WIRELESS COMMUNICATIONS AND MOBILE COMPUTING
Wirel. Commun. Mob. Comput. 2007; **7**:457–472
Published online 24 July 2006 in Wiley InterScience (www.interscience.wiley.com). DOI: 10.1002/wcm.365

Radio frequency identification: technologies, applications, and research issues

Yang Xiao[1]*,†, Senhua Yu[1], Kui Wu[2], Qiang Ni[3], Christopher Janecek[1] and Julia Nordstad[1]

[1]*Department of Computer Science, The University of Memphis, Memphis, TN 38152, U.S.A.*
[2]*Department of Computer Science, University of Victoria, Victoria, British Columbia, Canada*
[3]*Electronic and Computer Engineering Division, Brunel University, Uxbridge, West London, U.K.*

Summary

A radio frequency identification (RFID) system is a special kind of sensor network to identify an object or a person using radio frequency transmission. A typical RFID system includes transponders (tags) and interrogators (readers): tags are attached to objects/persons, and readers communicate with the tags in their transmission ranges via radio signals. RFID systems have been gaining more and more popularity in areas such as supply chain management, automated identification systems, and any place requiring identifications of products or people. RFID technology is better than barcode in many ways, and may totally replace barcode in the future if certain technologies can be achieved such as low cost and protection of personal privacy. This paper provides a technology survey of RFID systems and various RFID applications. We also discuss five critical research issues: cost control, energy efficiency, privacy issue, multiple readers' interference, and security issue. Copyright © 2006 John Wiley & Sons, Ltd.

KEY WORDS: auto-identification; reader; radio frequency identification (RFID); tag; ubiquitous computing; privacy

1. Introduction

The contemporary retailers are faced with a daunting challenge, that is, as the number of inventory items increases, they must find an inexpensive and mass-producible way to efficiently tag, categorize, and track assets and products. The most widely adopted method of product identification has long been barcode. The barcode is a vertically stripped identification tag printed on products, allowing retailers to identify millions of products. However, the barcode has limited capability and its constrained requirements. First, barcodes are limited in the amount of data they can carry: (1) most barcodes are one-dimensional integers, that is, ten digits long solely for identification [1]; (2) other two-dimensional barcodes have a larger storage from 62 characters to 249 characters, but they are still primary for identification [1]. There is very limited space to add other descriptive information or metadata to these barcodes. Second, barcodes require laser-scanning devices to reach very near to read and process them. The contemporary retailers are looking for more capable and efficient methods to identify and tag products, including the ability to read product

*Correspondence to: Yang Xiao, Department of Computer Science, The University of Memphis, 373 Dunn Hall, Memphis, TN 38152, U.S.A.
†E-mail: yangxiao@ieee.org

information far away such as many feet or yards. Many other groups are also benefitted if more capable means of product identification can be used. For example, security companies will benefit greatly if they can track company assets; warehousing companies will benefit a lot if they can instantly know the count and location of each item; even law enforcement benefits from a device that can uniquely identify every automobile on the road or a device that can instantly know the velocity of a moving automobile. Such a production identification device must be inexpensive, can be produced in great quantities, is capable of storing relatively large amounts of data, and is capable of being read from a distance. A promising solution is to use radio frequency identification (RFID) devices.

RFID uses radio frequency communications to label and identify objects and stores/retrieves data wirelessly and electronically. A typical RFID system includes transponders (also called tags) attached to objects and interrogators (also called readers), and they communicate wirelessly. Each tag carries information such as a serial number, a model number, location of assembly, and other data. When tags pass through the radio range of a reader, they communicate with the reader wirelessly and identify themselves [2].

RFID gains widespread usage in the fields of inventory management and tracking with low cost and ease of production. Commercial companies, such as Wal-Mart and Target, and government bodies, such as the U.S. Department of Defense, have announced to initiate RFID systems [3]. RFID has many applications including labeling products for rapid checkout, animal tagging, inventory tracking, access control for secure facilities, electronic toll collection, etc. [4]. Different applications require different requirements on RFID parameters, including cost, range, data capabilities, etc. RFID tags can be checked at a distance no matter whether they are visible or not.

Although RFID has existed since World War II as a method of identifying friendly aircrafts, it gains popularity only recently, and many challenges still exist in RFID systems. The purpose of this paper is to give an overview of RFID, describe the RFID technologies and their applications with examples of existing RFID systems, and discuss the research issues. Five main research issues: cost control, energy efficiency, privacy issue, multiple readers' interference, and security issue are discussed in this paper.

The rest of this paper is organized as follows. Section 2 provides a technology overview of the readers and the various types of RFID tags, and summarizes the difference between RFID tags and traditional barcodes. Operating frequency, application systems, and standardization efforts will also be introduced. In Section 3, various RFID applications currently available and under development are introduced. Section 4 discusses some research issues. Finally, we conclude this paper in Section 5.

