25

Shared Tag RFID System for Multiple Application Objects

Ji-Yeon Kim[1], Jong-Jin Jung[1], Yun-Seok Chang[1] and Geun-Sik Jo[2]
[1] *Daejin University,*
[2] *Inha University*
Korea

1. Introduction

Recently, the information technology has evolved toward the ubiquitous environment accessible to the network everywhere and every time. The ubiquitous environment can provide easy access to the devices and make one's economical benefit also. The RFID system is an important core technology in ubiquitous environment. RFID system consists of contactless devices to communicate each other by radio frequency. It provides technologies of automatic object identification in invisible range, read/write function and adaptability against various circumstances. These advantages make RFID system to be applied in various fields and expect one of the big markets in the area of human life such as traffic card system, toll gate system, logistics, access control, etc. As RFID tags identify many different types of objects, it is going to increase the tags that have to be carry in individual life. But it is uneasy for a person to control many tags in a hand because traditional RFID systems have restriction that is one tag per each object and it is difficult to distinguish tags without some kind of effort. That is why a tag is used to store identifying information just for a single object in common RFID applications.

We propose a multiple objects tag structure which can be shared by many different applications. As a tag is used to identify only one type of object, it is expected to have many tags increasingly by people or things. If a tag can be shared by many RFID application objects, it will be more efficient to RFID users and will be helpful to the information integration as well as device sharing. So, we design a RFID tag structure which has many different identifiers. This tag can be used to access many different RFID applications.

We also propose an efficient authentication protocol adapted to the multiple objects tag structure. We consider robustness of the authentication protocol against various attacks in the proposed scheme. RFID system often makes serious violation of privacy and security caused by various attacks through the weak wireless interface. Eavesdropping, location tracking, spoofing, message losses or replay attack can threaten RFID components anywhere and anytime. To protect RFID system from these kinds of attacks, researchers have studied several schemes such as Faraday cage scheme (mCloak, 2003), blocker-tag scheme (Juels et al., 2003), hash lock scheme (Weis et al., 2003), randomized hash lock (Weis et al., 2003), hash chain (Ohkubo et al., 2003) and variable ID scheme (Saito & Sakurai, 2003), etc. However, these schemes have restrictions that each object is just corresponding to one tag. So, it is

Source: Development and Implementation of RFID Technology, Book edited by: Cristina TURCU,
ISBN 978-3-902613-54-7, pp. 554, February 2009, I-Tech, Vienna, Austria

difficult to distinguish tags without additional cost. That is why a tag is used to store identifying information just for a single object in common RFID applications. Therefore, we design an authentication protocol to support multiple objects based RFID system. Especially, we focus on efficiency of the authentication procedure by considering security levels of objects stored in a tag. Multiple objects-based tag can be shared by various kinds of RFID applications. Therefore, we classify various RFID application objects shared in a tag into different groups by security levels and apply the appropriate authentication procedure to the object according to its security level. In this way, our proposed RFID authentication protocol is designed to adjust to the multiple objects tag structure and to operate differently according to the security level.

The proposed authentication protocol can guarantee for various attacks. We evaluated the efficiency and stability for the proposed scheme compared with common single tag RFID scheme through various experimental results. As the result, the proposed scheme maintained stable operation through the test of error rates and made reasonable results of computation time for authentication procedure in spite of its high security.

2. Basic requirements

The standardization organizations for RFID tags are JTC1(Joint Technical Committee 1) by ISO/IEC and EPC Global by GS1(Global Standard 1). Tag identifier is a number to distinguish a tag from others in communication with readers. International standard observes the structure of the number (TTAR-06.0013, 2003). Permanent unique ID named as chip ID or tag ID is masked within a tag by tag producer according to the ISO/IEC 15963 standard. Another identifier is item ID which is used to distinguish the tagged objects. Tag memory has the item ID under user's decision and standardization on item ID is still under discussing. Therefore, we would like to use the item ID as the name of object ID on multiple objects access. Fig. 1 shows the typical example of the multiple item IDs in a same tag.

RFID systems often make serious violation of privacy and security caused by various attacks through the weakness of their wireless interface. Vulnerabilities to eavesdropping, location tracking, spoofing, message losses or replay attack can threaten RFID components. These attacks may affect individual privacy and information security. Therefore, efficient security mechanism against attacks must be considered when RFID applications are designed.

