Tamper Detection in the EPC Network Using Digital Watermarking

A relevant problem in RFID technology is the lack of security measures in the wireless communication channel between the reader and tag. This article analyzes potential data-tampering threats and proposes solutions using fragile-watermarking technologies.

SHUIHUA HAN
Xiamen University

CHAO-HSIEN CHU
Pennsylvania State University

ZONGWEI LUO
University of Hong Kong

RFID technology (see the "RFID and the EPC Network" sidebar), which allows wireless data transmission using radio waves, has attracted significant attention in the fields of supply chain and manufacturing, as well as a wide range of business applications. RFID's adoption is driven mainly by mandated requirements from major market players such as Wal-Mart and the US Department of Defense, and recent technology advances in areas such as wireless technologies and electronic product code (EPC) network protocols. Standards development has further driven RFID adoption. For example, advances in ultra-high-frequency RFID systems provided the necessary read range for warehouse applications. RFID can now scan products' tags as pallets move through the warehouse door. The technology also helps to ease the workload by scanning cases on high shelves.

Although RFID has the potential to revolutionize how businesses operate, its implementation isn't straightforward. Many issues and challenges, including security and privacy concerns, high cost, lack of universally accepted standards, data integration, reliability, business process redesign, employee resistance to change, and technology choice, must be addressed. Regarding security and privacy concerns, mainstream RFID research has focused on solving privacy issues; security in general and data tampering in particular are still open questions (see the "Related Work in RFID Antitampering" sidebar).[1] So far, EPCglobal protocols haven't adequately addressed these security problems. Most RFID data is transmitted in open air without proper protection, which opens loopholes for eavesdroppers and attackers[2] and introduces threats that could hinder large-scale RFID deployment, especially in the open-loop business environment.

Digital watermarking, an emerging technology for data protection, is an inexpensive way to protect RFID data from illicit manipulation and duplication. In the last few years, researchers have studied fragile watermarking schemas for multimedia products and systems extensively.[3] However, most focus on digital images or video and audio data; little work has addressed RFID data integrity and security issues. To the best of our knowledge, Vidyasagar Potdar and colleagues' "Tamper Detection in RFID Tags Using Fragile Watermarking" is the first study to propose a fragile-watermark solution to detect data tampering in RFID tags.[4] However, more advanced functionality is necessary to address data-tampering problems. Potdar and colleagues considered only data tampering in RFID tags; they didn't include the system's robust factors such as watermark length and security functions' secrecy.[4] Moreover, their solution doesn't prevent tag forgery or cloning attacks. Other researchers have tried to extend the schema with more robust factors, such as tamper detection in all areas of the RFID tag,[5] with secret keys, for tag forgery and cloning.[6] Building on these ideas, we present a watermark-based method to prevent tamper attacks in all areas of the RFID network.

 1540-7993/11/$26.00 © 2011 IEEE

Possible Tamper Attacks

RFID's pervasive nature exposes tags to two kinds of possible accesses: physical access and RF communication access. In the former, attackers can rarely tamper with the tag without the tag owner's knowledge. RF attacks, on the other hand, can cause potential loss by altering data on rewritable memory tags.[7]

There are several possible ways to attack RFID systems. A program called RFDump showed how vulnerable RFID tags are.[8] Attackers can easily read, alter, or delete tags using an inexpensive reader plugged into a notebook. Attacks can occur anywhere in the EPC network, including tags, readers, middleware, the EPCIS (Electronic Product Code Information Services) repository, the EPCIS accessing application, the local ONS (object name service), and the enterprise application database. We can classify the possible data-tampering attacks into five categories.

