Mohammad Reshma* et al.
(IJITR) INTERNATIONAL JOURNAL OF INNOVATIVE TECHNOLOGY AND RESEARCH
Volume No.6, Issue No.4, June - July 2018, 8508-8511.

Intend And Accomplishment Of Protected Infrastructure In Disseminated RFID Systems

MOHAMMAD RESHMA
M.Tech Student, Department of ECE, Siddhartha Institute of Technology & Sciences, Narapally, Ghatkesar, Hyderabad, T.S, India.

I V PRAKASH
Assistant Professor, Department of ECE, Siddhartha Institute of Technology & Sciences, Narapally, Ghatkesar, Hyderabad, T.S, India.

Abstract: **Privacy protection is the primary concern when RFID applications are deployed in our daily lives. Due to passive tags that are computationally weak, the non-encryption-based simulation protocols have been recently developed, in which wireless jamming is used. However, the existing private tag access protocols without sharing secrets depends on impractical assumptions hence difficult to deploy. To tackle this issue we redesign RFID architecture by dividing RFID reader into an RF activator and Trusted Shield Device (TSD). Then we proposed new coding scheme namely Random Flipping Random Jamming (RFRJ), to protect the tags contents. Analysis and simulation results validate our distributed architecture with the RFRJ coding scheme, which protects tag's privacy against various adversaries like encoding collision, random guessing attack, correlation attack, eavesdropping, and ghost and leech attack.**

Keywords – **Bit Encoding; Coding; Jamming; Privacy Protection; RFID Security; Secret Communication;**

I. INTRODUCTION

The RFID technology is an electronic tagging technology that allows object to be automatically identified at a distance without a direct line of sight using electromagnetic waves for exchange of data. RFID enables a tremendous amount of applications, such as electric transportation payments, warehouse operations, supply chain management, animal identification, attendance system and more. Objects and their owners are automatically identified by an attached RF tag, which causes the privacy threat to individuals and organizations. Thus privacy protection is our main concern when RFID applications are deployed in our daily lives. Since passive tags are computationally weak devices, encryption based secured simulation are not possible. Hence instead relying traditional cryptographic operations, we employ physical layer technique called jamming to protects tag's data. The issues with the existing solutions, the privacy masking, randomized bit encoding (RBE), dynamic bit encoding (DBE) and optimized DBE (ODBE) takes the Impractical assumptions. In these solutions, all the bits transmitted by tag are masked or jammed where the receiver can read a bit only when 2 bits (the data bit and mask bit) are same. When 2 bits are different, it is assumed that the receiver is unable to recover the corrupted bit. However this assumption is too strong since a reader should be able to detect signals from two different sources. In reality, a receiver of a data bit will decode it as either 0 or 1 without knowing the bit collision. If there is a bit collision, either a signal strength of data bits from tag is stronger than that of jamming bits or vice versa. In other words, depending upon the location of the reader, it can read all the data bits or all the jamming bits. Also masking requires the perfect synchronization between the data bits and mask bit which is difficult to achieve in practice. In addition to this, DBE and ODBE have drawbacks that are

1) Two different source bits are encoded as same bit which fails simulation called encoding collision.

2) Tag's data encoded by this technique could eventually be cracked and repeatedly listen to backward channel (i.e. signal from tag to reader). So none of the above mentioned solutions protects the tag's data from various adversaries. To tackle this issue we put a new RFID architecture and a new coding scheme for protection against various adversary model.

II. LITERATURE SURVEY

Literature survey review is a vital to have an in-depth knowledge of ones intended research area and to learn more about subject matter. In this section we review the previous methods used for securing the data of the tags and what are their demerits which promote us to do this paper. A paper published in [1] by K. Sakai, W. S. Ku, R. Zimmermann and M. T. Sun had discuss about that the Choi and Roh Proposed a privacy masking where the data must be send with the masking ID, but here the receiver should know about the masking knowledge. Lim provides Randomized Bit Encoding (RBE) which provides the protection against guessing attacks for BC But both techniques can't provide protection against the unauthorized access. This paper introduces DBE where it encodes i th source bit based on all preceding (I - 1)th source bit and ODBE where it was design to improve security level from DBE by dynamically changing the maximum codeword length for each source bit. But both techniques have two drawbacks as encoding collision because of source bit and data bit are encoded as a single bit causes simulation to fail and another one is correlation attack where tag's data eventually be cracked so repeatedly listen to the backward channel. In [3] and [6] we studied about practical and real time wireless system because RFID is a real time wireless system and alsi about capabilities of low power wireless jammers because we distributed the RFID reader into RF activator and TSD where TSD is capable of bit level jamming. In [7] authors introducing RBE scheme that strength the privacy protection which is used together with backward channel protection method proposed by Choi and Roh. But this method faces the same-bit problem which then tackle by introducing trusted masking device (TMD) in place of RF reader for transmission of masking signals which makes increase in the cost of system. Weis provides solution by introducing randomized tree walking algorithm which then strengthens by Choi and Roh. But in this technique if application requires more than 60 tags then it troubles singulation overhead. Also it doesn't include termination condition and omits final phase that reads real tag ID. Again in [8] Bolotnyy and Robins introducing Randomized Pseudo random function tree walking algorithm which is mathematically complex.