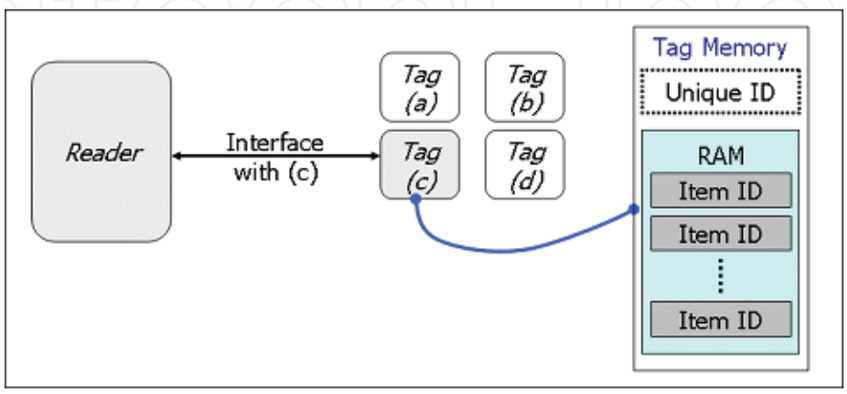

Fig. 1. Concept of tag identifier

Unprotected tags could be read by unauthorized readers. Attackers are used to eavesdrop on the general information stored in a tag such as serial number or code number from readers or tags though they can not understand the mean of the number. The attackers retransmit the eavesdropping data to the server and find out the critical information. With the eavesdropping data, the attackers also detect the tag location and analyze traffics. Therefore, RFID system has to be designed with data encryption and authentication protocol for preventing the attackers from replay of tapped data and location tracking. This reason makes the authentication protocol of RFID system may change the response of corresponding tag to the query of reader after each session. Spoofing is another type of attacks and it means that attacker joins in authentication protocol in the disguise of authorized tag or reader. To prevent the spoofing attack, RFID system has to control the authority of tag access in authentication protocol and must block the attacker' illegal information gathering. In addition to the above attacks, the attackers often intercept communications between reader and tag. This behavior causes loss of data which is important to authentication process. Therefore, the safe and reliable RFID systems should detect the interference coming from various kind of attack as many as it can.

3. Related works

Several papers have proposed the solution schemes against the attacks of privacy threat. There are two types of scheme: One is the physical scheme such as kill-command scheme, Faraday cage scheme and blocker-tag scheme. The other is the encryption scheme such as hash lock scheme, randomized hash lock, hash chain and variable ID scheme. In this study, we have focused on the encryption methods which are hot among researchers lately. The hash lock scheme is simple access control mechanism based on one-way hash function. It uses metaID to process authentication between reader and tag. The metaID is a temporary ID generated from one-way hash function with single key. Both the reader and tag store the metaID separately and match the key with metaID during the authentication process. A tag responds to all queries with only its metaID and decides whether the tag offers it or not. This scheme only requires a hash function on the tag and key management on the back-end database. So, it would be the best one of the cost-efficient solutions in the near future. Based on the difficulty of inverting a one-way function, this scheme also prevents unauthorized readers from reading tag contents. Maybe, spoofing attempts may be detected under this scheme but not prevented. The hash lock scheme can not prevent replay attack and location tracking either because the metaID has constant value. Randomized hash lock scheme improves the hash lock scheme and uses variable metaID. It can generate a different metaID with random number generator in every session. Therefore, a tag would not respond to queries from unauthorized readers. This scheme can prevent RFID tag from tracking but not replay attack and spoofing. Hash chain scheme uses two different hash functions to change the response message for reader. This scheme can prevent tag tracking and replay attack but still has weakness against spoofing. And actually, it is not practicable on account of their demand for circuit size and operation power because a tag has to keep two hash functions. Variable ID scheme changes tag ID by a random value in every session. For the replay attack, the scheme keeps transaction ID (TID) and last successful transaction (LST) in each session. However, this scheme may allow adversaries to track when LST was not updated on occurring message loss during the session.