2. RFID Technologies

Radio frequency identification (RFID) is a way to identify a person/object using radio frequency transmission. An RFID system includes tags, readers, and an application system. Information is exchanged wirelessly between a tagged object and a reader when they are tuned to the same radio frequency [5]. Tags are small items with various shapes, attached/imprinted on papers and attached to larger items for identification [6]. When an RFID 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 [2]. A reader picks up the radio frequencies of tags to communicate. An application system is the main workhorse of an RFID system, and makes sense of the data read from tags. An RFID system normally works as follows:

- A reader sends out a signal via a radio frequency;
- All tags are tuned to the reader's radio frequency and receive the signal with their antennas;
- Selected tags transmit their stored data;
- The reader receives the tag's signal with its antenna and decodes it;
- The reader transfers the data to the application system;

In the remainder of this section, we introduce various tags, readers, operating frequency, and an application system. At last, we compare RFID with barcode in detail, and introduce standardization efforts.

2.1. Tags

Tags/transponders vary in size and shape, and often look like small portions of paper on which metal patterns are printed. A tag is composed of an antenna and maybe a silicon chip, usually only containing small portions of information, while some tags can contain up to 1024 bits of information [7]. A tag's size ranges from the size of a grain of rice to two-inch squares [8]. RFID tags are easy to hide, for example, in the seams of clothes, between layers of cardboards, in plastic or rubber, and in consumer package design [9,33]. New RFID tags can be produced as small as tiny coded beads invisible to human eyes, and can be embedded in inks, currency, automobile paint, explosive, etc. [9]. Some tags are bendable and even capable of being torn without suffering data loss or transmission capabilities. Tags cannot sense the presence of other tags and therefore, an anti-collision algorithm is needed to reduce collision among tags. We will further discuss anti-collision algorithms in a later section about research issues.

Tags can be classified into chipless tags and chip tags, and can also be classified into passive tags and active tags. We will introduce them in the following subsections.

2.1.1. Chipless tags versus chip tags

Tags that do not contain microchips are called *chipless* tags. In other words, a chipless tag does not contain an integrated circuit chip. On the other hand, tags that do contain microchips are called *chip tags*. A chip tag contains an integrated circuit that can store more information than a chipless tag. Some chip tags are capable of processing data since chip tags normally include internal power source such as battery. However, chipless tags are less expensive than chip tags. A comparison of chipless tags with chip tags is shown in Table I.

The low cost of chipless tags makes them very appealing. Some chipless tags can cost as low as \$0.01–0.02 per tag for a bulk order of 100 000 tags or more, while some can cost less than one-hundredth of a penny if the tags are ordered in quantities of billions [6]. In contrast, chip tags are more than \$0.30 per tag if the tags are ordered in quantities of less than one million [6]. Current chip tags by Hitachi, a Japanese semiconductor company, are about \$0.43 per tag if the tags are ordered in 70 000 or more [9]. We can expect that costs of chipless tags and chip tags will further go down in the future.

Table I. Comparison of chipless tags with chip tags.

	Chipless tags	Chip tags
Chip	No	Yes
Cost	Less expensive	Relatively expensive
Storage	24 bits	96 bits and larger
Usage	Internal to an organization	Mass-market application
Radio range	Shorter	Relative longer
Chip size	Smaller	Relative larger
Weight	Lighter	Relative heavier

A chipless tag normally has a small range, often within only several inches, and it normally needs external power source. Furthermore, a cheaper chipless tag among chipless tags sometimes has a shorter range. In contrast, chip tags have a larger radio range but heavier than chipless tags due to integrated circuits included. Although the size and weight of chip tags may limit their usage in some applications, a chip tag has much larger data storage than a chipless tag. Chip tags with 96-bit codes represent 79 billion-billion numbers [4], while recent chip tag standards allow for greater data storage. For example, chip tags produced by Hitachi are about 0.3 mm^2 holding 128 bits of data [9]. Chipless tags are read-only, while chip tags can be read-only or read-write. Read-write chip tags' memory can be rewritten for many times.

2.1.2. Active tags versus passive tags

There are three types of tags: active, passive, and semi-passive. Active tags contain a small power source, that is, a battery, and have both an on-tag power source and an active transmitter [9]. Active tags have a larger radio range. For instance, they can be read from a long distance more than 100 feet away. As such, they are suitable for tracking items over long ranges, such as tracking shipping containers in transit [10]. Active tags can be reused many times and thus are good for logistics. Active tags may periodically transmit a beacon signal, which may be captured by readers [8]. Since active tags must operate on a limited power source over long periods of time, special materials such as complementary metal oxide semiconductor (CMOS) should be used for making active tags [14].