RFID Tag Tampering

We can divide tampering attacks on RFID tags into six types. In *data-impairing attacks*, adversaries use a reader to change the EPC number on tags in a supply-chain warehouse or retail store, disrupting business operations and causing a loss of revenue. In *wrong-data-insertion attacks*, adversaries replace tag data with new data containing erroneous values. Such attacks might lead to severe counterfeiting. In *data-deletion attacks*, adversaries erase tag data, setting all values including the EPC number to zero, to cause a loss of revenue.[9] In *tag-cloning attacks*, adversaries replicate RFID tags, which has proven to be very easy. All the necessary equipment, such as software and blank tags, is freely available. Tag clones can be used to counteract anti-counterfeiting measures in passports, drug labels, and so forth, and as a preparatory step in a large-scale theft scheme.[10] In *tag-swapping attacks*, thieves might replace an expensive item's label with a fake label containing a cheaper item's data. This attack has occurred on bar codes for years. *Tag-spoofing attacks* are a variation of tag cloning. The only difference is that spoofing doesn't involve physical reproduction of an RFID tag. Successful deployment of this attack requires specialized equipment that allows RFID tag emulation. Adversaries can use such an attack to access the restricted areas, sensitive information, and credentials.[9]

RFID Stream Tampering

In RFID applications, data is treated as a continuous stream instead of static datasets. When data is delivered over an unreliable wireless network, malicious parties can inject erroneous data. Potdar and colleagues presented a replay attack during an RFID streaming communication in which the attacker uses a tag's response to a rogue reader's challenge to destroy stream integrity. In such situations, RFIDs can be more vulnerable than other applications owing to their ability to be read at a distance.

RFID Database Tampering

The back-end database is the RFID system's backbone, and can be accessed at any time. It maintains detailed item information as well as tag data, which must match the data read from the RFID tag. Attackers might target the database by circumventing the organization's firewall and altering numerical values or deleting item data.

RFID and the EPC Network

Radio frequency identification (RFID) is a set of wireless technologies used to identify, capture, and transmit information from tagged objects to enterprise systems via radio waves. Early commercial RFID applications in the 1970s and 1980s were restricted to relatively few closed-loop applications—for example, security badges, toll passes, key cards, and gas-pump payment systems. Currently, most RFID tagging and tracking applications are used for operations in individual organizations.

To take RFID beyond the confines of a single organization and create value for the entire supply chain, a few breakthroughs are necessary. First, we need an interoperable, standardized way to uniquely identify items in the supply chain. Second, we need an interoperable, ideally standardized, means to discover and share the data that describes each identified item. Most important, we must reduce the RFID tags' manufacturing costs. All of these lead to the electronic product code (EPC) network.

The EPC network encompasses chip design standardization, employs EPCglobal technology, and is compatible with global standards, which results in lower RFID tag costs and helps improve supply-chain visibility for better control over the logistics process. However, the data storage capacity of those low-cost, passive tags is limited. EPC was designed to reduce cost per tag to make it more attractive to users. This has introduced considerable resource constraints and makes it difficult to provide adequate security measures for RFID.

One problem is the lack of security measures in the wireless communication channel between RFID reader and tag. Because the wireless channel isn't secure, attackers can eavesdrop at distances of up to several meters and discover the EPC stored in the tag.[1] Adding the necessary circuitry and power to the passive tags would increase cost. Although EPC Class-1 Gen-2 tags have enhanced security provisions to address some concerns, there is room for improvement. In particular, we need to focus on tags' low computational capacity, limited memory, and vulnerability to radio frequency access by hidden readers.[2]

References

1. A.N.M. Noman, K. Curran, and T. Lunney, "A Watermarking Based Tamper Detection Solution for RFID Tags," *Proc. 6th Int'l Conf. Intelligent Information Hiding and Multimedia Signal Processing*, IEEE CS Press, 2010, pp. 98–101.
2. F. Gandino et al., "Tampering in RFID: A Survey on Risks and Defenses," *Mobile Networks and Applications*, vol. 15, no. 4, 2009, pp. 1–15.

