# Security and Privacy in RFID and Applications in Telemedicine

*Yang Xiao, University of Memphis; Xuemin Shen, University of Waterloo*
*Bo Sun, Lamar University; Lin Cai, University of Waterloo*

## ABSTRACT

Radio frequency identification systems have many applications in manufacturing, supply chain management, inventory control, and telemedicine. In an RFID system, products and objects are given RFID tags to identify themselves. However, security and privacy issues pose significant challenges on these systems. In this article we first briefly introduce RFID systems. Then two RFID applications in telemedicine are proposed: studying supply and demand of doctors, nurses, and patients in hospitals and healthcare, and developing mobile telemedicine services. The security and privacy issues of RFID, and their solutions are discussed as well.

## INTRODUCTION

Radio frequency identification (RFID) systems can identify an object or a person using wireless transmission. An RFID system consists of RFID tags (also called transponders) and readers (also called interrogators). Readers broadcast queries to tags in their wireless transmission ranges for information contained in tags, and tags reply with required information such as identification (ID) numbers. Tags have very low cost (e.g., $0.05 each), limited storage, and limited computing capability. Some tags have no batteries and are powered via readers wirelessly. RFID systems have been gaining more popularity in areas such as supply chain management, automated identification systems, and anyplace requiring identification of products or people. For instance, Wal-Mart has recently attempted widespread adoption of RFID systems: all incoming inventory items from manufacturers contain RFID tags [1]; items enter a Wal-Mart store via a loading dock, and are interrogated by RFID readers, which interface with an application system to register items' identification codes and descriptions. The United States Department of Defense (DoD) and Department of Homeland Security (DHS) have started to push potential RFID adoption. While the DoD is looking into using RFID technology to track goods and materials (e.g., containers worth more than $5000), the DHS is looking into implementing RFID technologies to help fight global terrorism (e.g., studying how RFID technology speeds the movement of people crossing borders while reducing the threat of terrorism) [2]. European Central Bank planned to use RFID tags in Euro bank notes by 2005 as a tracking mechanism for law enforcement agencies to prevent criminal transactions [3].

An RFID system has also been applied in telemedicine, which employs wired or wireless communications to provide medical information and services. In 2003 Alexandra Hospital in Singapore used an RFID tracking system during the severe acute respiratory syndrome (SARS) outbreak. All patients, visitors, and staff entered the hospital using RFID ID cards so that if someone was diagnosed with SARS later, all individuals who contacted the person in the hospital could be immediately identified. In 2004 the Center for Aging Services Technologies (CAST), an organization run by Intel, demonstrated two RFID monitoring systems in Washington, DC [4]. RFID tags were affixed to medicine bottles, teacups, and other objects regularly used in the home. Caregivers receiving data from RFID readers attached to the back of individuals' hands can monitor seniors' daily activities by recording which and when tagged items have been picked up. In addition, the RFID systems can be used to manage medicine and hospital equipment, track critical care assets, and help doctors and nurses to keep tabs on their patients frequently and remotely.

However, there are risks of corporate espionage, consumer/personal privacy validation, and location privacy [5]. Security and privacy are two important issues in RFID systems. Tags are vulnerable to eavesdropping, traffic analysis, spoofing, or denial of service [6]. Unauthorized readers may access tags, so privacy might be invaded. Customers can be tracked via carried tags' responses no matter whether information in tags is protected or not, so location privacy may be invaded. Furthermore, inventory data


0163-6804/06/$20.00 © 2006 IEEE

has significant financial value among competitors of commercial companies.

Current RFID systems have not adopted cryptography due to limited resources. RFID tags are subject to surreptitious scanning, and it is difficult to achieve access control and data privacy, but they are highly mobile and contain sensitive personal information. The most challenging issue is that tags are highly resource-constrained, and therefore cannot support strong cryptographic primitives, tamper-resistant packaging, and other security enhancing features; for example, hash functions such as MD5 and SHA-1 are beyond the capabilities of today's tags [5].

In this article we first provide a brief introduction to RFID. Then two applications of RFID in telemedicine are proposed: studying supply and demand of doctors, nurses, and patients in hospitals and healthcare, and developing mobile telemedicine services. Finally, we present a discussion on security and privacy issues of RFID, as well as their solutions.

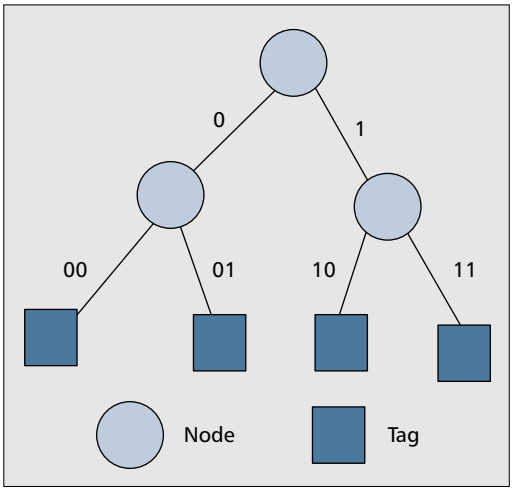


**Figure 1.** *Tree walking with tags' IDs with a length of 2 bits.*

*The RFID system is a contention-based system in which collisions happen if more than one tags respond to the reader's query at the same time. Contention resolution protocols include binary tree walking protocol, Aloha, etc.*

## Radio Frequency Identification System

An RFID system includes tags, readers, and an application system. When a tag attached to a person/object passes through an electromagnetic field generated by a reader and detects a signal from the reader, it identifies itself. Each tag includes a serial number, a model number, color, place of assembly, or other data. Tags that do not contain microchips are called *chipless* tags. On the other hand, tags containing microchips are called *chip* tags. There are two types of tags: *active* and *passive*. An active tag contains a small power source (e.g., a battery), whereas a passive tag does not contain any power source and uses the power generated by a reader. Most tags are passive due to the cost efficiency of mass production of passive tags. Readers are devices that read/interrogate tags, and each reader is equipped with antennas, a transceiver, and a processor. Operating frequency determines the capability of an RFID system, and the Federal Communications Commission (FCC) defines four different frequencies: low frequency at 125 Hz, high frequency at 13.56 MHz, ultra high frequency at 868–915 MHz, and microwave at 2.45 and 5.8 GHz. The corresponding ranges of these operating frequencies are approximately less than 0.5 m, 1 m, 3 m, and 1 m, respectively [7].