III. PROPOSED ARCHITECTURE

In this section, we proposed a new RFID system architecture for secure simulations as shown in fig.3.

3.1 Assumptions: We begin with listing physical layer assumptions as follow. 1. Bit level jamming is feasible. 2. An eavesdropper does not know if bit is jammed. 3. Probabilistic flipping model is used for a jamming environment.

3.2 New RFID Architecture An RFID reader is divided into two components, an RF activator and a trusted shield device (TSD). In our new architecture an RF activator queries a tag with long range signal (i.e., forward channel) and energized the tag. In this paper, for simplicity we consider the RF activator as the final destination of a tag's data by assuming the activator forwards the collected data to the back end server. A TSD works as RF listener and is capable of bit level jamming during reception of tag's reply. Hence our architecture consists of three components: an RF activator, a TSD, and RF tag. In this paper, we use random flipping random jamming, for the backward channel protection. A tag will send pseudo ID to TSD under jamming environment. This prevents adversaries from passive attacks, i.e., the random guessing attack, correlation attack, and eavesdropping. RFRJ coding provides protection against adversaries due to jamming while TSD successfully recovers data. A TSD is conceptually similar to the trusted masking device in [7] and medical device shield, but different in following functions.

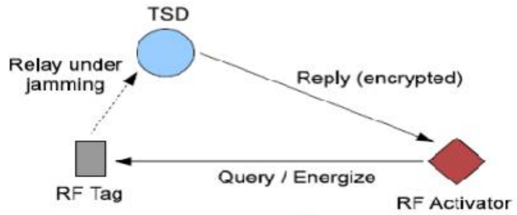

Fig.3 The proposed RFID architecture

1. On overhearing a query from an activator to a tag, a TSD jams a bit in a codeword. Hence jamming is possible as mentioned in assumptions.

2. If an unauthorized reader is tries to access a tag, a TSD jams against all bits of codeword so that the unauthorized reader can't read the content of transmitted data which is done by an authorized activator communicate with a TSD before a simulation process.

3. TSD intermediates only the backward channel.

With our new architecture we can achieve the following goals.

1. The forward channel is protected by having an activator querying tag based on the pseudo ID pace encoded by the RFRJ coding logic.

2. The RFRJ coding logic protects the backward channel against the random guessing attack, correlation attacks, and eavesdropping.

3. As we assume both an activator and a TSD have computational power, the relay channel can protected by the traditional cryptographic operations.

4. The proposed architecture defends against ghost and leech attacks. First, an adversary cannot forward an activator's query to a tag, since a TSD blocks all unauthorized accesses. Second, an adversary cannot obtain a tag's reply due to the jamming by TSD. Hence an adversary cannot impersonate a tag.

3.3 Random Flipping Random Jamming Coding: In this section, we present the random flipping random jamming coding logic.

3.3.1 Definition: Let r be an activator, s be a TSD, and t be an RF tag. An activator which intends to obtain data from a tag sends a query on the forward channel. When the tag replies to the TSD, it encodes every lb bits in the data |into an lc bits codeword with an encoding function E(.). Note that lb is not the length of an ID, but the unit to be encoded into a codeword. A coding scheme for private tag access is defined by the parameters, lb, lc , and C. Here, C is a set of codeword that could be used for encoding. During the transmission of a pseudo ID on the backward channel, the TSD

(IJITR) INTERNATIONAL JOURNAL OF INNOVATIVE TECHNOLOGY AND RESEARCH
Volume No.6, Issue No.4, June - July 2018, 8508-8511.

conducts bit level jamming. On receiving the tag's reply, the TSD decodes the received codeword by a decoding function D(.), and forwards the data to the activator via the relay channel. In general, we call lb-to-lc the RFRJ coding scheme. For instance, the coding scheme with lb = 1 and lc = 4 is said to be the 1 – to – 4 RFRJ coding scheme. The notations utilized in this paper are listed in below table.

