International Journal of Engineering In Advanced Research Science and Technology ISSN: 2278-256

January 2017
VOLUME-1
ISSUE-1
Page:7909-15

AN EFFICIENT AND SECURED RFID COMMUNICATION FOR MULTI PURPOSE APPLICATIONS

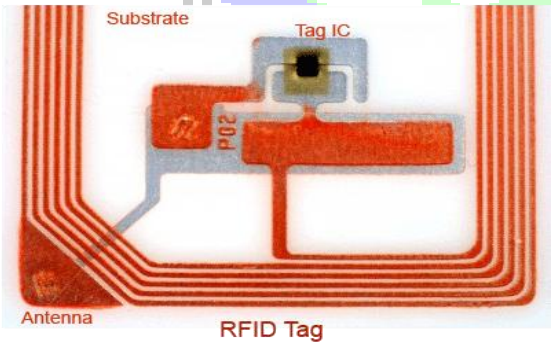
1. GUDAPURI SUDHEER, 2. MOHD.ABDUL SUMER, 3. GADDE RAMA KRISHNA
1. PG Scholar, Dept of ECE, SANA ENGINEERING COLLEGE,KODAD
2. Associate Professor, Dept of ECE, SANA ENGINEERING COLLEGE,KODAD
3. Associate Professor, Dept of ECE, SANA ENGINEERING COLLEGE,KODAD

ABSTRACT:
Radio Frequency Identification (RFID) is an electronic tagging technology that allows objects to be automatically identified at a distance without a direct line-of- sight using an electromagnetic challenge-and-response exchange of data. An RFID system consists of RF readers and RF tags. RF tags are attached to objects, and used as a unique identifier of the objects. Due to the computational power constraints of passive tags, non-encryption-based singulation protocols have been recently developed, in which wireless jamming is used. However, the existing private tag access protocols without shared secrets rely on impractical physical layer assumptions, and thus they are difficult to deploy. To tackle this issue, we first redesign the architecture of RFID system by dividing an RF reader into two different devices, an RF activator and a trusted shield device (TSD). Then, we propose a novel coding scheme, namely Random Flipping Random Jamming (RFRJ), to protect tags' content. Further, as an enhancement clock gating technique is implemented for memory organization schem for power reduction.

KEYWORDS: Random Flipping Random Jamming (RFRJ), Trusted shield device (TSD), clock gating technique, memoryorganization

INTRODUCTION:

RFID has been around since II World War but was viewed as too limited and expensive in functionality for most of commercial use. With advancement in technology, cost of system components has reduced and capabilities have increased, making RFID more popular. Léon Theremin invented a surveillance tool for Soviet Union in the year 1945. This tool retransmitted the incident radio waves along with audio information. Sound



RFID Tag

waves vibrated diaphragm that altered the shape of resonator, modulating reflected sound frequencies. This tool was not identification tag but a secret

listening device. But it is still considered as predecessor of the RFID technology due to it being energized, passive and stimulated by outside electromagnetic waves. Similar technology as IFF transponder was invented in UK in the year 1915 and was regularly used by allies in the II World War for identifying aircrafts as foes or friends. The transponders are used for by powered aircrafts till date. Invented in 1973, device by Mario Cardullo is known to be a true ancestor of the modern RFID. Initially the device was passive and was powered by interrogating signals and had transponder 16 bit memory for application as toll device. The basic patent by Cardullo covers application of RF, light and sounds as the transmission media. Early exhibition of the reflected power RFID tags, semi passive and passive was presented by Robert Freyman, Steven Depp and Alfred Koelle. This portable system used around 12 bit tags and worked at 915 MHz. And the first patent associated with abbreviation of RFID was approved to Mr. Charles Walton in the year 1983.

The role of RFID is not just confined to Aircraft identification anymore; it is also lending a hand in various commercial uses. Asset tracking is one of the most popular uses of RFID. Companies are using RFID tags on the products that might get stolen or misplaced. Almost each type of Radio frequency Identification and Detection system can be used for the purpose of asset management.

Manufacturing plants have also been using RFID from a long time now. These systems are used for tracking parts and working in process for reduction of defects, managing production of various versions and increasing output. The technology has also been useful in the closed looped supply chains for years. More and more companies are turning to this technology for tracking shipments among the supply chain allies. Not just manufacturers but

retailers also are using this RFID technology for proper placement of their products and improvements in the supply chain.
RFID also plays an important role in the access and security control. The newly introduced 13.56 MHz RFID systems provide long range readings to the users. The best part is that RFID is convenient to handle and requires low maintenance at the same time.

