ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.2 , No.2, Pages : 164-170 (2013)
Special Issue of NCRTECE 2013 - Held during 8-9 February, 2013 in SMK Fomra Institute of Technology, OMR, Thaiyur, Kelambakkam, Chennai

AUTHENTICATION OF THE WIRELESS RFID SYSTEM USING SECURITY PROTOCOL

D.P.Anusuya,Asst.Professor,
Karpapga Vinayaga College of Engineering and Technology,
Madhrandagam,Chennai,India.
anu.krish1988@gmail.com

D.P.Balasubramanian, PG Student
Department of VLSI
SMK Fomra Institute of Technology,
Kelambakkam, Chennai , India
950016667
Keyan.sivam@gmail.com

Abstract- *Radio Frequency Identification (RFID) system is a contact less automatic identification system that has attracted much attention recently. It consists of RFID tags, RFID reader and back-end server. The information stored in the RFID tag is easily exposed to the outside world. So various types of attacks are possible such as brute-force attack, eavesdropping and man-in-the-middle attack. The adversary can determine the security value of a RFID tag using a brute-force attack with a random number. This project focuses on the mutual authentication scheme, a technique in which the RFID tag information is protected from the adversary by exploiting the one-way property of the mutual authentication function. The motivation of this project is to secure an RFID system from privacy and forgery problems. The main aspect of this project is to provide security to the RFID system against the attacks of the adversaries. The various types of security attacks like brute- force attack, eavesdropping and man- in-the- middle attack are prevented by the proposed protocol. It provides mutual authentication between the RFID tag and the back-end server. Further, this method updates the secret value of the RFID tag in each communication.*

Keywords: *Radio Frequency Identification (RFID), RFID tag, RFID reader, Mutual Authentication, Brute- Force Attack, Eavesdropping, Man- in- the- Middle Attack.*

I. INTRODUCTION

Radio-Frequency Identification (RFID) is a technology that uses radio waves to transfer data from an electronic RFID tag or label attached to an object through an RFID reader for the purpose of identifying and tracking the object. RFID tags can be read from several meters away and beyond the line of sight of the reader [1]. The application of bulk reading enables an almost-parallel reading of tags.

The RFID tag's information is stored electronically [2]. The RFID tag includes a small RF transmitter and receiver. An RFID reader transmits an encoded radio signal to interrogate the RFID tag. The RFID tag receives the message and responds with its identification information. The RFID tag uses the radio energy transmitted by the RFID reader as its energy source. The RFID system design includes a method of discriminating several RFID tags that might be within the range of the RFID reader.

RFID can be used in many applications. RFID tags can be affixed with any object (cars, computer equipment and books) to track and manage inventory, assets, people, etc. The Healthcare industry has used RFID to reduce counting, looking for things and auditing items [3]. Many financial institutions use RFID to track key assets and automate compliance. In recent advances, social media RFID is being used to tie the physical world with the virtual world.

The advantages of an RFID system are as follows. An RFID tag is small in size and low cost, and massive amounts of RFID tags can be simultaneously recognized with radio frequency communication [4, 5]. However, RFID system has several security risks like privacy and forgery problems. Presently, there are many researchers aiming to solve the privacy and forgery problems with RFID system [6].

In existing researchers, the RFID tag information is easily exposed for various types of attacks, because they did not involved in any type of authentication protocols. Therefore, this paper proposes a mutual authentication protocol to solve the privacy and forgery problems for various types of attacks [7, 8, and 9].

Recently, new security protocols [10], [11], [12] have been proposed to reduce the computational load on the back- end server. One such protocol which we will call YL due to name of the author was introduced by Yanfei Liu in [9]. The author provides a detailed security analysis of the protocol and claims that YL achieves a list of security properties, including resistance to tracking, tag impersonation, replay, denial of service and compromising attacks [13].

The remainder of this paper is organized as follows: In chapter 2 we briefly review the literature survey in the name of related works and analysis. In chapter 3, we describe the proposed method with its salient features and hardware, security requirements. The implementation process of the proposed method is analyzed in chapter 4. Chapter 5 and 6 consists of result analysis and conclusion of the method respectively.

