International Journal of Networked and Distributed Computing, Vol. 1, No. 2 (April 2013), 79-88

Hybrid Approach to Ensure Data Confidentiality and Tampered Data Recovery for RFID Tag

Biplob Rakshit Ray
School of Information Technology
Deakin University,
Melbourne Burwood Campus, Australia
E-mail: brray@deakin.edu.au

Morshed Chowdhury
School of Information Technology
Deakin University,
Melbourne Burwood Campus, Australia
E-mail: muc@deakin.edu.au

Jemal Abawajy
School of Information Technology
Deakin University,
Melbourne Burwood Campus, Australia
E-mail: jemal.abawajy@deakin.edu.au

Received 24 May 2012
Accepted 13 November 2012

Radio Frequency Identification (RFID) is an emerging wireless object identification technology with many potential applications such as supply chain management, personnel tracking and healthcare. However, security vulnerabilities of the RFID system have been a serious concern for its wide adoption in many applications. Although there are lots of work to provide privacy and anonymity, little focus has been given to ensure confidentiality and integrity of RFID tag data. To this end, we propose a lightweight hybrid approach based on stenographic and watermarking to ensure data confidentiality, linkability resistance and integrity on the RFID tags data. The proposed technique is capable of tampered data recovering and restoring for RFID tag. It has been validated and tested on EPC class 1 gen2 tags.

Keywords: RFID, Tag data confidentiality and integrity, Stenography, Tampered data recovery, Linkability resistance.

1. Introduction

RFID is gaining attention as the core next generation object identification technology. With various strengths such as recognition speed, high identification rates and non-line of sight operation, RFID system has become very popular in many domains such as supply chain management, curb counterfeit, healthcare, etc. RFID differs from existing identification technologies such as barcode in that it can identify individual tags and has memory to store data. Generally, RFID system is composed of a set of tags, one or more readers and a back-end database server. RFID tags are generally classified as passive, active and semi-active. Passive tags are low cost and have little storage and computation capabilities and obtain power from the reader. In contrast, active tags have their own power source and more costly than the passive and semi-active tags.

The passive tags are cheaper and more popular than other type of tags. This paper will focus on passive tags only. The communication channel between the tag and the reader is over wireless radio frequency (RF). RFID tags store sensitive information which is pertinent to only a specific object only. The tag might contain different information sets based on its implication. Commonly, a tag might contain a product code, object class, patient identification code, credit card

information, passport number, etc. The tag is interrogated by the RFID reader when it gets in the readers reading vicinity and provides information stored on the tag to the reader. RFID tag can be "promiscuous", that is, it will communicate with any reader. Although RFID tag contains a very small amount of information, this information might be sufficient to take unfair advantage by competitors. Exposing part or all of the information stored in the tag could pose serious risk to individuals and business.

At present, one of the main issues with RFID technology is secure and scalable deployment. Within the security umbrella, there are several open issues such as confidentiality, tampering, tampered data recovery, etc.

Tag data confidentiality ensures that an illegitimate entity cannot use intercepted information for malicious or illegitimate activities and take business advantages using linkability property. Linkability is a property where intercepted/accrued data can be matched to draw some useful information. Ensuring confidentiality increases trust and reliability in the supply chain between partners. Linkability resistance discourages ransoms, illegal business advantage, etc.

Tampering is a critical threat which consists in the malicious changing of data recorded in tag memory. A tampered tag in supply chain becomes useless because it cannot convey reliable information. [1]

The EPC Manager (EM) and Object Class (OC) are very sensitive data which require confidentiality to increase trust and linkability resistance. None of the existing work addressed the issue. There are a number of existing techniques exist to ensure tamper detection and resistance. However, only one of them attempt on tampered data recovering and restoring which cannot detect or recover a tampered serial number of a tag.

In this paper we are proposing a hybrid technique which combined stenographic based technique (StenoCipher) and watermarking technique to ensure following:

- Confidentiality and randomness of tag's sensitive data such as EM and OC.
- Ensure linkability resistance of tag's sensitive data such as EM and OC.
- Tamper detection and restoring for EM, OC and serial number.

In section 2, we survey the existing literature on RFID security. In section 3, we formalize the problem description. In section 4, we propose the confidentiality, linkability resistance, tamper detection and recovery solution. In section 5, we provide a discussion of proposed scheme's applicability, presented comparative study and conclude the paper in section 6.

