Tamper Detection in RFID-Enabled Supply Chains Using Fragile Watermarking

ShuiHua, Han and Chao-Hsien Chu

Abstract—**While mainstream RFID research has been focused on solving privacy issues, security in general and data tampering in specific is still an open question. This paper analyzes potential security threats especially data tampering in RFID-enabled supply chains and proposes solutions how these threats might be addressed using fragile watermarking technologies. We first survey RFID system and its security problems, and then explain the importance of fragile watermarking schemes for RFID systems and possible applications using fragile watermarking to detect and locate any modification in RFID systems. Finally we suggest possible solutions using fragile watermarking for RFID-enabled supply chain.**

Index Terms—RFID-enabled supply chains, tamper detection, fragile watermarking.

I. INTRODUCTION

Recent advances in wireless technologies, cost reductions and efforts by EPC Global and industry giants, such as Wal-Mart, are causing the supply chain industry to shift toward broad adoption of radio frequency identification (RFID) technology based on emerging open standards. This is creating a large business opportunity for RFID industry

While RFID holds the potential of changing how businesses operate today, its implementation is not straightforward. A number of issues and challenges, such as security/privacy concern, high cost, lack of standards, data integration, the required business process redesign, reliability of the technology, employee resistance to change, and technology choice yet, need to be addressed [1]. While mainstream RFID research has been focused on solving privacy issues, security in general and data tampering in specific is still an open question. EPC Global has not adequately considered the security problem in protocol , and the literature mostly focused on using cryptographic mechanisms to protect RFID tags tampering, which is currently costly from a deployment perspective. Since most low cost RFID tags don't have enough computational power and storage capacity to perform encrypted communications, most RFID data is transmitted in open air without protection which leaves doors open for eavesdroppers and attackers. Considering this insecure communication practice, data tampering on RFID tags cannot be ruled out, which needs to be tackled if a large-scale RFID deployment is to be achieved in a cost effective manner.

Digital watermarking, an emerging technology for data protection, provides a promising cheaper way of protecting RFID data from illicit manipulation and duplication. In the last few years, fragile watermarking schemes for multimedia have been extensively studied. Although most of them focus on digital images and some have been extended to digital video and audio data, little work has been conducted to address the RFID data integrity and security issues using watermarking technologies. To our knowledge, [2] is the first study to propose a fragile watermark solution to identify data tampering in RFID tags. The detection is achieved by embedding a fragile watermark in the ID stream of the RFID tag. But their research is only the beginning steps to provide a foundation for more advanced functionality. Meanwhile, they only focus on data tampering on RFID tags but not the whole supply chain. This paper identifies potential security threats especially in data tampering in RFID-enabled supply chain and suggest how they might be addressed using a fragile watermarking technology. The contributions of this work include:

1) identifies the problems and requirements of tamper detection in RFID-enabled supply chain systems.

2) highlights the importance of fragile watermarking schemes for RFID systems.

3) surveys the relevant literature that addressed RFID data tampering and explored possible issues and challenges.

4) analyzes potential applications of using fragile watermarking on RFID systems—RFID tag, RFID network stream and RFID data storage. The rest of this paper is organized as follows. Section II provides background

Manuscript received December 19, 2007. This work was supported in part by Program for New Century Excellent Talents in Fujian Province University China and the National Security Agency under Grant H98230-07-1-0219

S. H. Han is with School of Management, Xiamen University, P.R. China . The paper was completed while he is a visiting professor at the Pennsylvania State University, PA, USA (corresponding author,phone:86-592-2515072, e-mail: hansh@xmu.edu.cn)

C. H. Chu is the founding director of the RFID Lab, College of Information Sciences and Technology, The Pennsylvania State University, University Park, PA 16802, USA (e-mail: chc4@psu.edu)

regarding RFID and EPC networks. Section III highlights the potential tamper attacks to EPC network. Section IV presents details of fragile watermarking scheme and proposes possible applications to detect and locate any modification in RFID. Categorization and review of existing RFID tampering detection approaches is provided in Section V. Section VI concludes this paper with summaries and suggestions for future work

I. BACKGROUND

RFID refers to a set of wireless technologies used to identify, capture, and transmit information from tagged objects to enterprise systems via radio waves. RFID is not a new technology; it was first used over sixty years ago by Britain military to identify aircraft in World War II. The early commercial applications involving RFID was during the 1970s and 1980s . These commercial applications have been restricted to a relative small number of close loop applications, for example security badges, toll passes, card-keys and gas-pump payment systems. Currently, most RFID tagging and tracking applications are used for operations within a company.