In contrast, passive tags do not include an on-tag power source. Passive tags are known as inductively coupled RFID tags. They are powered by the electromagnetic field generated by a reader and retrieve or transmit data back to a reader by modulating energy through a transducer [9]. They are energized by means of electromagnetic induction, namely by inductive coupling between the coil in the reader and the tiny coil in the tag. They use a capacitor to store the energy received until there is enough energy for the tag to transmit data [11,12]. Passive tags are smaller, lighter, and less expensive than active tags, and can only be read from a short-range distance of approximately

5–10 feet. Unlike active tags, passive tags do not periodically transmit a beacon signal.

Semi-passive tags also have a power source, which increases their working range and throughput. The main difference between active tags and semi-passive tags is that semi-passive tags still employ passive response from the tag to the reader [13].

2.2. Readers

Readers are devices that read/interrogate tags, and each reader is equipped with antennas, a transceiver, and a processor. In other words, a reader is an electronic component that is capable of communicating with tags and supplying energy to them. The antennas are used for sending/receiving radio signals, and the transceiver and the processor are used to encode/decode data. Readers normally look like circuit boards or handheld scanning devices, and are sometimes mounted in locations where they strategically sense tags. Handheld readers are mobile devices used for, for example, inventory or warehouse. During interrogating tags, a reader receives a tag's radio transmission, performs error checking, and communicates with an application system. Readers also provide power to passive tags by transmitting an energy field to wake up passive tags, powering chips, and enabling them to transmit/store data [9]. Examples of readers include retailer self check-outs, library book sensors, security exit sensors, sorters, and portable sensors. A reader has a finite range called *interrogation zone* [9], and the size of the zone depends on applications. Passive tags, relying on outside power have weak signals so that they have smaller interrogation zones, whereas active tags have larger interrogation zones. A reader must be able to read multiple tags within its range. Most readers have difficulty of interrogating tags in the presence of other readers, especially when mobile handheld readers are moving close to other readers. This issue will be further discussed in a later section about research issues.

2.3. Operating Frequency

Operating frequencies are subject to standardization. In the United States, Federal Communications Commission (FCC) defines frequencies that are publicly available. Operating frequency determines the capability of an RFID system, and the FCC defines four different frequencies: low frequency (LF) in 125 Hz, high frequency (HF) in 13.56 MHz, ultra high frequency (UHF) in 868–915 MHz, and microwave in 2.45 and 5.8 GHz [2]. The corresponding ranges of these operating frequencies are approximately less than 0.5, 1, 3, and 1 m, respectively [2].

An LF tag is normally a passive tag and thus its range is very short. It is relatively expensive because a longer and more expensive copper antenna is needed. An LF tag has better performance even when working in metal and in liquids, and has normal applications such as access control, animal tracking, vehicle immobilizers, etc. An HF tag is normally a passive tag too, and is less expensive than an LF tag. The range of an HF tag is between an LF tag and a UHF tag. An HF tag has applications such as smart cards, item-level tracking, libraries, etc. A UHF tag is normally an active tag with a battery. UHF tags offer good balance between range and performance, and multiple tags can be read at the same time. A UHF tag has applications such as pallet tracking, electronic toll collection, and baggage handling. A microwave tag has similar characteristics to a UHF tag, but it has faster reading rates. A microwave tag has the worst performance if working in metal and liquids as well as other materials so that it is good only for directional signal. A microwave tag has applications such as electronic toll collection.

2.4. An Application System

An application system interfaces with readers and is the main component of an RFID system, responsible for cataloging RFID tag information. Common applications include retailer point-of-sale system, library check-in and check-out system, security monitoring system, sorting application (e.g., U.S. Postal Service), etc.

Wal-Mart has recently attempted widespread adoption of RFID systems [9]. In Wal-Mart, all incoming inventory items from manufacturers contain RFID tags. The 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 application system records types, quantities, and locations of items.

2.5. RFID Versus Barcode

Nowadays, most items sold in the world carry identification numbers such as barcodes, which are read and processed by optical scanners. An automatic identification (Auto-ID) system is a class of technologies used for automatic identification of objects, people, and locations. RFID belongs to one of Auto-ID categories. RFID technology differs from barcodes

Table II. RFID versus barcode.

RFID	Barcode
Information is specific to the individual item	The same products have the same Universal Product Code or bar code number
It can be read from a distance; tags are scanned easily	It needs to be in plain view of the reader to be read
It can read through paper, fabric, and other materials that radio frequency waves can go through	It cannot
It can store hundreds or thousands of bytes of information	It is limited to 13 digits of information or a few hundred digits in the case of two-dimensional barcodes
Dozens of tags can be read at the same time with a single reader	Only a single barcode can be read at a time
Electronically deactivated	Deactivated by obliterating or obscuring it
Pretty robust and not as sensitive to dirt, smearing as barcodes and are not easily broken, and thus can be used in harsh environments, for example, snow, fog, ice, or paint	Useless in harsh environments
Perform limited processing	Read only
Limit who can read them by assigning a password to the tag	Any reader can read any compatible bar code
Enable tagged objects to 'speak' to electronic readers potentially over the entire course of a product's lifecycle	Has no ability
Small size of the tags allows to add them to most objects unobtrusively	Require plain surface to be affixed to
Being small, tags do not affect the look of the products for which appearance is important	Not the case sometime

in several ways and thus offers many advantages over barcodes. We summarize these differences and advantages in Table II.