2. RFID Security Issues and Related Work

The main aim of this section is to discuss the security issue in RFID systems and survey the relevant literature.

2.1. *Tag data format*

To clearly understand various security issues related to tag data, we have to have an established and clear discussion of tag data and its format. The EPC tag format is shown in Fig 1. The tag data format shown in Figure 1 is a General Identifier (GID-96) 96-bit EPC tag format, helps an application to identify an object. The EPCglobal Gen 2 tag encodes a header field, EPC manager, object class and serial number. [2]

Header	EPC Manager(EM)	Object Class (OC)	Serial Number
8 bits	28 bits	24 bits	36 bits

Fig. 1. EPC-96 bits Tag data format

The header field defines the overall length and format of the values of tag fields. The EPC manager identifies the company associated with the EPC. The object class number refers to the exact type of product being identified. The serial number field identifies the serial number of the product itself. There are two different sizes of Tag: the 64-bit scheme and the 96-bit scheme. The data is stored in a tag using a particular binary encoding. This encoding is a public document published by EPC global.

2.2. *Security properties and existing work*

Wong and Raphael identified five RFID security properties important for RFID adoption as stated in Fig 2. [3]

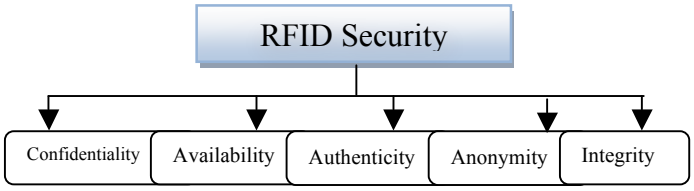

Fig. 2. Major Security Issues of RFID

Extensive research has been done to provide privacy using authenticity, availability and anonymity on tag data. We have investigated some authentication protocol to check its usefulness on tag data tampering and confidentiality.

Henrici et al.[4], Su-Mi Lee et al.[5] and Ray et al. [6] established mutual authentication schemes between the backend and the tag. In Henrici et al.'s[4] protocol

share secret ID between the back-end and the tag, gets updated upon successful identification but this protocol has a database desynchronization problem. In a desynchronization situation the tag can be easily traced. In [5], authors have proposed secret shared information based authentication does not have this desynchronization problem but it can be cryptographically weak against tampering with the tag since the ID is fixed. In [6], authors have mitigated desynchronised problem storing old ID in the database. In this scheme hashed ID is not continually identical and the ID is updated after each successful security check. As a result an attacker cannot trace the tag and/or any previous event of tag respectively. However, it is not authenticated reader which makes it weak on rogue reader's attack. Ray et al. suggested a protocol that has protection from desynchronised attack, change tag ID in each authentication and authenticated reader before transmission. It has stored authentic readers unique ID in database and used it to verify readers prior sending sensitive information. Abawajy proposes a tag authentication scheme called TagAuth which is used to prevent tag cloning. [7] This authentication mechanism relies on the high security and computation at the back-end side and allows for less computation in the tag itself. However, it did not address confidentiality and integrity property of tag data. Juels et al. discuss a hash based Access Control Protocol (ACP). [8] Here the tag is first in a locked state. When the tag moves to the unlocked state the reader can access the tag's details. However, this ACP is not providing full confidentially as in its unlocked state an individual can see the entire information of the tag in plain text. Social engineering and insider attack is possible by those accessing the data.

None of the above mentioned authentication protocol addressing confidentiality of EM and OC. These protocols are focused on privacy on the basis of protecting ID of the tag. However EM and OC can reveal same or more information to breach privacy and confidentiality of users. In addition, scientists have proved authentication protocols are not making tags tamper resistance. These protocols are vulnerable to attacks based on tampering. [3]

Availability is a research area addressed address by most of the security protocols such as preventing DoS (Denial of Service) attack, protection from de-synchronization attacked.

Yet now, very little focus has been given to ensure confidentiality and integrity of tag data. Confidentiality of tag data is to ensure that intruders accruing data by interception and/or tampering cannot be used to do meaning full traffic analysis. Public parts of EPC tags such as EM and OC can be used to draw useful information to find the nature of the business and object class involved in it.

Data tampering refers to attacks related unauthorized modifications and/or copying of data. Data tamping mainly cover following actions:

- Data impairing: changing of some useful bits of tag data in order to damage it which makes it unreadable too.
- Misleading data: data are altered, deleted, replaced, etc to represent incorrect object which mislead the entire business process and increase distrust.