To take RFID beyond the confines of a single organization and create value for the entire supply chain, a few breakthroughs are needed. First, there must be a standardized way of uniquely identifying items within the supply chain. Second, there must be a standard means of discovering and sharing the data that describes each identified item. This leads to the idea of the EPC (Electronic Product Code) Network. The EPC was developed by the Auto-ID Center, its goal was to develop a system that connects all objects to the Internet, the Internet of Things. A sub-goal of the Center, one that was needed to achieve the Internet of Things, was the development of a low-cost RFID protocol suitable for item-level tagging..

The low cost demanded for EPC tags causes them to be very resource limited. Performance of passive RFID tags is adversely affected by adding more functionality onto the silicon. Their range is reduced due to the larger power requirements of the tag. Typically, they can only store hundreds of bits; roughly have between 5000 and 10000 logic gates, and a maximum communication range of a few meters. Within this gate counting, only between 250 and 3000 gates can be devoted to security functions [3]. It is interesting to note that 20000 to 30000 gates are needed for a standard implementation of the Advanced Encryption Standard (AES). Thus, most RFID tags don't have enough computational power and storage capacity to perform encrypted communications.

II. POSSIBLE TAMPER ATTACKS

Current RFID protocols are designed to optimize performance with less attention paid to resilience and security [4]. Several possible attacks on RFID systems have been reported. For instance, using a small program called RFDump, [5] shown how vulnerable RFID tags can be: the tags could be easily read, altered or even deleted using an inexpensive tag reader which was plugged into a notebook.

Tamper attacks may occur anywhere in the EPC network, which include tags, readers, middleware, EPCIS (Electronic Product Code Information Services) repository, EPCIS accessing application, local ONS (object name service), and enterprise application database (see Fig. 1). Here, we focus our attention on data tamper attacks. For other threats, please refer to [2] and [6] for details. We classify the possible tamper attacks on RFID system into four categories based on the locations where they may be attacked:

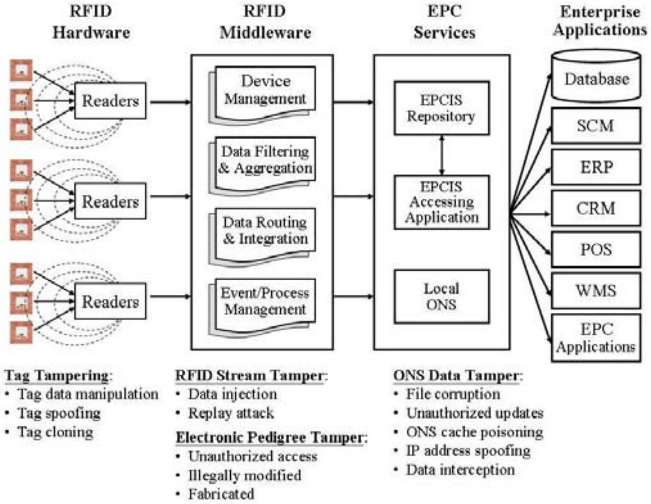


Fig. 1: Potential tamper attacks in RFID networks

1) *RFID tag tampers*. Tampering attacks on RFID tags can be divided into three types:

a) *Tag data manipulation*: Malicious RFID reader can either corrupt or manipulate the data contained in a tag. Using a reader one can write data into the memory banks of a tag to suit the adversary's requirements. Equipped with the misleading security features, the fake products can avoid closer inspection.

b) *Tag spoofing*: Spoofing, which imitates the behavior of a genuine label, presents a serious threat to an RFID system as it adds a new dimension to thieving. A thief may replace a valid item with a fake label or replace the label of an expensive item with that of a fake label with data obtained from a cheaper item. Fake labels may also be used to create imitation items. However, because removing and reapplying authentic labels is costly, this attack does not threaten RFID system in a large scale.

c) *Tag cloning*: The ability to create clones of tags can be used as a means to overcome counterfeit protection (e.g., in passports and drug labels) and as a preparatory step in a large scale theft scheme.

