

A Practical RFID Grouping Authentication Protocol in Multiple-Tag Arrangement with Adequate Security Assurance

Jian Shen* ** *** ****, Haowen Tan****, Yongjun Ren****, Qi Liu****, Baowei Wang****

*Jiangsu Engineering Center of Network Monitoring, Nanjing University of Information Science & Technology, China

**Jiangsu Technology & Engineering Center of Meteorological Sensor Network, Nanjing University of Information Science & Technology, China

*** Jiangsu Collaborative Innovation Center on Atmospheric Environment and Equipment Technology, Nanjing University of Information Science & Technology, China

**** School of Computer & Software, Nanjing University of Information Science & Technology, China

s_shenjian@126.com, tan_halloween@foxmail.com, renyj100@126.com, qrankl@163.com, wbw.first@163.com

Abstract—Radio Frequency Identification (RFID) is considered to be an authentication technology of great potential. Due to the bright future of low-cost RFID tags in practical situations, the authentication towards multiple tags and tag groups has become the research hotspot. However, there are many concerns about the security risks and privacy issues in lightweight RFID authentication scenarios. Many researches achievements have been made focusing on the existence of single tag in one object, while the arrangement that multiple tags attached to one object is out of consideration. In this paper, we propose a practical RFID grouping authentication protocol in multiple-tag arrangement with adequate security assurance. In our assumption, one object to be authenticated is attached with a group of RFID tags. The feedback towards various cases of the RFID tags is timely provided, which is necessary in practical situations. Additionally, the probable position and status of the object can be ascertained

with a number of tags combined with the object. Moreover, the protocol is proved to offer enough security assurances and have resistance to various attacks under the security analysis. The regular operation of RFID system will not be severely damaged by the incidents occurred during the authentication process.

Keywords—RFID, lightweight, grouping authentication, multiple tag, security.

I. INTRODUCTION

RFID technology does not require line-of-sight contact in the communication process, which is superior to the barcodes. The basic structure of RFID system is composed of three parts: the reader, the BPS and the RFID tags. The reader can contact with more than one RFID tags and acquires related information from the tags. Consequently, the evidence that one or more RFID tags are verified at the same time is generated after several communication passes. Note here that the RFID tag cannot directly contact with the BPS. Instead, the reader performs as the bridge between the tag and the BPS. As a result, the reader is assumed to have enough computation power and storage. As a matter of fact, the communication channel between the reader and the tag is not secure. The transmitted information is vulnerable to eavesdropping as well as other kinds of attacks. For example, the RFID tag releases radio signals to the reader through the wireless channel. Thus the location of the RFID tag can be acquired by the malicious reader from eavesdropping only with small expenses. The tracing towards the tag can be possible in this occasion.

The BPS, regarded as the database containing important information, also plays the role of verifier which decides the validity of the generated evidence received from the reader. Thus the BPS is considered to be trustworthy and reliable during the entire authentication procedure. Actually the BPS is assumed to have full authority of the entire RFID system.

The RFID tag, which can be divided into three varieties: active tag, passive tag and semi-passive tag, is the most concerned RFID device that is vulnerable to security risks. Thanks to the recent technology development, the cost of RFID tags

Manuscript received date is April 9, 2015. This work is supported by the research fund from Nanjing University of Information Science and Technology under Grant No. S8113003001, the National Science Foundation of China under Grant No. 61300237, No. 61232016, No. U1405254, and No. 61402234, the National Basic Research Program 973 under Grant No. 2011CB311808, the research fund from Jiangsu Technology & Engineering Center of Meteorological Sensor Network in NUIST under Grant No. KDXG1301, the research fund from Jiangsu Engineering Center of Network Monitoring in NUIST under Grant No. KJR1302, the 2013 Nanjing Project of Science and Technology Activities for Returning from Overseas, the CICAET fund, and the PAPD fund.

J. Shen (corresponding author, phone: 86-25-5873-1400, fax: 86-25-5873-1323, e-mail: s_shenjian@126.com) is with Jiangsu Engineering Center of Network Monitoring, Jiangsu Technology & Engineering Center of Meteorological Sensor Network, Jiangsu Collaborative Innovation Center on Atmospheric Environment and Equipment Technology, School of Computer & Software, Nanjing University of Information Science & Technology, Nanjing, 210044, China.

H. Tan is with School of Computer & Software, Nanjing University of Information Science & Technology, Nanjing, 210044, China, phone: 86-151-5181-3390, fax: 86-25-5873-1323, e-mail: tan_halloween@foxmail.com.