We can categories existing solutions in two categories as below:

- Tamper evidence and restoring: Techniques to detect the existence of tampering
- Tamper resistance: The ability to resist tampering.

Challenge response authentication [9], lockable or password protected memory and access control based protocol [10, 8] stenography based approaches [11] are fall on temper resistance category. On the other hand, watermarking approaches [13,18,19], write activity[15],stenography[11] fall on tamper evident and restoring category. The temper detection and restoring protocols can be further classified as protocols achieving temper detection only such as [12],[13],[14],[15] and protocols achieving both temper detection and recovery such as [11]. This point forward we will only discuss protocols on tamper evidence and restoring categories.

In [12], authors have proposed a tamper detecting technique using watermarking. It has generated an 8 bits watermark and embedded it in serial. The paper has used secret function to generate watermark using EM and OC of the tag. The authors have mentioned that short length of the watermark could affect the robustness of the tamper detection system. The main drawback of this system is that it is based on a secret function. Therefore, if an intruder or an opponent obtain the function, a huge modification of the system is required. In [14], which is an extended version of [13], authors have proposed a watermarking tamper detection algorithm. It used memory reserve for kill password to store watermark. However, note that many tag categories do not have kill password memory reserve. In addition, this might also create operation conflict.

In [14], authors have used OC and serial number to embed watermark in [14]. In [14], author has introduced chaotic mapping to determine embedding location of watermark. An intruder can easily find the OC without watermark as it is public part of the tag. The OC value without watermark can be used to find the watermark

embedded on OC as long as embedding function is public. It cannot restore tampered data of the tag.

Mohan et al. [11] proposed a tampered tag's data recovery and restoring scheme based on stenography. In this scheme authors have select a group of tags serial to store the secret pattern. The robustness of the scheme based on the secrecy of the location of the secret information. However, this information shall be shared by all the entities that are involved in the trade of tagged products. It also did not consider the risk of tag's serial number tampering. Yamamoto et al,[15] proposed a tamper detection solution based on a technique known as digitally signed journal bit it requires modification in the existing EPC tags specification.

This concludes the survey of the most relevant literature on RFID security. We have seen that existing literature have failed to address tampering issue entirely for all parts of tag data. Existing solutions has many drawback in terms of security and applicability with existing highly deployed EPC tag formats

3. Problem Description

Most of the attacker works for an economic motive. Keeping EPC manager and object class in clear text will raise the possibility that an intruder might match various tags EM and OC. An intruder might use those data to do data mining and find out which delivery is for which organization and which product type is in the delivery?

Confidentiality of tag data on the tag is essential to ensure secure operation of business. An intruder can use EM, OC to find out about the organization and the product associated with the organization. An intruder can use this information by combining with other available information such as shipment details to take competitive advantage, organization ransom and illegal use of user's preferences. By capturing suffecient transations and comparing them with others, an intruder or insider might reveal information about consignment and sell to people such as robbers, business competitors. Intruder might link EM and OC of different tags to find out organization's name, product type and probable shipment size. This is done using linkability property as same oraganization and same product type have same EM and OC. Object class can be used to reveal product type which is a breach of individual's privacy and cab be used for ill activities. An inside attacker can have more privilege to do harm, if tag information is open and easy to read.

Data tampering is also a key concern. For an example let's consider retail supply chain where multiple parties do business in a virtual collaborative environment by capitalizing trust of various parties and reliability of the systems information delivery. RFID system mostly relies on authenticity of information based on tag's serial or identification number. However, if the information is tampered for other fields such as EPC manager, Object Class, it might destroy reputation of a business. Same time tampered object class can put individual's social reputation in danger. For example, one politician ordered a t-shirt and during delivery object class is tampered with an illegal drug's OC. Revealing this information to public can ruin the career of that politician. Data tampeing can hinder main objective of the tag which is correctly identification of the object. To tackle tamper related attcks, tamper detection and recovery is a must requirment for wide adaption of RFID system in suppy chain and other similar industries.

After conduct a detail literature survey of RFID solutions we have identify that no one has presented a solution which protect security properties such as confidentiality, linkability resistance of EM and OC, tamper detection and tampered data recovery together. This gives us the rational to present our solution based on the principle of stenography (Stenocipher) to provide confidentiality and linkability for tag data such as EM and OC. A new embedding technique is used to embed watermark to provide integrity, in other words tamper detection and tampered data recover for tag's EM, OC and serial number.