2) *RFID stream tamper*. In RFID applications, data are treated as a continuing stream instead of static datasets, delivered over a wireless network. Since streaming data are usually transmitted over unreliable networks, malicious

parties can easily inject offensive data into the stream. [7] revealed a replay attack during RFID communications, which the attacker uses a tag's response to a rogue reader's challenge to impersonate the tag to destroy stream integrity. In such applications, RFIDs can be more vulnerable than other mechanisms, due to their ability to be read at a distance by covert readers.

3) *Electronic pedigree tamper*. In an attempt to ensure only authentic products are distributed through the supply chain, some regulatory agencies have implemented or are considering provisions requiring a pedigree for products [8]. Clearly an item's electronic pedigree plays a vital role through counterfeit and gray market detection, shrinkage avoidance and accurate and autonomous unit level inventory management, but if this electronic pedigree was accessed unauthorized, illegally modified, or fabricated, most of the aforementioned advantages may be lost .

4) *ONS data tamper*. ONS can be considered as a DNS (Domain Name System) server; therefore, the security threats related to DNS server are also applicable to ONS [8]. Threats in this category include file corruption, unauthorized updates, ONS cache poisoning, IP address spoofing, and data interception.

III. WHY FRAGILE WATERMARKING

Since RFID tag carries data which represent unique item identifiers as well as product details to which it is attached. This data is very significant and if this is tampered with, it can have severe consequences. Take Pharmaceutical industry for example, if the tags are tampered, they could represent wrong drug when scanned by the RFID reader, this case could be even worse when smart shelf are coupled with RFID technology, wrong drugs might be picked up and delivered because the tampered RFID tag could points to a different drug, and this could even result in incorrect diagnosis. Also, data tampering of this nature can raise repudiation issues in collaborative environments when this data mismatch occurs. In order to prevent information from intercepting or modifying by unauthorized parties while it is in transit across networks or resident on storage media, an effective data protection mechanism is needed [9].

A. Cryptographic Method and Its Limitations

Although message authentication is a simple approach to anti-counterfeiting RFID tag, this approach is not possible except for the tags using the ISO 14443 standard, because most RFID tags don't have enough computational power and storage capacity to perform encrypted communications.

To verify the integrity of RFID stream, we may also use a digital signature to sign packets in the stream individually. However the computational load on both the sender and the receiver is too high to make this approach practical. Also if a packet is missing, the authentication chain is broken and subsequent packets can not be authenticated.

Similarly, to check the integrity of database relations in electronic pedigree or ONS, a naïve method is to use the traditional digital signature [10]. Though this method is simple, there are some problems with it. First, the signature can only be used to verify whether the database has been modified or not; it cannot be used to localize and characterize the modifications. Second, if there is a need to make some necessary modifications to the database, we have to compute a new signature and discard the previous one. Besides, it is computationally intensive to generate and verify the signatures.

B. Requirements of RFID Security Protocol

It is clear that cryptographic mechanisms are not enough to ensure RFID data integrity. Considering the severe constraints imposed on the available power (include the antenna), the extremely computational capabilities, the small memory size and the characterize of IC design (e.g. number of gate available for security requirement), RFID security protocols must be lightweight in practice [4]. Also, security need not reside solely on the tag but the whole supply chain, the tag is only one piece of the security puzzle. It is worth to point out that for many applications, such as supply chain management, the counterfeiting of a single tag is not a worry. The counterfeiting of tags in bulk quantities is the issue that they worry about. Therefore, the ease with which a single tag can be counterfeited is not the only criterion. The ease with which tags may be counterfeited in bulk is the primary concern for retail and for pharmacy.

