International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue-17
December 2017

# Implementation of Modified RFID System Architecture for Secure Application

G Navya & K.Sivanagi Reddy
PG Scholar, Dept of ECE, SWEC, Hyderabad, TS, India

Associate Professor Dept of ECE, Hyderabad, TS, India

## ABSTRACT

*Security insurance is the essential concern when RFID applications are sent in our day by day lives. RFID (Radio Frequency Identification) is a technology whose employment will certainly grow in the following years. It is therefore necessary to consider the security issues that come out from the implementation of that type of systems. In this paper this present an approach to solve the security problems in RFID systems by designing a native security layer based on authentication and encryption algorithms. Because of the computational power requirements of inactive labels, non-encryption-based singulation conventions have been as of late created, in which remote is utilized. The current private label get to conventions without shared mysteries depend on unrealistic physical layer suspicions, and consequently they are hard to send. To handle this issue, initially overall the engineering of RFID framework by partitioning a RF per user into two unique gadgets, a RF activator and a trusted shield gadget (TSD). At that point, The propose of a novel coding plan, to be specific Random Flipping Random Jamming (RFRJ), to ensure label's substance. Investigation and recreation comes about approve and appropriated design with the RFRJ coding plan, which guards label's security against different opponents including the arbitrary speculating assault, relationship assault, phantom and-parasite assault, and eavesdropping. In this re-enactment The I sim test system And utilization of Xilinx 13.2version programming, in expansion the increment of bit length have been introduced, so the favorable position is that Reduced delay.*

**KEYWORDS:** RF activator, TSD, RFRJ, I sim test system.

## 1. 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. **Radio-frequency identification** (**RFID**) uses electromagnetic fields to automatically identify and track tags attached to objects. The tags contain electronically stored information. Passive tags collect energy from a nearby RFID reader's interrogating radio waves. Active tags have a local power source (such as a battery) and may operate hundreds of meters from the RFID reader. Unlike a barcode, the tag need not be within the line of sight of the reader, so it may be embedded in the tracked object. RFID is one method for Automatic Identification and Data Capture[1], Bars code is one of the most popular automatic identification technologies used for many years in inventory control systems and supply chain management like RADIO empower an enormous measure of uses, for example, recurrence ID (RFID) innovations inventory network administration [2], electric transportation installment, and stockroom operations [3].and their proprietors are consequently distinguished by an appended RF tag, which makes the protection danger people and associations. In this way, security assurance is the essential concern when RFID applications are conveyed in our everyday lives.

Since inactive labels are computationally frail gadgets, encryption-based secure re-enactment [4] are not reasonable and movement tracking [5]–[6]. Rather than depending on the conventional cryptographic operations, late works [7], [8], [9] utilize physical layer procedures i.e., fix [10], to ensure labels' information. With this approach, labels could be safely distinguished without pre exchanged shared keys. The issue with the current arrangements, the security concealing, randomized bit encoding (RBE), and dynamic piece encoding (DBE)/enhanced DBE (ODBE), is the unreasonable suppositions. In these arrangements, every one of the bits transmitted by a tag are masked (stuck) under the presumption of an added substance channel, where the beneficiary can read somewhat just when 2 bits (the information bit and cover bit) are the same. At the point when the 2 bits are extraordinary, it is expected that the collector can't recuperate the defiled bit. Be that as it may, this presumption is excessively solid since a per user must to have the capacity to identify signals from two unique

sources. In all actuality, a collector of an information bit will translate it as either 0 or 1 without knowing the bit crash. On the off chance that there is a bit impact, either the flag quality of information bits from the tag is more grounded than that of the fix bits, or tight clamp versa. As it were, contingent upon the area of the per user, it can either read every one of the information bits or all the fix bits. Likewise, covering requires the ideal synchronization between information bits and mask bits, which are hard to accomplish by and by read every one of the information bits or all the fix bits. Likewise, covering requires the ideal synchronization between information.

The rest of this paper is organized as follows in Section 2 provides total background information for this research. The design of new RFID architecture in Section no 3 and propose the RFRJ coding scheme in section 4.generlizaton of the RFRJ coding scheme is explained in section 5 security analysis are provided and discussion of bit increment length in Section 6 and simulation results are expressed in section 7.In section 8 , section 9 concludes this paper.