Even though RFID has evident advantages over barcode, traditional barcode-based systems still dominate the market since RFID systems are more expensive. Research has been done to find ways to reduce RFID cost and to address other technology issues. Many people believe that in the future RFID will totally replace traditional optical barcode systems.

2.6. RFID Standards

As mentioned before, operating frequencies are subject to standardization. In the United States, the FCC defines four different frequencies: LF, HF, UHF, and microwave.

Most RFID readers do not follow any standard because often RFID readers interface with custom applications, which are specific to their manufacturers and users. Lacking standard of RFID readers potentially causes interference among different readers, specifically when multiple RFID readers interrogate one RFID tag. While it is currently not a problem because of the relatively small-scale adoption of RFID tags, mobile RFID readers suffer from a lack of standardization so that interference may not happen a lot.

One standard organization working toward producing a standard for RFID technologies is EPCglobal, which develops the electronic product code (EPC) RFID standards in cooperation with the Auto-ID Laboratories, a joint venture between The Massachusetts Institute of Technology (MIT) and several other universities [15]. The EPC code is like the Universal Product Code (UPC) used in barcodes, except that it is much more detailed so that it can identify many more unique objects, even with Internet addresses [9]. MIT along with several other universities started the Auto-ID Center, which develops a low-cost RFID tag and is sponsored by over 100 global companies [9]. The joint standards between EPCglobal and the Auto-ID center include Auto-ID Class 0 and Auto-ID Class 1.

An EPC type 1 with 96 bits is shown in Figure 1, where header, EPC manager, and serial number identify EPC version, manufacturer (with number up to 268 million), and unique physical item (with number up to 68 billion), respectively.

Another standard organization working toward producing a standard for RFID technologies is International Standards Organization (ISO), including standards of ISO 18000-6 A, and ISO 18000-6 B.

The protocol standards specify a number of characteristics of RFID systems as follows [11,13,14,16]:

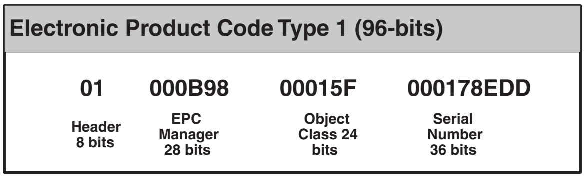


Fig. 1. 96-bit EPC type 1.

- Operating frequency: LF, HF, UHF, and Microwave;
- Access mode: read-only versus read/write;
- Memory type: read-only versus user programmable;
- Memory organization: length of blocks and special codes;
- Collision arbitration: it could be deterministic/slotted, adaptive, probabilistic binary tree search, and others. Anti-collision protocols are required to be able to read multiple tags simultaneously.
- Air interface: AM pulse width mod, pulse interval ASK, passive backscatter, FSK and others.
- Data rate
- Tag read speed
- Operating range, which is the distance between the coil of the tag reader and the tag: from a few centimeters to several tens of meters.
- Tag capacity
- Type of tag: passive, semi-passive, and active.

There is no 'best' standard, and different protocols are preferred for different applications. It is important to have an agreement on RFID standards throughout the industry and preferably throughout the world, but achieving global agreement would be a very challenging task due to the fact that different countries have different frequency bands available for this use and some governments have placed restrictions on emissions and other aspects that RFID is concerned with.

3. RFID Applications

The concept of RFID is used as a method to identify friendly aircrafts during World War II. Recently, RFID receives great attentions. Operating frequencies, tags, and readers can be designed differently for different applications. In some applications, tags are read one-by-one as RFID tags pass a reader on a conveyor belt, while in other applications, multiple tags can be read at one time. RFID systems find various applications where automatic identifications of objects, people or locations are needed. Some examples of applications are listed as follows. In 2001, Ford Motor Co. claimed that any future tire will include a UHF RFID tag to identify the vehicle's speed [9]. In November 2002, Gillette announced that it would replace barcodes in March 2003 by ordering 500 million UHF RFID tags [17], and also teamed up with Wal-Mart and Tesco PLC to test specially designed shelves for real-time tracking of inventory levels [18]. New Hanover County Public Library in North Carolina and three other libraries recently installed RFID self-checkout workstations and self-return book drop [9]. In 2003, Alexandra Hospital in Singapore used an RFID tracking system during the Severe Acute Respiratory Syndrome (SARS) outbreak, and all patients, visitors, and staff entering the hospital using an RFID ID card so that if someone is diagnosed SARS later, all individuals who contacted the person in hospital can be immediately identified [19]. More detailed applications of RFID technology are explored in this section as follows.