C. Fundamental of Watermarking

Digital watermarking, which allows an individual to add hidden copyright notices or other verification messages to digital media, can be a promising technique to protect RFID data from illicit manipulation and duplication. A generic watermarking model is depicted in Fig. 2. Where, *A(.)* is the attack mechanism; *S* is the original data before being watermarked; *D(.)* is the watermark detection function; *K* is the secret key used in both watermark embedding and watermark detection; and *M* is the watermark to be embedded in *S*. The watermark encoding function *E(.)* embeds *M* into *S* through *K*, and produces watermarked data *X*. Attackers may try to remove *M* from *X* by modifying *X* into *Y*. However, with a resilient watermarking scheme, the owner can still extract $M_0 = M$ from *Y* through *D(.)* and *K*.

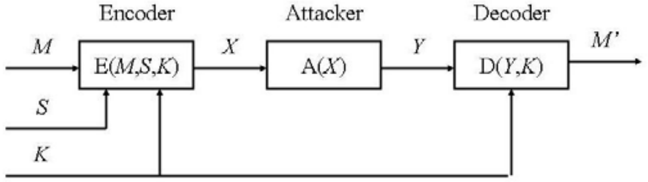


Fig. 2. A generic watermarking model

A good fragile watermarking scheme should satisfy the following desired properties [10]:

1) *The embedded watermark is imperceptible*: The embedded watermark should only introduce minor distortions

to the original data. Such modifications should not affect the usefulness of the data.

2) *Prevent illegal embedding and verification*: The whole process is governed by a key. Only an authorized person who has a key can embed, extract, and verify watermarks. This prevents unauthorized persons from inserting a false watermark or illegally verifying watermarks.

3) *Blind verification*: The original unmarked data should not be required for watermark verification.

4) *The extracted watermark indicates the locations of alterations*: In case of modifications, the embedded watermarks should indicate where the modifications are.

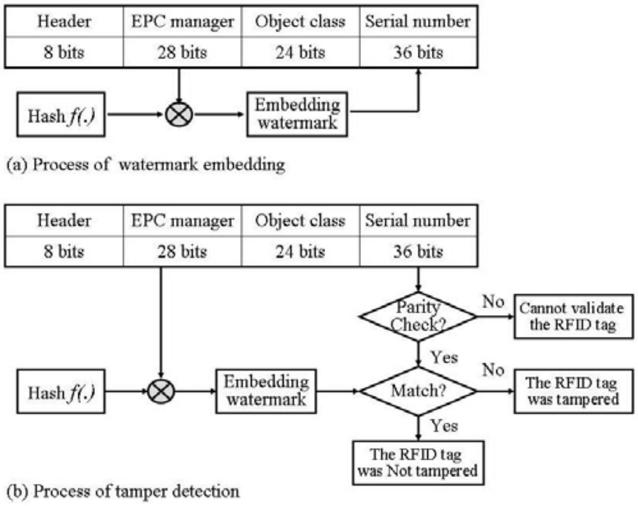
5) *Characterize alterations*: It is desirable that the embedded watermarks enable not only detection but also characterization of possible modifications so that it is possible to determine the kinds of modifications that have been made.

IV. RFID TAMPER DETECTION

There have been some research done to address the RFID data integrity issues using watermarking technologies [2] [7]. However, these researches are still limited which only focus on data tamper problem on certain portions of the RFID system such as RFID tag or RFID communications, but not the whole streaming of supply chain. In this section, we will reveal potential security threats especially in data tampering in RFID-enabled supply chain and show how they might be resolved using a fragile watermarking technology.

A. Tamper Detection in RFID Tags

[2] proposed a scheme to embed a fragile watermark in the serial number partition of the RFID tag. See Fig. 3. The process contains four stages:



(a) Process of watermark embedding

(b) Process of tamper detection

Fig. 3. Generic watermarking model for RFID tags

1) *Watermark generation*. The watermark is generated by using a pseudo random number generator (PRNG). The input is the data of EPC manager (EM) or Object Class (OC). EM or OC acts as a seed that generate a unique random number with a desired length (8bits).

2) *Selecting the embedding location*. The RFID tag data structure is composed of Header, EM, OC and serial number (SN). To embed a watermark, some redundant space within RFID tag signal will be used. However, Header, EM and OC are used for unique identification, modifying any of this data may interface with the existing standard; neither do they have enough room. Since SN can be decided by the manufacture at will and it offers enough redundant space to embed the watermark, the embedding location is chosen at SN portion.

3) *Watermark embedding*. An 8-bit watermark appended with an even parity bit is embedded to the first nine bits of the SN portion of RFID tag, show as Fig. 3(a).