ENCRYPTION-BASED PRIVATE AUTHENTICATION:

In this chapter, we present a new encryption-based private authentication proto- col, called Randomized Skip Lists-Based Authentication (RSLA).Radio Frequency Identification (RFID) is widely used to smooth the way of var- ious applications, such as library management [29], transportation payment, natural habitat monitoring, indoor localization [9, 39], and so on. In these systems, the ad- ministrator manages and monitors a large number of objects by reading passive RF tags attached to the objects with an RF reader. To protect the tag's content, low- cost cryptographic operations [40] are conducted during singulation process. Hence, on receiving the tag's reply, the reader must try all keys in the system to and the corresponding key that the tag used in order to decrypt the content. When it comes to a large-scale RFID system, the authentication process can take a long time. To accommodate this issue, a number of private tag authentication protocols with structured key management have been proposed. In these approaches, a unique key and a set of group keys are assigned to each tag. The group keys are shared among several tags and are used to con ne the search space of the unique key corresponding to a tag's reply. Based on how group keys are managed, they are categorized into two types: tree-based [29{32, 41, 42] and group-based protocols [33, 34]. In a tree-based protocol, tags are mapped to leaf nodes in the tree and keys are assigned to internal 14 nodes. Each tag has its unique key and a set of shared keys associated with the nodes from the leaf to the root. By traveling the tree, the reader can securely singulate tags. This results in high authentication efficiency, but discloses a large amount of information once tags in the system are compromised. On the contrary, in a group- based protocol, each tag has two kinds of keys: a unique key and a group key. With this approach, even if one of the group members is compromised, tags in other groups are intact. However, the authentication efficiency of this approach is low. Therefore, for large-scale RFID systems, the performance and privacy/security of key authentication are commonly seen as tradeoffs. In this research, we propose a scheme that provides both good performance and a high level of privacy/security for a large-scale RFID system. Since both tree-based and group-based structures have pros and cons, we take a different approach based on skip lists [43], a data structure with which operations are performed in a logarithmic order like a balanced tree. In our proposed scheme, an interrogator authenticates a tag by traveling skip lists from top to bottom with a random rotation at each level. The analysis and simulation results prove that the proposed scheme is both efficient on authentication complexity and resistant against compromise attacks.

NON-ENCRYPTION-BASED PRIVATE AUTHENTICATION:

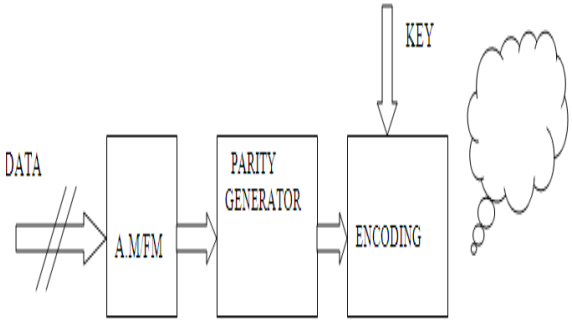
In this chapter, we address non-encryption-based private authentication problem. Since passive tags are computationally weak devices, encryption-based secure singulations [47] are not practical. Instead of relying on the traditional cryptographic operations, recent works [35{37] employ physical layer techniques, i.e, jamming [48], to protect tags' data. With this approach, tags could be securely identified without pre-exchanged shared keys. The issue of the existing solutions, the privacy masking [35], Randomized Bit En- coding (RBE) [36], and Dynamic Bit Encoding (DBE) / Optimized DBE (ODBE) [37], is the impractical assumption. In these solutions, all the bits transmitted by a tag are masked (jammed) under the assumption of an additive channel, where the receiver can read a bit only when two bits (the data bit and mask bit) are the same. When the two 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 the signal strength of data bits from the tag is stronger than that of the jamming bits, or vise versa. In other words, depending on the location of the reader, it can either read all the data bits or all the jamming bits. Also, masking requires the perfect synchronizationbetween data bits and mask bits, which is difficult to achieve in practice. In addition to this, DBE and ODBE have two drawbacks. One is encoding colli- sion, where two different source data bits could be encoded into the same codeword. This causes the singulation process to fail. The other drawback is more serious. Tags' data encoded by DBE or ODBE could eventually be cracked, should an adversary

International Journal of Engineering In Advanced Research Science and Technology ISSN: 2278-256

January 2017
VOLUME-1
ISSUE-1
Page:7909-15

repeatedly listen to the backward channel (i.e., signals from a tag to a reader). This approach is called *the correlation attack*. Moreover, none of theaforementioned solutions protect tags against ghost-and-leech attacks, i.e., impersonation of RF tags, similar to man-in-the-middle attacks. To tackle these issues, we put forth a new RFID architecture and a novel coding scheme for privacy protection against various adversary models. The contributions of this chapter are as follows:

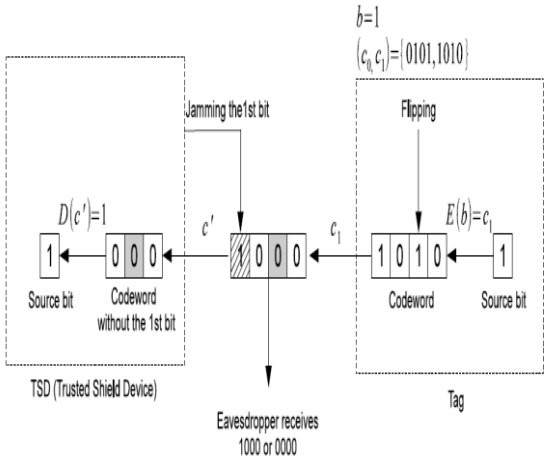
_ We redesign the system architecture of the non-encryption-based private tag access where an RF reader is divided into an RF activator and a TSD.



In order to send data in space, data is needed to be modulated. For that purpose, we are using Amplitude modulation. Error detecting codes should be added to detect any error occurred in space or not. Here, even parity generators are used for that purpose. After that encoding should be takes place to prevent data from hackers. One separate key is used for that encoding purpose. Yielded data is XOR'ed with key to get encoded data.

RANDOM FLIPPING RANDOM JAMMING CODING:

Let *r* be an RF 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 a *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 de_ned by the parameters, *lb*, *lc*, and *C*. Here, *C* is a set of codewords that could be used for encoding. During the transmission of a pseudo ID on the backward channel, the TSD 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.



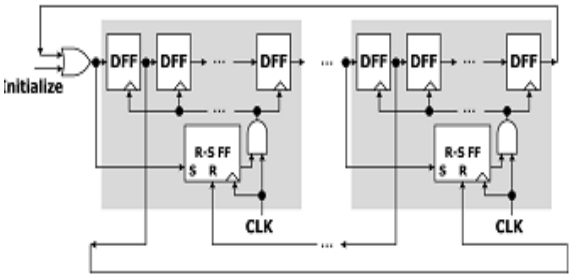
The proposed private tag access protocol works as follows. Suppose an RF acti- vator *r* plans to read an RF tag *t* without disclosing the tag's ID to an eavesdropper. In this section, we _rst consider the length of the encoding unit *lb* to be 1 in this chapter. Our idea can be applied to arbitrary values of *lb* and *lc*, where *lb* < *lc*. On receiving a request, the tag *t* extends a bit into an *lc*-bit codeword, where *lc* _ 4 must hold. When the tag transmits data over the backward channel, it randomly selects a bit in a codeword and intentionally ips it. Note that this process is done before the tag sends out the codeword, so the data sent by the tag always contains a one-bit error. On the other hand, the TSD, which is an RF listener with jamming capability, jams a single bit in the codeword. The jamming causes the selected bitto ip. Let *pj* (0 _ *pj* _ 1) be the probability that the bit jammed by the TSD is ipped. We denote *Is* and *It* as the indexes of the selected bits by the TSD and the tag, respectively. The TSD randomly selects any bit in the _rst half of the *lc* bits codeword, i.e., 1 _ *Is* _ ⌊ 1 2 *lc*⌋ , while a tag randomly selects a bit in the second half of the codeword, i.e., ⌊ 1 2 *lc*⌋ + 1 _ *It* _ *lc*. By doing this, we can guarantee that the TSD and the tag do not select the same bit. Thus, the codeword received by the TSD or an eavesdropper contains a two-bit error when jamming ips the *Is*-th bit and a one-bit error when jamming fails. For instance, in Figure 3.4, a source bit is encoded into a 4-bit codeword. The tag ips the third bit in the codeword, which is colored gray, and the TSD selects the _rst bit for jamming, which is crossed off. Assume the original codeword is 1010. Since the tag ips the third bit, it will send 1000 over the backward channel. Meanwhile, the TSD jams the

International Journal of Engineering In Advanced Research Science and Technology ISSN: 2278-256