4. Proposed Scheme

In this section, we state general overview, foundation, and design decisions of the scheme. It is followed by theoretical foundation, mathematical explanation and example of three stages of the scheme: generate stenocipher code, serial number preparation with EM, OC and serial code finally date tampering detection and recovery.

4.1. *General overview*

The proposed algorithm offers a solution to provide confidentiality and integrity of tag data. This will discourage intruders and inside attackers. Firstly, it will create stenocipher for EM and OC. Then the system will randomize the stenocipher of EM and OC to provide linkability resistance. Tag will have this randomize stenocipher (CCr) loaded instead of EPC manager and object class during manufacturing. Particular organization will buy tags from manufacturer and generate the tag serial (S1). The system will then xor the stenocipher of EM and OC. It will then xor the product from xored EM and OC value with serial number. Finally, the system will hash the final xord value as stated in eq (1) in Figure 3. Furthermore to detect, recover and restoring data tampering in tag's serial,

each tag serial will have a code(Scode) embedded in it. To detect data tampering on EM and/or OC, we will use reverse process of our scheme to find out the code and compare with stored backend data. To recover those tampered data we will use stored backend data and serial code. The serial code of next tag in the tag set will help us to recover tampered serial code.

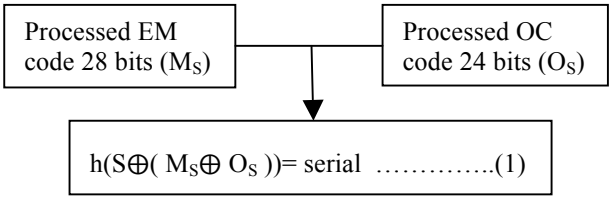

Fig.3. EM and OC embedding process

4.2. *Foundation of the scheme*

The proposed framework can be decomposed in three different stages:

Stage one – In this stage, system will generate stenocipher code for EM and OC. Then randomize the stenocipher(CCr). Write in the tag CCr of OC and EM. At the end tag leaves manufacturer's office. Detail of this stage is on sub section 4.4

Stage two – In this stage, system will generate serial code and prepare serial number. Serial number will be prepared using eq(1) to add EM and OC to it. It then embed the secret code in it. Finallly, write the serial into the tag which is capable to detect tampering and recover tampered EM, OC and serial. Detail of this stage is on sub section 4.5.

Stage three – Tamper detection and data recovery stage. Detail of this stage is on sub section 4.6.

4.3. *Design decisions of proposed scheme*

In order to address confidentiality, linkability resistance and tampering issues, the following requirements need to be met by the system:

(a) Stenocipher processed output should produce same length as input for EPC manager and Object Class.
(b) Stenocipher has to be generated in tag manufacturing time as organization cannot rewrite EPC manager and Object Class in tag. The manufacturer should write the randomize Stenocipher code in the tag and handover the real EPC manager and Object Class to the organization.
(c) The system should possess EM, OC and serial number to identify a tag's real EM and OC.
(d) Plain EM and OC should be stored in backend database for data verification and authentication.
(e) The Stenocipher code should be xored and hashed with the serial number. It has to be done in the organization which is using the tag.
(f) Backend database will store a random number r=rand (nEM or nOC) which is mapped with their specific EM and OC.
(g) A tag set must have a sequential pattern where each tag has a sequence number as shown below:

ϵ ={tag1,tag2,tag3,tag4….tagn}
where tag1=123456710, tag2=123456810, tag3=123456910……. Tagn = (123456710 + number of tags)

(h) Proposed system should support plug and play into a middleware system.

4.4. *Stenocipher solution – Stage one*

The detail of stenocipher generation process is shown in Table 1. In Table 1 we have explained the mathematical foundation of calculating stenocipher. Eq. (2) shows that firstly, the system will find next least prime number of the data block. It will then use Eq. (3) and (4) to find CCxy which is the building block of our stenocipher.

Table 1: Mathematical algorithm of stenocipher code

Inputs	Plaintext EM and OC
Outputs	Stenocipher code and randomize Stenocipher code of EM and OC.