4) *Tamper detection*. The data stored on EM is used to generate the watermark using the hash function *f(.)*, if the EM has changed, the generated watermark would be different from the one that embedded in the SN portion, then tampering can be easily identified, show as Fig. 3(b).

Although this is quite a novel method to integrate watermark and RFID technology together, it still has a lot of limitations. First, it can only work for EPC-96, but not for EPC-64, as the SN portion in EPC-64 only has limited 10 bits. Second, every time information hiding in RFID tag, it will occupy certain bits of SN portion of the RFID tag. So if we need to hide more information (including EM, OC, SN, TID, product properties etc.), it would be greatly reduced unique SN, making it infeasible. Also, the method has limited security because its security is ensured by keeping algorithm secret but not by a secret key. Moreover, the method can't prevent from tag forgery or tag cloning as the data in RFID tag does not change any bits in both situations.

One possible solution is to use the Code Division Multiple Access (CDMA) scheme, which supports multiple watermarks to be embedded synchronously. Thereby, we may use 8-10 bits to hide all these information together. Another possible solution is to hide some crucial information on RFID tags as shown below:

1) *RFID spoofing detection:* The basic idea is to hide the detailed properties of product in the respective RFID tag, the properties would be checked when the RFID reader scans the RFID tagged product at the point of sale (POS). This solution could then be used to detect tag spoofing.

2) *RFID cloning detection:* Since each transponder has a unique factory programmed chip SN (or transponder ID, TID) that is similar to the unique MAC address of PC network card, we can use the TID for cloning detection. Simple cloning attack can clone a similar tag SN, but can't clone TID without access to hardware manufacturing. So when unique tag identifier by manufacturer is embedded into RFID tag, we can easily detect RFID cloning.

3) *Expiry date detection:* We can also hide the expiry date of pharmaceutical drugs on the RFID tags [3]. This would prevent the sale of expired drugs, e.g. if an expired drug is scanned by the RFID reader, it would flash a signal indicating that this drug has already expired and should not be sold.

B. Tamper Detection in RFID Data Stream

When RFID tagged items are moved through physical supply chain, RFID data are treated as a continual stream which consists a sequence of data element in XML structure. The XML structure, as shown below, includes the following contexts: Tag ID, Discover Time, LastSeen Time, Antenna, and Read Count.

```
</Alien-RFID-Tag -List>
  <Alien-RFID-Tag>
  < Tag ID >8000 8004 2389 2371 </ Tag ID >
  <Discover Time> Thu Dec 04 10:14:49 PST 2007
  </Discover Time>
  <Last Seen Time> Thu Dec 04 10:14:49 PST 2007
  </Last Seen Time>
  <Antenna> 1< /Antenna >
  <Read Count>600</Read Count>
  </Alien-RFID-Tag>
</Alien-RFID-Tag -List>
```

Since the RFID streams are transmitted through unreliable network, malicious parties may easily inject offensive data into the stream. In order to authenticate completeness of RFID streams, two issues should be considered when signing streams. First, the signature scheme must be efficient enough to permit authentication on the fly without introducing delays. Second, the signature scheme must be robust enough that authentication remains possible even if some packets are lost.

1) *Problems and threat model.* To the best of our knowledge, there are four possible attacks to the RFID stream data:

a) *Attack 1: Content alteration*. Attackers may randomly or selectively modify some parts of the XML structure.

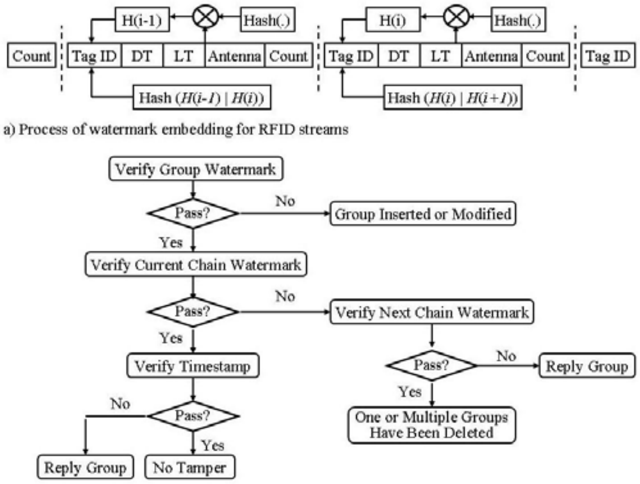
b) *Attack 2: Addition attack*. Attackers could insert one or multiple XML structures into the stream.

c) *Attack 3: Delete attack*. Attackers may delete one or multiple XML structures in the stream.

d) *Attack 4: Replay attack*. An attacker could copy a segment of a data stream and replay it later to the receiver.