## 2. LITERATURE SURVEY

Recent years have seen much developing consideration on RFID security. In any case, little work has been performed to address the security issues with regards to production network administration, which is precisely the real field for RFID applications. Existing RFID arrangements can't be connected straight forwardly in this field due to an arrangement of exceptional RFID security prerequisites to be tended to for production network administration. The real commitment of this paper is to recognize the novel arrangement of security prerequisites in supply affixes and to propose a useful plan of RFID correspondence conventions that fulfill the security necessities. In the past, the determination of assets to execute different distribution centre operation administrations was done exclusively by specialists. In this paper, a RFID-based Resource Management System (RFID-RMS) is intended to help clients to choose the most appropriate asset use packages for taking care of distribution centre operation arranges by recovering and examining valuable learning from a case-based information stockroom for arrangements in both efficient and financially calculating way. Furthermore, an unadulterated basic straight programming model utilizing a branch and bound calculation to characterize the ideal travel separation of forklifts is likewise created and In this paper, it present a randomized bit encoding plan that can strengthen the security assurance on RFID tags. This operation utilized together with the inverted channel technique proposed by Choi and Roh in \cite{choi}, which serves to ensure the interesting identifier of a RFID tag from the above given statement to short proximity eavesdroppers. Choi and Roh's strategy faces the `same-bit' issue, in which a few bits of the one of a kind identifier could be unveiled, along these lines uncovering basic data. Our proposed plot eases the `same-bit' issue to an immaterial level. Besides, we propose an upgraded framework demonstrate that can shield the special label identifier from the above given statement against busybodies, as well as against unapproved questioners also.

## 3. MODIFIED CODING SCHEME FOR RFID COMMUNICATION

### 3.1 INTRODUCTION

Radio frequency Identification (RFID) is in the broadest sense a technology that allows unique identification of objects by the use of radio signals [11]. If we use this general definition for RFID we can see that many RFID systems are already in use today, for example in access control cards for admission to buildings and cars, payment systems on toll roads and gas stations, the tracking of library books and with skiers using ski lifts.

A signal is sent by a reader to a transponder or tag, which wakes up and either reflects back a signal (passive system) or broadcasts a signal (active system) using its own power source, for example an onboard battery, back to the reader. A passive RFID tag has the advantage of being smaller and having a longer lifespan as it does not contain a battery. The active tag on the other hand, has an increased range and offers increased reading reliability. The most important factor that separates these two types of tags is the cost. Active tags are at least a factor 10 more expensive than passive tags. Passive tags are now available in large quantities for 10 cents a piece. The signal that an RFID tag transmits is usually a serial number of 64 or 96 bits. This serial number can be set by the manufacturer of the tag or be programmed by the end user depending on the type of tag that is used. Some tags only allow for one serial number to be written to the tag, which will then remain the same for the rest of its lifespan. Other tags allow unlimited updates of the serial number. For a complete and concise treatment of the technical aspects of RFID refer the reader to [12].

### 3.2 REQUIREMENT OF THE PROJECT

The proposed dispersed RFID engineering physically guards labels against Illusion and-parasite assaults. The proposal of novel coding plan, named irregular flipping and arbitrary fix (RFRJ), to shield the regressive channel from reserved enemies, i.e., the irregular speculating assault, relationship assault, and listening in. In this plan, a tag/TSD arbitrarily flips/sticks a bit in a codeword and keeps the list of the bits in mystery. RFRJ ensures that the TSD can get better of a tag's with one of the insider facts, yet a enemy can't get the labels. Since the inverter channel is ensured by the RFRJ coding plan, that can secure the forward channel (i.e., signals from a per user to a tag) by having a RF activator questioning in light of encoded information (or pseudo ID) space by RFRJ. Now sum up the RFRJ coding plan with the subjective source bits and codeword lengths. What's more, it demonstrate the greatest data rate of our RFRJ conspire that accomplishes the ideal mystery is 0.25. It direct hypothetical examinations for security of the proposed conspire, and demonstrate that RFRJ gives consummate assurance against reserved assaults in so far as fix is effective.