II. RELATED WORKS AND ANALYSIS

Jung-Sik Cho et al. [8] have discussed about the hash-based RFID mutual authentication protocol using a secret value to secure the RFID system from Brute- Force attack. A hash-based mutual authentication protocol is given as a solution to the privacy and forgery problems in RFID system. They designed a protocol to send a random number generated by a RFID tag to the back-end server without disclosure. Moreover it substitutes a random number with a secret value, which is employed in a response message.

Imran Erguler and Emin Anarim [5] have discussed about the attacks on an efficient RFID authentication protocol. The security of a recently proposed RFID authentication protocol that needs O(1) time complexity to find out the identifier of the RFID tag irrespective of the total number of the RFID tags is investigated by them.

Selwyn Piramuthu [10] has explained RFID mutual authentication protocols. As RFID-tagged systems become ubiquitous, the acceptance of this technology by the general public necessitates addressing related security/privacy issues.

Tzu- Chang Yeh et al. [13] have discussed about EPC Class 1 Generation 2 standard to secure the RFID system. The information transmitted in the air could easily be intercepted and eavesdropped due to its radio transmission nature. On top of this, its prevalence has brought the stress on its security and privacy issues. However, it is found vulnerable to DoS attacks. Due to the bad properties of the CRC function used in the protocol, the claimed security objectives are also not met.

III. PROPOSED METHOD

RFID system needs more security from the adversaries who produces the privacy and forgery problems. This protocol is designed to secure the RFID system from the adversaries. It uses a secret value for the RFID tag to identify and the secret value is updated for every session. RFID reader plays as an intermediate role between the back end server and the RFID tag. Both the RFID tag and the Back end server authenticate each other mutually.

This project focuses on the mutual authentication function-based scheme, in which the RFID tag's information is protected from the adversary by exploiting the one-way property of the hash function. This scheme uses a random number value and satisfies all the security requirements to solve the privacy and forgery problems. Mutual authentication protocol solves the drawbacks in the existing protocols with a minimum increase in structural design.

The main objective of this project is to generate an efficient mutual authentication protocol for RFID system. The mutual authentication protocol provides forward security to the RFID system to handle the security vulnerabilities such as Replay Attack, Eaves dropping and Brute- force attack. To provide security to the RFID system this protocol implements a hash based RFID mutual authentication protocol using a secret value. It is very difficult to eavesdrop the message, which is sent by the RFID tag to the back end server using mutual authentication protocol.

The RFID tag creates an response message alpha (α) by performing XOR ($\oplus$) operation using the random numbers (R_r, R_t) and identifiers (ID_k, RID_i). The RFID reader and the back end server extract the random number of the RFID tag (R_t) by removing the additional information in the response message.

IV. REQUIREMENTS, DESIGN AND IMPLEMENTATION

A. Hardware Requirements of the proposed method

A.1 RFID tag

RFID tags (Fig. 1) can be either passive, active or battery assisted passive. Passive RFID does not use a battery, while an active has an on-board battery that always broadcasts or beacons its signal. A Battery Assisted Passive (BAP) has a small battery on board that is activated when in the presence of a RFID reader.

