International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in

Vol.3., Issue.6., 2015
(Nov.-Dec.,)

RESEARCH ARTICLE

ISSN: 2321-7758

HARDWARE ACCOMPLISHMENT OF RFID CONCURRENT ASSERTION PROTOCOL

SIVA M[1], PAVAN B[2]

[1]PG Scholar, Kakinada institute of Engineering and Technology, A.P.

[2]Assist Prof, Kakinada institute of Engineering and Technology, A.P.

SIVA M

ABSTRACT

RFID technology emerged some time back and was not used that much because of lack of standardization and high costs. Latest technologies have brought costs down and standards are being developed. Today RFID is mostly used as a medium for numerous tasks including managing supply chains, tracking livestock, preventing counterfeiting, controlling building access, and supporting automated checkout. The use of RFID is limited by security concerns and delays in standardization. One of the main drawbacks of RFID technology is the feeble authentication systems between a reader and a tag. In general, "anemic" authentication systems that either divulge the keyword directly over the network or leak decent information while evolving the authentication to allow intruders to obtain or deduce or reckon the keyword. In this paper, we study the RFID tag-reader mutual authentication connives. A hardware implementation of the mutual authentication protocol for the RFID system is asserted. The proposed system was simulated using Modelsim XE II and synthesized using Xilinx synthesis technology. The system has been successfully implemented in hardware using an Altera DE2 board that included an Altera Cyclone II field-programmable gate array (FPGA). Finally, the output waveforms from the FPGA were displayed on the 32702A logic analysis system for real-time verification.

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

I. INTRODUCTION

RFID (Radio Frequency Identification) can be defined as follows: Automatic identification technology which uses radio-frequency electromagnetic fields to identify objects carrying tags when they come close to a reader. Data (identification number for instance) included in the electronic chip of the RFID label can be collected by the reader. This reader can also change the content of the label's memory [1-3].

However, RFID cannot be reduced to one technology. RFID uses several radio frequencies and many types of tag exist with different communication methods and power supply sources. RFID tags generally feature an electronic chip with an antenna in order to pass information onto the interrogator (also known as a base station or more generally, reader) [4].

The assembly is called an inlay and is then packaged to be able to withstand the conditions in

which it will operate. The information contained within an RFID tag's electronic chip depends on its application. It may be a unique identifier (UII, Unique Item Identifier or EPC code, Electronic Product Code, etc.). Once this identifier has been written into the electronic circuit, it can no longer be modified, only read. (This principle is called WORM Write Once Read Multiple). Some electronic chips have another memory in which users can write, modify and erase their own data. These memories vary in size from a few bits to tens of kilobits.

RFID basic tag reader authentication:

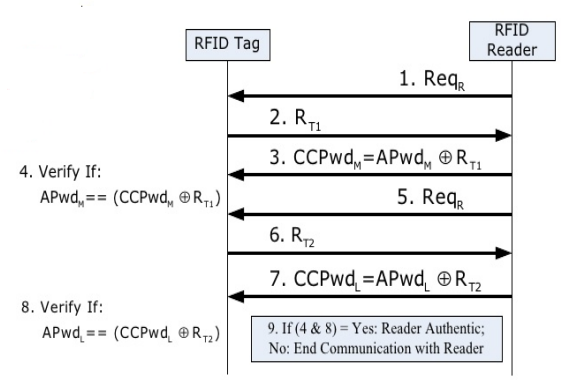

Fig: 1. Tag Reader authentication

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 [4]. The EPC global Class-1 Generation-2 (C1G2) ultrahigh frequency (UHF) RFID standard defines a 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) .

II. EARLIER WORK

In November 2013, EPC global ratified the new EPC Gen2v2 standard (version 2.2). Due to the awareness of security problems on the previous EPC Gen2 standard, the new EPC Gen2v2 standard features a number of backward compatible, optional security features including: Untraceable function to hide portions of data, restrict access privileges and reduce a tag's read range. Support for cryptographic authentication of tags and readers, to verify identity and provenance, as well as to reduce the risk of counterfeiting and unauthorized access.

According to the new EPC Gen2v2 standard, a tag may support one or more cryptographic suites that come from the ISO/IEC 29167 standard. In this paper, we propose a new authentication protocol that is different from those security mechanisms in the ISO/IEC 29167. Our protocol is compliant to the new EPC Gen2v2 standard, and the optional security features mentioned above can be satisfied. The proposed mutual authentication protocol is based on Variable Linear Feedback Shift Register (VLFSR) function which is a lightweight encryption function. A complete baseband system which provides sufficient security level for the passive UHF RFID is implemented at the ASIC level. The baseband system also serves as the central controller of the tag, and it is designed using some low power techniques .