## 3.3 Physical Layer Security

Physical layer security has been recently recognized as a promising new design paradigm to provide security in wireless networks. In addition to the existing conventional cryptographic methods, physical layer security exploits the dynamics of fading channels to enhance secured wireless links. In this approach, jamming plays a key role by generating noise signals to confuse the potential eavesdroppers, and significantly improves quality and reliability of secure communications between legitimate terminals [13]. Jamming attack is a serious threat to the wireless communications. Reactive jamming maximizes the attack efficiency by jamming only when the targets are communicating, which can be readily implemented using software-defined radios. In this paper, explore the use of the multi-input multi-output (MIMO) technology to achieve jamming resilient orthogonal frequency-division multiplexing (OFDM) communication[14] This is an unfavorable scenario for secrecy performance as the system is interference-limited. In the literature, assuming that the receiver operates in half duplex (HD) mode, the aforementioned problem has been addressed via use of cooperating nodes who act as jammers to confound the eavesdropper [15]. Cooperative jamming is an approach that has been recently proposed for improving physical layer based security for wireless networks in the presence of an eavesdropper. While the source transmits its message to its destination, a relay node transmits a jamming signal to create interference at the eavesdropper. In this paper, a scenario in which the relay is equipped with multiple antennas is considered. A novel system design is proposed for determining the antenna weights and transmit power of source and relay, so that the system secrecy rate is maximized subject to a total transmit power constraint, or, the transmit power is minimized subject to a secrecy rate constraint. Since the optimal solutions to these problems are difficult to obtain, suboptimal closed-form solutions are proposed that introduce an additional constraint, i.e., the complete Nulling of jamming signal at the destination[16].

Another application of physical layer security with jamming is the protection of medical devices in [17]. Wireless communication has become an intrinsic part of modern implantable medical devices (IMDs). Recent work, however, has demonstrated that wireless connectivity can be exploited to compromise the confidentiality of IMDs' transmitted data or to send unauthorized commands to IMDs—even commands that cause the device to deliver an electric shock to the patient. A shield is developed to intermediate all the communications between a medical device of patient and a reader from a doctor. A shield is capable of full-duplex communication, and protects the channel between a medical device and itself by jamming. On detecting an unauthorized readers access the shield interrupts the communication by jamming all transmitted bits .The authors implemented the shield with a small portable device that looks like a necklace and thus eavesdropper is almost impossible since an adversary must be at a very close position to the shield.

## 3.4 JAMMING MODELS

- Detect jamming by RSS.
- Detect jamming by PDR.
- Detect jamming by RSS & PDR.

Reactive jammers. Reactive jammers are aware of the target communication systems. They stay quiet when the channel is idle, but start transmitting radio signals (or even meaningful signals) to undermine ongoing communication as soon as they sense activity on the wireless channel.
Non-reactive jammers. Nonreactive jammers are not aware of any behavior of legitimate nodes and transmit the radio interference over the wireless channel following their own jamming strategies.

General model—In this model, P ½b0 ¼ 0jb ¼ 0; bj ¼ 0þ P½b0 ¼ 0jb ¼ 0; bj ¼ 1 ¼ 1 and P½b0 ¼ 0jb ¼ 1; bj ¼ 0 P½b0 ¼ 0jb ¼ 1; bj ¼ 1 ¼ 1. The likelihood that b0 ¼ 1 is comparative. This sticking model accomplishes idealize mystery, since the likelihood that the beneficiary interprets

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue-17
December 2017

b0 ¼ 0 is 0.5 at whatever point the sticking bits are really irregular.

## 3.5 Distributed RFID Systems

In the customary RFID framework, a RF per user has two parts, a transmitter (i.e., question transmission/empowering labels) and an audience (i.e., tuning in to a label's answer) as appeared in Fig. 1a, where a precious stone speaks to the transmission capacity of a per user, a circle speaks to the listening capacity of a per user, and a rectangle speaks to a tag. The correspondence scope of the regressive channel is substantially shorter than that of the forward channel, and in this manner per users must be sent in light of the short-run in reverse channel to get to all labels in the district as appeared in Fig.1

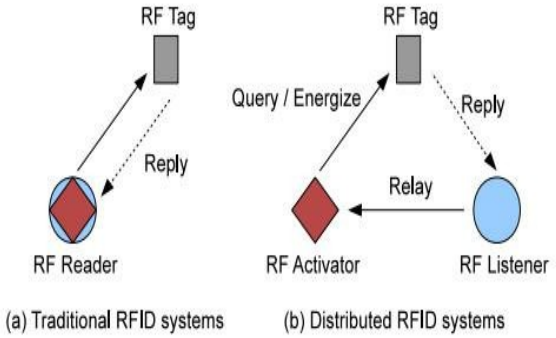


Fig 1.Distributed RFID System

## 3.6 Proposed System Architecture

The Proposed architecture specifies in new RFID system architecture for a secure singulation as in below figure.

