(\frac{3}{4})^n$	$(\frac{3}{4})^n/(\frac{7}{8})^n$ †	$(\frac{1}{2})^n$	YES	$O(1)PRF$	YES	$2PRF$	2

† If the malicious tag $\mathcal{T}$ gives one of $\{r_1,r_2,r_3\}$ to the adversary $\mathcal{A}$, the success probability of $\mathcal{A}$ is $(\frac{3}{4})^n$; if $\mathcal{T}$ gives two of $\{r_1,r_2,r_3\}$ to $\mathcal{A}$, the success probability of $\mathcal{A}$ is $(\frac{7}{8})^n$.

Outline. We organize the remainder of this paper as follows. In Section 2, we describe our new scheme. In Section 3, we analyze the security and privacy of our protocol. Finally, we give the conclusion of this paper.

2 Our Protocol

As shown in Fig. 1, the tag has an identifier ID, an alias identifier ID' which is actually used during the protocol run and is computed through a PRF function h initialized with $ID' := h(ID, s)$, and a secret key s that is viewed as a vector $(s_1, \ldots, s_n)$, where n is a security parameter. The reader has a database, consisting of pairs of (s, ID, TID, TID'), where TID and TID' are used as the index to search the tag's ID, and they are initialized with $TID := h(ID, s)$ and $TID' := h(h(ID, s), s)$ respectively. Both of the tag and the reader can compute a PRF and a (3, 3) threshold scheme. There are three phases in our scheme as in Fig. 1. We give the description of the protocol as follows.

Initialization Phase

(1) The tag generates a random nonce N_A of length n and transmits N_A along with ID' to the reader.
(2) The reader searches in the database using the index TID or TID'. If $ID' = TID'$, the reader will update its database as shown in Fig. 1. If success, it generates a random nonce N_B of length n and computes a $3n$-bit sequence

$\{H\}^{3n} = f(s, N_A, N_B, ID')$ and splits it into three shares: r_1, r_2 and v respectively. Furthermore, it obtains the value of r_3 by computing $r_3 = r_1 \oplus r_2 \oplus s$. Meantime, the reader sends N_B and v' to the tag. We denote by v' the value of v received by the tag.

(3) The tag receives N_B and v'. It also computes the same sequence H and splits it into three shares like the reader. After calculating v, it compares the values of v and v'. If they are same, the protocol continues. Otherwise the protocol fails. We point out that this step can detect the failure of the protocol at an early time, which makes the protocol more efficient.

Interactive Phase. The interactive phase is also called the fast bit exchange phase or the critical time phase, which consists of n rounds in total.

(1) The reader picks a random bit c_i, starts the clock and sends c_i to the tag.
(2) The tag makes corresponding response r_i according to both c_i and v_i and transmits r_i' to the reader. We denote r_i' by the value received by the reader.

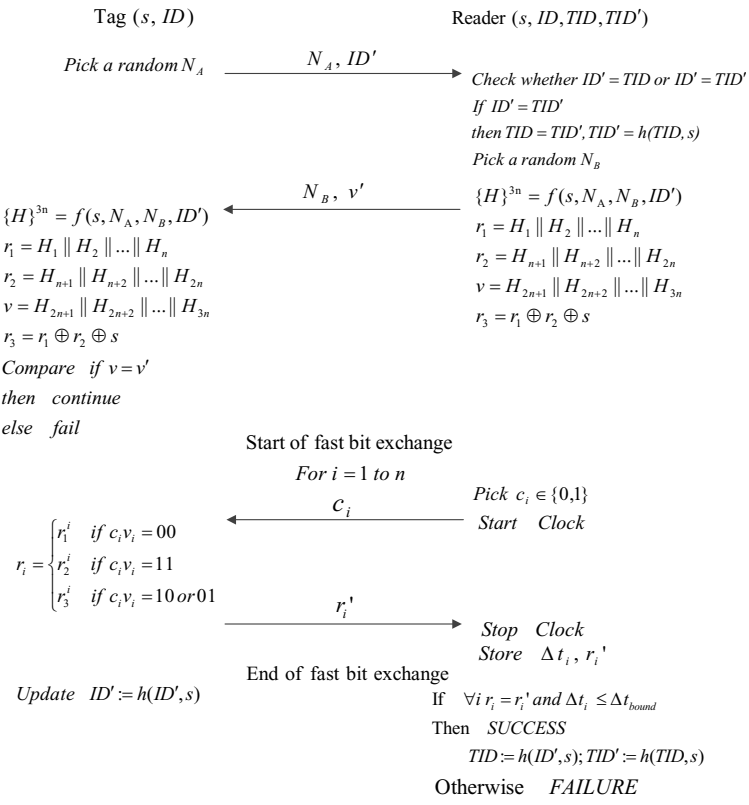

Fig. 1. Our distance bounding protocol

(3) Upon receiving r'_i, the reader stops the clock, stores r'_i and the measured RTT Δt_i.
(4) Repeat the first three steps for n times in total.