$xy=xy_{\mathbb{p}}+y'$ ……(2)

where $xy_{\mathbb{p}}$ = next least prime number of xy, y' = (xy-$xy_{\mathbb{p}}$) and (2<x+y).

if (length(EM or OC))/2 =0)
  main:
  if $x_{\mathbb{p}}'+y'>10$ then
    $10101*(xy_{\mathbb{p}}||y') = ((xy_{\mathbb{p}}+1)||CC_{xy}||y')$..(3)
  elseif $2\leq x_{\mathbb{p}}'+y'<10$ then
    $10101*(x_{\mathbb{p}}||y') = (xy_{\mathbb{p}}||CC_{xy}||y')$.(4)
  else:
    $CC_{xy}=xy||xy$
else:
  pad= (x_2+2||2)
  length(((EM or OC)||pad))/2)=0;
  go to main;

end. Where CC_{xy} = cipher code of xy, $x_{\mathbb{p}}'$ = first number of $xy_{\mathbb{p}}$, pad = an extra value added to increase appropriate length of the data, x_2 = right most unpaired value of EM or OC
The algorithm will process ab, x_1y_1, a_1 b_1 pairs using exactly similar process of xy pair. Finally, $CC = (CC_{xy} \oplus CC_{ab}) \| (CCx_1 y_1 \oplus CCa_1 b_1)$ ……..(5) Reader can use backend information to recalculate the cipher and compare it to received one.
$CCr = CC \oplus r$ ……. (6) where r=PRF(EM or OC), PRF = pseudorandom function

We have developed this code by multiplying 10101 with factored data derived from Eq. (2).The reason of using 10101 for multiplication is that it produces a sequential combination of data which shown in Eq. (3) and (4) in Table 1. Lastly, Eq. (5) use cipher code of each block and generate final cipher code (CC).To randomize the cipher code system generates a random number using PRF which uses EM or OC as function input. The system then uses Eq. (6) to generate CCr which ensures the linkability resistance of EM and OC. Then it writes the code (CCr) in the tag. This will ensure that even a same organizations EPC manager will have various different representations in the tag.

Table 2: Transformation of EPC Manager

EPC manager's hexa value	Decimal
54DD12C	8 8 | 9 8 | 5 9 | 0 0 x y | a b | x_1y_1 | a_1 b_1

Table 3: Stenocipher code generation for EM

Calculation	Stenocipher code
Input EPC Manager: $(54DD12C)_{16}$ = $(88985900)_{10}$	**Step 3:** CC_{EM} =((3433 ⊕ 0807) || (6363 ⊕ 0000))
xy=88, $xy_{\mathbb{p}}$ = 83, y′ =(88-83)=5 **Spet 1:** (10101*835) = 8434335	= 3662 || 6363 $=36626363_{10}$ $=22EDFBB_{16}$
using eq(3) and (4) we can derive CC_{xy} =3433 **Step 2:** Same way we can get CC_{ab} =0807 , CCx_1y_1 =6363 and $CCa_1 b_1$ = 0000	Output: StenoCipher of EPC Manager (CCEM) $=22EDFBB_{16}$ $=36626363_{10}$ Output: Randomize StenoCipher of EPC Manager (CC_r) $=22EDFBB \oplus PRF(EM)$ $=22EDFBB_{16} \oplus 76_{16}$ $=022edfc3_{16}$

As an example, Table 2 and 3 shows the conversion of EPC manager to stenocipher using proposed algorithm. EPC manager has 7(28bits in EPC-96) hexadecimal value. The system first converts the hexadecimal value to decimal value. Each pair of decimal value is considered as one block. Table 2 shows the transformation and pairing of EPC manager. Table 3 shows the conversion of four blocks of data from plain text to stenocipher using mathematical algorithm shown in Table 1. Finally, we have stenocipher code '22EDFBB' for '54DD12C'.Another example is shown in Table 4 which shows the conversion of OC to stenocipher using proposed algorithm.

Table 4: Stenocipher code generation for OC

OC	Decimal	Intermediate data	CC of O_S	CC_r
679A88	6789768**8**	66463322(decimal) = 3F6265**A**(Hexa)	$3F6265_{16}$	3f623f

The algorithm will ensure one to one mapping of EM and OC to a stenocipher code so that tag can be easilt identified even tag is storing randomized stenocipher in it. The code can be easily reversed using same principle used to generating cipher and tags serial. This scheme assumes that database has correct EM and OC number which mapped with their random numbers and it is accessible by the scheme. Correct EM and OC here works as the key. This will ensure confidentiality to ensure linkability resistance of EM and OC. Tags will only stores randomize stenocipher code of EM and OC.

