International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
Volume No.3 Issue No.6, pp : 755-759 1 June 2014

An Improved Fragile Watermarking Method for Tamper Detection in RFID Tag

Kishor T. Patil[1], Dr. Santosh K. Narayankhedkar[2]
[1]SIG College of Engg, Navi Mumbai, Research Scholar: SGB Amravati University, Amravati, India
[2]MGM's College of Engg. and Technology, Navi Mumbai, India
[1]ktpatil@rediffmail.com

Abstract *— **Tampering of RFID (Radio Frequency Identification) tag data results in misinterpretation of the object to which the tag is attached. Due to the advantages offered by RFID in the field of contactless auto identification, it is being used in the widespread range of applications. With growing adoption of RFID in industries, supply chain management, healthcare systems, security systems, government sectors, threats to take undue benefits from RFID systems are also increasing. Tag data tampering is one of that in which by changing the tag contents attackers can mislead the organisations adopting RFID system in their workflow. Detection of such tampering is essential to continue use of RFID system reliably. In this paper we have discussed the existing work of embedding a fragile watermark in the tag for tamper detection and proposed an improved method to overcome the shortcomings observed in the existing work.***

Keywords— EPC, Fragile watermark, RFID, tamper detection

I. INTRODUCTION

RADIO frequency identification (RFID) is a technology, in which a tiny Tag contains information related to the object to which it is attached. A RFID Reader collects information through signals and sends further to host computer for processing. Though initially viewed as an electronic replacement to barcode technology, [1], [2], mainly in supply chain for inventory management and real time monitoring, has grown much beyond that and being used in widespread applications in diverse field like identification of objects, animals, healthcare systems, libraries, e- passports, contactless credit cards, national security and military applications. The reliable use of RFID will continue and grow further if the security threats [] are identified and resolved timely. Data tampering in RFID tag is one of the threat in which tag data representing identification or location information or specification of object to which it is tagged, its type, price, date of manufacturing-expiry etc, depending on application, is modified by attacker. Such unauthorised alteration of tag data results in great loss. In this paper we have discussed about basic architecture of RFID system, data tampering, existing tamper detection methods and proposed an improved tamper detection method.

- *Key components of RFID system*

  The basic architecture of RFID system as shown in Fig. 1 consists of following components [3] namely:
  - Tag (Transponder)
  - Reader
  - Host computer

Tag: RFID "Tags" are small transponders that respond to queries from reader by wirelessly transmitting a serial number or tag information. Tags are usually attached to objects and consist of an antenna, a microchip and a battery (for active tags only). Passive Tags obtain energy from electromagnetic signal received from Reader by means of inductive coupling [4] Transmission range of passive tags is much less than active tags.

Reader: The "Reader" emits radio waves in ranges of anywhere from one inch to more than 100 feet depending on its power output and radio frequency used . Each Reader can only interrogate tags within its interrogation region [5]. Tags in the range of reader detects activation signal and transmits own identity to reader. The reader sends data received from tag to host computer (backend server) for processing.

Host Computer: data captured by reader is sent to computer for further processing. For example from received tag data in supply chain management, product type, its price, date of expiry etc is generated by the computer.

- *EPC structure*

The standardisation bodies such as the EPC global (Electronic Product Code) and the GS1 (Global Standardisation) are working together to propose and manage global standard for RFID tags. EPC Class 1 Generation 2, also known as Gen 2 or EPC-C1G2 is latest standard for 96 – bit EPC tag [6] An (EPC) structure is shown Table I.

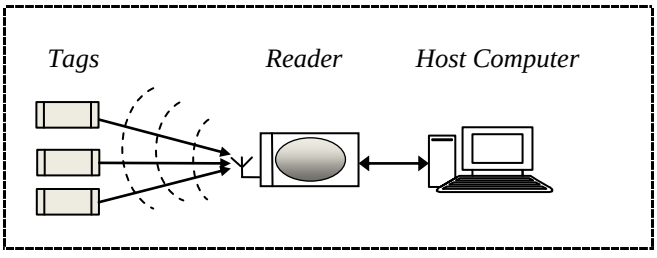

Fig. 1 RFID System Architecture

TABLE I: EPC-96 STRUCTURE

Header (H)	*EPC Manager (EM)*	*Object Class (OC)*	*Serial Number (SN)*
8 bit	*28 bit*	*24 bit*	*36 bit*

- *Header* : determines which EAN.UCC key is used and how many bits are allocated to the remaining sections
- *EM* : identifies the product manufacturer
- *OC* : which is a unique identifier for the product manufactured by the manufacturer
- *SN* : which is assigned to each item belonging to a class of product

II. TAMPERING PROBLEM IN RFID TAG

Due to limitation of storage capacity and computation power in low cost RFID tags, it is difficult to implement strong encryption schemes available for secure communication in RFID system. Further, as communication between reader and tag is wireless, it can be considered as insecure communication which can give easy access to unauthorised users. As shown by Lukas Grunwald [7], a small program called *RF Dump* can be easily used to read, alter or even delete tag data using an inexpensive RFID reader.

