International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-3 Issue-3, February 2014

Effective Anonymous Approach for Implementing RFID Reciprocated Endorsement Protocol

B.Kavipriya, S.Dhivya, J.Sivasankari, S,Sheik Farith, A.Jasmine

Abstract— Radio-frequency identification (RFID) is a wireless technology that utilizes radio communication to identify objects with a unique electrical identity. The widespread deployment of RFID technologies may generate new threats to security and user privacy. One of the main drawbacks of RFID technology is the weak authentication systems between a reader and a tag. In general, "weak" authentication systems that either leak the password directly over the network or leak sufficient information while performing authentication allow intruders to deduce or guess the password. In this paper, we study the RFID tag–reader mutual authentication scheme using protocol. A hardware implementation of the mutual authentication protocol for the RFID system is proposed.The proposed system was simulated using Modelsim XE II and synthesized using libero synthesis technology. The system hasbeen successfully implemented in hardware using prosaic nano chip using a FPGA.

Keywords—Field-programmable gate array (FPGA) implementation, mutual authentication, radio-frequency identification(RFID)

I. INTRODUCTION

Radio-Frequency IDentification (RFID) is a contactless identification technology that enables remote and automated gathering and sending of information between RFID tags or transponders and readers or interrogators using a wirelesslink. In recent years, RFID technology has gained rapid acceptance as a means to identify and track a wide array of manufactured objects. An RFID system is composed of three main components: tag, reader, and back-end database.RFID tags come in a range of forms and can vary in storage capacity, memory type, radio frequency, and power capability. An RFID tag typically consists of an integrated circuit for handling data and an antenna for receiving and transmitting a radio-frequency signal.

In the commercial setting, RFID tags contain an electronic product code (EPC) that can uniquely identify each and every tagged item . The RFID tag stores its unique EPC with related product information inside the tag's memory and sends these data whenever the reader requests them. The reader reads data from and writes data to tags by broadcasting the RF signals. After a reader queries a tag and receives information from the tag, the reader forwards the information to a backend database.

Manuscript published on 28 February 2014.
* Correspondence Author (s)
B.Kavipriya, ECE, ,UCETW, Madurai , Tamil Nadu, India
S.Dhivya, ECE, ,UCETW, Madurai , Tamil Nadu, India
J.Sivasankari, ECE, ,UCETW, Madurai , Tamil Nadu, India
S,Sheik farith, EEE ,CIET, Coimbatore , Tamil Nadu, India
A.Jasmine, ECE,, CIET, Coimbatore, Tamil Nadu, India

The back-end server plays an essential role inchecking the validity of the tags or reader, which is very important for privacy protection and security issues.

RFID standards are a major issue in securing high investments in RFID technology on different levels (e.g., interface protocol, data structure, etc.). There are two competing initiatives in the RFID standardization arena: ISO and EPC Global . The EPCglobal Class-1 Generation-2 (C1G2) Ultra high frequency(UHF) RFID standard defines the specification for passive RFID technology and is an open and global standard. The EPC C1G2 standard specifies the RFID communication protocol within the UHF spectrum (860 to 960 MHz). The standard specifies that a compliant RFID tag should containa 32-b kill password (Kpwd) to permanently disable the tag and a 32-b access password (Apwd). The reader then performs a bitwise XOR of the data or password with a random number from the tag to cover-code data or a password in EPC Gen 2.However, the EPC C1G2 standards do not fully support privacy invasion and data security issues. The simple kill and access commands specified in EPC C1G2 specifications are not enough to provide secure authentication function and data/privacy protection.

EPC C1G2 provides only very basic security tools using a 16-b pseudorandom number generator (PRNG) and a 16-b cyclic redundancy code (CRC). Despite many prospective applications,RFID technology has several privacy-related problems such as data leakage and data traceability, which should be resolved before RFID's pervasive employment. Many methods have been proposed to enhance the security of RFID systems, and the research for RFID security is quite extensive and growing. Most hash-based RFID protocols for mutual authentication have been proposed in the literature .Juels proposed a solution based on the use of pseudonyms, without any hash function.This mutual authentication protocol is based on a short list of pseudonyms that are stored on a tag. To resist cloning and eavesdropping, this protocol requires extra memory on the tag and needs a way to update the tag's pseudonym list. The communication cost is relatively high because of the tag data updates, which limits the practicalityof this scheme. operation and tag's access and kill passwords for the tag–reader mutual authentication scheme. However, this approach hasnot been implemented in hardware. The rest of this paper is organized as follows. In Section II, we present the background and previous work on the RFID reader-to-tag authentication protocol. The pad-generation function and protocol implementation is discussed inSection III. Section IV shows the implementation results of the mutual authentication scheme. Finally, we conclude the paper in Section V.