Related Work in RFID Antitampering

Because RFID tags carry unique item identifiers and details of the product to which they're attached, tampering with them has severe consequences. For example, if pharmaceutical tags are tampered with, they could represent the wrong drug when scanned by the RFID reader. This could be even worse when a smart shelf is coupled with RFID technology, as the wrong drugs might be picked up and delivered; it could even result in wrong diagnoses.[1] It can also raise repudiation issues in collaborative environments. To prevent unauthorized parties from tampering with information, an effective data protection mechanism is necessary.[2]

Currently, there are several approaches to detect RFID data tampering. We can roughly classify them into four different categories: symmetric cryptography, public-key cryptography, write activity record, and fragile watermarking.[3]

Symmetric-Cryptographic Method

In a symmetric crypto system, information is encrypted to ensure privacy.[4] Any data impairing is detected on decryption, so only authorized entities can check it. Wrong data insertion is possible only if the attacker has the secret key.

This schema is a simple approach to anticounterfeiting RFID tags because no special read/write protocol is required. However, it's feasible only for tags using the ISO 14443 standard. Most EPC tags don't have enough storage capacity to carry encrypted information. In addition, this method requires a high level of trust among the participants, because the system's robustness is based on the key's secrecy.

Public-Key-Cryptography Method

Paolo Bernardi and colleagues proposed an authentication approach based on the RSA encryption standard in which the tag's ID is encrypted and written in the user memory.[5] The authenticity checking corresponds to decryption of the number in the user memory. The tag and the corresponding product are false if the result doesn't correspond to the ID.

An advantage of this schema is that attackers can't insert erroneous data, because this action requires the knowledge of the secret key. In addition, it can prevent data copying, as copying of the signature from other tags generates false tags.

However, the authentication protocols require tags with larger memories and long data transmissions. Determining whether a tag is original or has been tampered with is impossible, and tamper evidence doesn't extend to other information contained in the tag. Authentication schemes based on public-key cryptography for RFID tags without cryptographic capability aren't effective antitampering approaches.

Write-Activity-Record Method

Akira Yamamoto and colleagues proposed a method based on the write activity record. In this approach, the RFID tag has a special memory area—tag private memory—that the tag can read and write but for which RFID readers have read-only privileges.[6] To check if data was overwritten, the tamper-detection method requires checking records in the tag private memory. If there's no overlap, the memory wasn't tampered with.

Because only the tag itself can write tag private memory, this approach allows the detection of all tampering actions and offers robust security solutions. The technology involves no cryptography or costly computation; any software can verify overlapping in the tag with a simple computation.

However, this method requires RFID tags to have additional memory and a special writing protocol. Although it detects all tampering actions, it assumes each rewriting operation is possible tampering, thus it isn't suitable for information systems that use the same memory area more than once. In addition, it can detect only tampering with written memory banks, but never wrong data insertion and data copying on unused banks.

Fragile-Watermarking Method

In "Tamper Detection in RFID Tags Using Fragile Watermarking,"

Cont. on p. 65

Electronic Pedigree Tampering

To ensure only authentic products are distributed through the supply chain, some regulatory agencies require an electronic pedigree for products, especially for prescription drugs.[11] The custody record provided by an electronic pedigree ensures that products were never in the wrong hands prior to consumption. However, if this e-pedigree is illegally accessed, modified, or fabricated, it might be unable to detect counterfeit products or shrinkage avoidance.

ONS Data Tampering

ONS can be considered a DNS (Domain Name Service) server, so, DNS server security threats, including file corruption, unauthorized updates, DNS cache poisoning, IP address spoofing, and data interception, also apply to ONS.

Tamper Detection Using Fragile Watermarking

Again, because the existing research addressing RFID data integrity issues using watermarking technologies focused only on RFID tags,[4,5] we try to extend the schema to the entire EPC network, addressing the attack areas beyond RFID tags.

Tamper Detection in RFID Tags

Because companies set the format of the first three

Table A. Evaluation of RFID antitampering approaches.