2) *Possible solutions.* A simple method for detecting tampering on RFID stream data is to embed watermark into every isolated XML structure. Using a secret key *K*, a secure hash value *H(i)* is first computed as the hash of the concatenation of all individual hash values of data elements in XML structure. Since the watermark is embedded into the SN portion of tag ID, a remaining problem is that although we can detect modification of XML structure and insertion of new XML structure we cannot detect the deletion of the whole XML structure[7] [9]. A fragile chaining watermarking algorithm was proposed in [7] to verify the integrity of streaming data. The data are first divided into groups on the fly according to a secret key and synchronization point. A watermark is embedded directly into the least significant bits of all the data elements of each group to ensure the completeness of the data stream. Watermarks are then chained across current group and next group. Therefore, no matter how much data are deleted, the deletion can be correctly detected. However, such a schema is quite limited when used in RFID stream. The problem is that the method assumes that data stream consists of numerical data elements can tolerate small distortion introduced by embedding in the least significant bits of each data element. The method is applicable to such applications as stock market analysis, sports ticker and environment sensing; however, for RFID data stream, the data element such as Tag ID and Antenna ID cannot tolerate this distortion. Directly embedding a watermark to the least two significant bits in Tag ID will cause the ID no long unique. Meanwhile, if one or multiple XML structures are inserted or deleted, the synchronization point may be added or missing, thus, causing incorrect grouping.

3) *Our solution.* We improve the group-chaining watermark to detect tamper on RFID stream. Please see Fig. 4 for details. Since the data are naturally divided into groups by individual XML structure, we proposed to embed a watermark directly into SN portion of tag ID in each group to ensure the completeness of the data stream. Watermarks are then chained across current group and next group.



a) Process of watermark embedding for RFID streams

(b) Process of tamper detection for RFID stream

Fig. 4. Watermarking model for RFID data stream

The logic of the watermark embedding algorithm is as follows:

a) First for each available XML structure, we compute a secure hash *H(i)* according to the secret key *K*.

b) Then a group of watermarks is embedded by selecting first *n* bits in the SN portion of tag ID.

c) After that, a chaining watermark is constructed based on both current group hash value and next group hash value, which similarly is embedded into tag ID of current XML structure.

d) In this way, the embedded watermarks are actually chained so that even if the whole XML group is deleted, the deletion is still detectable.

We can use the following procedure to verify the integrity of the coming RFID data streams:

Step 1: We first check the integrity of the XML group, a watermark constructed from the current group hash value is usually checked against the extracted group watermark in the current group. If they do not match, we can conclude tampering (group inserted or group modified) occurs; Otherwise (if the two group watermarks match), we need continue to verify the chaining watermark.

Step 2: A chaining watermark constructed from the current group hash value and next group hash value is checked against the extracted chaining watermark in the current group. If the two chaining watermarks match, and the discover time in current group is close enough to current time, the current group is authentic and the watermark detection is successful. However, if the timestamp does not match, we can say this group is a faked reply group. IF, however, the current chaining watermark does not match, we need farther verify the chaining watermark in next group. If the two chaining watermarks in next group match, we know one or multiple group is deleted, otherwise current group is a reply group.

C. Tamper Detection in RFID Database

EPCIS represent things that happen in the field (events) as meaningful information and to manage the contexts between events so that all sorts of phenomena can be traced. EPCIS can be used for counterfeit and gray market detection, shrinkage avoidance and accurate and autonomous unit level inventory management, but if this database was unauthorized accessed, illegal modified or fabricated, most of the aforementioned advantages may be lost.