3.1. Mining Human Activities

In Reference [20], the authors present an activity recognition system called the Proactive Activity Toolkit (PROACT) to extract human activities and to learn about their beliefs. In PROACT, tens to hundreds of interesting objects in the environment are attached with RFID tags, which cost roughly $0.40 each and look like postage stamps including adhesive backing. A database entry mapping an RFID tag and an object is built whenever tagging an object with an RFID tag. Users' daily activities can be detected and recorded by readers regarding the objects that the users touch, and the distances and the movements that the users make to objects. PROACT deduces users' activities based on sequence and timing of involved objects. PROACT can also produce the likelihood of various activities and the details of those activities, and produce some actions such as alerts.

3.2. Mobile Commerce

A dual-mode communication infrastructure for Wireless LAN (WLAN) and RFID tags mobile (m)-commerce applications is presented in Reference [21]. In a showroom of electronic devices such as digital camcorders and TVs attached with RFID tags, consumers can utilize PDA-size mobile computers to view these devices' webpages, evaluate their performance and features, compare prices, and place an order via WLAN. Retailers can also attach RFID tags to electronic article devices to enhance surveillance security. RFID technology will be pervasively deployed as m-commerce applications thrive.

3.3. Investigation of Motor Vehicle Accidents

Eyewitness of evidences at traffic accidents can be done with RFID tags [22], and the scheme works as follows. Each registered vehicle receives RFID devices (to attach the vehicle) with a programmed identical code, which along with the vehicle identification number are saved in databases. Handheld RFID readers used by policeman can obtain the coded information immediately after policeman arrive at the accident scenes so that databases are accessed for information such as the owner, the made, and the model of the vehicle. Time of fleeing driver can be also identified for hit-and-run accidents. Furthermore, positions of vehicles at their initial points of impact can also be obtained.

3.4. Asset Management, Warehouse Automation, Supply Chain Management

It is clear to see the advantages of RFID tags over the traditional barcodes when used for labeling merchandizes. The tags identify all consumer's or warehoused items, and each item can have a unique ID if using RFID, whereas with barcodes, all items in the same box would have the same ID.

With RFID technology, manufacturers have better control over the inventory by being able to track items and materials in the whole supply chain, for example, a company is able to know locations and arrival times of products at a warehouse. The process of inventory is more efficient and automated, and adjusting production according to the inventory levels becomes possible since manufacturers have access to this data. It is also possible to set up automatic replenishment at a distribution center or a retail store, for example, 'smart shelves' at Wal-Mart [11,23,24].

With RFID technology, manufacturers can cut labor costs since products can be marked and inventoried while on conveyor lines, or during the loading/unloading of trucks at dock doors, or while handling the loads in warehouses or distribution centers. This can be done automatically and thus leads to labor savings.

In case of a theft, with RFID technology, it is easier to find at which point theft occurred, for example, by comparing the number of shipped items scanned at one location against the number at the next location on the way; it is easy to identify and count items in a sealed box without having to open it.

It is also easier to tell counterfeit items from genuine ones by checking the serial numbers in tag IDs. It is convenient to control product recalls by quickly locating all the 'suspect' goods in the store and program their IDs into the registers to prevent customers from buying those items [11,23,24].

Consumers will have benefits such as being alerted when products are recalled and monitoring dosage of medications for the elderly, and such luxuries as automatic replenishment of refrigerators or ovens that read tags and cook the given products accordingly.

RFID technology makes it possible to track products throughout the supply chain. A growing infrastructure now provides pervasive communication with objects, whether in a warehouse or on the road, and enables a unified control system for stock level management, automatic pricing, delivery, invoicing, and product recall [11,23].

3.5. Implicit Human Computer Interaction: Wearable RFID Tag Readers

Implicit human computer interaction (HCI) is different from the traditional concept of HCI in that not only the explicit user's input but also the user activity is input to computers, which facilitates data input when dealing with wearable computers [16]. In such applications, the computer is required to have knowledge of the situation and the physical objects, which the user is dealing with to be able to recognize the user's actions and use them as input. One of the ways to implement this is to have a wearable tag reader and integrate different kinds of coils into clothing, or wear them on the body. A possible solution is described in Reference [16]. The authors have the tag reader operating in the continuous read mode and the types and placement of coils are determined by the usage scenario.