Y. Ren is with School of Computer & Software, Nanjing University of Information Science & Technology, Nanjing, 210044, China, phone: 86-187-6187-0612, fax: 86-25-5873-1323, e-mail: renyj100@126.com.

Q. Liu is with School of Computer & Software, Nanjing University of Information Science & Technology, Nanjing, 210044, China, phone: 86-185-5171-9567, fax: 86-25-5873-1323, e-mail: qrankl@163.com.

B. Wang is with School of Computer & Software, Nanjing University of Information Science & Technology, Nanjing, 210044, China, phone: 86-139-1292-6757, fax: 86-25-5873-1323, e-mail: wbw.first@163.com.

has been dropped to a relatively low level. At the same time, these low-cost tags have large probability to suffer from security attack and privacy leakage due to resource limitation in terms of computation, communication and memory. We assure that these security and privacy problems can be solved by adopting impeccable authentication protocols and secure strategies. Note here that the RFID tag referred in this paper is low-cost passive tag which gets power from the interaction with the reader.

As a matter of fact, many RFID authentication schemes have been presented in order to improve the security level and guarantee the regular operations of the RFID system. The researches focusing on grouping authentication of multiple tags and tag groups have become the primary tendency in RFID authentication field, while the security problems along with the privacy leakages remain barriers of practical use [1], [2].

As assumed in most of the protocols devoted to grouping authentication, single RFID tag is attached on one object. However, in the situation that the object is of big size, the RFID tag on a part of the object may not be within the communication range. Consequently, the object with other parts of it staying in the communication range cannot be identified. In other words, the detection probability of the object with single tag is not large in practical situations. The BPS cannot ascertain whether all parts of the object with large size is precisely in the supposed position so that the controlling power of the entire RFID system towards the objects is not adequate [3], [4], [5].

To meet the practical requirements, one object can be attached with multiple RFID tags in different parts. In this assumption, if all the tags on the object are identified, it is obvious that the object is well arranged in the right position. Note that the RFID tags on the object guarantee the integration of the object and increase the detection probability as well [6], [7], [8]. Even in the harsh situations where some tags on the same object may be compromised or missed, the RFID system can still identify the existence of the object with the rest of the tags. On the other hand, the precise location of the object can be arranged by identifying the tags, which indicates the new attempt for locating on low-cost RFID tags.

In this paper we propose a practical RFID grouping authentication protocol in multiple-tag arrangement with adequate security assurance. In our assumption, all the tags on one object are considered as one tag group. The BPS takes control of behaviors of all these tags and reader. The object can be placed in the accurate spot with small deviation according to our design, which is practical and creative in real applications.

This paper is organized as follows. In the following section, the related original protocols about grouping authentication are presented in brief. The detailed scheme of the proposed protocol is shown in Section III. Next is the security analysis of the protocol in Section IV. Then we conclude all this paper in Section V.

II. RELATED WORK

Many RFID grouping authentication protocols have been presented with the purpose of offering enough secure require-

ments and preventing possible attacks to the RFID system. J. Saito and K. Sakurai [9] proposed the original grouping proof using time stamp in order to alleviate the weakness of the protocol presented by Ari Juels [10], [11]. Generally speaking, it is the relatively earlier protocol in multiple tags authentication. In this protocol, the reader derives the time stamp from database and submits it to all the RFID tags. The tags of the protocol are divided into two parts: the ordinary product tags and pallet tag. However, the entire RFID system in this protocol does not provide enough resistance to replay attack.

The chaining proof protocol is proposed in 2007 [12]. The main idea of this protocol is to combine all the tags intended to be authenticated together and form a chain with purpose of integrity preserving. However, the identities of the tags under authentication are transmitted in plaintext, which makes the tags vulnerable to illegal tracing. In addition, this protocol also depends on certain reading order of the tags, which is not convenient for practical situation.

Reading order independent grouping proof [13] is proposed in order to meet the practical requirements. In the assumption, the reader has enough computational power and the pallet tag can be merged into the reader. As a matter of fact, this protocol is applicable for special use in supply chain. The structures that the reader is bound to the pallet tag offers new research topic.

H. Liu *et al.* proposed grouping-proofs-based authentication protocol [14] for distributed RFID systems. In this protocol, all the tags are divided into several groups and are sequentially checked. This protocol provides strong protection on privacy and is resistant to various attacks. However, the checking sequence of the tags is required to be arranged in advance.