Characteristics		Symmetric-cryptograph schema	Public-key-cryptography schema	Write-activity-record schema	Fragile-watermarking schema
Tag requirement	Large memory	Yes	Yes	No	No
	Special memory area	No	No	Yes	No
Special reading/writing protocol		No	No	No	Yes
Robustness	Security mechanism	Key secrecy	N/A	N/A	Function secrecy
	No data copying	No	No	Yes	Yes
	Strong trust with partners	Yes	No	No	Yes
Enable correction or update		Yes	Yes	Yes	No
Tamper localization		No	No	No	Yes

Cont. from p. 64

Vidyasagar Potdar and colleagues proposed a tamper-detection system based on watermarking technology.[1] The fragile watermark is generated by performing three one-way functions on the header, EPC manager, and object class, respectively. The watermark check requires knowledge of its location in the EPC and the adopted one-way functions.

The watermarking approach can be an effective low-cost solution because it requires no special features for RFID tags and the communication protocols between reader and tags. In addition, it can identify not only whether data tampering has occurred but also the location.

However, this schema has some limitations.[3] First, the watermarking is based on a secret function; if an adversary obtains the function, huge modifications will be required. Second, it can be applied only to EPC 96-compliant RFID tags. Moreover, it can't prevent tag spoofing or cloning because the data in RFID tags doesn't change any bits in either situation.

Performance Assessment

Table A summarizes the four RFID antitampering approaches' relative performance. Existing approaches lack robust schemas based on low-cost tags and schemas usable for generic applications. Watermarking-based schemas are an effective low-cost solution but should be extended to different kinds of RFID tags.

References

1. V. Potdar et al., "Tamper Detection in RFID Tags Using Fragile Watermarking," *Proc. 10th IEEE Int'l Conf. Industrial Technology*, IEEE Press, 2006, pp. 2846–2852.
2. H. Guo et al., "A Fragile Watermarking Scheme for Detecting Malicious Modifications of Database Relations," *Information Sciences*, vol. 176, no. 10, 2006, pp. 1350–1378.
3. F. Gandino et al., "Tampering in RFID: A Survey on Risks and Defenses," *Mobile Networks and Applications*, vol. 15, no. 4, 2009, pp. 1–15.
4. S. Spiekermann, "Critical RFID Privacy Enhancing Technologies," *IEEE Security & Privacy*, vol. 7, no. 2, 2009, pp. 56–62.
5. P. Bernardi et al., "An Anti-Counterfeit Mechanism for the Application Layer in Low Cost RFID Devices," *Proc. 4th European Conf. Circuits and Systems for Communications*, IEEE CS Press, 2008, pp. 227–231.
6. A. Yamamoto et al., "A Tamper Detection Method for RFID Tag Data," *Proc. 2008 IEEE Int'l Conf. RFID*, IEEE Press, 2008, pp. 51–57.

EPC data fields—used as unique identification for header, EPC manager (EM), and object class (OC)—Potdar and colleagues proposed embedding a fragile watermark in the RFID tag's serial number (SN) partition.[4] Building on this idea, we created a modified watermarking-based schema for RFID tags, as Figure 1 shows. The process comprises four stages:

- *Watermark generation*. We generate the watermark using a secure hash, where K is the secret key used in both watermark embedding and detection. The header, EM, and OC data act as seeds that generate a unique random number of a desired length (in this case, 8 bits).
- *Selecting the embedding location*. To embed a watermark, we have to use some redundant space in the RFID tag. However, the header, EM, and OC are used for unique identification; modifications of this data might conflict with the existing standard. In addition, they don't have enough room. If the manufacturer designs an SN with more than 36 bits to embed the watermark, we can use the SN as the embedding location.
- *Watermark embedding*. First, we randomly choose 8 bits from the RFID tag's SN, which then perform an XOR operation with the 8-bit watermark. Watermarked EPC data is produced, as Figure 1a shows.
- *Tamper detection*. The data stored on the header,