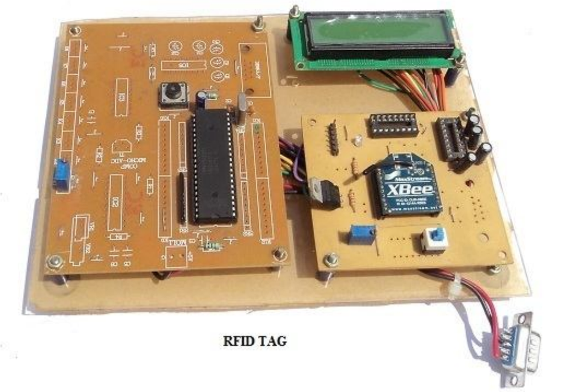

Fig. 1: RFID tag

A.2 RFID reader

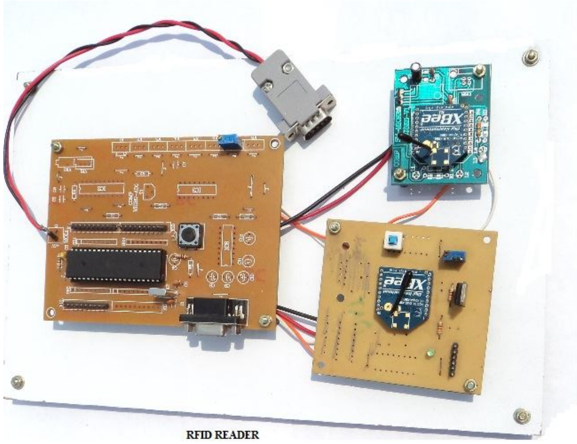

Fig. 2: RFID reader

RFID reader (Fig. 2) is the intermediate component between the host system and the RFID tag. Depending on the mobility of the RFID reader it is classified into two different types. They are fixed RFID reader and mobile RFID reader.

A.3 Battery

Batteries (Fig. 3) are used to provide power for both the RFID tag and RFID reader. These batteries will give Direct Current (DC). The batteries can be re-chargeable.

Fig. 3: Battery

A.4 Zigbee

The MC13191 Zigbee (Fig. 4) is a short range, low power, 2.4 GHz Industrial, Scientific, and Medical (ISM) band transceiver. The MC13191 contains a complete packet data modem which is compliant with the IEEE 802.15.4 Standard PHY (Physical) layer. Interface with the MCU is accomplished using a four wire serial peripheral interface (SPI) connection and an interrupt request output which allows for the use of a variety of processors.

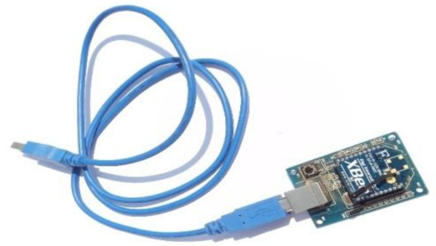

Fig. 4: Zigbee

A.5 Connection Setup

RFID tag and RFID reader are connected with their batteries respectively (Fig. 5 and Fig. 6). Zigbee transceiver is connected to the back-end server. RFID tag will show the TAG ID as 1 initially. If not press the reset button until it shows the TAG ID as 1. After the connection has been set up the front end application designed in visual basic is to be opened. Run the project, enter the port number where the Zigbee is connected.

The communication starts from the back end server by sending the request message R_r, RFID tag will now calculate the response message α and β. In the LCD the request message, Random number of the RFID tag R_t and response messages will be displayed one by one sequentially. The RFID reader now receives the transmitted data from the RFID tag and re-transmits it to the back end server.