3.6. Real World Bookmarks

Real world bookmarks are to associate physical objects with digital information such as URLs [16]. The authors in Reference [16] present example applications like binding physical objects to URLs so that depending on the object such as pen or wallet that the user picks up, an appropriate resource such as word processor or stock market news is opened automatically for his/her usage.

In Reference [25], the authors classify real world bookmarks into several categories: (1) augmenting books and printed documents, for example, associating a book with an equivalent or related electronic document; (2) augmenting small documents, for example, associating a business card with the person's webpage or having it trigger the generation of an email message with an appropriate address filled in; (3) document services, for example, associating a book with the URL of its page on Amazon.com; (4) setting context, for example, the computer interface will change according to a user's profile and preferences upon scanning the tag on his user ID; (5) transitory associations: a distinction is made between the 'put' and 'go to' actions, as in having two tags in a physical bookmark, one used to bind a current page with the bookmark, and the other to load the last saved association onto the display; (6) augmenting objects that are not documents: associating physical objects or different parts of one object with different URLs/electronic documents, for example, a wristwatch waved near a computer will open a calendar customized for the particular user for a given day.

3.7. Electronic Container Seal (E-Seal) in Container Security Initiative

Nowadays, most of the cargos entering the United States come in standard ocean containers [26]. It is essential to ensure security of the containers entering the country by monitoring and inspecting them along the way to reduce the danger of hazardous materials being smuggled [26]. The RFID technology plays an important role in the container security initiative. Adopting E-Seals is a good idea, but they cannot provide complete security of the containers because for E-Seals to be effective, there is a need to make sure that proper security procedures are carried out all the way along the supply chain. There exist different models and protocols for RFID-based E-Seals, and before this technology can be effectively used, there needs to be an agreement on the industry standards for the technology, on the frequencies and protocols, and compatibility of different models used in the world must be ensured [26].

3.8. Electronic Toll Collection and Road Pricing

Cars have active tags with unique serial numbers. When a car moves through a toll booth or is on the road, its tag can be read and an account corresponding to the serial number can be located in the database and charged. Popular examples are Mobil's SpeedPass and auto-pay systems on some toll roads [23].

3.9. Tagging Animals

There are many applications on tagging animals [23]

- Tagging household pets: when an animal is found and brought to a shelter, it is scanned to see if it has an implanted RFID tag. If there is a tag, the pet's owner can be easily found in a database by the tag's serial number.
- Tracking livestock: farmers can track their animals and the dairy production process using RFID implants in the animals.
- Identifying migration patterns: RFID technology has even been used to track the migration patterns of penguins.

Animal identification is mandatory in the European Union, and the U.S. is pressured to accept this practice nationwide, which currently is used only in some places. 'Microchipping' of animals not only serves the purpose of backing up traditional and less enduring identification methods like tattoos and ear tags, it is also done for public health concerns [27]. Animals suspected of Mad Cow disease and other diseases need to be tracked to the 'farm of origin.' Tagging animals facilitates and speeds up a number of processes in agriculture, like entering parameters into animal records.

Active RFID tags used on animals can be in the form of neck straps, and passive tags can be in the form of rumen boluses, electronic ear tags, or injectable microchips [27]. The type of tag is chosen according to the size and living patterns of the animals.

3.10. Tagging People

Most people would not want to wear an RFID tag and be tracked. However, there are certain groups of people who have interests in being tracked, for example, people at networking events and conferences would wear RFID-based badges to announce that they are available for communication or to make some information available about them [23].

There are some other groups of people who are believed to benefit from being tracked or who should be tracked for the sake of safety [23]. Criminals on parole should be tracked; patients with diseases like Alzheimer need to be monitored; and even newborn babies can benefit from this technology [23]. In some hospitals, special RFID-enabled baby bracelets are offered. If a baby is being removed from the building without a correct password entered, an alarm goes off. Also, it is possible to enforce checking a match between a mother's ID and a baby's ID [23].

3.11. Computing Environment for Aircraft Maintenance

The standard process of maintenance, repair, and overhaul (MRO) of aircrafts is a costly process in terms of time and money [28]. The cost of a plane being idle during unplanned maintenance has been estimated at $23 000 per hour. It will save aircraft companies a lot of money if MRO is made shorter. The proposed solution in Reference [28] improves the efficiency of the process employing the idea of movable asset management. In this system proposed in Reference [28], each tool has an RFID tag and each toolbox is able to sense its contents and report its state to the person. Each mechanic has a smart portable device allowing him to quickly check the availability and location of tools and instantly access documentation. With such a system, delays are minimized as a result of better planning and preparing necessary parts and tools ahead of time; human errors are prevented by having smart devices do the job; documentation process is automated; and efficiency is improved by cutting the time previously spent for looking for parts/documentation [28].