The RFID system is a contention-based system in which collisions happen if more than one tags respond to the reader's query at the same time. Contention resolution protocols include binary tree walking protocol, Aloha, and so on. In the following we introduce the binary tree walking protocol, the most popular protocol for RFID.

### Binary Tree Walking

Let $N$ denote the length of IDs of tags in bits. A binary tree can be built as follows. A node of depth $d$ ($d = 0, \ldots, N$) is labeled with a binary string $S$ of length $d$, and has two children with depth $d + 1$: the left child is labeled $S||0$ and the right child is labeled $S||1$, where $||$ stands for concatenation. The root is empty and its depth is zero, and there are $2^N$ leaves with depth $N$. These leaves represent IDs of all tags with length $N$. An example of the tree walking protocol with a length of 2 bits is shown in Fig. 1.

The binary tree walking algorithm is a recursive depth-first search for the reader to find all IDs of tags. The algorithm is recursively run from the root with depth first. When the reader queries a node with binary string $S$ with length $d$ (i.e., its depth is also $d$), all tags whose IDs have $S$ as the prefix response the next bit. Each tag in the left subtree of the node sends 0, and each tag in the right subtree of the node sends 1. If their next bits are different, a collision happens, and the reader sequentially runs the algorithm on the node with the label $S||0$ and the node with the label $S||1$. If there is no collision and all tags send the same bit $a$, the reader will sequentially run the algorithm on the node with the label $S||a$, ignoring the other child node. If the algorithm reaches a leaf, it outputs its $N$-bit ID. In this way, IDs of all tags are output.

## Applications of RFID in Telemedicine

We propose two RFID applications in telemedicine. The first application is to study supply and demand in hospitals and healthcare. The second application is mobile telemedicine using smart sensors. Related security and privacy issues are also discussed.

### Supply and Demand in Hospital and Healthcare

In this application supply and demand can be studied for doctors, nurses, and patients in hospitals and healthcare services. Doctors, nurses, and patients have RFID tags attached so that bottlenecks of supply and demand among them can be identified and improvements can be made possible. RFID tags can be built as plastic bands strapped onto wrists. In the tags only an ID is stored to reduce security and privacy attacks.

*Involved people must be fully aware of the RFID systems. A voluntarily-based scheme can be considered, but may not be effective since not all persons and places are involved. Pre-agreements may be considered as a better approach.*

The unique ID is associated with a database record saved in a server connected to RFID readers. In the database the record of a patient may include the patient's name, date of birth, gender, and a medical record number, billing, medical insurance, pharmacy, and so on. RFID readers can be fixed in each room or mobile in tablet-style PCs with wireless LAN connections. For doctors and nurses, tags are embedded in their access IDs, which are normally used to access all kinds of rooms.

Analysis of activities of doctors and nurses can be performed, especially in emergency rooms, such as measuring the flow of doctors and nurses, including the time periods they spend on some patients or wait for some conditions such as resource conflicting before doing something. Therefore, bottlenecks can be identified and improvements with high parallelism and reducing resource conflicts can be achieved.

Analysis of patient access services can also be performed, such as measuring patient flow including the time periods of patients spending on each stage of their treatment such as registration, waiting in the room, and waiting in the bed, etc. The RFID tags can track their locations and times (e.g., the time it takes to move from one area to another), as well as some medical tests.

There are privacy and security issues in this application. For the privacy issues, personal information of involved people such as patients, doctors, and nurses may be revealed to attackers or other unnecessary personnel. Involved people must be fully aware of the RFID systems. A voluntary scheme can be considered, but may not be effective since not all persons and places are involved. Pre-agreements may be considered as a better approach. Furthermore, security mechanisms should be used to protect the privacy of involved people. For instance, only an ID is stored in a tag to reduce security and privacy attacks. No one using a tag can access the database in which sensitive information is stored. Security mechanisms should be applied to the computer/communication system in which the database is located to prevent physical/remote accesses from any unauthorized personnel.

For security issues, first, tags are subject to cloned attacks. An attacker can clone an authorized person's tag ID if he/she can physically access the tag ID or scan the tag ID using an unauthorized reader, and then use the cloned tag ID to access places in the hospital. To reduce this kind of attack, the database should monitor all active tags' activities so that if there are tags with the same ID, an alert is produced to inform related personnel, and some proper security procedures should be followed. The above procedure can also avoid multiple-ID attack in which an attacker using multiple cloned tags pretends to have multiple identities. Second, tags are subject to revealing their IDs to an unauthorized reader. We discuss some security and privacy solutions that can be used to prevent revealing a tag's ID to an unauthorized reader in the next section. A more effective way is that a tag should be able to authenticate the reader via a procedure as follows. The tag randomly chooses a challenge text to ask the reader; the reader encrypts the challenge text using a pre-agreed key and sends back the output; then the tag judges whether the reader is authorized or not. When the reader is authenticated, the tag can issue its encrypted ID. The cost of this kind of tag may be a little bit higher, but it is reasonable for the particular application. More sophisticated schemes can be designed if cost is not an issue.

### Mobile Telemedicine Service

Wireless microsensor technology provides a unique opportunity for delivering quality healthcare to patients inside and outside hospitals. Intel's Caregiver's Assistant and Georgia Tech's Memory Mirror use RFID tags to monitor the activities of the elderly at home and help caregivers to improve the quality of healthcare [4, 8]. In addition to in-home monitoring, RFID tags can be used to monitor patients in a hospital, in an ambulance, and even in a disaster area [9]. In the following we propose a real-time patient monitoring system that can use smart sensors to collect patients' vital signs so that medical specialists can perform remote diagnosis anywhere and at any time. Intelligent location tracking functions will also be incorporated to locate mobile patients in case of emergencies. This system can substantially reduce response time to medical emergencies and improve the accuracy of remote diagnosis. The impact of the real-time patient monitoring system can be tremendous in benefiting healthcare providers as well as the entire healthcare industry, and improving the health of our society. The system can also be used in a variety of other important applications, from monitoring soldiers' conditions on a battlefield to tracking relief workers in a disaster area.