January 2017
VOLUME-1
ISSUE-1
Page:7909-15

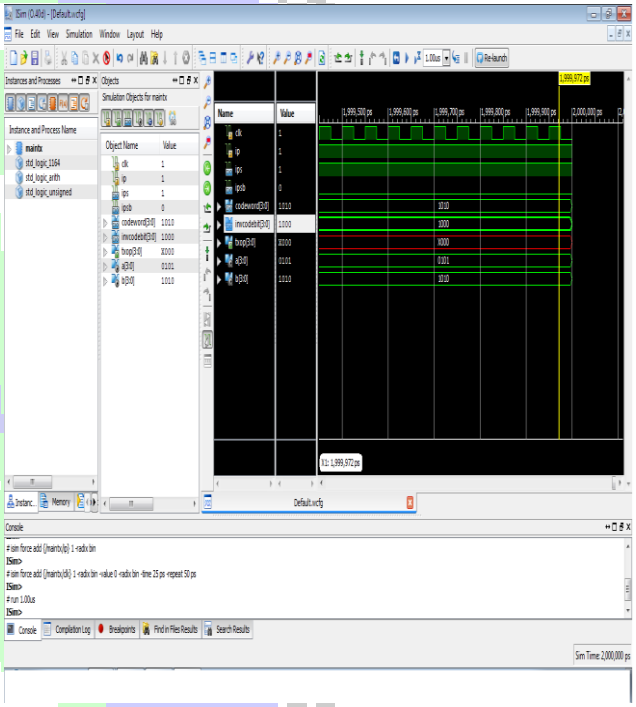
_rst bit. Hence, the Assume the original codeword is 1010. Since the tag ips the third bit, it will send 1000 over the backward channel. Meanwhile, the TSD jams the _rst bit. Hence, the TSD and the eavesdropper will receive *X*000, where *X* could be decoded to either 0 or 1. The TSD knows *Is*, and thus it knows one of the three bits may contain an error after excluding the jammed bit. However, the eavesdropper does not know which bitthe TSD jammed or which bit the tag ipped. For the eavesdropper, two of four bitsmay contain errors. Thus, the TSD and the eavesdropper have a differentamount ofinformation to decode the original codeword. In general, for 1-to-*lc*, TSDknows that there is a one-bit error out of (*lc* □ 1) bits while the eavesdropper knows there is a wo-bit error out of *lc* bits at best. Both the TSD and the tag keep the indexes of the bits they jammed/ipped insecret. 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 ofthe (*lc*□1) bits is ipped but not when two of the *lc* bits are ipped. Our new system architecture and our proposed private access protocol allow for an RF activator to securely collect RF tags' content without shared secrets. TSD and the eavesdropper will receive *X*000, where *X* could be decoded to either 0or 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 ipped. For the eavesdropper, two of four bits may contain errors. Thus, the TSD and the eavesdropper have a different amount of information to decode the original codeword. In general, for 1-to-*lc*, TSD knows thatthere is a one-bit error out of (*lc* □ 1) bits while the eavesdropper knows there is a two-bit error out of *lc* bits at best. Both the TSD and the tag keep the indexes of the bits they jammed/ipped in secret. The TSD has one of the secrets, but the eavesdropper knows neither ofthem. Therefore, with the coding scheme the receiver can decode a source bit when one of the (*lc*□1) bits is ipped but not when two of the *lc* bits are ipped. Our new systemarchitecture and our proposed private access protocol allow for an RF activator to securely collect RF tags' content without shared secrets. Our new system architecture and our proposed private access protocol allow for an RF activator .

Modified ring counter architecture for memoery organzation:



The above block diagram shows the power controlled Ring counter.First, total block is devided into two blocks. Each block is having one SR FLIPFLOP controller

RESULT:



CONCLUSION:

Security/privacy issue in RFID is one of the most significant concerns when we deploy RFID applications to the real world. Therefore, in this dissertation, we address private tag authentication and data verification problems. The private authentication safeguards tags' content during a singlation process and verify the authenticity of tags. Finally, propose 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 propose the RFRJ coding scheme, which when incorporated with the new architecture, works against a wide range of adversaries.

International Journal of Engineering In Advanced Research Science and Technology ISSN: 2278-256

January 2017
VOLUME-1
ISSUE-1
Page:7909-15

REFERENCES:

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

[2] 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.

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

[4] 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.

[5] 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 Comput. Commun., 2008, pp. 40–49.

[6] 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.

[7] 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.

[8] 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.

[9] A. D. Wyner,"The wire-tap channel," Bell Syst Tech. J., vol. 54, no. 8, pp. 1355–1387, 1975.

[10] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, "They can hear your heartbeats: Non-invasive security for implantable medical devices," in Proc.ACMSIGCOMMConf., 2011, pp. 2–13.

[11] H. Delfs and H. Knebl, Introduction to Cryptography: Principles and applications, 2nd ed. New York, NY, USA: Springer, 2007.

[12] 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.

[13] 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.

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

[15] EPCglobal, EPC radio-frequency identity protocols Class-1 Generation-2 UHF RFID Protocol for communications at 860 MHz-960MHz version 1.0.9 [Online]. Available: http:www.epcglobalinc. org/standards, 2005.

[16] J. B. Wilker, "An extremum problem for hypercubes," J. Geometry, vol. 55, pp. 174–181, 1996.

[17] 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

International Journal of Engineering In Advanced Research Science and Technology ISSN: 2278-256

January 2017
VOLUME-1
ISSUE-1
Page:7909-15