A RFID authentication protocol for multiple tag arrangement [15] is proposed by S. Dhal and I. S. Gupta in 2014. In the assumption multiple numbers of RFID tags are attached in one object in order to increase the detection probability. Based on it, we propose our grouping authentication protocol in this paper, which is relatively available in the practical situations.

III. PROPOSED AUTHENTICATION SCHEME

In this section we describe our RFID grouping authentication protocol which is available for the scenario that multiple tags are attached to one object with large size. Note that these tags in one object are classified into the same tag group. In our assumption, the sequence numbers of the tags in the group are delivered to the reader after mutual authentication with each other. We would like to emphasize that the real identifiers of the RFID tags are not used in our protocol, preventing the RFID system from tracing problem. The reader communicates with each tag according to their sequence number of the group and gathers all the secret information to generate the proof. The authentication process completes when all the tags in the group are verified successfully, which means that the tags are in the right position so that the object is safe and well arranged. In addition, unusual situations are under consideration [15], [16], [17]. For example, when some of the tags are broken or damaged, the reader can generate the proof containing other tags' secrets. Consequently, the BPS acquires the information

that some specific tags need to be repaired but the object remains safe, which is practical in real applications.

A. Problem Definition

We assume the occasion that a set of objects with large size need to be verified where each of the objects is attached with more than one RFID tags in its different parts. Note that the tags combined with the same object are considered as one tag group. The object is arranged to be successfully authenticated after all the tags of the tag group are fully verified, which guarantees that the object is precisely in the scheduled location. The proposed RFID authentication scheme should meet most of the security requirements without affecting its efficiency or increasing the cost. Moreover, the BPS should be available with the feedback of all the tags of the group. The disabled tag should be notified to the BPS for convenience of the facilities maintenance. Hence the invalid tag can be removed from the RFID authentication system in time.

B. Protocol Design

The protocol we propose in this paper is divided into four phases for better description. In the initialization phase, the RFID tags are initiated with group identifiers along with the sequence numbers as soon as being attached to the object. The number of the tags in the group g is assumed to be n . The reader acquires n tags' identities and combines them with the received random numbers from the BPS in the tag acquisition phase. The proof of group g is generated in the main authentication phase, which links the entire tag group. In the verification phase, the proof is delivered to the BPS. It is necessary to emphasize that the communication between the BPS and the reader and through secure channel, while that between the reader and the RFID tags are not safe and vulnerable to various attacks. The notations used in our proposed protocol are provided in Table I.

TABLE I
NOTATIONS

Notation	Description
BPS	Backend processing system
R_m	The m -th reader
g	The g -th tag group
T_i	The i -th tag of tag group g
n	Number of tags in tag group g
r_{R_m}	Pseudo-random number generated by the BPS
ID_{R_m}	Identifier of reader R_m
GID_g	Group identifier of tag group g
r_{T_i}	Pseudo-random number generated by the tag T_i
e_i	Sequence number of the tag T_i
S_g	Group secret of the tag group g
$r_{e_1}, \dots, r_{e_i}, \dots, r_{e_n}$	Pseudo-random numbers generated by the BPS
S_{T_i}	Secret of the tag T_i
Z_{GID_g}	Generated proof of the tag group g

1) *Initialization Phase*: In this phase, the initialization of the RFID tags is conducted. As we describe above, one object is assumed to be combined with several tags in order to ensure that this object is totally in the right position. The group information as well as the sequence number e_i is input in

the memory of RFID tag. Note that the tag referred to here can be the reusable tag, which means that the RFID tag can be attached to another object after the authentication process is completed. In this assumption, the tag will be through the initialization phase again and equipped with new secrets.

2) *Tag Acquisition Phase*: In this phase, the tags responding to the reader are registered after verification. According to our design, it is not necessary for the RFID system to collect all the n tags. The RFID system allows authentication towards more than one tag. We assume there are j tags in group that are successfully registered. When in extreme situations, only one tag which passes the authentication of the RFID system can prove that the object is not missing. But whether the object is precisely in the right position remains a question.