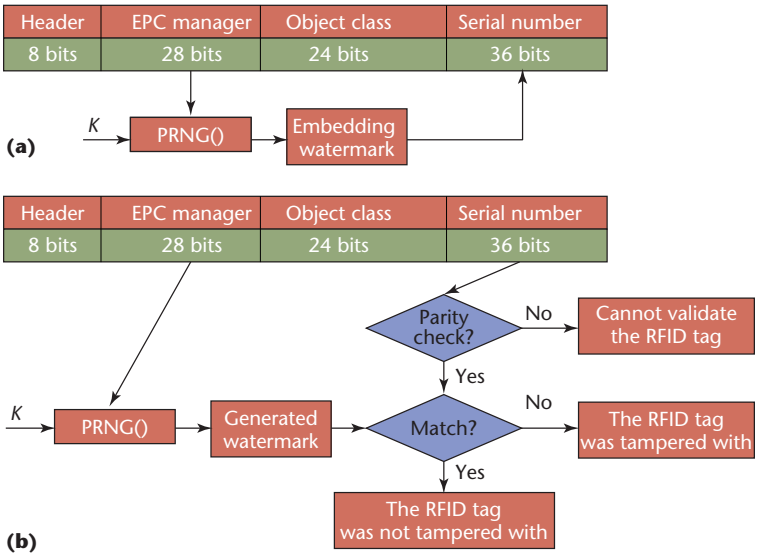

Figure 1. Watermarking model for RFID tags. (a) Watermark-embedding and (b) tamper-detection processes. The header, electronic product code (EPC) manager, and object class data act as seeds to generate the watermark using a secure hash function.

EM, or OC generates the watermark using the secure hash function. If the header, EM, or OC has changed, the generated watermark would differ from the one embedded in the SN. Then, we can detect tampering easily, as Figure 1b shows.

Although such a system allows tamper detection on the header, EM, and OC, it might not prevent tag cloning or spoofing because the RFID tag data doesn't change any bits in either situation. To prevent such attacks, we must hide some crucial information on the RFID tags. For RFID spoofing detection, we hide details of product properties that would be checked when the RFID reader scans the tag at the point of sale. Because each transponder has a unique factory-programmed chip SN, or transponder ID (TID), that is similar to the unique MAC address of a PC network card, we can use the TID for cloning detection. Simple attacks can clone a similar tag SN but can't clone TID without access to hardware manufacturing. So when the manufacturer's unique tag identifier is embedded in the RFID tag, we can detect RFID cloning easily.

Hiding the expiry date of pharmaceutical products could also prevent the sale of expired drugs.[3] For instance, if the RFID reader scans an expired drug, it could flash a signal indicating that the drug has already expired and shouldn't be sold.

Each time we hide information in the RFID tag, it occupies a number of bits of the tag's SN. Hiding more information (including EM, OC, SN, TID, and product properties) would greatly reduce space available for the unique SN, making it infeasible. To solve this problem, we propose the Code Division Multiple Access (CDMA) technique, which allows multiple watermarks to be embedded synchronously in the tag ID's SN. CDMA has been used widely in digital communication systems because of its cryptographic security and ability to achieve error-free transmission of the watermark in the maximum channel capacity.[9]

Figure 2 shows a watermarking system with spread spectrum communications. In this case, host data X is the communication channel, and multiple watermarks act as a signal transmitted through X. After that, the random-number SN portion of the RFID tag is replaced by the modulated signal, which can be used to detect multiple embedded watermarks. Details of this schema are outside this article's scope; we refer interested readers to "Multiple-Watermarking Scheme of the European Article Number Barcode Using Similar Code Division Multiple Access Technique."[12]

Tamper Detection in RFID Data Streams

There are four typical attacks on the RFID stream data:

- *Content alteration*. Attackers randomly or selectively modify some parts of the XML structure.
- *Addition attack*. Attackers insert one or multiple XML structures into the stream.
- *Delete attack*. Attackers delete one or multiple XML structures in the stream.
- *Replay attack*. Attackers copy a segment of a data stream and replay it later to the receiver.