So many security mutual authentication protocols have been proposed for passive UHF RFID. Chine classified these protocols into four classes. The first class is called "full- fledged class" that supports the conventional cryptographic function. The second class is called "simple" that should sup- port random number generator and one-way hashing function on tags. The third class is called "lightweight" protocols that require a random number generator and simple functions like CRC checksum. The fourth class is called "ultra-lightweight" protocols that only involve simple bitwise operation (like XOR, AND, OR, etc.). Due to the use of random number generator and VLFSR sample function, our protocol belongs to the lightweight class.

There are some cryptographic suites in ISO/IEC 29167 standard, but only few of them are suitable for passive UHF RFID, because most suites are based on conventional cryptographic functions. They belong to "full-fledged class". Besides, it seems that adding new lightweight security mechanisms to the standard remains possible.

Although researchers have proposed various mutual authentication protocols for passive

UHF RFID, few protocols were implemented at the ASIC level. Adam S. W. Man et al. employed AES encryption scheme to achieve a secure trans- action for passive UHF RFID at the ASIC level Due to the adoption of traditional AES cryptographic function, the chip area of tag is very large and the cost is high. Huang et al. implemented two lightweight authentication pro- tocols compliant to EPC Gen2 standard by FPGA instead of ASIC. Recently, Lopez et al. have implemented two lightweight authentication protocols compliant to EPC Gen2 standard at the ASIC level, but they didn't submit the results of their implementation with the EPC Gen2 baseband.

III. PROPOSED WORK

In this section, we propose a new mutual authentication protocol that provides security against attacks such as replay, traceability and de-synchronization. It can satisfy the security requirement of the new EPC Gen2v2 standard. According to the standard, every tag has a unique Electronic Product Code (EPC). Before the authentication, the reader should acquire the tag's EPC (UID) by ACK command. Every tag stores a SID (secure ID). The authentication is performed in the secured state of the RFID tag. In the proposed protocol, we assume that the communication between a back-end server and reader is secure. However, communication involving a reader and a tag is insecure, because it is based on radio frequency [14-18]. The following notations are used:

VLFSR	Variable LFSR function
UID	Unique ID of RFID tag
$SIDj$	j th session Secure ID of RFID tag Rr Random number generated by reader $Rt1$ Random number generated by tag
$Rt2$	Random number generated by tag
$\|\|$	Bit series connection
$\oplus$	XOR operation
mj	Secret value used in the j th session

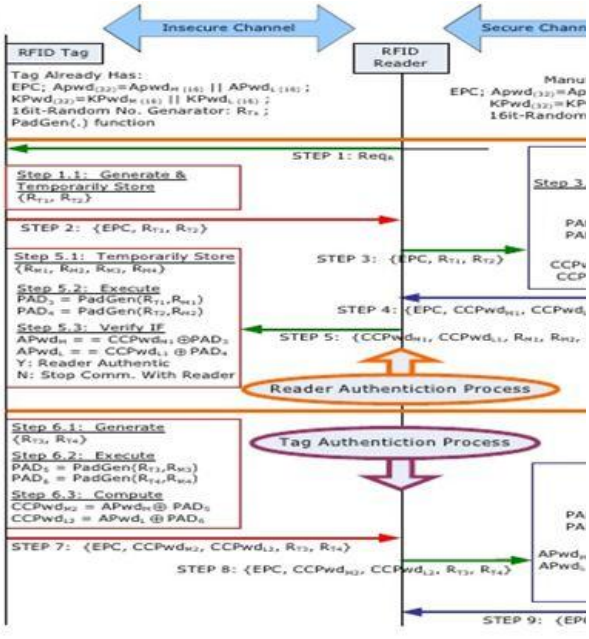

Fig.2. Proposed Tag Reader Authentication Scheme

Phase 1: The reader generates a random number Rr , and transmits the authentication command with Rr to the tag.

Phase 2: When the tag receives the authentication com- mand, it will generate two true random numbers $Rt1$ and $Rt2$ that come from the analog frontend of the tag chip. The tag utilizes the secret value mj and the random number $Rt1$ to get the value of βt by VLFSR function:

$$\beta t = \text{VLFSR}(Rt1 || Rr, mj) \quad (1)$$

Phase 3: The tag transmits βt and ($Rt2 || Rt1) \oplus SIDj$ to the reader.

Phase 4: The reader transmits βt , Rr , $(Rt2 || Rt1) \oplus SIDj$ and *UID* to the back-end server.

Phase 5: This is the back-end server authentication phase. In this phase, the back-end server authenticates the tag and reader, and updates the secret value [19].

The back-end server performs the following steps, based on the received information of each tag.