The detailed steps of this phase are as follows:

- The BPS generates a pseudo-random number r_{R_m} for the reader R_m . Then the BPS chooses the tag group to be authenticated and delivers $(ID_{R_m}, GID_g, r_{R_m})$ to the reader R_m through secure channel.
- The reader R_m computes $M_g = (GID_g \oplus ID_{R_m}) + (S_g \vee r_{R_m})$ and broadcasts (ID_{R_m}, M_g, r_{R_m}) to all the tags.
- The tag T_i of group g checks the validity of the received M_g and generates its own pseudo-random number r_{T_i} . Then T_i computes $N_{T_i} = [M_g - (GID_g \oplus ID_{R_m})] \vee r_{T_i}$ and $Q_{T_i} = e_i \oplus (S_g \vee r_{T_i})$. Next the tag T_i responds $(N_{T_i}, Q_{T_i}, r_{T_i})$ to the reader R_m .
- After receiving the information form the tag, the reader R_m checks validity of the acquired N_{T_i} and derives e_i from Q_{T_i} . After all the n tags have been collected or the timer has timed out, the reader sends $(ID_{R_m}, GID_g, e_1, \dots, e_j)$ to the BPS in the secure way.
- The BPS compares the received information with data in the database and replies to the reader with $(ID_{R_m}, GID_g, r_{e_1}, \dots, r_{e_j})$, where $r_{e_1}, \dots, r_{e_j}$ denote the pseudo-random numbers generated for each tag separately. The reader stores all this in its memory for the authentication in the next phase.

The brief description of this phase is shown in Fig. 1.

3) *Main Authentication Phase*: As the important section of the entire authentication process, this phase focuses on gathering the secrets of each tag and combining them following their sequence numbers e_i . Instead of using the tag's identifier, we compute $TempID_{T_i}$ as the temporary identifier during the communication between the reader and the tags, which shows enough resistance to the tracing problem towards the RFID tags. In the authentication process, the reader will not terminate the authentication process when the requested tag does not give the respond. Instead, the reader will skip to the next tag after the timer times up. The entire RFID system will not be interfered by abnormal tags or tag groups, which makes it more efficient.

The detailed steps of this phase are as follows:

- The reader R_m computes $r'_{T_1} = r_{T_1} \oplus r_{e_1}$ and $TempID_{T_1} = (GID_g \oplus e_1) \vee (r'_{T_1} \oplus ID_{R_m})$ and delivers $(Q_{T_1}, TempID_{T_1}, First, r_{e_1})$ to the first tag in group g .
- The first tag T_1 checks the validity of the received $TempID_{T_1}$ from the reader and computes $Z_{GID_g} =$

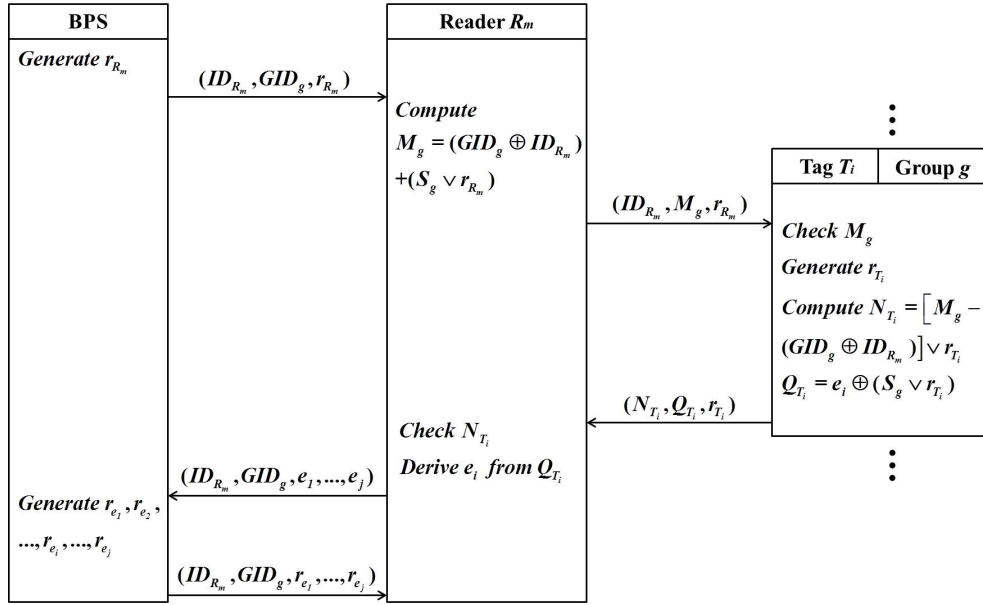


Fig. 1. Tag acquisition phase of the proposed protocol

$TempID_{T_1} \vee (r_{e_1} + S_{T_1})$ and $C_{T_1} = (e_1 \oplus r'_{T_1}) \vee N_{T_1}$. Then $(TempID_{T_1}, C_{T_1}, Z_{GID_g})$ is replied to the reader.