A large number of microsensors can be attached noninvasively to patients to collec electrocardiogram (ECG), pulse rate, basal temperature, and other vital signs. RFID tags are used to identify patients' locations so that in case of emergency, patients can easily be found. These medical sensors can transmit their data wirelessly to some special sensors, called cluster heads, for further processing such as compression. The processed data are then transmitted to a tablet-style PC, a wireless personal digital assistant (PDA), or a cellular phone. These devices not only display and store the data locally, but also forward the data to remote medical specialists over a wireless LAN (WLAN)/metropolitan area network (MAN) or cellular network. Medical specialists can monitor patients' vital signs, anywhere and at any time, and perform remote diagnosis as well as commands/queries to the sensor network (e.g., to activate more sensors in a particular area). Intelligent location tracking functions using RFID are adopted to locate mobile patients in case of emergencies. Figure 2 illustrates a possible architecture for such a patient monitoring application.

In a typical ambulance system, a camera takes an ambulance patient's video clips and transmits it to the consultation unit of a medical center. At the same time, the emergency medical paramedics (EMPs) use a wireless cellular connection to talk to doctors or medical professionals. An ambulance workstation continuously collects data from the patient's body and sends it

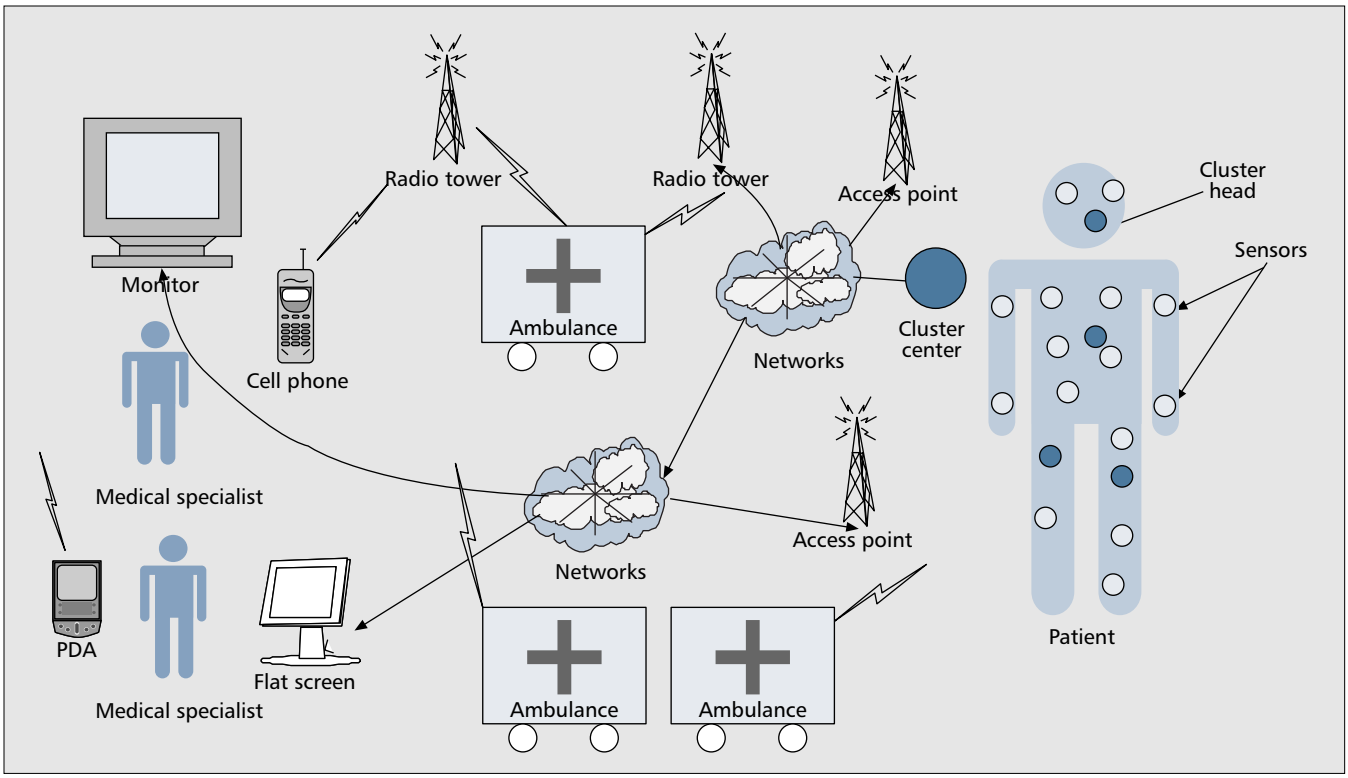


**Figure 2.** *Mobile telemedicine architecture.*

to the doctors. Serious patients or elderly people can use second-highest priority calls to communicate with the medical center by carrying a special piece of equipment called a medical phone, which communicates with the base station (BS) directly. For instance, a medical phone can be made through a regular cell phone with a standard infrared (IrDA) port that can collect sensing data from body microsensors. Patients may also use medical watches instead of medical phones to relay sensing data to other sensor nodes or the medical specialist of their respective cell. These watches, however, have much lower battery power than medical phones and can only relay their data through multihop routes to other nodes (e.g., a nearby medical phone) or a medical specialist. If the patients carry a medical phone and establish a call with the medical center using it, the system will assign a lower priority to it than that of serious patients.

Medical specialists periodically send queries to the sensor network and then collect medical data based on patients' responses. The medical specialists keep a connection with the medical center in order to receive commands at any time and transmit patient data. Since the specialists work in two kinds of networks — sensor networks (for handling medical query) and cellular networks (when communicating with the hospitals) — they will have an internal frequency transfer circuit and protocol interface to guarantee their dual-operation mode. The call between a medical specialist and a medical center is assigned a lower priority than normal patients' calls.