Whereas unauthorised reading is concerned with privacy, confidentiality and deleting tag data may invalidate tag which could have an adverse effect in management system, but modification (altering) tag data, referred as *data tampering* is a major issue which needs to be addressed specially for ***secure and reliable*** deployment of technology. Consider a warehouse scenario: if the data on tag is tampered with, it could result in shipping wrong items from warehouse. As an example, if the malicious reader changes the information on RFID tag from apple to orange, then the package containing oranges may be shipped when intention was to ship apples. Thus trust, quality of service and reputation, all may get affected. Replacing data on higher price items tag with lower price may give monitory benefit to a buyer in supermarket (economic loss of supermarket), is another example and many other can be listed where data tampering can severely affects integrity.

Thus tampering in RFID tag refers to altering data stored on RFID tag by attacker for the purpose of its own benefit and / or to disrupt the business of the organisations.

It is necessary to trace out any such data alteration by attackers to avail advantages offered by RFID technology safely and reliably. This is what called as Tamper Detection in RFID system.

III. RELATED WORK

To address the tampering problem in RFID, concept of fragile watermark is introduced by Vidyasagar Potdar et al. [8] Fragile watermark, generated by using tag data is inserted in tag itself. At reader side using same procedure watermark is generated again and matched with the inserted watermark on tag. Matched watermarks validate the tag as un-tampered one else tags are invalidated as watermarks differ if tag data is tampered. Scope is there to further strengthen the pioneer work in tamper detection proposed by [8]. They considered either EM or OC part as input for watermark generation. Possibility is there that tampering of tag data which is not included in watermark generation goes undetected. Secret key needs to be strengthened further. Secret key embedding location proposed is continuous in SN part of tag, which can be comparatively easily located by attacker. Parity bit added to detect tampering in secret key itself is misleading if even number of bits are tampered. Out of 9 bits used from SN part, 8 bits are used for embedding secret key. With 8 bits, maximum 256 secret patterns can be generated. With growing number of tags beyond 256, secret patterns generated will be repeated. Thus watermark computed with tampered tag data may match with embedded watermark and tag can be validated as un-tampered tag!!!

Block diagram in fig. 2, shows Watermark generation, embedding in (a) and watermark matching process for tamper detection at reader side in (b).

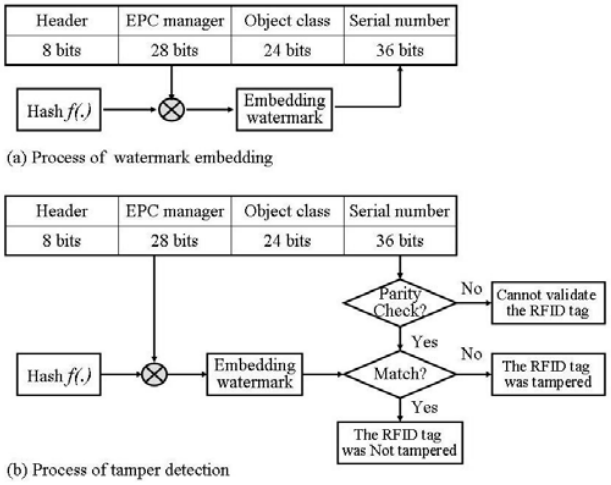

Fig. 2 Basic block diagram to illustrate tamper detection

Use of reserved memory in the tag for 32 bit kill and/or access passwords to embed the watermark generated by taking inputs from H, EM, OC and SN is proposed in [9].

The main purpose of the 32 bit *kill password*, specified in the EPC-C1G2 RFID tag standard, is for the *kill function* to ensure consumer privacy by permanently killing or in some cases turning the tag into sleeping mode an RFID tag after the point of sale [11]. Use of this *kill function* is not applicable to all RFID applications, so this space can be used for embedding

watermark. This is claimed by [9] referring the dispute about use of *kill function* in research community [10] [11]. Thus, using memory reserved for *kill / access* password, in general, is not acceptable.