- The reader checks the validity of C_{T_1} and sends $(Q_{T_2}, TempID_{T_2}, Z_{GID_g}, r_{e_2})$ to the next tag of the group.
- The tag T_2 computes $Z_{GID_g} = [TempID_{T_2} \vee (r_{e_2} + S_{T_2})] \oplus Z_{GID_g}$ and $C_{T_2} = (e_2 \oplus r'_{T_2}) \vee N_{T_2}$. Note that Z_{GID_g} is generated with the value from the previous tag T_1 .
- The process continues to operate in this way and finally the reader acquires private secret information of all the activated legal tags.

The brief description of this phase is shown in Fig. 2.

4) *Verification Phase*: In this phase, the reader sends the generated proof Z_{GID_g} as well as the sequence numbers of all the legal tags to the BPS through secure channel. When all the tags in group g pass the authentication, it is certain that the object is in the right place. However, if only some of the tags are successfully authenticated, we can still guarantee that the object is here, while it is not totally in the right place. In addition, the BPS can be aware of the identities of the disabled tags, which is convenient for facilities maintenance without checking all the tags.

The brief description of this phase is shown in Fig. 3.

IV. SECURITY ANALYSIS

In this section, we analyze the security properties of our protocol in order to prove that our protocol is reliable. The proposed protocol is resistant to various kinds of attacks. The RFID system has large potential in the practical situations because it is convenient for the system to deal with different kinds of occasions. Moreover, only simple computations are required for the RFID tag, which is appropriate for market promotion of low-cost passive tags. In addition, the key information of the tag is preserved in every communication session, showing strong privacy protection to the tags. In addition, the

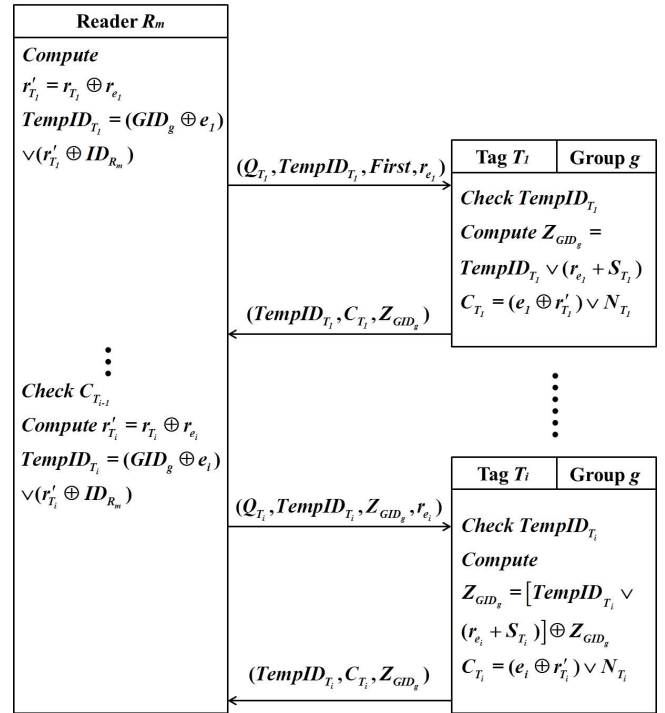


Fig. 2. Main authentication phase of the proposed protocol

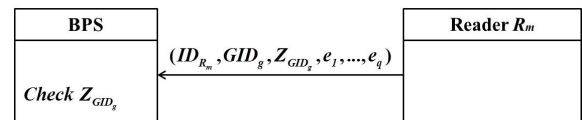


Fig. 3. Verification phase of the proposed protocol

proposed protocol is resistant to the tracing problem towards the specific RFID tags. The BPS takes control of all the authentication processes and can monitor the changes of the entire system, which improves the security and is available for practical use.

A. Replay Attack

In our protocol, the pseudo-random number generator is in use with the purpose of preventing the replay attack. As we describe above, in the tag acquisition phase, the random numbers r_{R_m} and r_{e_j} are all generated by the BPS and delivered to the reader through secure channel. In this situation, the BPS takes full control of the key generation. As for communication between the reader and the RFID tags, the tag itself generates the random number in the tag acquisition phase of every session. Thus the reuse of the previous messages cannot pass the verification of both the tag and the reader. As a result, the replay attack is prevented.