With the advent of wireless microsensors such as pulse oximetry, pH monitoring, echocardiogram, and Berkeley Motes, and an aging society with more people requiring long-term care, it is the perfect timing to develop a sensor network for patient monitoring. Wireless sensors are very small in size (e.g., a Mote is the size of a quarter), and can easily be attached to patients and allow the patients to move around freely. Moreover, since they have wireless communication capability, wireless sensors allow physicians to monitor their patients remotely. This kind of sensor network is also extremely versatile. They can also be used to monitor people working in dangerous conditions, such as firefighters in a burning building, relief workers in a disaster area, and soldiers on a battlefield.

Sensors can be connected wirelessly, although currently most of them are connected through wired links. Some telemedicine examples of current sensors are listed below.

**Pulse oximetry:** An oximeter is a small machine that measures the amount of oxygen in the blood. To obtain this measurement, a small sensor (e.g., a Band-Aid) is tapped onto a finger or toe. When the machine is on, a small red light can be seen in the sensor. The sensor is painless, and the red light does not become hot.

**pH monitoring:** It is a measurement of the acidity inside the esophagus that it is helpful in evaluating gastroesophageal reflux disease (GERD). A thin plastic tube is placed into a nostril, guided down the throat, and then into the esophagus. The tube stops just above the lower esophageal sphincter, which is at the connection between the esophagus and the stomach. At the end of the tube inside the esophagus is a sensor that measures pH, or acidity. The other end of the tube outside the body is connected to a monitor that records the pH levels for a 12- to 24-hour period. Normal activity is encouraged

RFID tags can be killed and re-activated before consumers walk out of the stores or upon purchase. For instance, a reader can kill a tag by sending a killing command with a short 8-bit password. However, in many situations, killing tags is unworkable or undesirable.

during the study, and a diary is kept of symptoms experienced or activity that may be suspicious for reflux, such as gagging or coughing. The pH readings are evaluated and compared to the patient's activity for that time period.

**Echocardiogram —** What types of problems do children with Down syndrome typically have? About 40 to 50 percent of babies with Down syndrome have heart defects. Some defects are minor and may be treated with medications, while others may require surgery. All babies with Down syndrome should be examined by a pediatric cardiologist, a physician who specializes in heart diseases of children, and have an echocardiogram (a procedure that evaluates the structure and function of the heart by using sound waves recorded on an electronic sensor that produces a moving picture of the heart and heart valves) in the first two months of life so that any heart defects can be detected.

The design of the discussed sensor network architecture for patient monitoring will not only be guided by system design goals common to all sensor networks (e.g., energy efficiency and high sensing coverage), but also reflect the special needs of healthcare providers and patients. Sleep scheduling mechanisms are used to extend the monitoring lifetime of the sensor network. Because microsensors are usually powered by batteries and are prone to other types of failures, a large number of redundant sensors are deployed, and scheduling mechanisms are used that allow sensors to work and sleep alternately in order to maximize their total working time. Tracking mechanisms can be done using RFID tags that allow patients to be located during emergencies.

Security/privacy aspects of this architecture should also be considered as the previous application about studying supply and demand of doctors, nurses, and patients. However, this application involves more people, parties, and devices; therefore, more comprehensive schemes on security and privacy need to be carefully designed. In addition, the involved wireless networks, such as WLANs, cellular and sensor networks, RFID systems, and the integrations of them should be secure. Security mechanisms are also necessary for RFID usage for location tracking in this application. In the following section we discuss the security and privacy issues in RFID systems, as well as their solutions.

## Security and Privacy Issues and Solutions

In RFID systems universal deployment of tags may create new security and customer privacy issues. For instance, customers' items can be scanned by un-authorized personals collecting customers' information for different purposes, and passive eavesdroppers can listen to interactions between tags and authorized readers. Therefore, passive eavesdroppers may have more ability than authorized readers so that signals broadcasted by authorized readers can be heard several hundreds of meters away, whereas authorized readers can only hear signals of tags nearby [6]. A reader/attacker can potentially discover individuals' informational preferences without their permission if they carry items with RFID tags, revealing privacy information by linking an ID of a tag to a person in a database. These may be used, for instance, to collect information on unsuspecting people nearby, or to have household items report on the presence of certain other items in the owner's home that could be used against the owner, or to store extra identifiers in the tags.

In the following, we first present several mechanisms to enhance privacy such as killing tags, shielding tags, locking tags, re-encrypting tags, silent tree walking, regulating tags, selective blocking tags, anonymous tags, and hash-based anonymous tags. Then attacks and lightweight encryption algorithms are discussed. Since security and privacy are closely related, we do not make explicit distinctions between security solutions and privacy solutions in this article.

### Killing Tags

RFID tags can be killed and reactivated before consumers walk out of stores or upon purchase. For instance, a reader can kill a tag by sending a killing command with a short 8-bit password. However, in many situations, killing tags is unworkable or undesirable (e.g., stores may need scanning tags if products are returned by costumers), and some tags require reusability in some applications [10].

### Shielding Tags

Tags can be shielded using special containers made of metal mesh or foil. However, most of products cannot be placed in such containers. Furthermore, after products are taken out of the containers for daily usage, they can still be scanned by unauthorized personal. Another approach of shielding tags is to let tags broadcast jamming signals to prevent from readings, but this scheme wastes energy and causes inferences to other systems.

### Locking Tags

A randomized hash lock protocol for private authentication is proposed in [6]. A tag with an ID saved in memory has two states: locked and unlocked. The tag can be locked to prevent revealing information using the *ID*, and a locked tag can be unlocked using another key *K*, where $ID = hash(K)$ and *hash* is a one-way hash function. Locking a tag can be done via a wireless channel or physical contact, and the mapping (*K*, *ID*) can be stored in a database. A locked tag responds to all queries with ID. Some attacks include:

- Spoofing can be detected but not prevented. A replay attack is possible since an adversary can obtain a tag's ID via querying a locked tag, and then spoof that tag in a replay attack to a reader, which will reveal the key to the spoofed tag. However, the reader can find a mismatch between contents of the spoofed tag and those in the database.
- A tag can be unlocked for a short time to prevent hijacking. The reader should know IDs to obtain keys.