4.5. *Serial code generation and Serial number preparation – Stage two*

This stage details serial code generation and embedding process.

Inputs	Serial number, Stenocipher code of EM and OC and serial code.
output	Tamper proof RFID tag serial number.

Step1: *Prepare the serial code number to recover serial tampering:* To detect tampering on serial number, we have developed a serial code (hexa sum) generating technique which will help to detect and recover data tampering. Eq. (7) shows detail process of serial code (Scode) generation. Each decimal number of the tag serial will be summed up to generate the code which will be xord with r to ensure randomness of the code. A detail of tag code generating process is shown in Figure 4.1.

$SCode=((d+e+f+g+h+i+j) \oplus r)$ …… (7)

Where "defghij" is the serial number of the tag and r=random number used with stenocipher of OC r=PRF(OC)

Step 2: *Prepare the serial number to detect tampering:* In this step firstly we use Eq. (1) to prepare serial. Secondly xor Scode with it to prepare final serial number for a tag. The process is shown below in Eq. (8) below.

$(serial_1 \oplus Scode_n) \rightarrow (serial_2 \oplus Scode_1)....$
$\ldots\ldots\ldots\ldots\ldots\ldots\rightarrow (seial_n \oplus Scode_{(n-1)})$ ……(8)

Please note position of xoring depends on the sequence number of the serial in the set. A detail embedding position discovery process is shown in Table 5. Each tag will be embedding with a serial code value of its previous tag member of the set. An example calculation of this serial code generation is shown in Table 6. Table 6 uses SHA-256 hash algorithm and select only first 8 hexa values. This will make sure we can store the hash code in available 36 bits serial spaces of the tag.

4.6. *Tamper detection and data recovery – Stage three*

Inputs	Serial number, Tampered stenocipher, Data from DB.
Outputs	Recover tampered EM and/or OC. Serial number recovery if tampered.

Detection uses reverse process of embedding to find the correctness of watermark using backend secure data. If it mismatch then tampering has been detected. The algorithm is using S and backend database data to recover tampered data. The recovery process is detailed below with the help of Table 7, Table 8, Eq. 9, Eq.10 and Eq.11.

Table 7: Tampered tag data

Description	Tag data
Tampered(s1) tag	C64**F**E97E
Not tampered(s2) tag	046D40A6

Suppose s1 is tampered. The system can detect it using backend database and Eq. (9) as shown below:

$h(s1 \oplus (M_S \oplus O_S)) \neq h(s1^{DB} \oplus (M_S \oplus O_S)^{DB})$
and $SCode_n = SCode_n^{DB}$ ……(9)

Eq. (9) will be true if EM and/or OC are tampered. The system will re-write the EM and/or OC if it has access to it otherwise reject the tag all the time. In this step we are assuming that serial number is not tampered.

$h(s1 \oplus (M_S \oplus O_S)) \neq h(s1\ DB \oplus (M_S \oplus O_S)\ DB)$
and $SCode_n \neq SCode_n\ DB$ ……..(10)

Eq. (10) will be true if serial of the tag is tampered. In this situation reader interrogates all tag members of the set in the area. It finds the missing sequence number among the existing authentic tags. It then asks the next tag of missing tag for the secret it has stored for tampered tag.

$((s2 \oplus (EM \oplus OC)) \oplus SCode_1) - (s2 \oplus (EM \oplus OC)) = SCode_1$…… (11)

The system uses Eq. (11) to reveal the Scode of tag1 and uses Table 8 below to recover the serial of tag1.

Table 8: Detection and recovery process

Step 1: s1 – 0448**88**F	Step 2: ask s2 – what is the secret key?
Step 3: S2 return 1C(serial code) = 28 Present tag(s2)=29 =1234568 (this can be drawn from DB)	Step 4: Finally, The s1 must be 1234567 = 28 Serial found!

5. Comparative study and applicability test

In this section, we have compared our protocol with existing similar one to present the betterment of our proposed scheme. We have also detail the suitability test of our scheme to present applicability of proposed protocol using existing hardware.

5.1. *Comparative study*

We have compared our proposed protocol with existing similar protocols [11], [12],[13],[14] and [15]. We have compared on the basis of security protection, compatibility and techniques used. Our analysis shows that our protocol has better security protection for tag's data and for RFID systems. It can be adapted without any modification of existing hardware. In Table 9, we have presented the comparison of the proposed protocol with existing ones. In the comparison table: the symbol √ means protocol satisfies the titled description, the Δ means partially satisfied, the X sign means, it does not satisfies the titled description.

