Volume : 2 | Issue : 5 | May 2013 • ISSN No 2277 - 8179

Secured Authentication Protocol for RFID System Using XOR Scheme

Engineering

KEYWORDS : Electronic Product Code, Class-1 Generation-2, Radio Frequency Identification system

Mohanavelu S. PG Student,SRM University, Kattankulathur.

Ramya T. Assistant Professor, Department of Electronics and Communication Engineering, SRM University, Kattankulathur

ABSTRACT

Abstract- In an Authentication process of RFID systems the tag/reader/server communicates over an insecure channel due to "weak" authentication protocols. The EPC-C1G-2 specification has some serious security problems, so the password either leak directly over the network or leaks the sufficient information i.e., while performing authentication that allow hackers to deduce or guess the password. To overcome this weak authentication a specially designed pad generation function is used to improve security. The Pad Gen function is used to produce a cover-coding pad to mask the tag's access password before the data transmission. Hence a mutual authentication protocol with XOR scheme is proposed to avoid the data leakage and data traceability during the data transmission .This system model is simulated in Modelsim and synthesized using Xilinx ISE software.

1. Introduction

RADIO-FREQUENCY identification (RFID) is a contact-less identification technology that enables remote and automated gathering and sending of information between RFID tag's or transponders and readers or interrogators using a wireless link. In recent years, RFID technology has gained a rapid acceptance as a means to identify and track a wide array of manufactured objects. It is composed of three main components: tag, reader and Server.

RFID tag's come in a range of forms and can vary in storage capacity, memory type, radio frequency and power capability. Most of these tag's contain only a unique Electronic Product Code(EPC) number and further information about the product is stored on a network of databases, called the EPC-Information Services(EPC-IS).Through the wireless interface, each tag can report data when queried over radio by an RFID reader.

RFID readers can only recognize tag's in proximity; a data tag that is out of range cannot be read by a reader. Secured Authentication protocol is described in this paper. The rest of this paper is organized as follows. In Section 1, we present the Background and previous work in the RFID reader-to-tag authentication protocol in section 2.

The enhanced pad generation (PadGen) function is discussed in Section 3. Section 4 shows implementation results of the proposed mutual authentication scheme. Finally, we conclude this paper in Section 5.

1.2 EPC GLOBAL CLASS-1 GENERATION-2 STANDARD

The EPC global Class-1 Generation-2 (C1G2) ultra-high 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 960MHZ).The standard specifies that a complaint RFID tag should contain a 32-bit kill password (Kpwd) to permanently disable the tag and a 32-bit 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.

2.1 Components of an RFID System

The RFID system consists of various components which are integrated. This allows the RFID system to deduct the objects (tag) and perform various operations on it. The integration of RFID components enables the implementation of an RFID solution. The RFID system consists of following three components

- Tag (attached with an object, unique identification).
- Reader (receiver of tag information, manipulator).
- Server (overall information about the tag and the manufacturer).

2.1.1 Tag's

Tag's contain microchips that store the unique identification (ID) of each object. The ID is a serial number stored in the RFID memory. The chip is made up of integrated circuit and embedded in a silicon chip. RFID memory chip can be permanent or changeable depending on the read/write characteristics. Read-only and rewrite circuits are different as read-only tag's contain fixed data and cannot be changed without re-program electronically.

On the other hand, re-write tag's can be programmed through the reader at any time without any limit. There are three types of tag's the passive, semi-active and active. Semi-active tag's have a combination of active and passive tag's characteristics. So, mainly two types of tag's (active and passive) are being used by industry and most of the RFID system.

2.1.2 Reader

RFID reader works as a central place for the RFID system. It reads tag's data through the RFID antennas at a certain frequency. Basically, the reader is an electronic apparatus which produce and accept a radio signals. The antennas contains an attached reader, the reader translates the tag's radio signals through antenna, depending on the tag's capacity. The readers are expected to collect or write data onto tag (in case) and pass to computer systems.