Check Result Phase. The tag updates its ID' by $ID' := h(ID', s)$. The reader checks the received answers $(r'_1, r'_2, ...r'_n)$ and the delay time $(\Delta t_1, \Delta t_2, ...\Delta t_n)$. If every response r'_i matches the expected value r_i and every delay time $\Delta t_i \leq \Delta t_{bound}$ where Δt_{bound} is a given bound which indicates the tag is within the neighbor area, then the protocol succeeds and the reader also updates its database. Otherwise, the protocol fails.

Remark 1. There is no fault-tolerance here, for we only consider noiseless communication. As to the noisy communication, we can use two numbers T_1, T_2, denoted as the number of positions for which $r_i \neq r'_i$ and $\Delta t_i > \Delta t_{bound}$ respectively. If $T_1 + T_2 > T$ where T is a given threshold, then the protocol fails.

3 Security Analysis

We consider an active polynomial time adversary $\mathcal{A}$ who has the ability to eavesdrop, modify, inject and remove messages exchanged between all parties in the system. Furthermore, we consider a strong $\mathcal{A}$ which can also observe the result of a protocol run and even be able to observe the result of each round of a protocol run. We assume that genuine tags will not give their secret keys to attackers.

N_A and N_B are both randomly chosen so that they are used like a one-time pad. Actually, the presence of N_A and N_B are used to prevent replay attacks and also allow the reader to authenticate the tag in the result check phase, for only the tag and the reader know the shared secret key s, N_A and N_B simultaneously. Since H is an output of the PRF function f, the adversary can't recover s by decoding H even if she/he can obtain part of H, that is v, which is used to allow the tag to authenticate the reader. We will give a detailed analysis on the security and privacy of our scheme as follows.

Impersonation Fraud Resistance. Without s, the adversary can generate the correct r_i with probability negligibly different from $\frac{1}{2}$ since f is a PRF. Thus the best the adversary can do is to guess the response randomly with success probability $\frac{1}{2}$ when receiving a challenge in each round of the fast bit exchange phase. Overall, the adversary's success probability is $(\frac{1}{2})^n$, which is negligible.

Distance Fraud Resistance. In this attack, the adversary can generate r_1, r_2, r_3 and v and thus can get through the first slow phase easily. However, during the fast bit exchange phase, without knowing c_i, the adversary still needs to guess the corresponding answer r_i from $\{r_1, r_2, r_3\}$ and sends it to the reader in advance in order to make the delay time measured by the reader within the bound. Therefore, at each round the success probability is $\frac{1}{2}(\frac{1}{2} \times 1 + \frac{1}{2} \times \frac{1}{2}) = \frac{3}{4}$ and after n rounds, the adversary's success probability is $(\frac{3}{4})^n$, which is negligible.

Mafia Fraud Resistance. Again, without s, the adversary cannot compute the response strings r_1, r_2 and r_3 before the fast bit exchange phase. When carrying

out a Mafia fraud attack, the attacker has two choices: using pre-ask strategy or not. Using the pre-ask strategy, the adversary slightly accelerates the clock signal provided to the tag and transmits an anticipated challenge bit c_i' before the reader sends its challenge bit c_i. In half of all cases, the adversary will guess the right challenge bit, that is $c_i' = c_i$, and thus can get the correct value r_i from the tag in advance. Afterwards, the adversary runs the fast phase with the authentic reader. In the other half of all cases, the adversary can simply reply with a guessed response bit when interacting with the reader, which will be correct with the probability of $\frac{1}{2}$. Therefore, in each round, the success probability of the adversary is $\frac{1}{2} \times 1 + \frac{1}{2} \times \frac{1}{2} = \frac{3}{4}$. If the attacker doesn't use the pre-ask strategy, she/he will have to guess the challenge bit c_i with a success probability of $\frac{1}{2}$ before receiving it when executing the fast bit exchange phase with the reader. Thus we consider the adversary's success probability in each round as the maximum one, that is $\frac{3}{4}$. To sum up, the adversary can get through the whole protocol with probability of $(\frac{3}{4})^n$, which is negligible.