1) *Problem.* In EPCIS, the database relations contain independent tuples with little redundancy, and there is no enforced relationship between the tuples. These present new technical challenges for fragile database watermarking schemas.

2) *Possible solutions*. One of the simplest approaches is to use a tuple-based watermark schema proposed by [9]. The idea of this method is as follows: Some bits of attributes of tuples are modified according to an embedding key to embed watermark bits, but the watermark bit embedded in a tuple has nothing to do with those embedded in other tuples. Although this method can still detect attributes modification and tuple insertion, it cannot detect tuple deletion.

In order to add relationship between the tuples, we can have two possible options: One is to use the group-based watermark schema proposed in [9] and the other one is to use the chaining watermark schema proposed in [7].

For group-based watermark schema, all the tuples are first divided into groups according to the number of groups *g*, the hash value of embedding key *K*, and the primary key Tag ID. Only the person who knows *K* and *g* can determine which group the tuple belongs to. By grouping, the tuples are no longer independent, the relationship between them are enforced. Next, watermarks are embedded into each group independently. In each group, there are two kinds of watermarks: tuple watermark *W1* and attribute watermark *W2*. For tuple watermark, the hash value is generated by all attributes values of the same tuples; the attribute watermark is formed according to message authentication code and the same attribute of all tuples in the group. In this way, the embedded watermarks actually form a watermark grid, which helps to detect, localize and characterize the modification.

However, since grouping is controlled by an embedding key and the number of groups, while one or multiple tuples is modified or inserted, it may cause different result of grouping. This will unavoidably cause detection failure. For example, if one modified tuple changes from one group to another group, then tuple deletion is found in the first group and tuple insertion is found in the second group, despite tuples deleted do not affect grouping result. To avoid such a situation, for each group, we may first compare the extracted tuple watermark with the watermark constructed from the hash value of all attributes at the same tuple. If these two don't match, we then conclude that one or multiple attributes of the tuple was modified or this is an inserted tuple. After that, we discard all these tuples from the grouping. We then continue to compare the extracted attribute watermark with the watermark constructed from the hash value of same attribute of all tuples. If the two match, we know no tamper in this group; otherwise, one or multiple tuple are deleted.

It is worth to note that if the number of groups is one, the group-based watermark schema turns to be the database-oriented watermark schema. In the database-oriented watermark schema, all the tuples are related together, also there should be no more changes in grouping so that the embedded watermarks can localize and characterize alteration to the database. But if there is a need to make necessary modifications to the database, we have to compute a new attribute watermark and discard the previous one. Besides, it is computationally intensive to generate and verify the attribute watermark.

3) Now let us turn to the chaining watermark schema proposed in [7]. Here we make some extension of this method to fit for RFID database. The basic idea is first embedding tuple watermarks into each tuples of database, then constructing a chaining watermark based on both the current tuple hash and the hash of next tuple, show as figure 4. In this way, the embedded watermark are actually chained so even if the tuple is deleted, the deletion is still detectable. Chaining watermark seems a good solution, but still limited. Although it has good localization capability, it can not distinguish the alteration each other. For example, if a tuple's forward chain and backward chain are deleted, the tuple will be similar to a tuple inserted, therefore it can't tell if there is a tuple inserted or tuple deleted.

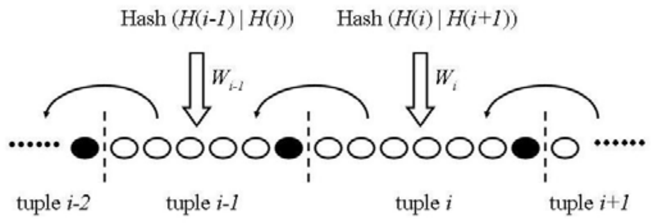


Fig. 5. Chaining watermark

4) Performance analysis. In general, we can classify the watermarking schema for database into four types: tuple-based method, group-based schema, database-oriented schema and chaining-based method. We have examined the database watermarking schemas in the open literature and summarized their relative performance, in terms of localization, characterize alteration, security, update and computational costs, in Table I. As can be seen from the table, there is no perfect database watermarking method that can gain all desired performances. Tuples-basis method has low computing cost, however it has bad localization. While group-based method and chaining-based method have good localization, their characterize alteration is low. While database-oriented method has good localization and characterize alteration, its computational cost and update cost is relatively high.