5.2. *Applicability with existing readers and tag*

We have tested our prosed scheme with an EPC class 1 gen 2 tag using ISC.MU.02 reader by using ISO start middleware version 09.00.01. FIGURE 4 and 5 shows the implementation result. Our scheme is completely suitable for existing EPC tags to provide confidentiality and integrity. The best part of this scheme is that we can deploy this scheme using existing RFID readers, middleware and tag which makes it very economic and reasonable.

Figure 4 above shows EPC class 1 gen2 tag data in current industry standard. We have used ISC.MU.02 UHF reader to write data shown in Figure 4. In Figure 5, we have used our proposed randomize stenocipher data to store EM and OC. In addition we have stored serial number with SCode. The new data on tag is shown in Figure 5. It shows that proposed scheme is fully applicable to existing tags formats using conventional readers.

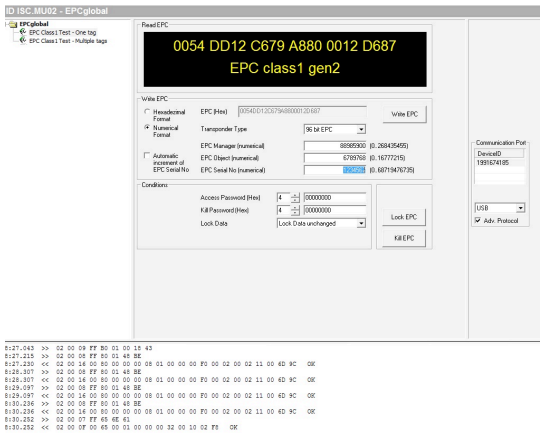

Fig. 4. Tag Data before applying our scheme

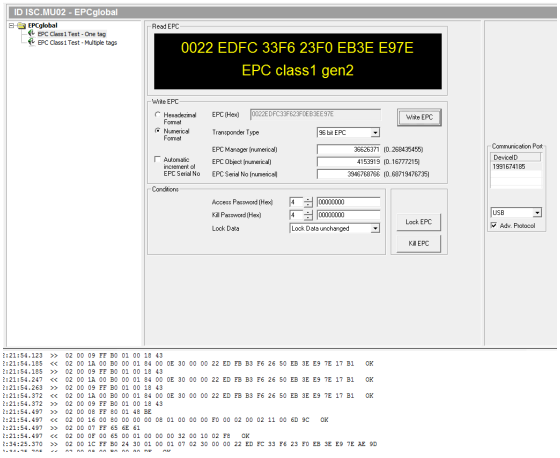

Fig. 5. Tag data after we have transformed using our scheme

6. Conclusion and Future Work

In this paper we have proposed a stenographic technique to protect tags confidentiality. Little or no research of RFID arena has been done to ensure confidentiality, linkability resistance` of EM and OC for stopping outside and inside attackers. In addition we have also proposed a code embedding technique to recover EM, OC and serial number. Previous research on this arena has only able to recover EM and OC after tampering. Our proposed scheme can recover also serial number. This was the first phase of this scheme where we have established theoretical base and check its suitability on existing EPC tag format. In future, we are planning to test this technique against various attacks related to tampering and linkability.

Acknowledgements

Authors would like to thank reviewers for their valuable comments and suggestions.

Table 5: Embedding serial number with serial code

Rules to find a embedding position:
if n>tb then
if tb-pt =1 then
start embedding SCode with first position of the successive tag.
else:
start embedding the SCode in the position where position=pt
 	
Where , n= total set member, tb =total length of the tag serial and pt= present serial code embedded position

Serial number after performing operation in Eq. (1) is "$d_1e_1f_1g_1h_1i_1j_1$" and tb=7.

Table 5: Embedding serial number with serial code(continued)

d_1(First digit pt=1)	e_1(second digit pt=2)		i_1(second to last pt=6)	d_1(First byte pt=1)
Tag1's serial code will be xored with "d_1e_1".	Tag2's serial code will be xored with "e_1f_1".	....	Tag6's serial code will be xored with "i_1j_1". (tb-pt)=(7-6)=1	Tag7's serial code will be xored with "d_1e_1".