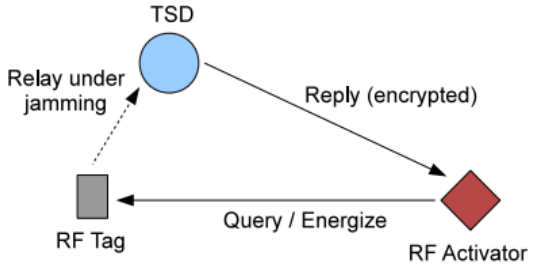


Fig 2. Proposed RFID architecture

As before discussed in Section 3.3 and 3.4 about physical layer security and bit level jamming. The new RFID architecture has been implemented. The below diagram shows difference in traditional RFID system and Distributed RFID system area utilizations.

The New RFID Architecture An RF reader and an Rf activator , further an RF reader divided into 2 components an RF activator and a TSD(Trusted Shied Device) device. In New Architecture an RF Activator Queries a tag with a long range signal( i.e Forward channel) and energies the tag. At TSD receives tag's reply with a short range signal(i.e Backward channel) an it send reply to the activator viq an encrypted applications , a reader forwards tags data to the back-end server. For simplicity in this paper consider the RF activator as the final destination of the tags data by assuming the activator forwards collected data to the back-end server. A TSD works as on RF listener and it is capable of bit level jamming during reception of a tags reply. Therefore new RFID System architecture consists of 3 components: an RF activator, a TSD , and RF tags

The introducing of new coding scheme of RFRJ technique for forward channel. A tag will send encoded data to TSD under jamming environment. Such that we can control passive and eavesdropping attacks, such that RFRJ coding scheme ensures that eavesdroppers cannot decode the original data due to jamming technique. While TSD successfully recovers the recovers the original data from the imperfect data received from RF tag.

When an unauthorized reader tries to access tag a TSD jams against all bits of codeword's so that unauthorized reader cannot read the content of the transmitted data.

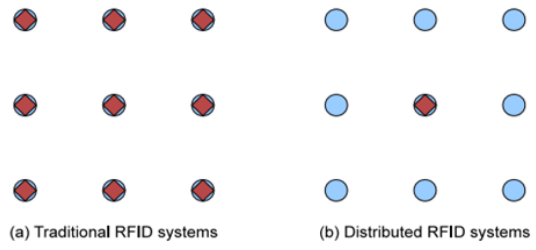


Fig 3.Distributed RFID System deployment

The above figures shows the distributed RFID system and traditional system. In traditional RFID the 9 listeners (circles) and nine transmitters (diamonds) are required for data transmission where as distributed system required only one transmitter and 9 listeners such that the cost reduction is reduced for more reliable and secure data transmition.

**RANDOM FLIPPING RANDOM JAMMING**

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue-17
December 2017

The RFRJ technique works as the irregular flipping arbitrary Fix of coding plan. Let 'r' be a RF activator, 's' be a TSD, and 't' be a RF tag. An activator which means to acquire information from a tag sends an inquiry on the forward channel. At the point when the label answers to the TSD, it encodes each lb bits in the information into a lc bits code word with an encoding capacity Eð:þ. Note that lb isn't the length of an ID, however the unit to be encoded into a codeword. A coding plan for private label get to is characterized by the parameters, lb, lc, and C .He Both the TSD and the label keep the records of the bits they stuck/flipped in mystery. The TSD has one of the mysteries, hence this manner we can Random flipping and Random Jamming bits have been implemented.

## Implementation of RFRJ technique for codeword 1-to-4

The 1 to 4 coding technique the case of a tag replies a codeword 1010. Let TSD jams the first bit and tag flips the Third bit. If the jamming is succeeds, an eavesdropper will receive X000. The TSD knows jammed bit it could be either 0 or 1 and it also knows the received bit contains an error after excluding jammed bit, Thus the eavesdropper cannot decode the original codeword because he didn't knows which bit is jammed and flipped, So by using 1-to -4 coding technique is efficient and secure because its information is 1/3, the perfect secrecy cannot achieve.