4. RFID scheme for accessing multiple objects

4.1 Tag structure

Multiple objects tag is a new type of RFID tag structure that has multiple objects simultaneously for many RFID readers. As increasing the RFID system applies on individual life, people are expected to have several tags to identify the different types of objects. It causes serious problem on managing different tags in one's pocket and needs a new method to handle multiple objects in a simple way. But it is not easy to control many tags because traditional RFID systems can handle only one tag per each object. In ubiquitous computing environment, information integrating and device sharing have been increased on the various application areas and now we need an efficient solution to simplify the control and management method. Therefore, if there is a kind of method to share one tag for many RFID applications, it can be suitable for the ubiquitous computing environment in many ways. We propose a multiple objects tag structure which can be shared by different RFID applications. That is, the proposed tag is recognized by many different RFID readers. Fig. 2 shows the concept of multiple objects tag.

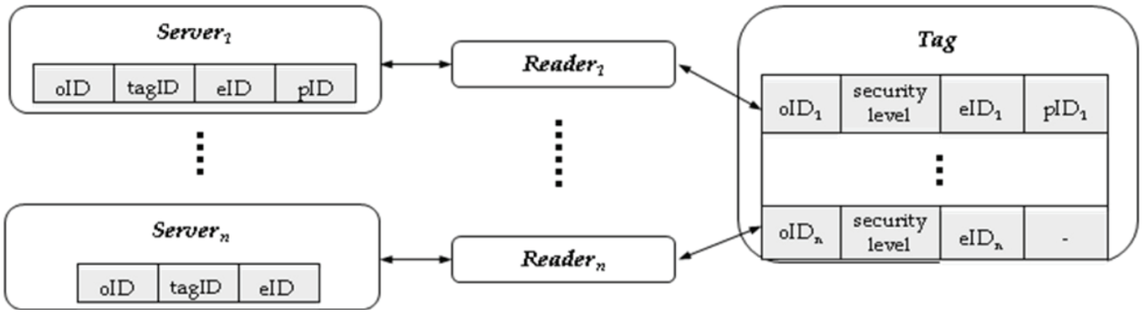

Fig. 2. Proposed multiple objects tag structure

As shown in Fig. 2, we need some types of IDs to design multiple objects tag. We define several types of data which are called tagID, oID, eID and pID. These IDs should be stored in tag memory and back-end database in server respectively as shown in Table 1.

RFID components	Stored data
Server	oID, tagID, eID, pID
Tag	oID, security level, eID, pID

Table 1. Data stored in server and tag

The meanings of each stored data are as follows:

- *tagID* is an unique identifier of a tag. It is used to distinguish tags each other in RFID system. In the proposed multiple objects tag, tagID is used as the key to create eID for distinguishing each distinct object.
- *oID*(object ID) is an identifier to distinguish different objects in multiple objects-based RFID system. In usual RFID systems, a key saved in a RFID tag is used to identify an object in a specific application. We define this key as oID. The multiple objects tag means that a single tag has more than an identifier for each distinct object with same *tagID*. This tag structure integrates different identifiers for different applications into data memory in a tag. The oID is stored in tag memory and server database

respectively. When a reader transmits a query to a specific tag, the query includes an oID.

- *eID*(encrypted ID) is an encrypted value to identify a certain object. In actual cases, multiple objects application causes security problem in multiple identifiers accesses and needs some appropriate method to tie up between identifier and object with security. To satisfying this specific need, we generate a new identifier with SEED encryption algorithm (IETF RFC 4269, 2003) using both tagID and oID. That is, the SEED algorithm takes both oID and tagID as input keys. The SEED is one of the famous block cipher algorithm developed by the KISA (Korean Information Security Agency) and broadly used throughout South Korean public and industry field. Since decryption of the SEED encryption value without input keys is very hard and expensive work, physical replication of tag is not worth for attacks. These characteristics of SEED provide a high level security and reliability in RFID systems. Therefore, we employ SEED algorithm on key encryption to identify a corresponding object. We call the encrypted identifier as *eID*. Different eIDs are generated by SEED algorithm using oIDs even if they have the same tagID. The numbers of eIDs are equal to the numbers of oIDs. These pairs of IDs are stored in a tag memory and back-end database respectively when the system is initialized. According to the object type, two or more eIDs can be stored in a tag. When a certain type of reader transmits query to a tag during wireless connection, the tag searches corresponding eID which is fit for the reader's object type.
- *pID*(partial ID) is a temporary version of eID which is generated by hash function embedded in a tag. It is a variant of eID made within a tag using random value transmitted from a reader. When a certain type of reader transmits query to a tag during wireless connection, the tag searches corresponding eID which is fit for the reader's object type. Then, the tag makes a variable ID with a random value which is transmitted from the reader when it queries to the tag. We call it *pID*. The pID is changed into different value at every session. The last successful pID is maintained in database and a tag. If the authentication process ends successfully, the tag and the server update the existing pID to prevent attack's threat. In the RFID system based on multiple objects tag, a tag or a server can perceive illegal adversaries' spoofing or replay attack by comparing its stored pID with the attacker's.

