The Research of RFID System's Authentication Based on the Information Hiding Feature

Lian-Jie Wang, Jonathan Jen-Rong Chen
Department of Information Management,
VaNung University
Email: { jiewang, jonathan }@vnu.edu.tw

Abstract—**RFID is a technology of automatic wireless identification and data acquisition. Meanwhile, the topic of RFID is a very popular issue in the field of technology. No Matter in software or hardware, there are many suppliers and demanders who invested a lots of resources to seek the efficiency and profit by using RFID technology. Therefore, many different solutions related to RFID application were proposed. Nevertheless, the increase of the RFID applications caused the issues of the protection of product and privacy came out. To solve this kinds of problems, various schemes were proposed. The purpose of the proposals is to find a safe protection method which can combine the RFID feature.**

In our research, we proposed a verification method between Reader and Tag of RFID. The method is to maintain the operation speed, the cost of Tag; and, to let the Reader can safely identify that the Tag is normal or forged. By using this kind of verification method, we can achieve the safe degree of information hiding and difficulty of attack. In the meantime, we can maintain the accuracy of RFID's operation and promote the efficiency of RFID system. Therefore, our system not only can promote the safety of various applications but also can make no difference to the whole system's safety operation.

***Index Terms*—RFID, Reader, Tag, Information Hiding**

I. Introduction

Under the rigorous competition environment of the globalization market, the enterprises have instant processing and the contingency ability of the fast response become the essential condition to survival. RFID receives each enterprise's attention in the last few years. The enterprises hope can use the characteristic and the operation of RFID to make the fast response and immediate processing, then strengthens itself competitive power.[2] Like the Wal-Mart, the leader of American merchandise retail sales, manages the inventory using RFID. JR Japanese Railroad Company and Taiwan's MRT apply RFID to the ticket system. Even the militarily application, the American DoD, uses the RFID application in weapon and commodity storage and transport. [3]

With the various trades and widespread application, many manufacturers invest massive resources to carry on the hardware design and the software, to develop more business opportunities, and create higher profits. However under this extensive and a great deal of application, spread out a safe subject gradually. Manufacturers and consumers are troubled by the problem of information privacy and transmission of data preservation. Therefore, the academia and research institutions have been made to raise the various solutions and countermeasures. To aim at RFID characteristic and find out the problem smoothly, the RFID applied level is able to getting more extensive and security. [5]

II. Background and motive

RFID uses the radio wave to make the recognition technology. It includes Tags Reader with the back-end server, as well as related application software systems. RFID is different from the traditional bar code. Bar code must be scanned at close range in order to obtain relevant information and its read rate depends on the clarity of the barcode. Relatively, RFID use wireless to capture, collect information. Compared to the convenience, RFID is easier to apply than the bar code. Therefore RFID is valued and develops gradually. However there is the cost problem of RFID, because of the Tag massive uses, the Tag expense consumption is quite considerable, reading equipment and server are expensive as well. Moreover the enterprises have to consider the standard of RFID to meet the integration between them. In this study, from the point of view of security, we investigate the safety of the identifying information passed between Tag and Reader. ID information will be simple operation to achieve the Tag concealment to ensure the RFID system will not to be theft, improper use and invasion by invaders. Research premise is based on the assumption that server and reader is in a secure environment. For information transfer between Reader and Tag do a fast operation to encrypt it, to identify whether it is normal or fake at the same time. In order to achieve the concealment, make the security of the RFID system.[7,8]

III. Method

3.1 Design of authentication scheme

In the last few years, many scholars proposed schemes about RFID tags validation to protect the tag's security such as Wong [9] use the shift key to verify tag and Quadratic Residues used by Chou [1]. Under the normal situation, these ways can reach to hide ID information. Then prevent ID information from encountering stealing or falsely use. Suppose in the information of Tag and Reader deliver, there are abnormal Tag or Tag was modified in order to obtain delivery ID. Or the observant and conscientious persons attempt to pick information from the Reader. If the transmission messages deliver between Tag and Reader without scheme that hides ID, then probably invaders can get delivering information. Therefore we design the scheme of identification, by this kind of operation to conceal the ID data that needs to be delivered, ensure to deliver of the security of information. Also can make use of this kind of way to find out an iniquity in tag or counterfeited tag. [4,6]

3.2 Our Scheme

In the general environment, the communication of Reader and Tag adopts a normal way or encrypts an identification message generally is omitted discussed here.

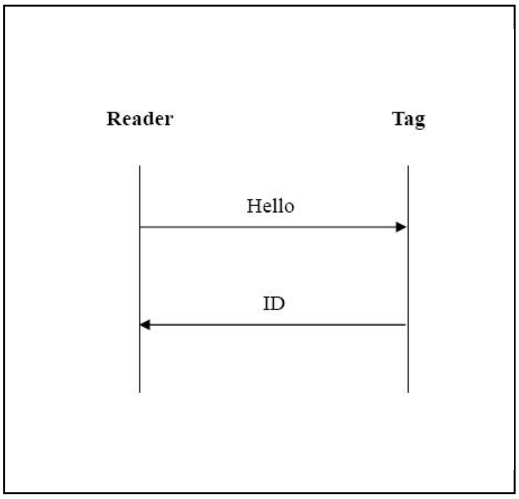

Fig. 1 General procedure

However, there are problems in the environment which are the tags mixed with a defect, this kind of tag can also deliver part of information. While exchanging messages to disrupt the operation of the system, the defect tag may capture the ID and other related information. By this time we adopt the design scheme to handle the delivery information of Reader and Tag.