B. Eavesdropping

The malicious reader may try to get the secret information through eavesdropping during the communication process, which is the most common way for the adversary to damage the RFID system. In our scheme, the identifiers of the tags as well as the secret keys are all under encryption. We apply temporary identifier $TempID_{T_i}$ to the communication between the tag and reader so that it is not easy for the adversary to acquire key information of the specific tag through eavesdropping. The transmitted messages don't directly reveal the identifier of the tag so that the detected information is unreadable for the adversary. Moreover, the BPS takes control of the generation of all the random numbers. Consequently, these random numbers are necessary ingredients of the final generated proof, which ensures the variability. As a result, the entire RFID authentication system in our protocol is resistant to eavesdropping.

C. Physical Attack

In our design of this protocol, we assume that the adversary is able to destroy the tags physically and get all the secret information of the destroyed tag. The physical attack is always possible if the adversary can get access to the RFID tag physically. In this situation the detailed information stored in the memory of the tag is not safe anymore. The adversary can get full authority of the RFID tag and acquire the secret information. In RFID authentication field, physical attack is inevitable so that we have to take it into our security consideration. Our purpose is to ensure that the entire RFID system will not be compromised because of the acquired information from the tag. In some occasions, the adversary may even manage to clone the tag and use it to cheat the RFID system. However in our protocol, one object is attached with a group of RFID tags. The object can be authenticated with several disabled tags in the group. In order to interrupt the authentication process, the adversary has to damage all the tags in the group, which is difficult and worthless. As the

important facility of the entire RFID system, the reader and the BPS are assumed to be well protected in safe place [1], [10], [18]. As a result, physical attacks towards the reader and the BPS are not taken into consideration in this paper. As a matter of fact, we attach significance to the security requirements of the RFID tag more than the reader and the BPS.

D. Man-In-The-Middle Attack

Our protocol is resistant to man-in-the-middle attack. As we describe above, in our protocol, the adversary cannot collect the ID or secret key of the tag. In the main authentication phase, we assume the situation that the message $(TempID_{T_i}, C_{T_i}, Z_{GID_g})$ sent by the RFID tag is blocked by the adversary. The adversary cannot get the real ID and sequence number of the RFID tag. The reader will skip to the next tag after the timer times out, and the object can still be recognized without the message of the blocked tag. In conclusion, the man-in-the-middle attack is prevented [15], [19], [20].

E. Tracing attack

In the RFID authentication area, tracing attack towards the RFID tag, especially the low-cost passive tag, remains big threat to both the RFID system and the users of the RFID tags. Tracing attack can be classified into two kinds: tracing attack during the session and tracing attack between two successful sessions. On the one hand, in order to prevent tracing attack during one session, the delivered messages between the reader and the tags are all under encryption. The use of temporary identifier provides strong protection through tracing during the session. On the other hand, with the use of random number r'_{T_i} , the temporary identifier of the tag is changed after every successful authentication session. Thus it is difficult for the adversary to trace the specific tag through the relevance between two successful authentication sessions. As a result, tracing attack between two successful sessions is still impossible.

F. De-Synchronization Attack

In the de-synchronization attack, an adversary disturbs the interactions between a tag and a reader by intercepting or blocking the messages. In our protocol, the real ID of the tag is not applied in the authentication process. Instead, temporary identifiers are used in our protocol and these identifiers are available for one session. As a result, it is not necessary for the low-cost RFID tags to update their secrets in every session. In addition, the RFID tags are relatively independent of each other. The privacy information stored in one tag is not relevant to that of the others. The compromising through single tag will not affect the entire group and the RFID system. In this occasion, if one or more tags are blocked for several times, the tags can also contact with the reader. In a word, the RFID tags in the group will not suffer from de-synchronization attack according to our design [15], [21], [22].

G. Forward Security

In our protocol, if the adversary obtains the secret information of the RFID tag in the present session, the secure information of the previous sessions will not be leaked to the adversary. The temporary identifier in every session is generated and valid only in the present session, which means that the secret information is not related to the previous session. The secret information as well as the identifier of the RFID tag will be initialized at the beginning of every authentication session. The adversary cannot acquire essential messages of the previous sessions from the compromised tag since the information is only used for one session. In a word, the forward security property is provided in the proposed protocol.

Comparison of security assurance: We have compared the proposed protocol with some existing RFID authentication protocols. The result of the comparison is given in Table II below. The possible attacks are specified using the symbols *a*, *b*, *c*, etc. The meanings of the symbols are written under the table.