4.2 Authentication protocol using security level

To ensure the security and safety between tag and reader, we focused on encryption of IDs and authentication. As mentioned above, server and tags store the eIDs generated by SEED encryption algorithm respectively when RFID system initialize. The SEED algorithm provides a high level security and reliability in RFID systems. We also designed an authentication protocol by considering of robustness against privacy threats such as location tracking, spoofing, re-play and message loss. When we designed the protocol, we noticed the important characteristics about security of RFID applications. Multiple objects tag can be used on many kinds of RFID applications. These various applications are classified into two groups. One is that the security maintenance is very important such as financial system. The other is that the security maintenance is relatively less important. Therefore, we defined two types of security levels to represent strength of security for applications as high and low. In addition, we designed the authentication protocol which consists of high level procedure for high security level and low level procedure for low security level. As the result, we classify

various RFID application objects into two groups with security level and apply the different authentication procedure to the groups. In this way, our proposed RFID authentication protocol is designed to adjust to the multiple objects tag structure and to operate differently according to the security level. The proposed authentication protocol includes the following steps.

1. The reader sends a query to the tag. The query includes a pair of values *(oID, RNo)*. *oID* represents the type of current RFID application object and *RNo* is a random value generated each session. *RNo* is composed of two parts of value in expression (a). *RNo* is not included in the query at the low level procedure.

$$RNo = R_{Forward\_no} \,||\, R_{Backward\_no} \quad \text{(a)}$$

2. The tag searches eID corresponding to the oID and check its security level. For the objects with high security level, it creates a pID for the eID using *RNo* by bit masking operation. If the tag memory has 128bits block size and holds the pair of (oID, eID) for an object in the same block, the size of eID can be *(128 – size of oID)* bits. We decide bi-directional masking points ($R_{Forward}$, $R_{Backward}$) for eID in the expressions (b) and (c).

$$R_{Forward} = R_{Forward\_no} \bmod (\text{sizeof eID} / 2) \quad \text{(b)}$$

$$R_{Backward} = R_{Backward\_no} \bmod (\text{sizeof eID} / 2) \quad \text{(c)}$$

$R_{Forward}$ is the starting point of forward masking in the eID and $R_{Backward}$ is the starting point of backward masking in the eID. The tag creates a pID through two steps. First step, it makes two 32 bits strings by bit masking operation using both $R_{Forward}$ and $R_{Backward}$. Next, it creates a 64 bits pID by concatenating two masking operation results. These operations are shown in Fig. 3. The creation of *pID* in this step is omitted in the low level procedure.

Fig. 3. Creation of pID

Since the tag maintains the pID generated through the last successful authentication process in its memory, the reader may be an illegal adversary in current session if pID in current session is equal to the stored value in tag memory. When the pID does not match to the one stored in tag memory, the tag recognizes the reader as legal and send the pID. If the illegal reader obtained the message at the step (1) in the former session, it would disguise as an authorized reader and retransmit the obtained message as replay attack. However, the tag can perceive replay attack by comparing stored pID with present one. In that case, the tag will not transmit the value to the illegal reader because the pID does not be changed. The pID is the most important key value in our scheme. As mentioned above, a temporal one-time key of pID can keep tag from spoofing attack and location tracking. The last successful pID can also prevent RFID components from illegal adversaries' spoofing or replay attack. Since the pID can be created by bit masking operation in a simple way, it can be easily processed in most of the low-cost RFID systems.