Researchers have proposed several solutions. A simple method for detecting RFID stream data tampering is to embed watermarks into every isolated XML structure. Using a secret key K, a secure hash value $H(i)$ is first computed as the hash of concatenation of all individual hash values of the XML structure's data elements. Because the watermark is embedded in the tag ID's SN, we can detect XML structure modification and insertion, but we can't detect deletion of the whole XML structure.[11,13] In "Chaining Watermarks for Detecting Malicious Modifications to Streaming Data," Huiping Guo and colleagues proposed a fragile-chaining-watermarking algorithm to verify the streaming data's integrity.[11] The data is first divided into groups on the fly according to a secret key and a synchronization point. A watermark is embedded directly in the least significant bits of all the data elements of each group to ensure the data stream's completeness. Watermarks are then chained across the current group and next group. Therefore, no matter how much data is deleted, it can be detected correctly.

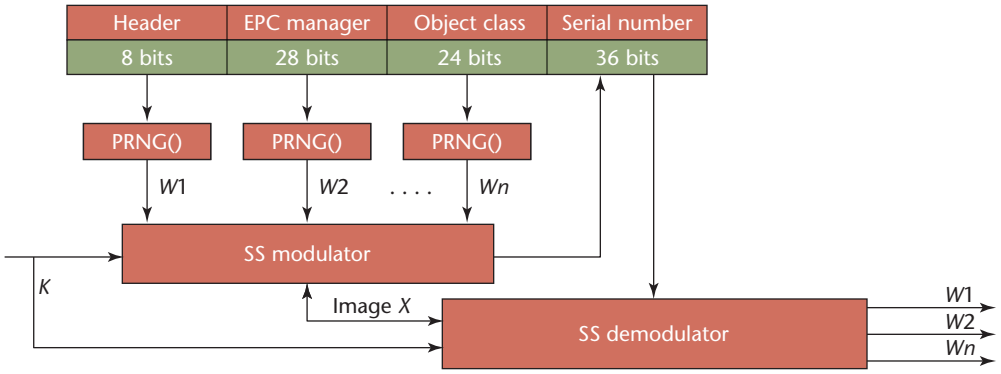

Figure 2. Code Division Multiple Access watermarking model for RFID tags. We can use this model to detect multiple embedded watermarks. (*W*1 and *W*2 are watermarks generated by electronic product code data fields.)

However, such a schema is limited when used in RFID streams. The problem is that the method assumes that a data stream consists of numerical data elements and can tolerate small distortions introduced by embedding in the least significant bits of each data element. We can use the method for such applications as stock market analysis, sports tickers, and environment sensing. But for RFID data streams, data elements such as tag ID and antenna can't tolerate this distortion. Directly embedding a watermark in the two least significant bits in tag ID will cause the ID to no longer be unique. And, if one or multiple XML structures are inserted or deleted, the synchronization point might be added or go missing, thus causing incorrect grouping.

Because the data is naturally divided into groups by individual XML structures, we propose a modified group-chaining method.[6] A watermark is embedded directly in the first n bits of the tag ID's SN in each group to ensure the data stream's completeness. Then a chaining watermark is constructed on the basis of both the current group's hash value and the next group's hash value, which is also embedded in the current XML structure's tag ID. Such a method not only ensures each group's data integrity but also successfully detects when multiple groups are deleted.

Tamper Detection in RFID Databases

EPCIS can be used for counterfeit and gray-market product detection, shrinkage avoidance, and accurate and autonomous unit-level inventory management. However, if someone accesses the database without authorization, or illegally modifies or fabricates it, these advantages might be lost.

In EPCIS, the database relationships contain independent tuples with little redundancy, and there is no enforced relationship between the tuples. This presents new technical challenges for fragile database watermarking schemas.