II. RELATED WORK

Epc class 1 generation 2 standard

An access password is required before data are exchanged between a reader and a single tag. The access password is a 32-b value stored in the tag's reserved memory. If this password is set, then the reader has to have the valid password before the tag will engage in a secured data exchange. These passwords can be used in activating kill commands to permanently shut down tags, as well as for accessing and relocking a tag's memory.

To cover-code data or a password in Gen 2, a reader first requests a random number from the tag. The reader then performs a bitwise XOR of the data or password with this random number and transmits the cover-coded (also called ciphertext) string to the tag. The tag uncovers the data or password by performing a bitwise XOR of the received cover-coded string with the original random number. In addition, the tag conforming to the EPC C1G2 standard can support only a 16-b PRNG and a 16-b CRC checksum that are used to detect errors in the transmitted data. Fig. 1 describes the EPCglobal C1G2 communication step between a reader and a tag. A detailed description of each step is as follows.

1. The interrogator issues a Req_RN and sends a request message to a tag.
2. The tag responds by backscattering a new 16-b random number RN16.
3. The interrogator then generates a 16-b ciphertext string comprising a bitwise XOR of the 16-b word to be transmitted with this new RN16, both MSB first, and issues the command with this ciphertext string as a parameter.
4. The tag decrypts the received ciphertext string by performing a bitwise XOR of the received 16-b ciphertext string with the original RN16.

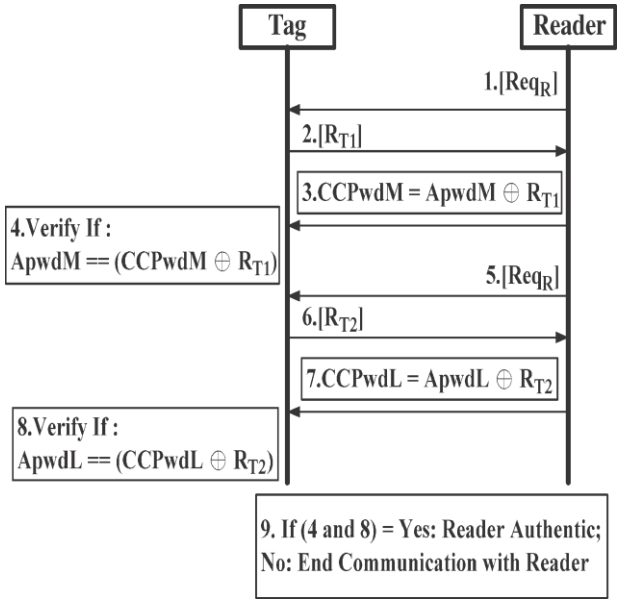


Fig.1. One-way reader-to-tag authentication scheme proposed by EPCglobal .

5. The interrogator issues a Req_RN to obtain a new RN16
6. The tag responds by backscattering a different RN16.
7. The interrogator then transmits a 16-b ciphertext string generated from the 16 LSBs of the tag's access password XORed with the RN16 generated at step 6).
8. The tag performs a bitwise XOR operation of the received 16-b ciphertext string and the RN16 to decrypt the received ciphertext string for verification.

III. PAD GENERATION

A. Original Scheme

The PadGen function is the key component in constructing the 16-b pads to cover code the two 16-b access password halves (ApwdM and ApwdL). The pad-generation function retrieves the individual bits of the Apwd and Kpwd from the memory locations by manipulating random numbers and concatenates these bits to form a 16-b pad. A brief description of the PadGen function is provided in the following. Let us represent the 32-b Apwd and Kpwd in binary (base 2) as

$$Apwd = a_0\, a_1\, a_2\, a_3 \cdots a_{31} \quad (1)$$

$$Kpwd = k_0\, k_1\, k_2\, k_3 \cdots k_{31} \quad (2)$$

The 16-b random numbers R_{Tx} and R_{Mx} generated by the tag and manufacturer in hexadecimal (base 16) are