3.12. Battery-Free Wireless Sensors

Wireless sensors have a variety of applications, but it is a challenge to produce a source of energy that is tiny and long lasting but supplies enough power for the sensors to communicate data through wireless means. Applying the RFID technology here can be a good solution, or at least a better one than batteries and ambient power scavenging.

Wireless identification and sensing platform (WISP) is a project [24] that attempts to use RFID for powering wireless sensors. To implement this approach, a number of passive RFID tags are augmented with sensors so that the tags can send the sensed data when interrogated by a tag reader. The sensed data from tags can be read from a distance of up to 8 m, the reading rate can be up to 2000 bits per second, and as mentioned in the tag properties, RFID tags can be very small and can be read through other materials (with some exceptions) [24].

However, there are certain challenges in the way of such systems. Often sensor networks span over large (sometimes outdoor) areas, but for RFID the read distances are limited (to overcome the limitation would mean to provide a lot of equipment); also long-range tags have a problem of collision and getting too little energy from the reader, and are sensitive to some environmental conditions. Although it is not totally clear at the moment how to convert the RFID system of tags and readers into wisps and make tags transmit sensed data, this new approach seems feasible and can potentially prove very useful.

3.13. Wal-Mart

In June 2003, Wal-Mart, one of the biggest corporations in the world, announced that its top 100 suppliers would be required by January 2005 to put RFID tags on cases and palettes of consumer goods shipped to Wal-Mart distribution centers and stores [29]. Furthermore, Wal-Mart required its remaining 12 000 supplies to follow suit with the mandate of having RFID tags on all pallets and cases by 2006. Naturally, when Wal-Mart moves, its suppliers and other companies follow. In fact, history shows that when Wal-Mart moves on a technology that has massive potential in the retail and supply chain industry, it is sure to find widespread use and success. When Wal-Mart declared in 1984 to use barcode as a better way to manage inventory, barcode became huge success soon after [9]. No supplier of Wal-Mart can risk losing Wal-Mart's business, which is the reason that it is highly unlikely for a supplier to deny Wal-Mart's mandated RFID adoption.

Moreover, the cost savings that Wal-Mart says it might gain from the adoption of RFID technologies are staggering and sometimes enough to drive other industries to jump on the RFID technology bandwagon. Wal-Mart savings, in fact, are estimated to be $8.4 billion annually, which is greater than the total revenue of half of Fortune 500 companies combined [29]. Clearly, Wal-Mart sees a significant advantage of employing RFID technologies.

3.14. The U.S. Department of Defense

The United States Department of Defense (DoD) and the United States 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, for example, tracking containers worth more than $5000 [30], the DHS is looking into implementing RFID technologies to help fight global terrorism, for example, studying how RFID technology speeds up the movement of people crossing borders while reducing the threat of terrorism [29].

3.15. Libraries

Libraries, related to supply chain industries will benefit from the adoption of RFID technologies, and have potentials for widespread adoption of RFID tags.

Books are organized according to their types and subjects, and specific books are more-or-less uniquely identified by ISBN. The ISBN number does identify one particular individual printing of books, but all the copies of one particular book indexed in the Library of Congress, similar to UPC, that is, ISBN, identifies only a book's title, author, publisher, and date of publication. Therefore, based on ISBN, a librarian cannot know which individual book has been checked out. Previous solutions to the problem include the use of barcodes, but barcodes are quickly reaching the limits of their capabilities. This leads to RFID adoption by libraries. Libraries began to use RFID technologies by the late 1990s, and 130 libraries in North America adopted RFID systems for library check-in and check-out system [29].

4. RFID Research Issues

There are many technical issues for the RFID technology that need to be resolved such as cost control, energy efficiency, privacy issues, multiple readers' interference, and security issues. They are discussed in the following sections.

4.1. Cost Control

The ultimate goal of RFID proponents is to see the adoption of RFID technologies and systems on a global scale. RFID proponents have long heralded the day when RFID tags, readers, and applications are developed and put to use everywhere. However, such a widespread adoption is dependent on a couple of factors: first, willing participants, and second, economically viable RFID technologies.

Tag price is one critical issue: chip tags are not normally available below $0.3 if ordering less than one million tags, and chipless tags are normally $0.01–$0.2 if ordering 100 K tags [31]. Developing new, faster, and cheaper tags is an ongoing process [31]. An RFID reader typically costs $1000 (U.S.) or more [31]. Currently, RFID tags are more expensive than barcodes. This is one of the most important factors in limiting the usage of RFID technology. It has been estimated that if a cost as low as ¢0.09 per tag is achieved, RFID tags will have a cost-benefit advantage over barcodes and will replace barcodes altogether. Some companies have admitted that switching to RFID systems is so far unaffordable to them and they will only make the switch when the price of a tag drops to ¢0.05. Aggressive cost reduction policy is essential for the success and wide acceptance of the RFID technology across the industries [14]. But ongoing research aiming to find a way to produce RFID equipment at a fraction of the current cost and the pressure coming from retail leaders like Wal-Mart will eventually overcome this obstacle on the way of RFID technology to dominance in the market.