3. The tag transmits *pID* to the current reader for objects with high security level, whereas the tag transmits *eID* to the reader for objects with low security level. Therefore, the omission of step (2) can reduce computation time in the low level procedure.
4. After the reader receives the response message from the tag, it sends a message to the corresponding server. This message contains both *RNo* and *pID* in the high level procedure or *eID* in the low level procedure
5. Server retrieves proper encrypted ID with the *RNo* and partial ID pair in database. If there is a match, the server decrypts the encrypted ID by SEED decryption algorithm and resolves tag ID. At the end of this session, the server starts service to the reader.

The proposed authentication protocol is shown in Fig. 4.

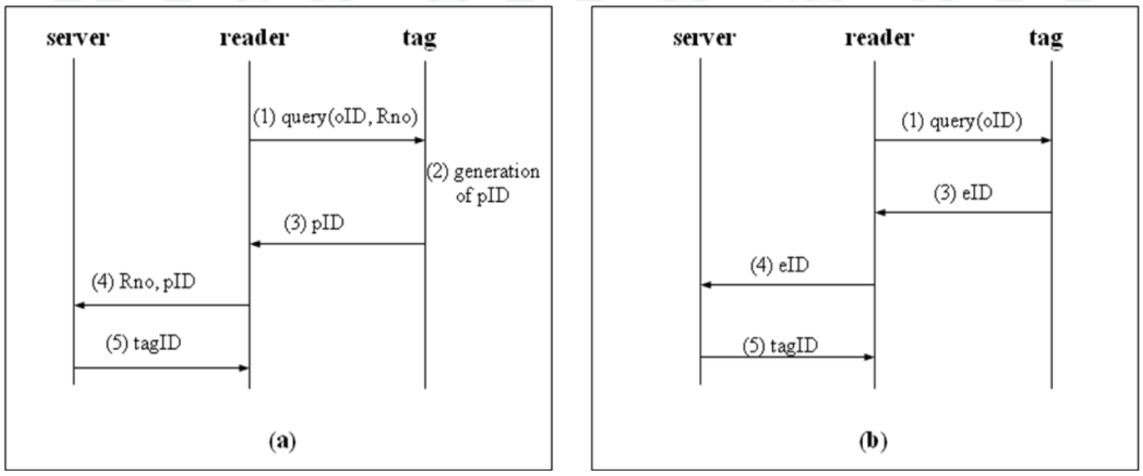

Fig. 4. The proposed authentication protocol: (a) high level procedure and (b) low level procedure

5. Evaluation

5.1 Evaluation of security

The proposed authentication protocol can keep its security for various kinds of attack. To prove this guarantee, we had evaluated the security of our scheme against the attacks as follows:

- Eavesdropping: The information tapped by attackers can be used for spoofing or location tracking. To solve this problem, a query message of reader should contain random value and then the tag should respond to the reader with variable value using this random value in the proposed scheme. In addition, this scheme will not let an attacker have any security information because the response message of variable pID is not complete value but the partial masking value of eID.
- Location tracking and replay attack: Since the tags respond differently for each query in our scheme, attackers can not catch the source of ID as well as the original value of ID. Therefore our scheme guarantees anonymity and supports blocking replay attacks.
- Spoofing: In our scheme, unauthorized readers have no way of joining in authorization process since readers should make a specified random value and transmit it to the tags. If an unauthorized reader uses the eavesdropped value again in current session, tags or server can be aware of abnormal status by comparing current pID with the stored one.

On the other hand, if an unauthorized tag catches a random value from the reader, it can not create the correct pID without eID either. In addition, though an unauthorized tag catches the pID by eavesdropping, the tag is unable to reuse it because the random value for pID is changed in every session.

- Message loss: The eID is non-volatile and fixed in the tag memory. Therefore, even if there is some data loss during the authentication process by transmission interference, the tag does not have to recover the data in the proposed scheme.

Table 2 shows the comparison of the proposed multiple objects tag scheme with the several existing schemes from the viewpoint of security.