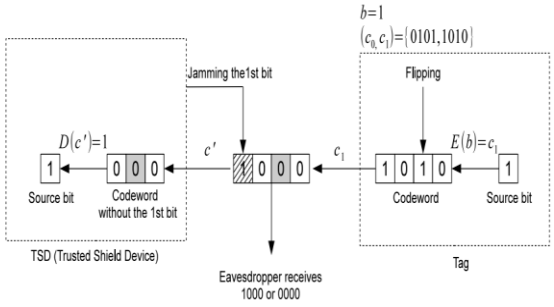


Fig 4.The 1:4 code word with RFRJ technique

## 3.7 Extension of Proposed RFID architecture

### 1 to 6 coding technique:

The 1 to 6 coding technique is the Extension of Proposed RFID Architecture Now a tag replies a codeword 100001. Now TSD jams 1st bit and tag flips third bit . the eavesdropper receives 000101.The TSD knows jammed bit it could be either 0 or 1 and it also knows the received bit contains an error after excluding jammed bit, Thus the eavesdropper cannot decode the original codeword because he didn't knows which bit is jammed and flipped. So by using 1-to -6 coding technique it is more efficient and secure because its information is 1/3, the perfect secrecy cannot achieve.

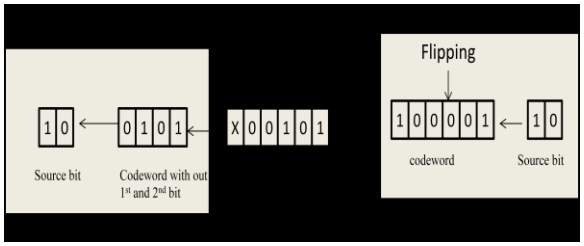


Fig 5 The 1:6 code word with RFRJ technique

## 4. RESULTS AND APPLICATIONS

The Spartan®-3 Generation of FPGAs contains five platforms, choosing Spartan 3E the following simulations Exists.

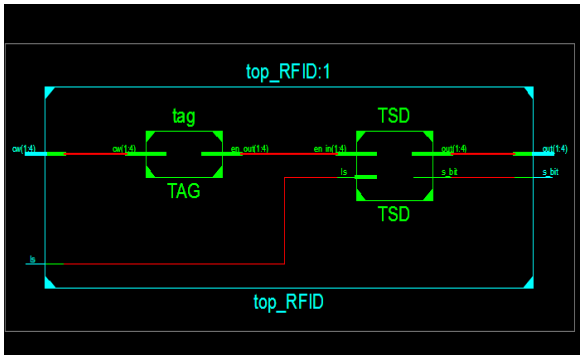


Fig 5: RTL Schematic of proposed system.

| Device Utilization Summary (estimated values) | | | [-] |
|---|---|---|---|
| Logic Utilization | Used | Available | Utilization |
| Number of Slices | 1 | 704 | 0% |
| Number of 4 input LUTs | 1 | 1408 | 0% |
| Number of bonded IOBs | 7 | 108 | 6% |

Fig 6: Area report of proposed system.

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue-17
December 2017

```
Data Path: cw<2> to out<2>
                           Gate     Net
  Cell:in->out      fanout   Delay   Delay  Logical Name (Net Name)
  ----------------------------------------  ------------
   IBUF:I->O             3   1.106   0.451  cw_2_IBUF (cw_2_IBUF)
   OBUF:I->O                 3.169          out_2_OBUF (out<2>)
  ----------------------------------------
  Total                      4.726ns (4.275ns logic, 0.451ns route)
                                     (90.5% logic, 9.5% route)
```

\ Fig 7: Timing report of proposed system.

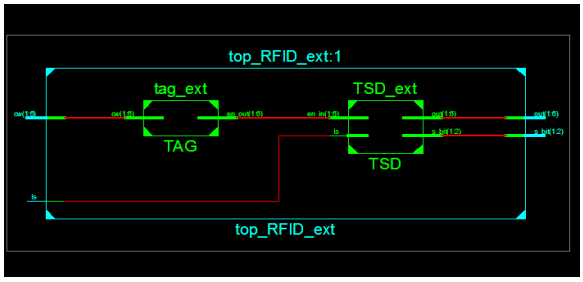


Fig 8: RTL Schematic of Extension system.

| Device Utilization Summary (estimated values) | | | [-] |
|---|---|---|---|
| **Logic Utilization** | **Used** | **Available** | **Utilization** |
| Number of Slices | 1 | 4656 | 0% |
| Number of 4 input LUTs | 1 | 9312 | 0% |
| Number of bonded IOBs | 14 | 232 | 6% |