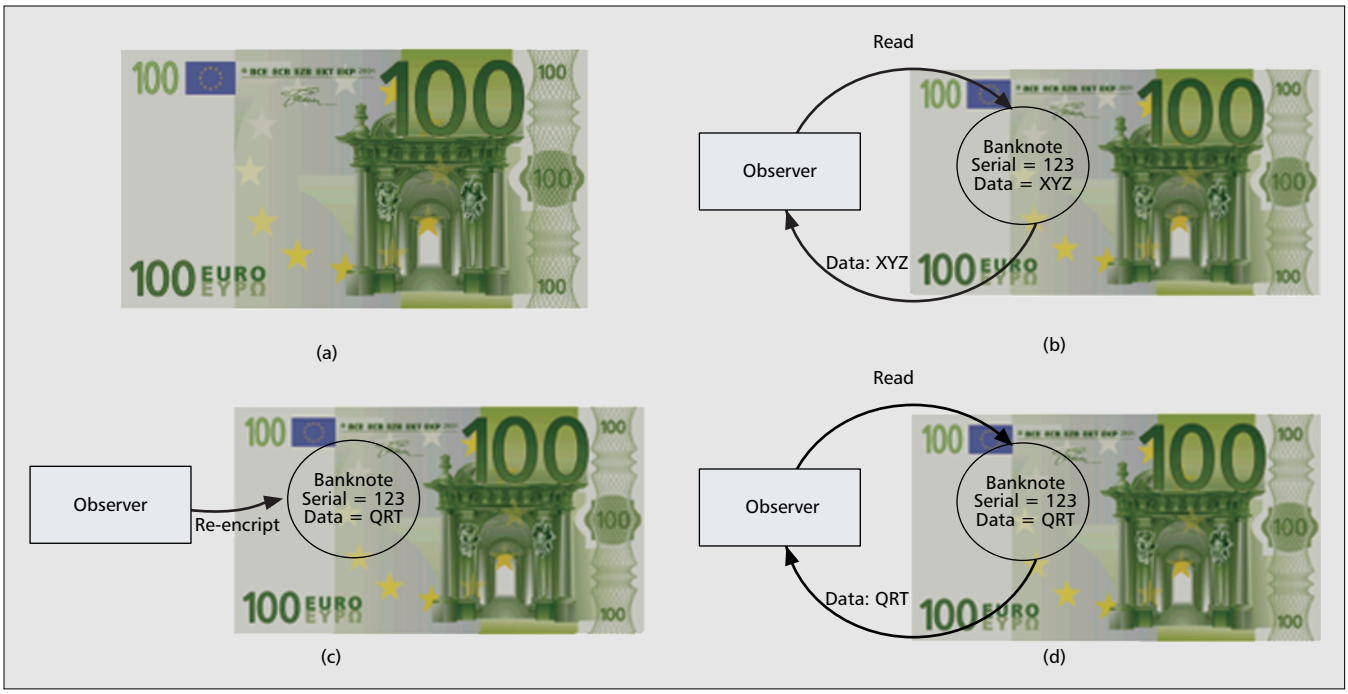


**Figure 3.** *Euro bank notes and re-encryption: a) EURO bank notes; b) before re-encryption; c) re-encryption; d) after re-encryption.*

To prevent spoofing, the above locking approach can be further improved if the number of tags in the database is small. A tag responds to queries with $(r, hash(ID||r))$ instead of $ID$, where $r$ is a random number and $||$ is the concatenation function. The reader can find the corresponding $ID$ via exhaustive search; this can be achieved if the number of tags in the database is small, but may be impractical for retailers. To further secure ID bits in the output of the hash function in the scheme, if each tag and reader share a secret key $k$ and a pseudo-random function ensemble, $F = \{f_n\}_{n \in N}$, is supported, a tag replies with $(r, ID \oplus f_k(r))$, where $r$ is a random number, and the reader needs to conduct an exhaustive search. To avoid storing IDs, but instead store keys in a database, a tag can rely on $(r, (ID||hash(ID)) \oplus f_k(r))$. However, consumers may find inconvenience in managing lock/unlock patterns, and may not even be aware of the existence of tagged products. Furthermore, tag cost may also increase with lock and unlock functions. This locking scheme is neither private nor secure against passive eavesdroppers, and an attacker can query a tag to learn $(r, ID \oplus f_k(r))$, with which the attacker later can impersonate that tag to the reader [11].

## Re-Encrypting Tags

In [3] re-encrypting serial numbers of bank notes in tags using a public key is proposed in order to reduce the linkability of different appearances. In [12] another scheme for re-encrypting tags is proposed using multiple public keys to re-encrypt a ciphertext without knowing the associated public key. Since both schemes require external computing stations in stores, they may need many resources [10].

A solution is proposed in [3] to address the problem presented by RFIDs on bank notes by being able to re-encrypt the data contained on the bank notes using a static secret key along with a public key system, shown in Fig. 3, similar to the public key systems already in use for encrypting Internet traffic, which includes a small random factor in generating the cipher text. This tactic avoids many problems of using simple encryption with a static key, such as the problem of what would need to happen if the key needs to be changed. A key change for the bank notes would be a nightmare to pursue, so instead the burden of the keys is moved off to law enforcement agencies, banks, and merchants. With the small random factor added to the encryption process, the problem of generating a cipher text as unique as the bank note's serial number is avoided. The ability to re-encrypt the data on the bank note's tag prevents an observer from being able to link a particular cipher text to a particular banknote with 100 percent certainty, despite any means of visually verifying the bank note's identity such as an optical reader or simply picking up the bill to inspect it.