	Location tracking	Spoofing	Replay attack	Message loss
Hash lock	x	x	x	x
Randomized hash lock	o	x	x	o
Hash chain	o	o	x	o
Variable ID	o	x	o	x
Proposed scheme	o	o	o	o

Table 2. Comparison in security (o: strong, x: weak)

5.2 Evaluation of efficiency

Almost existing schemes are not practicable on account of their demand for circuit size and computing power. Those schemes often require heavy operation in tag but the proposed scheme requires small operation. In the multiple objects RFID tag scheme, a tag computes bits masking once only for eID. This operation is simply compared with the other complicated hashing operations. On the other side, the server processes the tagID encryption with SEED algorithm for each tag in the proposed scheme when the system is initialized. The server also executes bit masking operations of n/2(n: numbers of ID in database) times on an average using message of (*RNo*, pID) to retrieve exact eID. If there is matched one, the server processes decryption of the retrieved eID once only by SEED algorithm. As the result, the proposed scheme guarantees more privacy and security than the existing schemes. Table 3 shows the comparison of the schemes from the viewpoint of efficiency.

	Tag	Reader	Server
Hash lock	hashing: 1	-	-
Randomized hash lock	randomizing: 1 hashing: 1	hashing: n/2	-
Hash chain	hashing: 2	-	hashing: (n/2)*i (i: update count)
Variable ID	hashing: 3	randomizing: 1	randomizing: 1 hashing: 3
Proposed scheme	bit masking: 1	randomizing: 1	bit masking: n/2

Table 3. Comparison in efficiency

5.3 Experimental results

We have simulated the proposed scheme and made experimental results about efficiency and stability for the scheme. To evaluate efficiency of the scheme, we have measured the computation time to perform one session in the proposed authentication procedures. One session means the stage to process the communication from server to tag via reader. To evaluate stability of the scheme, we have analyzed average error rates occurred during the authentication procedure. The experimental results were made under the environment as the reader of 13.56 MHz band, the tag with 2 Kbits of read/write memory and the communication standard of ISO15693. The experimental results are shown in Fig. 5.

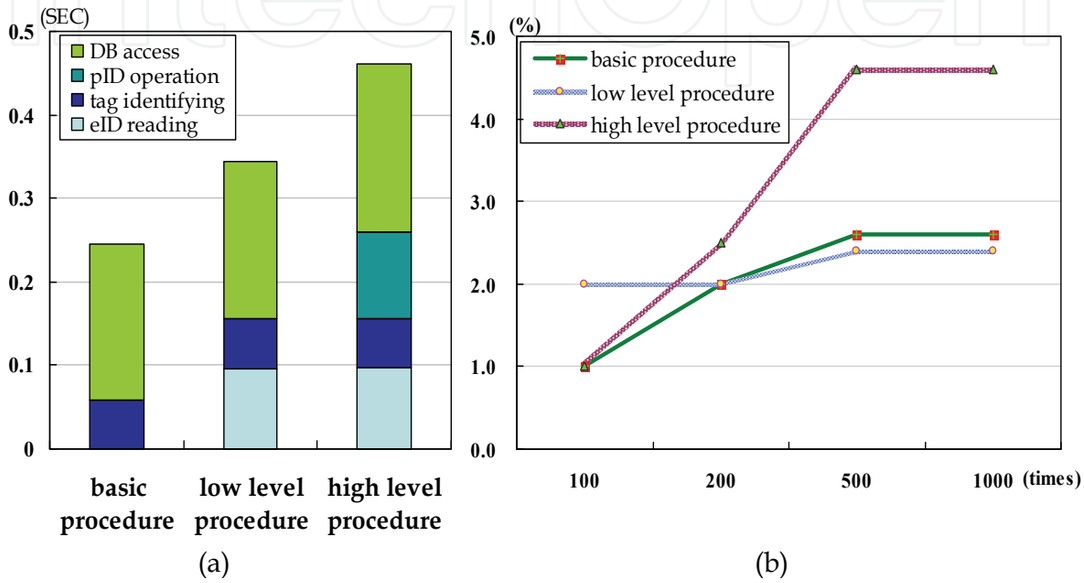

Fig. 5. Evaluation of the proposed scheme: (a) computation time and (b) error rate

Fig. 5(a) shows the comparison results of computation time values for three procedures: low level procedure, high level procedure and basic procedure of non-security level procedure in common RFID system. The values have been measured by 200 times repeatedly for different tags in the same condition. As shown in Fig. 5(a), the value of high level procedure is the largest in three cases but does not exceed double value of the basic procedure and the value of low level procedure is little more than the value of basic procedure. It means that the proposed scheme has reasonable computation time in spite of its strong security. In addition, we note that our scheme can save computation time of authentication procedure by using security levels because the scheme applies low level procedure to objects with low security level in multiple object tag. Fig. 5(b) shows the comparison results of average error rates for the above three procedures. As the result, all of the cases have similar error rates. The results show that the proposed multiple objects-based RFID system can be applied to areas of real environment.