$$R_{Tx} = d_{t1} d_{t2} d_{t3} d_{t4} \quad (3)$$

$$R_{Mx} = d_{m1} d_{m2} d_{m3} d_{m4}. \quad (4)$$

Each digit of R_{Tx} and R_{Mx} is used to indicate a bit location in Apwd, and these bits are concatenated to form a 16-b output in hexadecimal (base 16) representations as

$$\text{Apwd} - \text{PadGen}(R_{Tx}, R_{Mx})$$
$$= ad_{t1}\, ad_{t2}\, ad_{t3}\, ad_{t4} \,||\, ad_{t1+16}\, ad_{t2+16}\, ad_{t3+16}\, ad_{t4+16}$$
$$ad_{m1}\, ad_{m2}\, ad_{m3}\, ad_{m4} \,||\, ad_{m1+16}\, ad_{m2+16}\, ad_{m3+16}\, ad_{m4+16}$$
$$= d_{v1} d_{v2} d_{v3} d_{v4}$$

Where $d_{v1}d_{v2}d_{v3}d_{v4}$ is a decimal notation.

The PadGen is again performed over Kpwd using the previously generated $d_{v1}\ d_{v2}\ d_{v3}\ d_{v4}$ to indicate a bit location in Kpwd, and these bits are concatenated to form a 16-b PAD. The resulting PAD would then be expressed as follows

$$PAD = Kpwd - padgen(Apwd - PadGen(RT_X, RM_X), (RT_X))$$
$$= kpwd - padgen\,(d_{v1}\, d_{v2}\, d_{v3}\, d_{v4}\,, RT_X)$$
$$= kd_{v1} kd_{v2} kd_{v3} kd_{v4} \,||\, kd_{v1+16} kd_{v2+16} kd_{v3+16} kd_{v4+16}$$
$$Kd_{t1} kd_{t2} kd_{t3} kd_{t4} \,||\, kd_{t1+16} kd_{t2+16} kd_{t3+16} kd_{t4+16}$$
$$= h_{p1} h_{p2} h_{p3} h_{p4},$$

Where $h_{p1}h_{p2}h_{p3}h_{p4}$ is a hexa decimal notation.

IV. DESIGN AND IMPLEMENTATION

A. Data encoding architecture

According to the EPC C1G2 protocol, a tag communicates with an interrogator using backscatter modulation, in which the tag switches the reflection coefficient of its antenna between two states in accordance with the data being sent. Tags encode the backscattered data as the Miller modulation of a subcarrier at the data rate.A binary "1" is constant during a symbol time, and a binary "0" has a state transition in the middle of a symbol,The frequency divider divides the original clock signal frequency by two and is processed as a clock signal to trigger the first register. The encoder is triggered by the original clock signal. The first input register is used to save the input data for further encoding processes. The encoded information will be stored in the register and will output the final results in sequence.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

The encoding result is bit- wised with a subcarrier through the XNOR gate.

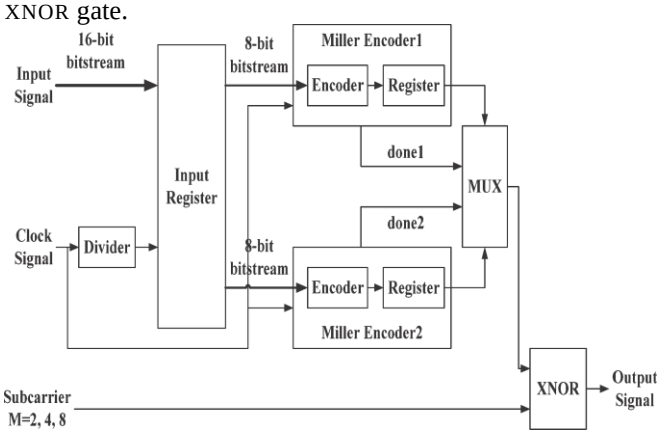


Fig. 2 MMS data-coding architecture.

B. Mutal authentication architecture

The working principle is as follows-when the RFID ATM card is brought into the vicinity of the ATM centre, the reader reads the account number and details of card holder. Then this information is sent into the microcontroller which finally reaches the computer. Here details are checked for genuineness and a message is sent to the card holder whether to proceed the transaction or not. This is done with the help of hyper terminal which is present in windows operating system. In real- time it can also be replaced by either GSM or CDMA technology.