Yamamoto, et al., proposes a tamper detection solution [12] which is based on a technique known as a digitally signed journal [13]; in which they proposed a technique to record memory write activities (write journal) onto a specially designed tag memory area by the tag itself. This area is readable from standard reader/writers but cannot be written. By using this technique, a reader/writer can write memory area without restriction, while records of the write journal are write-protected from the reader/writer without any password. If malicious user overwrites a part of the user memory, that activity is effectively recorded in the history area, so users can detect such kind of writes. Since write journal can be read by standard a reader/writer, middleware or application can verify the modification activities, to find whether there are unwanted writes happened or not. This proposal is promising but it requires modification in the existing EPC-C1G2 tags.

Using memory reserved for Kill / access password cannot be a good option and can block tag.

In [14], Kelvin et.al proposed to use SN as well as OC fields as a watermark embedding location. The object class is used to identify the product manufactured by manufacturer. It may follow some product convention taxonomy where the first two digits might represent the classification of that product; the next two may be the age of the product and so on. Hence modifying any of this data might interfere with existing industry standard.

In some proposals, efforts are made to identify location i. e. whether EM part or OC part of tag is tampered. Taking only EM part for generating watermark cannot detect any attack on OC part and if OC only taken as input for generating watermark, tampering in EM part cannot be detected.

The chaotic fragile watermarking proposed in [15] not only has the ability of tamper detection but also the ability of tamper discrimination in RFID tags.

Trying to distinguish whether EM or OC part is tampered is not going to help much as whether EM part is tampered or OC part is tampered, result is: “Tag is tampered”!!! Distinguishing which part is tampered can be helpful if we are surely able to restore the tampered data back to original value. This is difficult because even watermark embedded can also be tampered. In [8], a parity bit is added to detect tampering in watermark, however if even number of bits in watermark are changed, tampering cannot be detected..

IV. Proposed Work

Going through referred literature we found that tampering in RFID is a major issue and many researchers have contributed well to detect any such tampering using limited resources like memory, power and computing time. Though data tampering is comparatively easy, tamper detection methods should be as complex as possible to block attackers to trace to maintain security of tamper detection mechanism.

We propose here an improved tamper detection method by increasing complexity in secret pattern generation and embedding location.

Proposed method:

Step1. *Input for generating watermark (w_g)*

As shown in fig 2 EPC-96 tag consists of 8 bit Header, 28 bit EPC manager, 24 bits Object Class and 36 bit Serial Number. Of this EM and OC fields are potential members which can be tampered by attackers. Nothing can be gained by attackers by tampering other fields of Tag. Hence here we form a bit string as an input for generating watermark by combining all bits from EM and OC in random. As an example first 4 bits of OC followed by 5bits of EM followed by 3bits of OC followed by 6 bits of EM and so on till all bits from EM and OC are taken. In addition *padding bits* are inserted in this bit string at a predefined location.

Step2. *Watermark generation*

12 bit watermark (w_g) is generated by hashing Bit string formed in step 1.

Why 12 bit watermark?

With 8 bit watermark, we can have maximum 2^8 =256 watermark patterns. So appearance of repetition of watermark generated, when tag number exceeds 256, is but natural. So, probability is there that even if some bits of EM or OC are tampered still same watermark pattern as that of original tag is generated and tag is finally approved as un-tampered tag!!

Here we increase watermark bits to 12. With 12 bits watermark, we can have 2^{12} = 4096 watermark patterns so we can have more number of secret patterns. We cannot further compromise with SN part of Tag, so limit to 12 bits only. SN here will be limited to 24 bits instead of 28 bits as with 8 bit watermark, which can still be acceptable.

Step 3. *Watermark embedding*

At the time of tag registration, reader/RFID middleware, computes the watermark as above. 12 bit watermark is embedded at predefined distributed locations in 36 bit SN part of Tag. Remanning 24 bits will define serial number of the tag.

International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
Volume No.3 Issue No.6, pp : 755-759 1 June 2014

w_{i-12} = watermark bits, s_{1-24} = Serial number bits

Watermark embedded in SN of Tag :

$$\{w_{1-12}, s_{1-24}\} = \{s_1 s_2 w_1 s_3 s_3 s_4 s_5 s_6 w_2 w_3 \ldots\ldots\ldots\ldots w_{12} \ldots\ldots s_{24}\}$$

Step 4. *Watermark extraction and tamper detection*

To check tampering, reader will compute the watermark once again by following same procedure by which watermark was generated and embedded at the registration time, as above. The watermark computed now will be compared with the watermark extracted from tag SN from the locations where it was embedded in SN.
If computed and extracted watermark mach, no tampering is concluded and tag is validated otherwise tag is tampered and invalidated and blocked from further processing.

Process of watermark generation and tamper detection is shown in fig 3.