Fig 9: Area Report of Extension system.

```
Data Path: cw<2> to out<2>
                           Gate     Net
  Cell:in->out      fanout   Delay   Delay  Logical Name (Net Name)
  ----------------------------------------  ------------
   IBUF:I->O             3   1.106   0.451  cw_2_IBUF (cw_2_IBUF)
   OBUF:I->O                 3.169          out_2_OBUF (out<2>)
  ----------------------------------------
  Total                      4.726ns (4.275ns logic, 0.451ns route)
                                     (90.5% logic, 9.5% route)
```

Fig 10: Timing Report of Extension System

## COMPARISON TABLE:

| Parameter | Proposed system | Extension system |
|---|---|---|
| Timing | 0.472ns | 0.472ns |
| Power | 0.014W | 0.034W |
| Area % Utilization | 6% | 6% |

## Applications:

This project is mainly applicable in

1. Used in MNC's (To grant access to employees)

2. Security at Shopping Malls.

## 5. CONCLUSION:

A system is proposed for secure data transmission is designed in Xilinx System Generator. The system is in behavioral model so code is written in behavioral model and generated by using Xilinx system generator and simulation And Synthesis is performed, Due to this proposed system the optimized area and power are obtained. Based on these proposed system the increment of bit length applied i.e 1-to-6 code word is done for more secure data transmission.

## REFERENCE

[1] Automatic Identification and Data Collection (AIDC) Archived May 5, 2016, at the Wayback Machine.

[2] H. K. H. Chow, K. L. Choy, W. B. Lee, and K. C. Lau, "Plan of a RFID case-based asset administration framework for stockroom operations," Expert Syst. Appl., vol. 30, no. 4, pp. 561– 576, Feb. 2006.

[3] A. Juels,"RFID security and protection: An examination review," IEEE J. Sel. Ranges Commun., vol. 24, no. 2, pp. 381– 394, 2006

[4] L. M. Ni, Y. Liu, Y. C. Lau, and A. Patil, "LANDMARC: Indoor Location Sensing Using Active RFID," in ACM Wireless Networks, 2004.

[5] Y. Liu, L. Chen, J. Pei, Q. Chen, Y. Zhao, "Mining Frequent Trajectory Patterns for Activity Monitoring Using Radio Frequency Tag Arrays," in Proceedings of IEEE PerCom, 2007.

[6] Y. Liu, Z. Yang, X. Wang, and L. Jian, "Location, Localization, and Localizability," in Journal of Computer Science and Technology, 2010.

[7] W. Choi, M. Yoon, and B.- h.Roh, "In reverse channel assurance in view of randomized tree strolling calculation and its investigation for securing RFID label data and protection," IEICE Trans., vol. 91-B, no. 1, pp. 172– 182, 2008.

[8]T.- L. Lim, T. Li, and S.- L.Yeo, "Randomized piece encoding for more grounded in reverse direct insurance in RFID frameworks," in Proc. IEEE sixth Annu.Int. Conf. Unavoidable Comput. Commun., 2008, pp. 40– 49.

[9]K. Sakai, W.- S.Ku, R. Zimmermann, and M.- T. Sun, "Dynamic piece encoding for security insurance against connection assaults in RFID in reverse channel," IEEE Trans. Comput., vol. 62, no. 1, pp. 112– 123, Jan. 2013.

[10 ]L. Sang, "Planning physical primitives for secure correspondence in remote sensor systems," Ph.D. exposition, Department of Computer Science and Engineering, The Ohio State University, 2010.

[11]S. Garfinkel and B. Rosenberg, “RFID Applications, Security and Privacy”, Addison-Wesley, July 2005.

[12]K, Finkenzeller, “RFID-Handbook, Second Edition”, Wiley & Sons, April 2003.

[13] Kanapathippillai Cumanan, Hong Xing, Peng Xu, Gan Zheng, Xuchu Dai, Arumugam Nallanathan, Zhiguo Ding, George K. Karagiannidis

[14]Q. Yan, H. Zeng, T. Jiang, M. Li, W. Lou, Y. T. Hou, "Mimo-based jamming resilient communication in wireless networks", *Proc. IEEE INFOCOM*, pp. 2697-2706, Apr./May 2014.

[15] Gan Zheng, Ioannis Krikidis, Jiangyuan Li, Athina P. Petropulu, Bjorn Ottersten

[16] Lun Dong, Zhu Han, Athina P. Petropulu, H. Vincent Poor

[17]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 ACM SIGCOMM Conf,2011,pp,2-13.