TABLE I: PERFORMANCE ASSESSMENT OF DATABASE WATERMARKING SCHEMA

	Tuples-basis	Group-based	Chaining-based	Database
Localization	bad	good	good	good
Delete detection	X	√	X	√
Modify detection	√	X	X	√
Insert detection	√	X	X	√
Security	low	high	low	medium
Update cost	One tuple	One or two groups	Two tuples	Whole database
Computational cost	low	Medium	low	high

D. Tamper Detection in ONS

In order to track down the relevant database, an ONS converts the manufacturer ID stored in the EPC into a web address. These ONS servers work analogously to the DNS used in the Internet. Tampering detection in ONS is similar to EPCIS. Please refer to Section V.C for details.

V. CONCLUSION

With recent advances in RFID technologies, the low-cost and high visibility value of this technology brings them the potential for massive deployment. Though RFID adoption is an emerging trend in supply chain management, the use of RFID has also triggered significant security and privacy concerns [2]. To minimize costs, most RFID tags don't have enough computational power and storage capacity to perform basic encrypted communications. Thus, traditional RFID related cryptography and security research may not be applied directly in this field. RFID security issue is still an open research question.

This paper highlights potential security threats especially in data tampering in RFID-enabled supply chain and shows how these threats might be resolved using a fragile watermarking technology. Here our security analysis focus on Gen 2 tag which is secure for its intended application, the retail supply chain, but not for many other applications. We have discussed various security attacks on Gen2 RFID systems, explored possible tampering detection using fragile watermarking on Gen 2 RFID tags, RFID data streams, ONS servers and enterprise database, surveyed relevant literature that has addressed the RFID data tampering issue, and discussed challenge and possible solutions. We provide a comprehensive approach to address data tampering problem in RFID in the hope to inspire more research in this field.

ACKNOWLEDGE

This work was part supported by Program for New Century Excellent Talents in Fujian Province University China and by the National Security Agency under Grant H98230-07-1-0219.

REFERENCES

[1] Y. Li and X. H. Ding, "Protecting the RFID communication in supply chains," Proc. of the 2nd ACM Symposium on Information, Computer and Communications Security (AsiaCCS'2007), March 20-22, 2007, Singapore, pp. 234-241.

[2] V. Potdar and E. Chang, "Tamper detection in RFID tags using fragile watermarking," 10th IEEE International Conference on Industrial Technology (ICIT2006), Mumbai, INDIA, Dec. 15–17, 2006

[3] M. Potdar, E. Chang and V. Potdar, "Applications of RFID in pharmaceutical industry," 2006 IEEE International Conference on Industrial Technology, 15-17 Dec. 2006

[4] P. Peris-Lopez et al., "RFID systems: a survey on security threats and proposed solutions," International Conference on Personal Wireless Communications, 2006. URL: http://lasecwww.epfl.ch/~gavoine/download/papers/PerisHER-2006-pwc.pdf

[5] L. Grunwald, "RFDump can hack RFID tags." URL: http://www.rfidgazette.org/2004/07/lukas_grunwalds.html

[6] M.Lehtonen, T. Staake, F.Michahelles and E.Fleisch, "From identification to authentication-A review of RFID product authentication techniques," Workshop on RFID Security 2006, July 2006.

[7] H. Guo, Y. Li, and S.Jajodia, "Chaining watermarks for detecting malicious modifications to streaming data", Information Sciences , Vol. 177, No. 1, 2007, pp281-298

[8] EPCglobal, "Pedigree ratified standard ," Version 1.0 as of January 5th, 2007. URL: http://www.epcglobalinc.org/standards/pedigree/pedigree_1_0-standard-20070105.pdf

[9] H. Guo, Y. Li, A. Liu and S.Jajodia, "A fragile watermarking scheme for detecting malicious modifications of database relations", Information Sciences, Vol. 176, No. 10, 2006, pp 1350-1378

[10] R. Agrawal and J. Kiernan, "Watermark relational databases," Proc. of the 28th Int. Conf. on Very Large Data Bases, 2002. URL: http://citeseer.ist.psu.edu/661572.html