Terrorist Fraud Resistance. It's trivial to see that the malicious tag cannot give all the r_1, r_2 and r_3 to the attacker, for the attacker will be able to recover the secret key s easily by $s = r_1 \oplus r_2 \oplus r_3$. Since v is sent as plaintext in our protocol, the malicious tag can give it to the adversary directly. Hence we will consider the following two scenarios.

First, we consider the situation that the malicious tag gives v and one of r_1, r_2 and r_3 to the attacker. Without loss of generality, we assume that it gives her/him r_1 and v. When receiving a challenge bit c_i, the adversary knows both c_i and v_i, and also knows the answer when $c_i v_i = 00$. However, she/he doesn't know the value of r_2^i or r_3^i, which means when $c_i v_i \neq 00$, she/he has to guess the value of the answer. Suppose we use $P_{k_i=j}$ to denote the probability of $k_i = j$, then the probability that the adversary replies correctly is $P_{c_i=0} \cdot (P_{v_i=0} \cdot P_{[v_i=0|c_i=0]} + P_{v_i=1} \cdot P_{[v_i=1|c_i=0]}) + P_{c_i=1} \cdot (P_{v_i=0} \cdot P_{[v_i=0|c_i=1]} + P_{v_i=1} \cdot P_{[v_i=1|c_i=1]}) = \frac{1}{2}\left(\frac{1}{2} \times 1 + \frac{1}{2} \times \frac{1}{2}\right) + \frac{1}{2}\left(\frac{1}{2} \times \frac{1}{2} + \frac{1}{2} \times \frac{1}{2}\right) = \frac{5}{8}$. Similarly, we can calculate the adversary's success probability when she/he gets r_2 or r_3 respectively. It is interesting to point out that when giving the attacker r_3, she/he will guess the right answer with probability of $\frac{3}{4}$. That is, the adversary can get though the protocol with a maximal probability of $(\frac{3}{4})^n$, which is negligible.

Then, we consider the situation that the malicious tag gives the adversary two of r_1, r_2 and r_3. With a similar analysis, we can compute the adversary's maximal success probability is $(\frac{7}{8})^n$. One interesting thing is that once passing the protocol, the adversary will know she/he has replied with all the correct responses and furthermore she/he can recover part of the secret key s according to $s_i = r_1^i \oplus r_2^i \oplus r_3^i$. For example, if we assume that the malicious tag gives the adversary $\{v, r_1, r_2\}$, and the protocol run succeeds, then the adversary understands that she/he has guessed all the correct responses when the actual response should be r_3^i. As is shown in the protocol, there's an average probability of $\frac{1}{2}$ that the response is r_3^i. Hence after one successful protocol run the adversary can obtain $\lfloor \frac{1}{2} n \rfloor$ bits of s. We point out that the probability of recovering secret key is a conditional probability, where the condition is the adversary has passed the

distance bounding protocol successfully. If the adversary's success probability is negligible, then the probability of recovering the secret key is also negligible.

Distance Hijacking Attack Resistance. We only consider the situation of distance hijacking attacks in single-protocol environment. To launch a distance hijacking attack in our protocol, the adversary first impersonates a reader to communicate with an exploited tag. The tag will send the preliminary information to the reader, that is N_A and ID. Upon receiving N_A and ID, the attacker acting as a fraudulent tag sends N_A and her/his own identity ID' to the authentic reader. Finally, the exploited tag will execute the fast bit exchange phase with the reader. However, the exploited tag computes H with $\{H\}^{3n} = f(s, N_A, N_B, ID)$, while the authentic reader computes H with $\{H\}^{3n} = f(s', N_A, N_B, ID')$, where s' is the shared secret key between the attacker and the authentic reader, and the authentic reader searches s' out in the database according to the attacker's identifier ID'. Therefore, the success probability of the adversary is $(\frac{1}{2})^n$, when the values of pseudo-random string H computed by the reader and the tag are same with different inputs.

Privacy. As we have mentioned above, ID' is initialized with $ID' := h(ID, s)$, where ID is the tag's identity. Upon communicating with the reader, the tag transmits ID' instead of ID to the reader. What's more, the tag will update the value of ID' at the end of fast bit exchange phase(see Fig. 1). Since h is a PRF, if the adversary can tell if two sessions have the same tag involved, it means that it can distinguish two different outputs generated by a PRF with non-negligible probability, which is impossible. Hence our protocol supplies the property of untraceability for tags.