TABLE II
COMPARISON RESULT

	<i>a</i>	<i>b</i>	<i>c</i>	<i>d</i>	<i>e</i>	<i>f</i>	<i>g</i>
Grouping proof [9]	<i>N</i>	<i>P</i>	<i>N</i>	<i>N</i>	<i>N</i>	<i>P</i>	<i>N</i>
Chaining proof protocol [12]	<i>Y</i>	<i>P</i>	<i>N</i>	<i>P</i>	<i>N</i>	<i>N</i>	<i>P</i>
GUPA [14]	<i>Y</i>	<i>Y</i>	<i>N</i>	<i>Y</i>	<i>Y</i>	<i>Y</i>	<i>P</i>
APCMA [15]	<i>Y</i>	<i>Y</i>	<i>N</i>	<i>Y</i>	<i>Y</i>	<i>Y</i>	<i>Y</i>
Our protocol	<i>Y</i>	<i>Y</i>	<i>Y</i>	<i>Y</i>	<i>Y</i>	<i>Y</i>	<i>Y</i>

a: Replay attack, *b*: Eavesdropping, *c*: Physical attack, *d*: Man-in-the-middle attack, *e*: Tracing attack, *f*: De-synchronization attack, *g*: Forward security, *Y*: Satisfy, *N*: Not satisfy, *P*: Partially satisfy

V. CONCLUSION

In the grouping authentication of RFID tags, the use of multiple tags in one object not only increases the detection probability, but also provides the chance for accurate positioning of the object, which satisfies the practical requirements. In this paper we propose a practical RFID grouping authentication protocol in multiple-tag arrangement with adequate security assurance. In our assumption, the entire authentication process is in the control of the BPS. The feedback towards various cases of the authentication process is also provided. Moreover, with multiple tags combined with the object, the accurate position of the object can be arranged. The RFID system in our protocol shows enough resistance to various attacks and security risks. We are working to improve our protocol in order to make it more efficient and practical in the future work.

REFERENCES

- [1] A. Juels, "Rfid security and privacy: a research survey," *Selected Areas in Communications, IEEE Journal on*, vol. 24, no. 2, pp. 381–394, Feb 2006.
- [2] —, "Yoking-proofs for rfid tags," in *Pervasive Computing and Communications Workshops, 2004. Proceedings of the Second IEEE Annual Conference on*, March 2004, pp. 138–143.
- [3] J. Ha, J. Ha, S. Moon, and C. Boyd, "Lrmap: lightweight and resynchronous mutual authentication protocol for rfid system," in *Ubiquitous Convergence Technology*. Springer, 2007, pp. 80–89.
- [4] B. Gu, V. Sheng, K. Tay, W. Romano, and S. Li, "Incremental support vector learning for ordinal regression," *Neural Networks and Learning Systems, IEEE Transactions on*, vol. 26, no. 7, pp. 1403–1416, July 2015.
- [5] J. Shen, S. Moh, and I. Chung, "A priority routing protocol based on location and moving direction in delay tolerant networks," *IEICE TRANSACTIONS on Information and Systems*, vol. 93, no. 10, pp. 2763–2775, 2010.
- [6] H.-Y. Chien and S.-B. Liu, "Tree-based rfid yoking proof," in *Networks Security, Wireless Communications and Trusted Computing, 2009. NSWCTC '09. International Conference on*, vol. 1, April 2009, pp. 550–553.
- [7] L. Bolotnyy and G. Robins, "Generalized yoking-proofs for a group of rfid tags," in *Mobile and Ubiquitous Systems: Networking Services, 2006 Third Annual International Conference on*, July 2006, pp. 1–4.
- [8] J. Li, X. Li, B. Yang, and X. Sun, "Segmentation-based image copy-move forgery detection scheme," *Information Forensics and Security, IEEE Transactions on*, vol. 10, no. 3, pp. 507–518, March 2015.
- [9] J. Saito and K. Sakurai, "Grouping proof for rfid tags," in *Advanced Information Networking and Applications, 2005. AINA 2005. 19th International Conference on*, vol. 2, March 2005, pp. 621–624 vol.2.
- [10] S. Piramuthu, "On existence proofs for multiple rfid tags," in *Pervasive Services, 2006 ACS/IEEE International Conference on*, June 2006, pp. 317–320.
- [11] D.-Z. Sun and J.-D. Zhong, "A hash-based rfid security protocol for strong privacy protection," *Consumer Electronics, IEEE Transactions on*, vol. 58, no. 4, pp. 1246–1252, November 2012.
- [12] C.-C. Lin, Y.-C. Lai, J. Tygar, C.-K. Yang, and C.-L. Chiang, "Coexistence proof using chain of timestamps for multiple rfid tags," in *Advances in Web and Network Technologies, and Information Management*. Springer, 2007, pp. 634–643.
- [13] Y. Lien, X. Leng, K. Mayes, and J.-H. Chiu, "Reading order independent grouping proof for rfid tags," in *Intelligence and Security Informatics, 2008. ISI 2008. IEEE International Conference on*, June 2008, pp. 128–136.
- [14] H. Liu, H. Ning, Y. Zhang, D. He, Q. Xiong, and L. Yang, "Grouping-proofs-based authentication protocol for distributed rfid systems," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 24, no. 7, pp. 1321–1330, July 2013.
- [15] S. Dhal and I. Gupta, "A new authentication protocol for rfid communication in multi-tag arrangement," in *Computing for Sustainable Global Development (INDIACom), 2014 International Conference on*, March 2014, pp. 668–673.
- [16] J. Shen, S. Moh, and I. Chung, "Comment: enhanced novel access control protocol over wireless sensor networks," *IEEE Transactions on Consumer Electronics*, vol. 56, no. 3, pp. 2019–2021, 2010.
- [17] J. Shen, H. Tan, J. Wang, J. Wang, and S. Lee, "A novel routing protocol providing good transmission reliability in underwater sensor networks," *Journal of Internet Technology*, vol. 16, no. 1, pp. 171–178, 2015.
- [18] J.-S. Cho, S.-S. Yeo, S. Hwang, S.-Y. Rhee, and S. K. Kim, "Enhanced yoking proof protocols for rfid tags and tag groups," in *Advanced Information Networking and Applications - Workshops, 2008. AINAW 2008. 22nd International Conference on*, March 2008, pp. 1591–1596.
- [19] J. Shen and I. Chung, "Buffer scheme optimization of epidemic routing in delay tolerant networks," *Journal of Communications and Networks*, vol. 16, no. 6, pp. 656–666, 2014.
- [20] X. Leng, Y. Lien, K. Mayes, K. Markantonakis, and J.-H. Chiu, "Select-response grouping proof for rfid tags," in *Intelligent Information and Database Systems, 2009. ACIIDS 2009. First Asian Conference on*, April 2009, pp. 73–77.
- [21] Z. Fu, X. Sun, Q. Liu, L. Zhou, and J. Shu, "Achieving efficient cloud search services: Multi-keyword ranked search over encrypted cloud data supporting parallel computing," *IEICE Transactions on Communications*, vol. E98-B, no. 1, pp. 190–200, 2015.
- [22] S. Sundaresan, R. Doss, and W. Zhou, "Rfid tags - grouping proof with forward security," in *RFID-Technologies and Applications (RFID-TA), 2013 IEEE International Conference on*, Sept 2013, pp. 1–6.