Table

Symbol	Definitions
r	The RF activator r
s	The TSD s
t	The RF tag t
b	The bit b
B	The source bits $\{b_1, b_2, b_3, \ldots\}$
c	The codeword c
C	A domain of codeword $C = \{c_0, c_1, c_2, \ldots\}$
l_b	The length of source bits $\lvert B \rvert$
l_c	The length of a codeword $\lvert c \rvert$
E(.)	The function $E: \{0,1\}^{lb} \rightarrow \{0,1\}^{lc}$
D(.)	The function $D: \{0,1\}^{lc} \rightarrow \{0,1\}^{lb}$
p_j	Probability that a jammed bit is flipped
I	The index of a bit in a codeword

In the below fig.4, a source bit is encoded onto a 4-bit codeword. The tag flips the third bit in the codeword and the TSD selects the first bit for jamming. Assume the original codeword is 1010. Since the tag flips the third bit, it will send 1000 over the backward channel. The TSD jams the first bit. Hence, the TSD and eavesdropper will receive X000, where X could be decoded to either 0 or 1. The TSD knows Is , and thus it knows one of the three bits may contain an error after excluding the jammed bit. However, the eavesdropper does not know which bit the TSD jammed or which bit the tag flipped, for the eavesdropper, two out of the 4 bits may contain errors. Thus, the TSD and eavesdropper have a different amount of information to decode the original codeword. In general, for 1b–to–lc , TSD knows that there is a 1 bit error out of (lc – 1) bits while the eavesdropper knows there is a two-bit error out of lc bits at best.

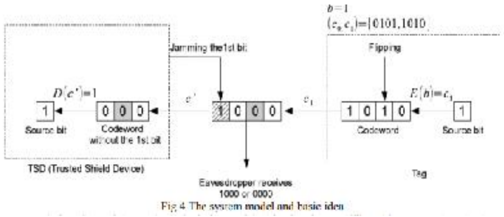

Fig.4 The system model and basic idea

Both the TSD and the tag keep the indexes of the bits they jammed/flipped in secret. The TSD has one of the secrets, but the eavesdropper knows neither of them. Therefore, with the coding scheme the receiver can decode a source bit when one of the (lc – 1) bits is flipped but not when two of the lc bits are flipped. Our new system architecture allows for an RF activator to securely collect RF tag's content without shared secrets of data.

3.4 The Single Bit RFRJ Coding Scheme: We proposed the RFRJ coding scheme with parameter lb=1 and lc=4. Note that lc=3 does not work and lc=4 is the most efficient in terms of communication cost. Let b be a source bit and c be a codeword. The encoding function E(.):{0, 1}◊{0, 1}4 is defined by E(b)=c0 if b=0 and E(b)=c1 if b=1. The encoding function E(.) must ensure that the humming distance between c0 and c1 denoted by H(c0, c1) is four. There are 16 such (c0, c1) pairs that can be used for private tag access. We call them as 4 bit codeword pair.

3.4.1 Definition(Valid 4 bit codeword pair): When lc=4 a codeword pair (c0, c1) corresponding to a source bit pair (0, 1) is said to be valid when the humming distance between c0 and c1 is four i.e., (0000, 1111), (0001, 1110), (0010, 1101), (0100, 1011), (1000, 0111), (0011, 1100), (0110, 1001), (0101, 1010) and (c0, c1). Let c' be the received codeword in which up to 2 bits could be flipped. We define the decoding function as D:{0, 1}4◊{0, 1}. Since a TSD knows the index of the jammed bit, the decoding function ignores the jammed bit. A tag also flips a bit which is unknown to the TSD, and the 3 bits contain the flipped bit after the TSD removes the jammed bit. Let H(b, b', i) be the humming distance between b and b' after removing the ith bit from b and b'. D(c') outputs 0 when H(c', c0, Is)H(c', c1, Is). note that H(c', c0, Is)=H(c', c1, Is) never happens.

Result And Analysis

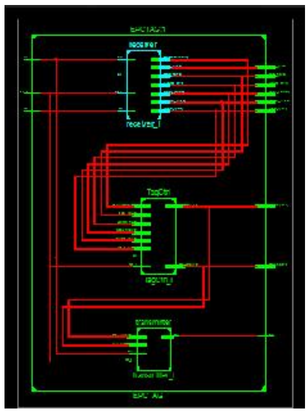

Fig.6 Simulation result with input 0101

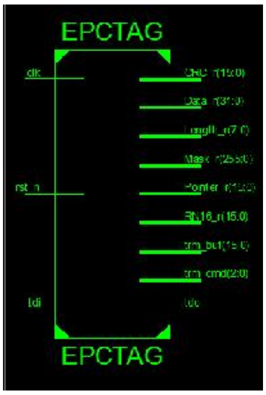

Fig.5. Schematic diagram.