2.2 RFID System

The RFID tag's 32-bit Access password and 32-bit kill passwords in achieving tag–reader mutual authentication. Their scheme uses two rounds of PadGen to compute a cover-coding pad. The first round performs PadGen over the access password, while the second round performs PadGen over the kill password. The PadGen function is used to create the 16-bit pads for "cover coding" the access password.

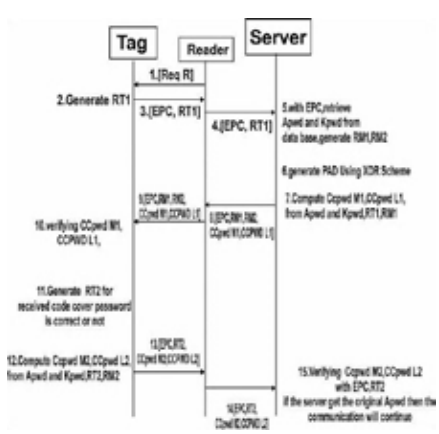

Figure 1: Functional Block Diagram of RFID System.

2.2.1 A Stepwise description of RFID System

1. The reader issues a Req_R_N command to the acknowledged tag.
2. The tag then generates two 16-bit random numbers, namely, R_{T1} and R_{T2}, and backscatters them with its EPC to the reader. The reader forwards these messages to the manufacturer.
3. The manufacturer matches the received EPC to retrieve the tag's access password (A_{pwd}) and kill password (K_{pwd}) from the back-end database.
4. The manufacturer then generates and stores two 16-bit random numbers, namely, R_{M1} and R_{M2}. The "cover-coded passwords" for the 16-bit MSBs (CCPwdM1) and the 16-bit LSBs (CCPwdL1) are computed by the PadGen function.
5. CCPwdM1, CCPwdL1, and EPC along with four 16-bit random numbers, namely, R_{M1}, R_{M2}, R_{M3}, and R_{M4}, generated by the manufacturer are transmitted to the reader, which, in turn, forwards them to the tag for verification.
6. To authenticate the tag, the tag generates another two random numbers RT3 and RT4 along with the received RM3 and RM4 used to compute CCPwdM2 and CCPwdL2 with the PadGen (R_{Ti},R_{Mi}) function.
7. CCPwdM2, CCPwdL2, and EPC along with two 16-bit random numbers, namely, *RT*3 and *RT*4, are transmitted to the reader, which, in turn, forwards them to the manufacturer for verification.

3. XOR Scheme

The PadGen function is used to create the 16-bit Pads for "cover coding" the access password. This scheme is more difficult for recover the access password under the correlation attack or to forge successful authentication under the dictionary attack. The PadGen function is the key function used to produce a cover-coding pad to mask the tag's access password before transmission. The implementation of the PadGen function also requires the random number generator to produce R_{Tx} and R_{Mx}.

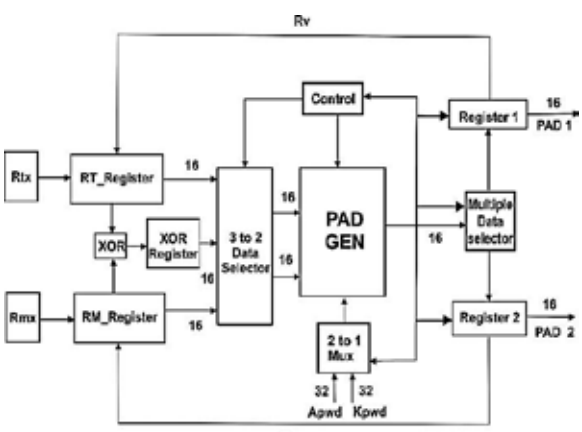

Figure 2: Block Diagram of XOR Scheme

3.1 Access Password

An access password is required before data are exchanged between a reader and a single tag. The access password is a 32-bit 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.

3.2 Kill Password

The access passwords can be used in activating kill commands to permanently shut down tag's, as well as for accessing and relocking a tag's memory. These passwords can be used in activating kill commands to permanently shut down tag's.