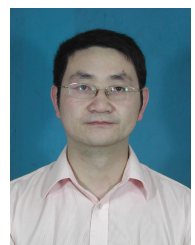


and ubiquitous sensor.

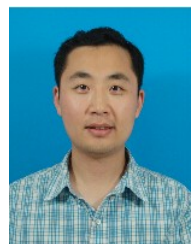
Jian Shen received the B.E. degree from Nanjing University of Information Science and Technology, Nanjing, China, in 2007 and the M.E. and Ph.D. degrees in Computer Science from Chosun University, Gwangju, Korea, in 2009 and 2012, respectively. Since late 2012, he has been a faculty member in the School of Computer and Software at Nanjing University of Information Science and Technology, Nanjing, China. His research interests include computer networking, security systems, mobile computing and networking, ad hoc networks and systems,



Haowen Tan received the B.E. degree in 2013 and is currently working toward the M.E. degree at Nanjing University of Information Science and Technology, Nanjing, China. He focuses on the security and privacy issues in radio frequency identification. His research interests include authentication protocol design, security formal modeling and analysis.



Yongjun Ren obtained the PhD degree in the computer and science department at the NanJing University of Aeronautics and Astronautics, China, in 2008. Now he is serving as a full time faculty in the NanJing University of Information science and Technology. His research interests include network security and applied cryptography.



Qi Liu received his BSc degree in Computer Science and Technology from Zhuzhou Institute of Technology, China in 2003, and his MSc and PhD in Data Telecommunications and Networks from the University of Salford, UK in 2006 and 2010. His research interests include context awareness, data communication in MANET and WSN, and smart grid. His recent research work focuses on intelligent agriculture and meteorological observation systems based on WSN.



Baowei Wang received his B.S. and Ph.D. degrees in Computer Science from Hunan University in 2005 and 2011, respectively. He is currently working as a lecturer in School of Computer and Software, Nanjing University of Information Science and Technology. His research interests include steganography, wireless networks and securing ad hoc networks.