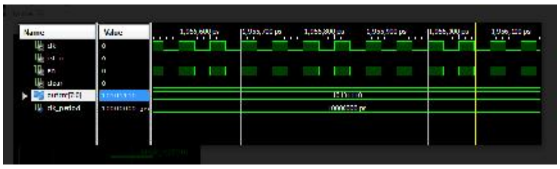

Fig.6. Output results.

IV. CONCLUSION

A number of existing methodologies for the detection of the attacks and their solution have been studied and algorithm was proposed for the same in the RFID system. In this paper, we first proposed a novel distributed RFID architecture which divides the RF reader into two parts: an RF activator and a TSD, each tailoring for a specific function of an RF reader. In addition, we proposed the RFRJ coding scheme, which when incorporated with the new architecture, works against a wide range of adversaries including random guessing attack, correlation attack, ghost and leech attack, and eavesdropping. The physical layer assumptions of the proposed RFID architecture and the encoding scheme are readily available. In addition, the hardware cost of the new architecture is theoretically cheaper than the existing RFID systems. We believe the proposed architecture will serve the foundation of the next generation RFID systems.

V. REFERENCES

[1] K. Sakai, W.-S. Ku, R. Zimmermann, and M.-T. Sun, "Dynamic bit encoding for privacy protection against correlation attacks in RFID backward channel," IEEE Trans. Comput., vol. 62, no. 1,pp. 112–123, Jan. 2013.

[2] L. Sang and A. Arora, "A shared-secret free security infrastructure for wireless networks," ACM Trans. Auton. Adaptive Syst., vol. 7,no. 2, pp. 23:1–23:21, 2012.

[3] M. Jain, J. L. Choi, T. M. Kim, D. Bharadia, S. Seth, K. Srinivasan, P. Levis, S. Katti, and P. Sinha, "Practical, real-time, full duplex wireless," in Proc. 17th Annu. Int. Conf. Mobile Comput. Netw., 2011,pp. 301–312.

[4] L. Sang, "Designing physical primitives for secure communication in wireless sensor networks," Ph.D. dissertation, Department of Computer Science and Engineering, The Ohio State University, 2010.

[5] D. D. Donno, F. Ricciato, L. Catarinucci, A. Coluccia, and L. Tarricone, "Challenge: Towards distributed RFID sensing with software-defined radio," in Proc. 16th Annu. Int. Conf. Mobile Comput. Netw., 2010, pp. 97–104.

[6] L. Sang and A. Arora, "Capabilities of low-power wireless jammers," in Proc. INFOCOM, 2009, pp. 2551–2555.

[7] T.-L. Lim, T. Li, and S.-L. Yeo, "Randomized bit encoding for stronger backward channel protection in RFID systems," in Proc. IEEE 6th Annu. Int. Conf. Pervasive.

[8] W. Choi, M. Yoon, and B.-h. Roh, "Backward channel protection based on randomized tree-walking algorithm and its analysis for securing RFID tag information and privacy," IEICE Trans., vol. 91-B, no. 1, pp. 172–182, 2008.

[9] A. Czeskis, K. Koscher, J. R. Smith, and T. Kohno, "RFIDs and secret handshakes: Defending against ghost-and-leech attacks and unauthorized reads with context-aware communications," in Proc. 15th ACM Conf. Comput. Commun. Security, 2008, pp. 479–490.

[10] Y. Li and X. Ding, "Protecting RFID communications in supply chains," in Proc. 2nd ACM Symp. Inf., Comput.Commun. Security, 2007, pp. 234–241.

[11] J. Myung, W. Lee, J. Srivastava, and T. K. Shih, "Tag-splitting: Adaptive collision arbitration protocols for RFID tag identification," IEEE Trans. Parallel Distrib. Syst., vol. 18, no. 6,pp. 763–775, Jun. 2007.

[12] H. K. H. Chow, K. L. Choy, W. B. Lee, and K. C. Lau, "Design of a RFID case-based resource management system for warehouse operations," Expert Syst. Appl., vol. 30, no. 4, pp. 561–576, Feb.2006.