There is a possibility of a rogue merchant, who has their own merchant-only key for re-encrypting bank notes, purposefully re-encrypting the notes with misleading information so that customers who receive the bills now have to deal with the hassle of having their money flagged as potentially counterfeit when they try to spend it at another merchant or deposit it at the bank. Not mentioned in [3] is the scenario where the secret keys are somehow exposed: how easy it would be for someone to discover the access key for a bank note is discussed in [13]. They simply have to listen in on the "conversation" between the reader and the tag, for instance, by standing near a cash register. Once this key is discovered, it is then simple to store random data on the bank note, effectively tak-

*The RFID Bill of Rights addresses privacy issues via regulation on consumers' knowledge of existence of RFID tags, removal/deactivated upon purchase, consumers' data accessibility of tags, consumers' service accessibility, and knowledge of the time, location, and reason of accessing tags.*

ing it out of circulation by destroying the ability of the RFID bank note system to verify the bank note in question. Given that many stores have a policy of not returning suspected counterfeit bills, this opens up the possibility of a scam by an unscrupulous store owner. Another one of the main problems with re-encryption is the added burden of the infrastructure needed to implement this method, which includes the added computational costs for readers and the time needed to re-encrypt the bills. The question is raised in [13] of how practical it is to expect the bank notes to be re-encrypted often enough to prevent tracking of bank notes by a nefarious reader. Merchants may not want to re-encrypt every bank note they obtain, because of time issues (just imagine your favorite store trying to handle not only a busy business day such as the day after Thanksgiving, but also the re-encryption of the banknotes at the same time), so it is left to banks to reliably re-encrypt the bank notes they come across. However, depending on personal spending habits, a bank note may go a long time before being passed over to a merchant, much less to a bank. This gives plenty of time for someone to track a bank note and be reasonably sure that it is the same bank note previously seen.

### Silent Tree Walking

The signal from a reader to tags in the downlink is stronger than those from tags to the reader in the uplink. Therefore, an adversary may hear a downlink channel far away, but may not hear uplink channels. Such asymmetry of downlink and uplink may cause a security problem for an anticollision tree walking algorithm since the reader broadcasts some bits of tags' IDs.

In [6] a silent binary tree walking scheme is presented to avoid broadcasting insecure tags' IDs in the downlink. In the binary tree walking scheme the reader requests all tags to send their next bit of ID, and if there is no collision, all tags share the same bit, and the reader requests the next bit. On the other hand, the reader requests parts of the tags to proceed if there is a collision.

Information in the downlink may be heard by an eavesdropper, but tag responses may not be heard since the eavesdropper is assumed to have a longer distance to tags than that between the reader and tags. It is assumed that tags share some common prefix, which can be used to conceal a portion of IDs transmitted in a downlink channel; for example, for two tags with partial ID values $a_1a_2$ and $a_1\bar{a_2}$, the reader, which obtains $a_1$ via the uplink, which cannot be heard by the eavesdropper, sends $a_1 \oplus a_2$ or $a_1 \oplus \bar{a_2}$ in the downlink channel as the next request without revealing $a_2$ to the eavesdropper. Furthermore, asymmetry of downlink and uplink can be used to conceal information ($v$) from the faraway eavesdropper; for example, the reader sends $r \oplus v$ in the downlink, where $r$ is a random number generated by a tag and sent previously in the uplink channel. However, the scheme does not defend against active attacks, and the assumption of a common and secret string shared by all tags may be unrealistic.

### Regulating Tags

The *RFID Bill of Rights* addresses privacy issues via regulation on consumers' knowledge of the existence of RFID tags, removal/deactivation upon purchase, consumers' data accessibility of tags, consumers' service accessibility, and knowledge of the time and location of, and reasons for accessing tags [10].

### Selective Blocking Tags

A selective blocking scheme using binary tree walking to protect consumers from unauthorized scanning of RFID tags is proposed in [10]. In the scheme a blocker tag selectively blocks RFID readers. The same scheme can be used to conduct a denial-of-service attack, described in a later section. A blocker tag can be implemented with two antennae or two separate tags, and can be a privacy protection tool. It can block a particular zone or zones of IDs using a binary tree walking algorithm. However, the tag cost is relatively high.

### Anonymous Tags

Several schemes were proposed in [15] to either conceal a permanent ID of a tag that has a rewritable memory with a user-chosen private ID or assign a partial ID sequence to a user-assignable tag so that users can control the uniqueness of IDs from local to global without revealing the relationship between the ID and the object. For the first approach, each tag has a read only memory (ROM) in which a permanent ID is saved, and a rewritable memory in which a private/temporary ID is saved. ROM and rewritable memory cannot be used at the same time, and ROM can be read by the user only if the rewritable memory has null value. The user can change the private/temporary ID, as well as access ROM by removing the private/temporary ID. For the second approach, a partial ID sequence for local uniqueness can be divided.

### Hash-Based Anonymous Tags

In [16] data and location privacy are enhanced with a one-way hash-function to conceal tags' IDs. A tag's ID will be changed upon each read action to prevent eavesdropping, message interception, spoofing, man-in-the-middle attacks, and replay attacks. Let $R \rightarrow T$ denote that the reader transmits to a tag, and vice versa. The operations are listed as follows: $R \rightarrow T$: $hash(ID)$; $T \rightarrow R$: ($hash(ID)$, $DB - ID$, $hash(TID \oplus ID)$, $\Delta TID$); $R \rightarrow T$: x, $hash(x \oplus TID \oplus ID)$, where $ID$ is the ID of the tag, $hash(.)$ is a one-way hash function, $DB - ID$ is the database ID, $TID$ is the transaction ID, $x$ is a nonce, $\Delta TID = TID - LST$, and $LST$ is the last successful number. In the above procedures a tag is singularized out of many using binary tree walking via $hash(ID)$; the tag increases its transaction number ($TID$) by one, and sends ($hash(ID)$, $DB - ID$, $hash(TID \oplus ID)$, $\Delta TID$), where $hash(TID \oplus ID)$ is to avoid a replay attack and authenticate the tag; then at last, the tag can authenticate the reader via $R \rightarrow T$: $x$, $hash(x \oplus TID \oplus ID)$.

### ATTACKS OF RFID

If binary tree walking is used, a denial-of-service attack can easily be carried out as follows [10]. An attacker with two antennae or made of two tags can simultaneously send both 0 and 1 whenever (or sometime) the reader queries the next bit, so the reader assumes that partial or all $2^N$ IDs exist, where $2^N$ is a huge number when $N$ is large (e.g., 128).

A denial-of-service attack can easily be launched via blocking tags' IDs if binary tree walking is used. The attack can also be detected if a large number of IDs are blocked. But a smarter attacker may randomly block some bits so that the attack will be difficult to identify. A better detection mechanism is based on pre-known ranges of tags' IDs. The number of tags out of range can be used as a metric to detect attacks.

A clone attack can be carried out if installing a cloned replacement tag that authenticates itself successfully to the reader due to weak or no authentication [5].