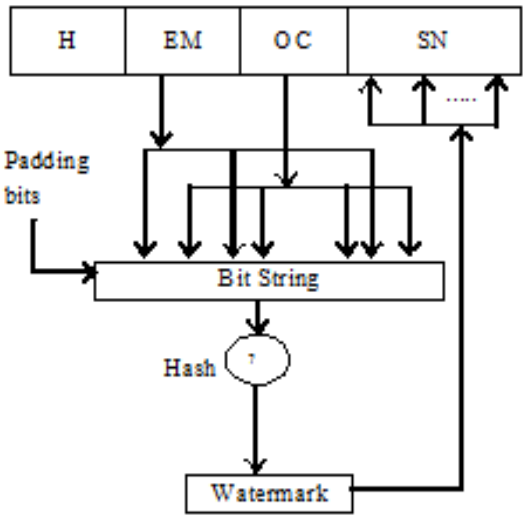

Fig. 3 (a)

In fig 3(a), watermark generation from a bit string formed by chaotic placement of EM and OC bits along with padding bits is shown.
An example is shown in fig 3 (b). Watermark inserted in SN at different locations is shown by underlined bold letters. EM and OC bits tampered by attacker are shown by underline. For tamper detection, reader computes the watermark from tag under consideration. The computed watermark is matched with the watermark extracted from known locations of SN. In this example as EM and OC bits are tampered, watermark computed will not match with extracted watermark from SN and hence tampering is detected.

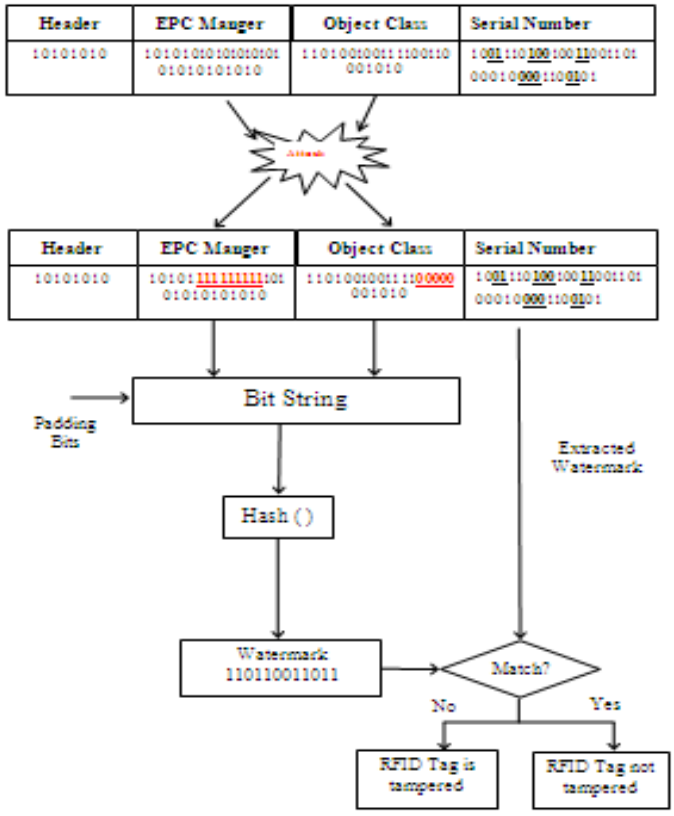

Fig. 3 (b)

Fig 3. (a) Watermark generation and embedding; (b) Tamper Detection.

Improvements achieved:

- In contrast to either EM or OC field considered, or random bits from EM and OC are considered as input for generating watermark, where tampering of bits that are not considered as input goes undetected, here we use all bits of EM and OC for watermark generation which ensures tampering in any of the bit of EM and OC.
- Forming a complex bit string by combining bits from EM and OC along with padding bits for generating watermark is comparatively difficult to trace to attackers as compared to taking EM and OC part as it is, as an input for generating watermark.
- Proposed 12 bit watermark produces much more secret patterns (4096) as compared with 8 bit secret pattern (256). Watermark repetition with growing number of tags is shown in fig. 4 with the help of graph. More the repetition of secret patterns more is the probability of tampered tag having same watermark as that of original un-tampered tag. As a result tampered tag also can be validated as un- tampered tag. Probability of generation of same watermark for many tags is much higher if we have only 256 watermark patterns. And, thus

tampered tag may also be assigned with the same watermark as that of the original tag. Whereas, with 12 bit watermark we can have 4096 unique watermark patterns which is much higher as compared to 256, and thus possibility of assigning same watermark to the tampered tag, though cannot be overruled in large number of tags, but still reduced drastically.