Remark 2. Our protocol prevents the de-synchronization attack by using both TID and TID'. When launching a de-synchronization attack, the adversary either prevents the tag updating ID', for example by modifying v' sent from the reader to the tag, or prevents the reader updating TID and TID' in the check result phase, for example by tampering the value of response bits sent from the tag to the reader so that the protocol will fail. It's not difficult to see no matter the adversary stops the tag or the reader from updating its data, the value of ID' sent by the tag will always be equal to either TID or TID'. That is, the tag is always synchronized with the reader.

4 Conclusion

In this paper, we proposed a new efficient mutually authenticated distance bounding protocol that is resistant to all the current attacks. Our protocol also protects privacy of tags through an anonymous method, which achieves untraceability and prevents de-synchronization attacks. To our best knowledge, it is the most efficient method to provide the untraceability for the tag in RFID distance bounding protocols.

References

1. Brands, S., Chaum, D.: Distance Bounding Protocols. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 344–359. Springer, Heidelberg (1994)
2. Hancke, G., Kuhn, M.: An RFID Distance Bounding Protocol. In: 1st International Conference on Security and Privacy for Emerging Areas in Communications Networks, pp. 67–73. IEEE Computer Society (2005)
3. Munilla, J., Peinado, A.: Distance bounding protocols for RFID enhanced by using void-challenges and analysis in noisy channels. In: Wireless Communications and Mobile Computing, vol. 8, pp. 1227–1232. Wiley Interscience, Hoboken (2008)
4. Tu, Y.J., Piramuthu, S.: RFID Distance Bounding Protocols. In: 1st International EURASIP Workshop in RFID Technology, Vienna, Austria (2007)
5. Reid, J., Nieto, J.G., Tang, T., Senadji, B.: Detecting Relay Attacks with Timing-Based Protocols. In: Proc. of the 2nd ACM Symposium on Information, Computer, and Communications Security - ASIACCS 2007, pp. 204–213. ACM, New York (2007)
6. Kim, C.H., Avoine, G., Koeune, F., Standaert, F.X., Pereira, O.: The Swiss-Knife RFID Distance Bounding Protocol. In: Lee, P.J., Cheon, J.H. (eds.) ICISC 2008. LNCS, vol. 5461, pp. 98–115. Springer, Heidelberg (2009)
7. Kim, C.H., Avoine, G.: RFID Distance Bounding Protocols with Mixed Challenges. IEEE Trans. on Wireless Communications 10(5), 1618–1626 (2011)
8. Avoine, G., Lauradoux, C., Marin, B.: How Secret-sharing can Defeat Terrorist Fraud. In: Proc. of the 4th ACM Conference on Wireless Network Security - WiSec 2011, pp. 145–156 (2011)
9. Desmedt, Y.: Major security problems with the 'unforgeable' (Feige)- Fiat- Shamir proofs of identify and how to overcome them. In: SecuriCom 1988, 6th Worldwide Congress on Computer and Communications Security and Protection, SEDEP Paris, pp. 15–17 (1988)
10. Cremers, C., Rasmussen, K.B., Capkun, S.: Distance Hijacking Attacks on Distance Bounding Protocols. In: IEEE Symposium on Security and Privacy- S&P 2012, pp. 113–127. IEEE Computer Society, Los Alamitos (2012)
11. Juels, A., Rivest, R.L., Szydlo, M.: The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. In: 8th ACM Conference on Computer and Communications Security -CCS 2003, pp. 103–111. ACM (2003)
12. Weis, S.A., Sarma, S.E., Rivest, R.L., Engels, D.W.: Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In: International Conference on Security in Pervasive Computing -SPC 2003, pp. 201–212 (2003)
13. Ohkubo, M., Suzuki, K., Kinoshita, S.: Cryptographic Approach to "Privacy-Friendly" Tags. In: RFID Privacy Workshop (2003)
14. Henrici, D., Muller, P.: Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers. In: 2nd IEEE Annual Conference on Pervasive Computing and Communications Workshops (2004)
15. Paise, R., Vaudenay, S.: Mutual Authentication in RFID: Security and Privacy. In: ACM Symposium on Information, Computer and Communications Security – ASSIACCS 2008, pp. 292–299. ACM (2008)
16. Juels, A., Weis, S.A.: Defining strong privacy for RFID. ACM Trans. on Information and System Security 13(1) (2009)