One of the simplest approaches is the tuple-based watermark schema proposed in "Tamper Detection in RFID-Enabled Supply Chains Using Fragile Watermarking."[6] We modify some bits of tuples' attributes 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 detect attribute modification and tuple insertion, it can't detect tuple deletion. To add relationships between the tuples, we have two possible options—the group-based watermark schema and the chaining-based watermark schema.

For the group-based watermark schema proposed in "Chaining Watermarks for Detecting Malicious Modifications to Streaming Data," all 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.[13] Only those who know K and G can determine to which group the tuple belongs. By grouping, the tuples are no longer independent, and the relationships between them are enforced. Next, watermarks are embedded in each group independently. Each group has two kinds of watermarks: a tuple watermark $W1$ and an attribute watermark $W2$. For the tuple watermark, we generate the hash value using the values of all attributes of the same tuple; the attribute watermark is formed according to the message authentication code and the same attribute of all tuples in the group. In this way, the embedded watermarks form a watermark grid, which helps to detect, localize, and characterize the modification. However, because grouping is controlled by an embedding key and the number of groups, when one or multiple tuples are modified or inserted, different grouping results might occur and cause detection failure.

It's worth noting that if the number of groups becomes one, the group-based watermark schema becomes the database-oriented watermark schema.

Table 1. Performance assessment of database watermarking schemas.

	Tuples based	Group based	Chaining based	Database oriented
Localization	Bad	Good	Good	Good
Delete detection	No	Yes	No	Yes
Modify detection	Yes	No	No	Yes
Insert detection	Yes	No	No	Yes
Security	Low	High	Low	Medium
Update cost	One tuple	One or two groups	Two tuples	Whole database
Computational cost	Low	Medium	Low	High

In the database-oriented watermark schema, all the tuples are related, and there should be no grouping changes, so the embedded watermarks can localize and characterize alterations to the database. But if database modifications are necessary, we have to compute a new attribute watermark and discard the previous one. Generating and verifying the attribute watermark is computationally intensive.

We extend Guo and colleagues' chaining-based watermark schema to fit the RFID database.[11] The idea is to first embed tuple watermarks in each database tuple, then construct a chaining watermark on the basis of both the current tuple's hash and the next tuple's hash. In this way, the embedded watermarks are actually chained so even if the tuple is deleted, the deletion is detectable. Although the chaining-based watermark schema has good localization capability, it can't distinguish alterations from one other. For example, deleting a tuple's forward chain and backward chain is similar to an inserting tuple; therefore, the schema can't tell whether a tuple was inserted or deleted.

In general, we can classify the watermarking schema for a database into four types: tuples-based method, group-based schema, chaining-based method, and database-oriented schema. We examined the database watermarking schemas in the open literature and summarized their relative performances in terms of localization, characterization of alteration, security, and update and computational costs. As Table 1 shows, no database watermarking method can achieve all desired security parameters. The tuples-based method has low computing cost but bad localization. The group- and chaining-based methods have good localization, but their characterization of alteration is low. And although the database-oriented method has good localization and characterization of alteration, its computational and updating costs are relatively high.

Tamper Detection in Electronic Pedigree

E-pedigree can prevent costly mistakes by tracking an item. For instance, medical mistakes can be life threatening if the medication has been tampered with. E-pedigree stays with the drug, and if it goes to a suspicious site, informs the pharmacist before the drug is prescribed. Regulations allow the use of digital signatures on e-pedigrees so they can be self-authenticated upon receipt, without employing methods that require communication with each upstream owner of the drug, making it more difficult to tamper with.

Tamper Detection in ONS

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 on the Internet. For such situations, a chaining-based watermark schema can be embedded in a tag's SN portion in each ONS tuple. Details of tampering detection in ONS are similar to EPCIS.