An RFID system is usually comprised of:

(a) The RFID tag, which contains a digital number associated with the physical object that it is attached

(b) The RFID reader which is connected to a backend database. The reader is also equipped with an antenna, a transceiver and a processor that broadcasts a radio signal in order to query the tag and read its contents.

According to their energy resources and computational capabilities RFID tags are distinguished into passive and active. Passive tags, unlike active ones, do not have an internal source of energy and therefore they have smaller size and computational resources.

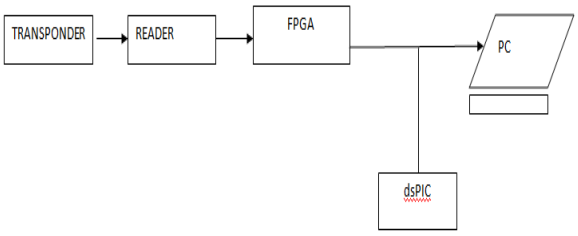


Fig. 3 RFID block diagram

The maximum reading distance of a tag varies from a few centimeters to approximately ten meters. Also, its cost is about13 cents per tag and is expected to decrease to 5 cents within the next few years.

A fundamental requirement of pervasive systems in general, is the ability to uniquely identify things and entities .By satisfying this requirement RFID technology bring along with it the benefits of maintaining user‟s confidentiality under any circumstances .With their wide deployment, low cost tags have unfortunately been object of various kinds of attacks raising serious concerns.

RS232 is a asynchronous serial communication protocol widely used in computers and digital systems. It is called asynchronous because there is no separate synchronizing clock signal as there are in other serial protocols like SPI and I2C. The protocol is such that it automatically synchronize itself. We can use RS232 to easily create a data link between our MCU and standard PC

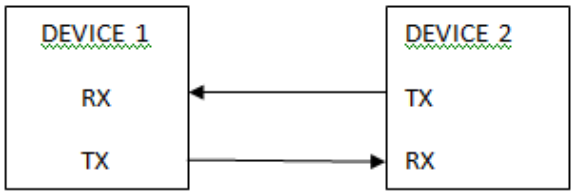


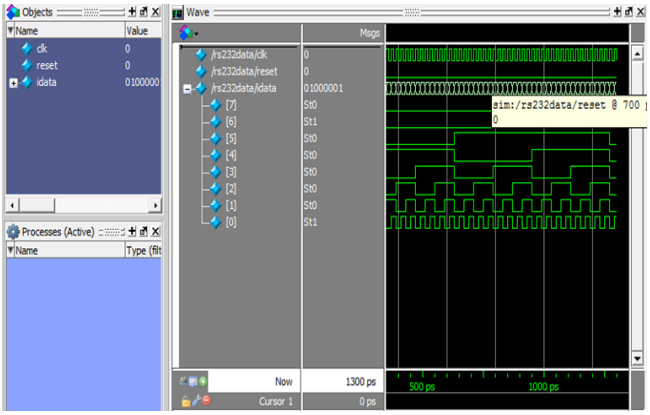
Fig. 4 RS232 Transmission

In RS232 there are two data lines RX and TX. TX is the wire in which data is sent out to other device. RX is the line in which other device put the data it need to sent to the device. One more thing about RS232. We know that a HIGH =+5v and LOW=0v in TTL / MCU circuits but in RS232 a HIGH=-12V and LOW=+12V. Ya this is bit weird but it increases the range and reliability of data transfer. Now you must be wondering how to interface this to MCUs who understand only 0 and 5v? But you will be very happy to know that there is a very popular IC which can do this for you! It is MAX232 from Maxim Semiconductors.

As there is no "clock" line so for synchronization accurate timing is required so transmissions are carried out with certain standard speeds. The speeds are measured in bits per second. Number of bits transmitted is also known as baud rate**.** Protocol we chose the speed as 9600bps (bits per second). As we are sending 9600 bits per second one bits takes 1/9600 seconds or 0.000104 sec or 104 uS (microsecond= 10^-6 sec).

C. Simulation and Implementation results

Coding for the proposed design was done in verilog language in libero technology and the simulation was carried out in model sim actel 6.6 d,and implemented in pro asic nano 3 on FPGA board, further the dspic coding was carried out in embedded c language and it is compiled using mikro c pro. The simulation result for the proposed scheme is shown below.