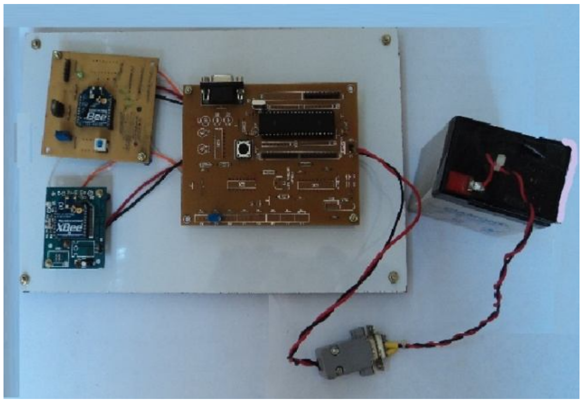

Fig. 5: RFID reader connected with battery

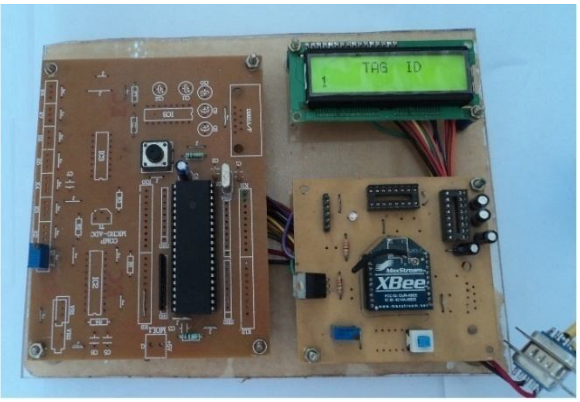

Fig. 6: RFID tag with LCD

B. Security requirements of the proposed method

The security requirements are defined in terms of confidentiality, indistinguishability, forward security, and mutual authentication. These requirements are the criteria used to evaluate the proposed mutual authentication protocol. Confidentiality requires that all of the information is securely transmitted during all communications.

Attacks	**Problems**	**Security requirements**
Eavesdropping	User privacy problem	Confidentiality
Traffic analysis	Location privacy problem	Confidentiality
Brute-force attack	Location privacy problem	Indistinguishability
Replay attack	Forgery problem	Forward security
Man-in-the-middle attack	Forgery problem	Mutual authentication

Table 1
Classification of attacks and problems, security requirements

Characteristics:

1. Reduces the computational complexity at the back end server.
2. Extraction module takes place in RFID reader itself.
3. Both the random numbers (R_r and R_t) changes in every communication.
4. This method provides forward security to the RFID system by providing confidentiality based on unpredictable variations in the response message.

C. Design of the proposed method

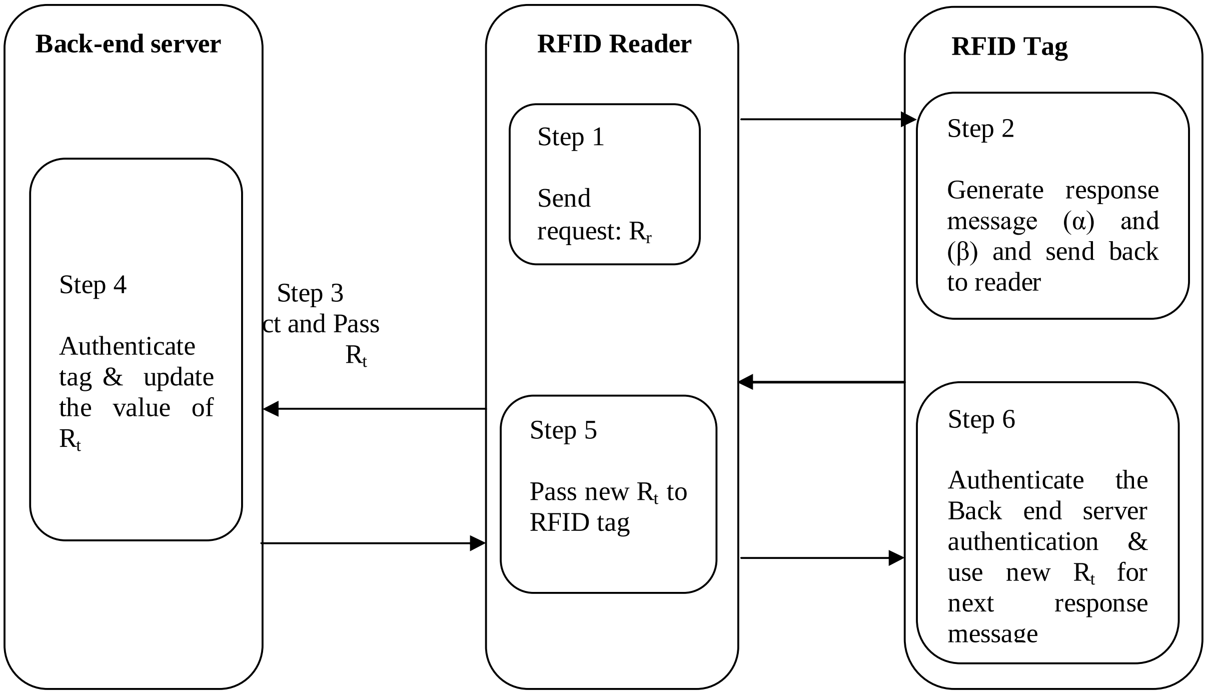
Back-end server
RFID Reader
RFID Tag
Step 1
Send request: R_r
Step 2
Generate response message (α) and (β) and send back to reader
Step 3
ct and Pass
R_t
Step 4
Authenticate tag & update the value of R_t
Step 5
Pass new R_t to RFID tag
Step 6
Authenticate the Back end server authentication & use new R_t for next response message