Table 6: Serial code generation and embedding process

Label	Values		
Sequence no.	Tag 1	Tag 2	Last tag of the set(Tag n)
Plain text serial in decimal	1234567_{10}	1234568_{10}	1297899_{10}
Calculation for tag serial generation	h(S_1 ⊕(EM⊕OC)) =h(12D687⊕(22EDFBB⊕3F6265)) =h(12D687⊕0211bdde) =h(02036b59) = $eb3ee97e_{16}$	$05ad40a6_{16}$	$d0449353_{16}$
Serial code generation	$1+2+6+7+8+9+9=45_{10}$=**2D**$_{16}$ = this is the SCode of tag n	$1+2+3+4+5+6+7=28_{10}$=**1C**$_{16}$ = this is the Scode of tag 1	**2C**$_{16}$ = this is the Scode of n-1 tag.
Processed serial for writing to a tag.	**c6**3ee97e $_{16}$	0**46**d40a6$_{16}$	etc

Table 9: Summary of comparative study

Protocols	Tamper evidence	Restoring tampered data	Linkability resistance for OM and OC	Technique/s used	Applicability with existing hardware	Robustness
Mohan et al. [11]	√	√	X	Stenography	√	Δ
Potdar et al. [12]	√	X	X	watermarking	Δ	Δ
Noman et al. [13]	√	X	X	Watermarking	√	√
Noman et al. [14]	√	X	X	Watermarking	Δ	Δ
Yamamoto et al. [15]	√	X	X	Write activity	X	X
Proposed protocol	√	√	√	Hybrid(Watermarking and stenography)	√	Δ

References

1. Gandino, F, Montrucchio, B & Rebaudengo, M (2010). 'Tampering in RFID: A Survey on Risks and Defenses', Mobile Networks and Applications, vol. 15, no. 4, pp. 502-16.
2. EPCglobal.http://www.epcglobalinc.org/standards/tds
3. Dennis M.-L. Wong and Raphael C.-W. Phan(2006). RFID systems: Applications versus security & privacy implications, IDEA group, 2006.
4. Dirk Henrici and Paul MÄuller, (2004). Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers, IEEE International Workshop on Pervasive Com-puting and Communication Security- PerSec, pp.149-153.
5. Su-Mi Lee, Young Ju Hwang, Dong Hoon Lee, and Jong In Lim, (2005). Efficient authentication for low-cost RFID systems, International Conference on Com-putational Science and its Applications - ICCSA, pp. 619-627.
6. Ray, Chowdhury and Pham (2010). Mutual Authentication with Malware Protection for RFID System. Annual International Conference on Information Technology Security (ITS 2010). I-24 - I-29
7. J. Abawajy. (2009). Enhancing RFID Tag Resistance against Cloning Attack, 3rd International Conference on Network and System Security, pp.18-23.
8. Ari Juels, Ronald L. Rivest, and Michael Szydlo(2003). The blocker tag: Selective blocking of RFID tag for consumer privacy, 8th ACM conference of Computer and Communication Security, page 103-111
9. MF3ICD21, MF3ICD41, MF3ICD81 (2009) MIFARE DESFire EV1 contactless multi-application IC. Product short data sheet. Rev. 02
10. EPC radio-frequency identity protocols class-1 generation-2 UHF RFID protocol for communications at 860 MHz–960 MHz (2004)
11. Mohan, M., et al.(2006) Recovering and restoring tampered RFID data using steganographic principles. in Proceedings of the IEEE International Conference on Industrial Technology (ICIT06)
12. Vidyasagar Potdar, Elizabeth Chang(2006). "Tamper Detection in RFID tags using Fragile Watermarking," To Appear in the Proceedings of the IEEE International Conference on Industrial Technology (ICIT06), Mumbai, INDIA.
13. Noman, ANM, Curran, K & Lunney, T (2010). 'A Watermarking Based Tamper Detection Solution for RFID Tags', in Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2010 Sixth International Conference on, pp. 98-101.
14. Noman, KCaTLaANM (2011). 'Tamper Detection for Low Cost RFID Tags: Using Watermarking with Chaotic Mapping', International Journal of Engineering and Technology, vol. Volume 1 no. No. 1, p. 6.
15. Yamamoto, A, Suzuki, S, Hada, H, Mitsugi, J, Teraoka, F & Nakamura, O (2008). 'A Tamper Detection Method for RFID Tag Data', in RFID, 2008 IEEE International Conference on, pp. 51-7.