Other attacks on privacy issues have been discussed in previous subsections.

### LIGHTWEIGHT AUTHENTICATION

Since tags are highly resource-constrained, lightweight cryptographic primitives are needed. In [5] five lightweight authentication algorithms are proposed to prevent theft and clone attacks. Let $x$ denote a random challenge. We briefly introduce the following five algorithms.

**XOR-with-Two-Keys:** $R \rightarrow T$: $x \oplus k_1$ and $T \rightarrow R$: $x \oplus k_2$, assuming that the tag and the reader share two independent and randomly chosen keys, $k_1$ and $k_2$. The rekeying could be done as follows: in the $i$th run, the reader randomly chooses a new key $k^{(i)}$ and: $R \rightarrow T$:($x^{(i)} \oplus k^{(i)}$; $k^{(i)} \oplus k^{(i-1)}$) and $T \rightarrow R$: $x^{(i)} \oplus k^{(0)}$. However, the rekeying can be broken with two observed consecutive runs: if an attacker listens to the $(i-1)$th and $i$th runs, ($x^{(i-1)} \oplus k^{(i-1)}$; $k^{(i-1)} \oplus k^{(i-2)}$) and ($x^{(i)} \oplus k^{(i)}$; $k^{(i)} \oplus k^{(i-1)}$), it is easy to obtain $x^{(i-1)} \oplus k^{(i-1)} \oplus x^{(i)} \oplus k^{(i)} \oplus k^{(i)} \oplus k^{(i-1)} = x^{(i-1)} \oplus x^{(i)}$, which does not have the key information at all. A fix can be $R \rightarrow T$: $x^{(i)} \oplus k^{(i)}$ and $T \rightarrow R$: $x^{(i)} \oplus k^{(0)}$, where $k^{(i)}$ is a permutation of $k^{(i-1)}$. The scheme suffers a first-time key establishment problem due to limited resources.

**Subset:** $R \rightarrow T$: $x \oplus k$ and $T \rightarrow R$: $f(x)$,where $k$ is the key, $f(x)$ is a function, and $x = (x_L, x_R)$. For the function $f(x)$, the $j$th bit of $x_R$ addresses a bit of $x_L$, and is considered the $j$th bit of the output vector.

**Squaring:** $R \rightarrow T$: $x$ and $T \rightarrow R$: $k_L \oplus ((k_R + x)^2 \bmod 2^n)$, where $k = (k_L, k_R)$ with $2^n$ bit length.

**RSA:** $R \rightarrow T$: $x$ and $T \rightarrow R$: $E(x \wedge k)$,where $E$ is the encryption of RSA and $\wedge$ is bitwise.

**KNAPSACK:** $R \rightarrow T$: $(d \oplus k, \kappa(x, d))$ and $T \rightarrow R$: $x \oplus k'$, where $k$ is an $m$-bit key, $k'$ is an $n$-bit key, $x$ is an $n$-bit challenge, $d$ is an $m$-bit trapdoor, and $\kappa$ is a punctured multiplicative knapsack.

Although the above algorithms are relatively lightweight, they can be attacked by a powerful attacker. There is always a trade-off between strength of security and complexity.

In [11] the authentication of the reader is studied as follows: $R \rightarrow T$: hello; and $T \rightarrow R$: $x$; and $T \rightarrow R$: $k \oplus x$ so that the tag can verify whether the reader has a key. If each tag has a unique key, distinguishing different tags, especially new tags, is an issue for a reader. In other words, it is difficult for two entities to share a secret and authenticate each other without revealing their identities to a third entity. If it is impossible for an attacker to distinguish between two different tags with two secret keys, the scheme is considered private. Mutual authentication between the tag and the reader is also proposed in [11] as follows: $R \rightarrow T$: Hello, $x_1$; $T \rightarrow R$: $x_2$, $ID \oplus f_s(0,x_1,x_2)$; $R \rightarrow T$: $f_s(1,x_1,x_2)$, where $f_s(.)$ is a pseudo-random function. In addition, a tree-based private authentication scheme is presented.

## DISCUSSIONS AND FUTURE RESEARCH DIRECTIONS

Some enhanced mechanisms have been suggested in [6] as follows:

- Mechanisms and devices are needed to detect unauthorized read attempts or transmissions.
- Tags can be designed to scream when killed for detection of denial-of-service attacks.
- A master key can be printed in packages of products as a barcode or number to access the functionality of tags of purchased products (e.g., to lock/unlock the tags).

The drawback of the selective blocking scheme is that it can be used maliciously to launch denial-of-service attacks to disrupt business or help theft. Furthermore, the selective blocking scheme may not be good for energy efficiency.

Hardware-efficient hash functions, lightweight symmetric encryption, message authentication codes, and random number generators for RFID need future research. A lightweight symmetric cipher can reduce cost and improve efficiency.

The solutions discussed above can be used selectively to prevent revealing a tag's ID to an unauthorized reader. Our research on providing detail security solutions for the two proposed RFID applications in Telemedicine is under way.

## CONCLUSION

RFID technologies are being applied in telemedicine to improve the quality of healthcare and reduce medical errors because of the aging population, shortage of qualified healthcare personnel, increasing medical errors due to drug management and site infection, and so on. In this article we have proposed two RFID applications in telemedicine to study supply and demand of doctors, nurses, and patients in hospitals and healthcare, and to develop mobile telemedicine services. We have provided a comprehensive survey on security and privacy issues in RFID systems, and their solutions. On the other hand, there are many open practical issues such as designing more realistic and efficient security and privacy solutions, and at the same time there should be strong mechanisms against all kinds of attacks.

*A smarter attacker may randomly block some bits so that the attack will be difficult to identify. A better detection mechanism is based on pre-known ranges of tags' IDs. The number of tags out of ranges can be used as a metric to detect attacks.*

*Hardware efficient hash functions, lightweight symmetric encryption, message authentication codes, and random number generators for RFID need future research. A lightweight symmetric cipher can reduce cost and improve efficiency.*


## ACKNOWLEDGMENT

This research has been partially supported by a research grant from NSERC, Canada. The authors would like to thank Dr. Lan Wang for her preliminary work in mobile telemedicine service.