- If SN is further compromised, i.e. more bits from SN are used for watermark embedding, and if available bits of SN are sufficient for that product, unique watermark pattern for all tags can be assured.

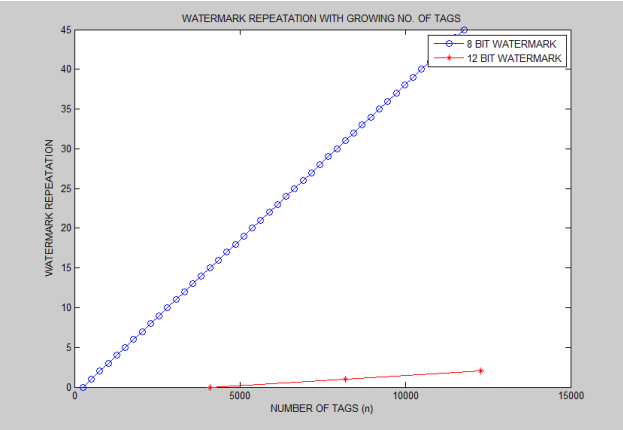

Fig. 4 watermark repetition Vs number of tags for 8 bit and 12 bit watermarks.

V. CONCLUSION

We have presented here in this paper an improved tamper detection method which is more complex to trace to attackers and hence secure. We addressed here issue of watermark secret pattern repetition and resulting possibility of validation of tampered tag i.e. non-detection of tampering, with existing solutions proposed by researchers with 8 bit watermarks. The proposed 12 bit watermark reduces such possibility drastically.

REFERENCES

i. *M.R. Rieback,B. Crispo, and A. S. Tanenbaum, "the evolution of RFID security," IEEE PerCom 06, pp. 62-69, January –March 2006.*

ii. *C.C.Tan and Q Li, " A robust and secure RFID based prdigree system" ICICS, 2006.*

iii. *Klaus Finkenzeller, RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification, 2003 John Wiley & Sons, Ltd. ISBN: 0-470-84402-7*

iv. *Z. G. Prodanoff, "Optimal frame size analysis for framed slotted Aloha based RFID networks," Comput. Commun., vol. 33, no. 5, pp. 648–653,Mar. 2010*

v. *C. Wang, M. Daneshmand, and K. Sohraby, "Optimization of tag reading performance in generation-2 RFID protocol," Comput.Commun., vol. 32, no. 11, pp. 1346–1352, July 2009*

vi. *EPC global Inc., "EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz -960 MHz Version 1.4", 2008.*

vii. *Lukas Grunwald, "RFDump Can Hack RFID Tags" , Available online: http://www.rfidgazette.org/2004/07/lukas_grunwalds.html Accessed on Sunday, 29, October 2006*

viii. *Vidyasagar Potdar, Elizabeth Chang, "Tamper detection in RFID tags using fragile watermarking," International Conference on Industrial Technology, Mumbai, India, 2006, vol.12, pp.2846-2852.*

ix. *Ali Nur Mohammad Noman et al, "A Watermarking Based Tamper Detection Solution for RFID Tags" 2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing. 978-0-7695-4222-5/10 2010 IEEE DOI 10.1109/ IIHMSP.2010.32*

x. *Juels, A.: RFID Security and Privacy: A Research Survey, An invited paper, IEEE Journal on Selected Areas in Communications, vol. 24 no. 2, pp. 381-394, February 2006.*

xi. *Spiekerman,S., Evdokimov S. : Privacy Enhancing Technologies for RFID - A Critical Investigation of State of the Art Research, IEEE Privacy and Security, 2009.*

xii. *Yamamoto, A.; Suzuki, S.; Hada, H.; Mitsugi, J.; Teraoka, F. \& Nakamura, O. A Tamper Detection Method for RFID Tag Data, IEEE International Conference on RFID, 2008, 51-57.*

xiii. *S. Suzuki and M. Harrison, "Data Synchronization Specification", Auto-ID Labs AEROID-CAM-007, 2006.*

xiv. *Kevin Curran, Tom L, Ali N M, "Tamper detection for low cost rfid tags: using watermarking with chaotic mapping", International Journal of Engineering and Technology Volume 1 No. 1, October, 2011. pp. 27-32.*

xv. *Ming-Quan Fan, Hong-Xia Wang, "Tamper Discrimination in RFID Tags Using Chaotic Fragile Watermark", 2009 International Conference on Networks Security, Wireless Communications and Trusted Computing, 978-0-7695-3610-1/09 2009 IEEE ,DOI 10.1109/ NSWCTC.2009.91*