3.3 Data Selector

Multiplexers are used as one method of reducing the number of logic gates required in a circuit or when a single data line is required to carry two or more different digital signals. Here the three register are selected simultaneously for XOR operation with control block instructions.

3.1.4 PadGen function based on XOR operation

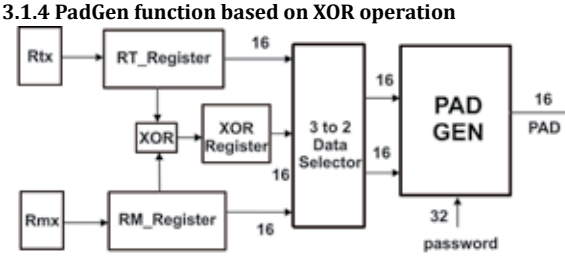

Figure 3: Block Diagram For PadGen Function

Step 1:

$$R_T \oplus R_M = R_T \oplus_M = d_{x1}d_{x2}d_{x3}d_{x4} \quad (1)$$

Step 2:

$$A_{pwd}\text{-PadGen}(R_T, R_T \oplus_M) \quad (2)$$

$$= a_{dt1}a_{dt2}a_{dt3}a_{dt4} \_ a_{dt1} + 16a_{dt2} + 16a_{dt3} + 16a_{dt4} + 16 \times \_ a_{dx1}a_{dx2}a_{dx3}a_{dx4} \_ a_{dx1} + 16a_{dx2} + 16a_{dx3} + 16a_{dx4} + 16 = d_{W1}d_{W2}d_{W3}d_{W4\ (base\ 10)}$$

Step 3:

$$K_{pwd}\text{-PadGen}(R_V, R_W) \quad (3)$$

$$= k_{dV1}k_{dV2}k_{dV3}k_{dV4} \_ k_{dV1} + 16k_{dV2} + 16k_{dV3} + 16k_{dV4} + 16 \times \_ k_{dW1}k_{dW2}k_{dW3}k_{dW4} \times \_ k_{dW1} + 16k_{dW2} + 16k_{dW3} + 16k_{dW4} + 16$$

$$= h_{q1}h_{q2}h_{q3}h_{q4\ (base\ 16)} = PAD1$$

Step 4:

$$R_V \oplus R_W = R_V \oplus R_W = d_{s1}d_{s2}d_{s3}d_{s4\ (base\ 10)} \quad (4)$$

Step 5:

$$K_{pwd}\text{-PadGen}(R_V, R_V \oplus R_W) \quad (5)$$

$$= k_{dV1}k_{dV2}k_{dV3}k_{dV4} \_ k_{dV1} + 16k_{dV2} + 16k_{dV3} + 16k_{dV4} + 16 \times$$

$$\_ k_{ds1}k_{ds2}k_{ds3}k_{ds4} \times \_ k_{ds1} + 16k_{ds2} + 16k_{ds3} + 16k_{ds4} + 16$$