Fig. 7: Design of proposed protocol

D. Implementation of the proposed method

The following steps are followed to implement the method (Fig. 7):

1. The RFID reader sends request message as a random number R_r to the RFID tag.

2. After receiving RFID reader's request message, RFID tag calculates alpha (α) and beta (β) using the ID of the RFID tag, RFID reader's random number R_r, RFID tag's random number R_t and a group ID of the random number RID_i and sends this as a response message.

3. The RFID reader forwards the RFID tag's response to the back end server.

4. The back end server extracts the random number of the RFID tag R_t.

5. Backend server then updates the RFID tag's random number and sends back to the RFID reader.

6. Reader transmits the new random number of the tag to the RFID tag. Both the Back end server and the RFID tag authenticate each other mutually.

The RFID reader initiates the communication by sending a request message (R_r) which is the random number of the reader. Upon receiving the request message the RFID tag creates a response message alpha (α) and beta (β) using the XOR ($\oplus$) operation. Alpha (α) = ID_k ($\oplus$) RID_i ($\oplus$) R_r ($\oplus$) R_t, Beta (β) = ID_k($\oplus$) RID_i, Where ID_k is the RFID Tag ID, RID_i is the group ID of random numbers, R_r is the RFID reader's random number, R_t is the RFID tag's random number, Alpha (α), beta (β) are response messages. After receiving the response message the RFID reader passes it to the back-end server. Backend server knew the random number of the RFID reader (R_r) and the alpha (α), beta (β) values. The back-end server extracts the R_t RFID tag's random number and updates the random number for next communication.

V. RESULT ANALYSIS

The implementation of the proposed protocol is based on the random numbers. The RFID tag and the RFID reader use the random number for communicating each other. The inputs given in this method are the RFID reader's random number, RFID tag's random number, the group ID of the random number and the ID of the RFID tag.

The intermediate outputs of this implemented system are the alpha and beta values, the updated random number of the RFID tag. The updated random number of the RFID tag is used for further communications.

In the RFID reader side the random number of the RFID reader is changing for each communications randomly. The RFID tag calculates the intermediate output such as alpha, beta and sent back to the RFID reader. In the Back-End server side the Rt is extracted and updated.

RFID reader side	**RFID tag side**					**Back-end server side**	
R_r	**R_t**	**ID_k**	**RID_i**	**A**	**β**	**Extracted R_t**	**New R_t**
7	2	1	1	5	0	2	4
6	4	1	1	2	0	4	6
5	6	1	1	3	0	6	7
4	7	1	1	3	0	7	5
9	5	1	1	12	0	5	3
2	3	1	1	1	0	3	2

Table 2
Result Analysis

Finally, we prove that the proposed protocol solves the privacy and forgery problems by satisfying all of the security requirements.

VI. CONCLUSION AND FUTURE WORK

An efficient RFID mutual authentication protocol is designed and implemented. The hardware is designed to adapt the requirements of the proposed protocol. The basic RFID communication is established between the RFID tag and the RFID reader. Based on the RFID reader's request the response message is generated by the RFID tag. RFID tag's information is extracted by the back-end server. The random number of the RFID tag is updated in each communication by the back-end server. Front end design is developed using Visual Basic to view the transactions of RFID tag, RFID reader. The proposed protocol is implemented successfully. The security analysis of a mutual authentication protocol using a random number is completely studied and implemented.