The data are generated in the simulation results and the same data is loaded in the transponder, the FPGA will authenticate the data and send the data to the dspic where the processing of the signals takes place and it will show the result on the lcd or the another pc.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

V. CONCLUSION AND FURTURE WORK

In this paper, the functionality of the MMS design were verified using the verilog hardware descriptionlanguage and we identified, that threats from cloned fake RFID tags, malicious snooping RFID readers, and unauthorized tag's data manipulation can only be prevented by incorporating a tag-reader mutual authentication scheme. We also analyzed the security weakness of the one-way reader-to-tag authentication scheme proposed by EPCglobal Class 1 Gen 2 UHF RFID Protocol. We then proposed a simple cost-effective, light-weight, and practically secure tag-reader mutual authentication scheme that adheres to EPCglobal standards. Our scheme utilizes the protocol implementation,for achieving tag-reader mutual authentication. Therefore, in our scheme, the tag'saccess password is never exposed even to the stockholder's reader (protectionfrom insider attacks), yet we accomplish tag-reader mutual authentication. Stolen cards can be blocked and traced using the GSM technology, it is implemented successfully. The hardware implementation of an RFID tag–reader mutual authentication scheme is also presented and still we can further increase the privacy by implementing the reader effectively.

REFERENCES

[1] P. Peris-Lopez, T. Li, L. Lim, J. C. Hernandez-Castro, and J. M Estevez- Tapiador, “Vulnerability analysis of a mutual authentication scheme under the EPC class-1 generation-2 standard,” in Proc. RFIDSec, Jul. 2008, pp. 52–63.

[2] C.-C. Yuan, K.-H. Huang, H.-L. Li, and Y.-J. Huang, “The design of encoding architecture for UHF RFID applications,” in Proc. Asia-Pacific Microw. Conf., Hong Kong, Dec. 16–19, 2008, pp

[3] D. M. Konidala, Z. Kim, and K. Kim, “A simple and cost effective RFID tag–reader mutual authentication scheme,” in Proc. Int. Conf. RFIDSec, Jul. 2007, pp. 141–152

[4] Radio Frequency Identification for Item Management, 2nd ed., ISO/IEC 18000, Jul. 1, 2008.

[5] A. Juels, “RFID security and privacy: A research survey,” IEEE J. Sel.Areas Commun., vol. 24, no. 2, pp. 381–394, Feb. 2006.

[6] S. Garfinkel and B. Rosenberg, Eds., RFID : Applications, Security, and Privacy. Reading, MA: Addison-Wesley, Jul. 2005

[7] R. Want, “Enabling ubiquitous sensing with RFID,” Computer, vol. 37, no. 4, pp. 84–86, Apr. 2004

[8] I. Vajda and L. Butty’an, “Lightweight authentication protocols for low-cost RFID tags,” in Proc. 2nd Workshop Security Ubicomp 2003, pp. 1–10.

[9] W. Stallings, Cryptography and Network Security: Principles Practices, 3rd ed. Englewood Cliffs, NJ: Prentice-Hall, 2003.

[10] E. Y. Choi, S. M. Lee, and D. H. Lee, “Efficient RFID authentication protocol for ubiquitous computing environment,” in Proc. EUC Workshops, vol. 3823, LNCS, Berlin, Germany, 2005, pp. 945–954

B.Kavipriya received the B.E. degree from AnnaUniversity, SIT, Madurai in 2010, and the M.E. degree from Anna University, SIT, in 2012.Working as Assistant Professor in the department of ECE, *UCETW*

S.Dhivya received the B.E. degree from AnnaUniversity, RVSCET, Dindigul in 2009, and the M.E. degree from Anna University, PSYCET, in 2012.Working as Assistant Professor in the department of ECE, *UCETW*

J.Sivasankari received the B.E. degree from Annamalai University, Chidambaram in 2008, and the M.E. degree from Anna University, SIT, in 2012.Working as Assistant Professor in the department of ECE, *UCETW*

S,Sheik farith received the B.E. degree from AnnaUniversity, KCET, Virudhunagar in 2010, and the M.E. degree from Anna University, RCET, in 2012.Working as Assistant Professor in the department of EEE, *CIET*

A.Jasmine received the B.E. degree from AnnaUniversity, SIT, Dindigul in 2010, and the M.E. degree from Anna University, RCET, in 2012.Working as Assistant Professor in the department of ECE, *UCETW*