$$= h_{r1}h_{r2}h_{r3}h_{r4\ (base\ 16)} = PAD2.$$

4. Design and Implementation Results

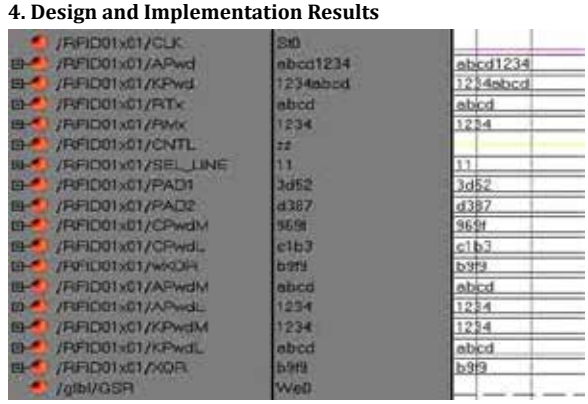

Figure 3: Simulation Output for XOR Scheme

In each PAD function is computed based on one set of (R_{Tx},R_{Mx}), which is transmitted in the open space. In contrast to the PadGen proposed by Konidala et al., the present proposed PAD function is computed based on one set of (R_V ,R_W), which is not transmitted openly. R_V and R_W are computed based on A_{pwd}-PadGen(R_{Tx},R_{Mx}) and A_{pwd}-PadGen(R_{Tx},$R_{Tx} \oplus R_{Mx}$), respectively. PAD1 and PAD2 are then generated by K_{pwd}-PadGen(R_V,R_W) and K_{pwd}-PadGen(R_V,$R_V \oplus R_W$), respectively. The R_V and R_W values were calculated within the tag's and readers. Therefore, an adversary would not be able to correlate all the bits in A_{pwdM} and A_{pwdL}.

1. A_{pwd}-PadGen(R_{Tx},R_{Mx})=$d_{v1}d_{v2}d_{v3}d_{v4}$=R_V.R_{Tx},R_{Mx},and A_{pwd} are selected the inputs for PadGen operation,and the calculation results R_V by XOR-PadGen operation are stored in reg-

Volume : 2 | Issue : 5 | May 2013 • ISSN No 2277 - 8179

ister for further manipulation.

2. A_{pwd}-PadGen(R_I,$R_T \oplus R_M$)=$d_{w1}d_{w2}d_{w3}d_{w4}$=R_W. Through mux selection, R_T , $R_T \oplus R_M$, and A_{pwd} are chosen as inputs for PadGen operation. The calculation result R_W is stored in register for further computation.

3. K_{pwd}-PadGen (R_V,R_W) = $h_{q1}h_{q2}h_{q3}h_{q4}$=PAD1. The PAD1 can then be obtained by mux selecting R_V, R_W, and K_{pwd} as inputs for XOR-PadGen operation.

4. K_{pwd}-PadGen(R_V,$R_V \oplus R_W$)=$h_{r1}h_{r2}h_{r3}h_{r4}$=PAD2. Similarly, the PAD2 can then be obtained using R_V,$R_V \oplus R_W$, along with K_{pwd} for XOR-PadGen operation.

5. Conclusion

To improve the security level of the original reader-to-tag authentication protocol proposed under the EPC C1G2 specification, the PadGen functions are used to protect the Access password against exposure. The main advantage of this XOR scheme is that it does not require the implementation of any special cryptographic hash functions/keys within the tag and a center server/database. The PadGen function was modified to strengthen the security of the mutual authentication scheme. The PadGen functions based on XOR operation and in association with the tag's A_{pwd} and K_{pwd} are used to generate the PAD. The proposed protocol using the manipulated values within the tag's and reader to enhance the PadGen operation is a more secure method for mutual authentication.

REFERENCE

[1] Yu-Jung Huang, Senior Member, IEEE, Wei-Cheng Lin, and Hung-Lin Li, "Efficient Implementation of RFID Mutual Authentication Protocol", ieee transactions on industrial electronics, vol. 59, no. 12, december 2012. | [2] Y. J. Huang, C. C. Yuan, M. K. Chen, W. C. Lin, and H. C. Teng, "Hardware implementation of RFID mutual authentication protocol," IEEE Trans. Ind. Electron., vol. 57, no. 5, pp. 1573–1582, May 2010.. | [3] S. Piramuthu,"Lightweight cryptographic authentication in passive RFID-tagged systems," IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.,vol. 38, no. 3, pp. 360–376, May 2008. | [4] Hung-Yu-chien, "A New ultra-light weight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity" | [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] Information Technology-Radio Frequency Identification for Item Management—Part 6: Parameters for Air Interface Communications at 860 MHz to 960 MHz, ISO/IEC 18000-6:2004/amd:2010. [Online]. Available: http://www.iso.org/ | [7] H. M. Sun and W. C. Ting, "A Gen2-based RFID authentication protocol for security and privacy," IEEE Trans. Mobile Comput., vol. 8, no. 8, pp. 1052-1062, Aug. 2009. |