I. According to the *UID* that comes from a tag to find the matching SID_j in the database.

II. Extracts $Rt1$ and $Rt2$ from $Rt2||Rt$

III. Finds the secret value mj from the Mj table based on $SIDj$.

III. DESIGN AND IMPLEMENTATION

According to the EPC C1G2 protocol, a tag communicates with an interrogator using back scatter modulation, in which the tag switches the reflection coefficient of its antenna between two states in accordance with the data being sent.

A multiplexer was utilized to allow for the selection of EkwdM, EkwdL, BCPwdL, or BCPwdM. The multiplexer then can perform the XOR operation to obtain the following bark-coded keywords or the entry keyword for mutual authentication:

BCPwdM1 = EkwdM ⊕ PAD1 Eq(1)
BCPwdL1 = EkwdL ⊕ PAD2 Eq(2)
EkwdM = BCPwdM2 ⊕ PAD3 Eq(3)
EkwdL = CPwdL2 ⊕ PAD4 Eq(4)

IV SIMULATION RESULTS

Simulations of the proposed design were conducted in the Altera Quartus II design environment and implemented in a Altera Cyclone II EP2C70F896C6 FPGA on an Altera DE2 board.

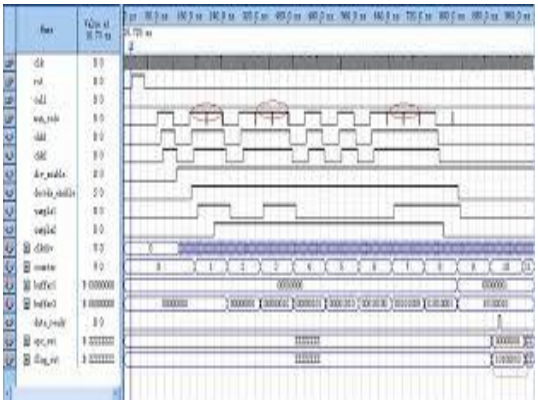

Fig.3. Simulation results for Pad Generation

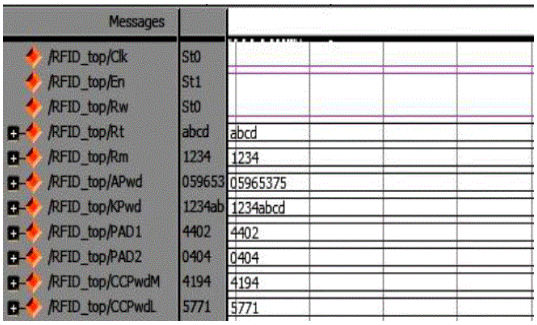

Fig.4. FPGA Pad Generation Results

V. CONCLUSION

In this paper Base on security analysis, our protocol is secure against most of the known attacks. The design of a complete baseband system with the new authentication protocol for passive UHF RFID is presented. Because the use of VLFSR, the traditional encryption function and hash function is not necessary. The main feature of this new approach is to design secure RFID protocol with efficient hardware requirements to meet the demand of secure lowcost RFID systems or WSN. In order to reduce the power consumption, some low power design strategies are adopted in this system. Simulation and implementation results verify that the design is fully compatible with EPC Gen2 standard and demonstrate that low-cost and low-power requirement can be achieved. In addition, as compared with some recently research results about EPC-Gen2 baseband [12-16].

The simulation results for the power performance ofthese different encoding schemes were performed on a Prime ofPower Synopsys platform. Because the EPC Gen2 standard forClass 1 tags supports only a very basic security level, three different types of pad-generation function were examined for tag-reader mutual authentication protocol in the RFID system environment. The proposed scheme is feasible in improving the weakness of the EPCglobal C1G2 communication authen-tication scheme. The hardware implementation of an RFID tag-reader mutual authentication scheme is also presented. This architecture performs the PadGen function and tag's entry and destroy keywords in achieving tag-reader mutual authentication. The verification results on the Altera DE2 board that includes an Altera Cyclone II FPGA board are consistent with the simulation counterparts using Modelsim XE II.

REFERENCES

[1]. L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey,"*Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.

[2]. K. Finkenzeller, *RFID Handbook: Fundamentals and Applictions in Contactless Smart Cards and Identification*. 2nd ed. New York, NY, USA: Wiley, 2003.

[3]. D. Brenk *et al.*, "Energy-efficient wireless sensing using a generic ADC sensor interface within a passive multi-standard RFID transponder," *IEEE Sensors J.*, vol. 11, no. 11, pp. 2698–2710, Nov. 2011.

[4]. S. Shrestha, M. Balachandran, and M. Agarwal, "A chipless RFID sensor system for cyber centric monitoring applications," *IEEE Trans. Microw. Theory Techn.*, vol. 57, no. 5, pp. 1303–1309, May 2009.