The RFID reader reduces the computational complexity at the back-end server by extracting the R_t at reader itself. The back-end server's task is only to update the R_t value and to send back to the reader. The security analysis of the proposed protocol is done against various types of attacks, like brute-force attack, traffic analysis, location tracking, replay attack and man-in-the-middle attack.

In the future the existing hardware will be modified to suit the implementation of the hash based RFID mutual authentication protocol using a secret value. The secret values for the next communication will be generated by the back-end server using a hash function. The RFID reader can be designed in such a way that it can perform few functions on the data transmitted by the RFID tag and pass it to the back-end server. The random number which is used for communication can be replaced by means of a secret value for providing better security to the RFID system. The possible attacks like Eavesdropping, Brute-force attack and Man-in-the-Middle attack will be prevented by the proposed protocol.

REFERENCES

[1] Chen, Y. C., Wang, W. L., Hwang, M. S., "RFID authentication protocol for anti-counterfeiting and privacy protection", Proceedings of the 9th International Conference on Advanced Communication Technology, ICACT 2007, pp. 255-259.

[2] Chien, H. and Chen, C. "Mutual authentication protocol for RFID conforming to EPC class 1 generation 2 standards", Computer Standards & Interfaces, 29 (2): 254-259, February 2007.

[3] Cho, J. S., Yeo, S. S., Kim, S. K., “An analysis of RFID tag authentication protocols using secret value”, 2007 International Conference on Future Generation Communication and Networking (FGCN 2007), Vol. 1, December 2007, pp. 481-486.

[4] Finkenzeller, K., “ RFID Handbook”, second ed., Wiley & Sons, 2002.

[5] Imran, E. and Emin, A., “ Attacks on an Efficient RFID Authentication Protocol”, 10th IEEE International Conference on Computer and Information Technology (CIT) 2010.

[6] Irfan S., Tharam D., Elizabeth C., Song H., “A survey of RFID authentication protocols based on hash-chain method”, Third International Conference on Convergence and Hybrid Information Technology – ICCIT 2008, vol. 2, November 2008, pp. 559-564.

[7] Jihwan L., Heekuck O., SangJin K., “A new hash-based RFID mutual authentication protocol providing enhanced user privacy protection”, ISPEC 2008, LNCS, vol. 4991, April 2008, pp. 278-289.

[8] Jung-Sik, C., Sang-Soo, Y. and Sung, K. K., “Securing against brute-force attack: A Hash-based RFID mutual authentication protocol using a secret value”, Elsevier Journal on Computer Communications, Mar. 2010.

[9] Liu, Y., “An efficient RFID authentication protocol for low-cost tags,” In Proceedings of the 2008 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing-EUC 2008, pages 706-711, Shanghai, China, December 2008. IEEE Computer Society.

[10] Selwyn, P., “RFID mutual authentication protocols”, Elsevier Journal on Decision Support Systems, Apr. 2010.

[11] Song, B. and Mitchell, C. J., “RFID authentication protocol for low-cost tags”, In V. D. Gligor, J. Hubaux, and R. Poovendran, editors, ACM Conference on Wireless Network Security- WiSec’08, pages 140-147,Alexandria, Virginia, USA, April 2008, ACM Press.

[12] Tsudik, G., “YA-TRAP: yet another trivial RFID authentication protocol,” In Fourth IEEE Annual Conference on Pervasive Computing and Communications- PerCom 2006, pages 640-643, Pisa, Italy, March 2006. IEEE Computer Society.

[13] Tzu-Chang, Y., Yan-Jun, W., Tsai-Chi, K. and Sheng-Shih, W., “Securing RFID systems conforming to EPC Class 1 Generation 2 standard”, Elsevier Journal on Expert Systems with Applications, 2010.

[14] Weis, S., Sarma, S., Rivest, R., Engels, D., “Security and privacy aspects of low-cost radio frequency identification systems”, International Conference on Security in Pervasive Computing, March 2003, pp. 201-212.

[15] Yang, J., Park, J., Lee, H., Ren, K., Kim, K., “Mutual authentication protocol for low cost RFID”, Proceedings of the workshop on RFID and Lightweight Cryptography, July 2005, pp. 17-24.