Although RFID adoption is an emerging trend in healthcare and supply-chain management, the use of RFID has triggered significant security and privacy concerns. This article highlights potential security threats especially in the form of data tampering in RFID or EPC networks and shows how these threats might be resolved using a digital watermarking technology. Tampering detection is considered one of the important enabling technologies for product anticounterfeiting, which can be applied to ensure the information system or network integrity and provides a technological foundation for digital forensics.

We intend to carry this research further to apply in various application domains, especially in logistics, supply-chain management, and healthcare, to help ensure integrity in product traceability and confidence in product trustworthiness. □

Acknowledgments

The National Science Foundation of China partially supported this work under grants 70971112 and 70902042.

References

1. A. Jules, "RFID Security and Privacy: A Research Survey," *IEEE J. Selected Areas Comm.*, vol. 24, no. 2, 2006, pp. 381–394.
2. L. Mirowski et al., "An RFID Attacker Behavior Taxonomy," *IEEE Pervasive Computing*, vol. 8, no. 4, 2009, pp. 79–84.
3. C. Collberg et al., "Watermarking, Tamper-Proofing, and Obfuscation Tool for Software Protection," *IEEE Trans. Software Eng.*, vol. 28, no. 8, 2002, pp. 735–746.
4. V. Potdar et al., "Tamper Detection in RFID Tags Using Fragile Watermarking," *Proc. 10th IEEE Int'l Conf. Industrial Technology*, IEEE Press, 2006, pp. 2846–2852.
5. A.N.M. Noman, K. Curran, and T. Lunney, "A Watermarking Based Tamper Detection Solution for RFID Tags," *6th Int'l Conf. Intelligent Information Hiding and Multimedia Signal Processing*, IEEE CS Press, 2010, pp. 98–101.
6. S. Han and C.-H. Chu, "Tamper Detection in RFID-Enabled Supply Chains Using Fragile Watermarking," *Proc. 2008 IEEE Int'l Conf. RFID*, IEEE Press, 2008, pp. 109–115
7. F. Gandino et al., "Tampering in RFID: A Survey on Risks and Defenses," *Mobile Networks and Applications*, vol. 15, no. 4, 2009, pp. 1–15.
8. L. Grunwald, "RFDump Can Hack RFID Tags," 29 July 2004; www.rfidgazette.org/2004/07/lukas_grunwalds.html.
9. A. Juels, R. Rivest, and M. Szydlo, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy," *Proc. 10th ACM Conf. Computer and Comm. Security*, ACM Press, 2003, pp. 103–111.
10. S. Spiekermann, "Critical RFID Privacy Enhancing Technologies," *IEEE Security & Privacy*, vol. 7, no. 2, 2009, pp. 56–62.
11. H. Guo et al., "A Fragile Watermarking Scheme for Detecting Malicious Modifications of Database Relations," *Information Sciences*, vol. 176, no. 10, 2006, pp. 1350–1378.
12. W.Y. Chen, "Multiple-Watermarking Scheme of the European Article Number Barcode Using Similar Code Division Multiple Access Technique," *Applied Mathematics and Computation*, vol. 197, no. 1, 2008, pp. 243–261.
13. H. Guo et al., "Chaining Watermarks for Detecting Malicious Modifications to Streaming Data," *Information Sciences*, vol. 177, no. 1, 2007, pp. 281–298.

ShuiHua Han *is a professor at Xiamen University. His research interests include RFID, supply-chain management, and operations and technology innovation. Han has a PhD in computer software from the Huazhong University of Science and Technology. Contact him at hansh@xmu.edu.cn.*

Chao-Hsien Chu *is a professor of information sciences and technology at Pennsylvania State University. His research interests include information assurance and security, RFID and the Internet of Things, and operations and technology innovation. Chu has a PhD in management science and information systems from Pennsylvania State University. Contact him at chc4@psu.edu.*

Zongwei Luo *is a senior researcher at the University of Hong Kong. His research interests include RFID and the Internet of Things, service science and computing, technology adoption, and innovation management. Luo has a PhD in computer science from the University of Georgia. Contact him at zwluo@eti.hku.hk.*