## REFERENCES


[1] A. Cavoukian, "Tag, You're It: Privacy Implications of Radio Frequency Identification (RFID) Technology," *Info. and Privacy Commissioner*, Ontario, 2004.
[2] Rockwell Automation, "RFID in Manufacturing: A Practical Guide on Extracting Measurable Value from RFID Implementations in Plant and Warehousing Operations," *Global Manufacturing Solutions*, June 2004.
[3] A. Juels and R. Pappu, "Squealing Euros: Privacy Protection in RFID-Enabled BBanknotes," *Financial Cryptography '03*, R. Wright, Ed., Springer-Verlag, 2003.
[4] M. Baard, "RFID Keeps Track of Seniors," http://www.wired.com/news/medtech/0,1286,62723,00.html, Mar. 2004.
[5] I. Vajda and L. Buttyan, "Lightweight Authentication Protocols for Low-Cost RFID Tags," *Proc. 2nd Wksp. Sec. in Ubiquitous Comp.*, 2003.
[6] S. A.Weis et al., "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems," *Proc. Int'l. Conf. Sec. in Pervasive Comp.*, 2003.
[7] Allied Bus. Intelligence, "RFID White Paper," 2002.
[8] Intel press release, "Intel Showcases Innovative Wireless Sensor Networks for In-Home Health Care Solutions," Washington, DC., Mar. 2004
[9] F. Hu and S. Kumar, "Multimedia Query with QoS Considerations for Wireless Sensor Networks in Telemedicine," *Proc. SPIE ITCom '03*, 2003.
[10] A. Juels, R. L. Rivest, and M. Szydlo, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy," *Proc. ACM CCS '03*, 2003.
[11] D. Molnar and D. Wagner, "Privacy and Security in Library RFID Issues, Practices, and Architectures," *Proc. CCS '04*, 2004.
[12] P. Golle *et al.*, "Universal Re-encryption for Mixnets," *RSA Conf. Cryptographers' Track '04*, LNCS 2964. Springer-Verlag, 2004, pp. 163–78.
[13] G. Avoine, "Privacy Issues in RFID Banknote Protection Schemes," *Proc. Int'.l Conf. Smart Card Research and Advanced Apps. '04*, Aug. 2004.
[14] S. Garfinkel, "An RFID Bill of Rights," *Tech. Rev.*, Oct. 2002, p. 35.
[15] S. Inoue and H. Yasuura, "RFID Privacy Using User-Controllable Uniqueness," *MIT RFID Privacy Wksp. 2003*.
[16] D. Henrici and P. Muller, "Hash-Based Enhancement of Location Privacy for Radio-Frequency Identification Devices Using Varying Identifiers," *Proc. PERCOMW '04*, 2004.


## BIOGRAPHIES


YANG XIAO [SM'04] (yangxiao@ieee.org) worked at Micro Linear as a medium access control architect involved in the IEEE 802.11 standard enhancement work before he joined the Department of Computer Science at the University of Memphis in 2002. He was a voting member of the IEEE 802.11 Working Group from 2001 to 2004. He currently serves as Editor-in-Chief for *International Journal of Security and Networks* (IJSN) and for International Journal of Sensor Networks (IJSNet). He serves as an associate editor or on editorial boards for the following refereed journals: (Wiley) *International Journal of Communication Systems*, (Wiley) *Wireless Communications and Mobile Computing*, *EURASIP Journal on Wireless Communications and Networking*, and *International Journal of Wireless and Mobile Computing*. He served as lead or sole guest editor for five journals during 2004–2005. He has served as a TPC member for more than 60 conferences including ICDCS, ICC, GLOBECOM, and WCNC. He serves as a referee for many funding agencies, as well as a panelist for the U.S. National Science Foundation. His research areas include wireless networks, mobile computing, and network security. He has published more than 120 papers and book chapters in these areas.

XUEMIN (SHERMAN) SHEN [M'97, SM'02] (xshen@bbcr.uwaterloo.ca) received a B.Sc. (1982) degree from Dalian Maritime University, China, and M.Sc. (1987) and Ph.D. (1990) degrees from Rutgers University, New Jersey, all in electrical engineering. Currently, he is with the Department of Electrical and Computer Engineering, University of Waterloo, Canada, where he is a professor and associate chair for graduate studies. His research focuses on mobility and resource management in interconnected wireless/wired networks, UWB wireless communications systems, wireless security, and ad hoc and sensor networks. He is a co-author of three books, and has published more than 200 papers and book chapters in wireless communications and networks, control, and filtering. He was Technical Co-Chair for IEEE GLOBECOM '03, ISPAN '04, QShine '05, IEEE Broadnets '05, and WirelessCom '05, and Special Track Chair of the 2005 IFIP Networking Conference. He serves as Associate Editor for *IEEE Transactions on Wireless Communications*; *IEEE Transactions on Vehicular Technology*; *Computer Networks*; *ACM Wireless Networks*; *Wireless Communications and Mobile Computing* (Wiley); and *International Journal of Computers and Applications*. He has also served as Guest Editor for *IEEE JSAC*, *IEEE Wireless Communications*, and *IEEE Communications Magazine*. He received the Premier's Research Excellence Award (PREA) in 2003 from the Province of Ontario, Canada, for demonstrated excellence of scientific and academic contributions, and the Distinguished Performance Award in 2002 and 2004 from the University of Waterloo, for outstanding contributions in teaching, scholarship, and service.

BO SUN [S'01, M'04] (bsun@cs.lamar.edu) received his Ph.D. degree in computer science from Texas A&M University, College Station, in 2004. He is now an assistant professor in the Department of Computer Science at Lamar Universit. His research interests include the security issues (intrusion detection in particular) of wireless ad hoc networks, wireless sensor networks, cellular mobile networks, and other communications systems.

LIN CAI (lcai@bbcr.uwaterloo.ca) received a B.Sc. degree in computer science from Nanjing University of Science and Technology, Nanjing, China, in 1996, and an M.A.Sc. degree in electrical and computer engineering from the University of Waterloo, Canada, in 2005. She is currently working toward a Ph.D. degree in the same field at the University of Waterloo. Her current research interests include network performance analysis and protocol design for multimedia applications over IP-based wireless networks.