6. Conclusion

We proposed a new RFID scheme including the multiple objects tag structure and the authentication protocol to give more privacy than existing schemes. The proposed multiple objects tag structure can maintain more than one object ID for different applications in a tag

and allow applications to access them simultaneously. So, each application can share a tag on the multiple objects and it can result many tags in one tag. The proposed authentication protocol supports the proposed multiple objects tag structure and keeps the RFID components from various attacks without heavy system load. Especially, the protocol is designed to perform authentication procedure efficiently according to security level of object. We evaluated the security and efficiency of the proposed RFID scheme for several types of attacks. The evaluation results show that the proposed scheme has better performance in security and efficiency than existing schemes.

The multiple objects-based RFID scheme is just at the beginning in our study. We proposed basic concept on multiple objects tag structure in this study. For the deep research and implementation, RFID reader has to be physically redesigned to support the proposed multiple objects tag structure. We are going to design the RFID components fit with the proposed authentication protocol based on multiple objects tag with embedded SEED algorithm in further study.

7. References

Garfinkel, S. & Rosenberg, B. (2005). *RFID: Applications, Security and Privacy*, Addison Wesley, ISBN 0-321-29096-8

IETF RFC 4269 (2005). The SEED encryption algorithm, IETF(The Internet Engineering Task Force)

Juels, A.; Rivest, R. L. & Szydlo, M. (2003). The blocker tag: selective blocking of RFID tags for consumer privacy, *Proceedings of 10th ACM Conference on Computer and Communications Security(CCS 2003)*, pp. 103-111, Washington DC., USA, October 2003

Kim, J.; Jung, J.; Ko, H.; Joe, S.; Lee, Y.; Chang, Y. & Lee, K. (2007). A design of authentication protocol for multi-key RFID tag, *Proceedings of APWeb/WAIM 2007*, pp. 644-653, Lecture Notes Computer Science 4537, Springer-Verlag

mCloak (2003). http://www.mobilecloak.com

Ohkubo, M.; Suzuki, K. & Kinoshita, S. (2003). Cryptographic approach to "Privacy-friendly" tags, *RFID Privacy Workshop @MIT*, November 15 2003

Saito, J. & Sakurai, K. (2004). Variable ID scheme of anonymity in RFID tags, *Proceedings of the 2004 Symposium on Cryptography and Information Security*, Vol. 1, pp. 713-718, Sendai, Japan, January 2004

TTAR-06.0013 (2006). Technical report on numbering an RFID tag, *TTA Technical Report*, TTA(Telecommunication Technology Association)

Weis, S.A.; Sarma, S.E.; Rivest, R.L. & Engels, D.W. (2003). Security and privacy aspects of low-cost radio frequency identification systems, *First International Conference on Security in Pervasive Computing*, pp.201-202, Lecture Notes in Computer Science 2802, Springer-Verlag

Development and Implementation of RFID Technology

Edited by Cristina Turcu

ISBN 978-3-902613-54-7
Hard cover, 450 pages
Publisher I-Tech Education and Publishing
Published online 01, January, 2009
Published in print edition January, 2009

The book generously covers a wide range of aspects and issues related to RFID systems, namely the design of RFID antennas, RFID readers and the variety of tags (e.g. UHF tags for sensing applications, surface acoustic wave RFID tags, smart RFID tags), complex RFID systems, security and privacy issues in RFID applications, as well as the selection of encryption algorithms. The book offers new insights, solutions and ideas for the design of efficient RFID architectures and applications. While not pretending to be comprehensive, its wide coverage may be appropriate not only for RFID novices but also for experienced technical professionals and RFID aficionados.

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

IntechOpen