3.2.1 Definition

Hello: Reader search whether there is the existence of Tag

p,q are big primes

c: counter (the initial value is 0)

ID: the identify data of tags

A: the total number of record ID in the database

3.2.2 The initial phase

1 $n = p \times q$

2 $p_1 = 4pq + 1$

3 $g^p \equiv 1(\mathrm{mod}\, p_1)$

4 $g^{x_{j,1}} \equiv y_{j,1}(\mathrm{mod}\, p_1)$

5 $g^{x_{j,2}} \equiv y_{j,2}(\mathrm{mod}\, p_1)$

3.2.3 The Message transmission phase

1 Reader sends out a request message toward Tag

2 After Tag receives a Reader request message, counter+1

3 Tag takes its ID information operating with the $x_{j,1}$,$x_{j,2}$ and then it sends back with S value to Reader

$$S \equiv x_{j,1}^c \times ID_j + x_{j,2}^c(\mathrm{mod}\, n)$$

4 Receiving the S which sends back by Tag, Reader compare all ID stored in database

```
for j = 1 to A do
    $\frac{g^S}{y_{j,2}^c} \overset{?}{\equiv} y_{j,1}^{c \times ID_j}(\mathrm{mod}\, p_1)$
End for
```

If the above-mentioned equations hold, then Return j, Reader confirms that ID is a record j in database.

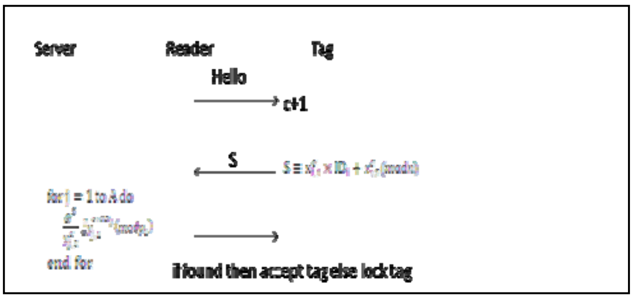
Server
Reader
Tag
Hello
c+1
S
S ≡ x^c_{j,1} × ID_j + x^c_{j,2} (mod n)
for j = 1 to A do
g^S / y^c_{j,2} ≟ y_{j,1}^{c×ID_j} (mod p_1)
end for
if found then accept tag else lock tag

Fig. 2 Validation procedure

Through this kind of validation procedure, our scheme can let the ID information included in the variable, and can't be arbitrarily eavesdropped. In the meantime our scheme can compare received Tag ID with the ID stored in database to validate its tag is correct or not to avoid illegal Tag attempt counterfeits or the interception. Then our scheme isolates the illegal Tag avoids the problem by Tag influence, overall system can work normal.

IV. CONCLUSION

We conclude that the use of such means for validating to avoid excessive use of complex calculations and to maintain the efficiency of the whole RFID system. At the same time, Tag and Reader in the mutual process of delivery can maintain the hiding ability of ID and avoid transmission of ID information be stolen. By this method the illegal Tag will be rule out, to protect the system and improve overall system security. Thus, our scheme decreases the burden of component operation and meets the requirements of general application.

REFERENCES

[1]Chou, J.-S., G.-C. Lee, and C.-J. Chan, "A Novel Mutual Authentication Scheme Based on Quadratic Residues for RFID Systems," IACR Cryptology ePrint Archive, 2007. vol.: pp. 9-11

[2] EPCglobalwebsite. http://www.epcglobalinc.org/

[3] Garfinkel, S. and B. Rosenberg, RFID Applications, Security, and Privacy. 2005: Addison Wesley

[4] Han, D. and D. Kwon, "Vulnerability of an RFID authentication protocol conforming to EPC Class 1 Generation 2 Standards," Computer Standards & Interfaces, 2009. vol. 31(4): pp. 648-652

[5] Juels, A., "Yoking-Proofs for RFID Tags " Proc. IEEE Int. Conf. Digital object identifier, 2004. vol.: pp. 138-143

[6] Kirschenbaum, I. and A. Wool, "How to build a Low-Cost, Extended-Range RFID Skimmer, IACR Cryptology ePrint Archive," IACR Cryptology ePrint Archive, 2006

[7] Liu, A.X. and L.A. Bailey, "PAP: A privacy and authentication protocol for passive RFID tags,"

Computer Communications, 2009. vol. 32(7-10): pp. 1194-1199

[8] Ryu, E.-K. and T. Takagi, "A hybrid approach for privacy-preserving RFID tags," Computer Standards & Interfaces, 2009. vol. 31(4): pp. 812-815

[9] Wong, K.H.M., P.C.L. Hui, and A.C.K. Chan, "Cryptography and authentication on RFID passive tags for apparel products," Computer in Industry, 2005. vol. 57: pp. 342-349