While concerns are great and skeptics are prevalent when any new technology enters the scene with promising new capabilities and improved efficiency, attention should be carefully paid to potential cost savings. RFID technologies are inheritably useful in industries where they can potentially make the most impact in both efficiency of operations and in cost savings to operations. One such industry that expects to see significant cost savings due to RFID implementations is retail stores and supply-side management companies. For example, Wal-Mart, by implementing RFID technologies, expects to see cost savings that would rival the revenues of most other companies [29]:

- $6.7 billion in reduced labor costs (no barcode scanning required);
- $600 million in out-of-stock supply chain cost reduction;
- $575 million in theft reduction;
- $300 million in improved tracking through warehousing and distribution centers;
- $180 million in reduced inventory holding and carrying costs;

Lowering tag and system costs will enhance further the adoption of RFID technology, and two ideas have recently been proposed [4]:

- To reduce assembly cost by using a tag fluidic self-assembly process, in which active silicon component floats around and bonds to the antenna assembly in a liquid medium, and the silicon device is the same shape to lock into its target so that many devices can be produced at once during the bonding process.
- To reduce cost by using entire plastic RFID tags built from plastic transistors on a flexible substrate so that all parts of a tag are created at the same time.

The research issue in cost control is how to design much cheaper and high quality tags.

4.2. Energy Efficiency

An RFID network has following characteristics: (1) a very large number of tags per reader, for example, in a warehouse application, each reader handles thousands of tags; (2) tags must be very small; and communication messages are normally short and simple. Tags can conserve energy by entering a sleep state when not in communications, and the ratio of energy consumed between the sleep and wake states is typically on the order of 100 or more [32]. This section studies how to save energy of tags with batteries.

Three different protocol approaches are presented in Reference [32], that is, grouped-tag TDMA protocols, directory protocols, and pseudorandom protocols, combining the fairness with low energy requirements while maintaining acceptable access delays. Assume that there is one reader and N tags through a radio channel of bandwidth B under packet-oriented network. An *access protocol* is a *transmission scheduling strategy* at the reader, and a *wake-up schedule* at each tag, which determines the slots in which the tag is awake.

4.2.1. *Time-division multiple access (TDMA)*

TDMA is a deterministic protocol, assigning each tag a slot during which period it may receive transmissions. In other slots, the tag goes to sleep. This protocol is very energy efficient, but if there are a large number of tags, the delay is very large.

4.2.2. *Grouped-tag TDMA protocol*

The grouped-tag TDMA protocol for energy conservation divides tags into $[N/x]$ disjoint groups, where x is the number of tags per group, and assigns each slot to a group. Compared with the TDMA scheme, the average energy consumption per slot decreases x times, but the average delay decreases by x times too. The drawbacks of the grouped-tag TDMA protocol include wasting significant energy when tags continue to wake up cyclically although the reader does not have packets for the tags, and the degraded performance if packets' destination distribution is heavily clustered [32].

4.2.3. *Directory protocol*

In the dictionary protocol, the reader accumulates k packets, broadcasts a directory listing the destinations, and transmits the k packets. Tags listen to the directory to find out whether/when packets are scheduled, and wake up periodically to give the reader an opportunity to start a directory transmission. This approach is better than the grouped-tag TDMA in terms of fairness if the destination distribution is heavily clustered. But, if the size of the directory is too large, reading the directory wastes a lot of energy.

4.2.4. *Random access protocol*

In the random access protocol, the reader randomly selects one of the packets in the queue to transmit, and the packet is successfully received if and only if the destination tag of the packet is awake. Tags are awake with probability p. The scheme has very low energy consumption, but the chance that the destination tag can receive the packet is small.

4.2.5. *Pseudorandom protocol*

In the pseudorandom protocol, tags run the same pseudorandom number generator and determine their wake/sleep slots with different seeds known by the reader to avoid a complete overlap of schedules. If the reader knows the seed, it can determine the schedules of the tags. This scheme is good for heterogeneous traffic patterns.

4.2.6. *Research issue of energy efficiency*

Comparing the grouped-tag TDMA, the dictionary protocol, and the pseudorandom protocol, the grouped-tag TDMA has the best performance under either a low traffic load or a uniform destination distribution [32]. The pseudorandom protocol is better than the directory protocol in terms of energy saving and delay, except when the destination distribution becomes heavily clustered, in which case the directory protocol is the best scheme [32].

Therefore, designing a better energy efficient scheme is still a research issue, and deserves further investigations.

4.3. Privacy Issues

The RFID technologies involve many privacy issues. Allowing remote access and data sharing implies abuse usage of private information. When customers purchase RFID-tagged items, their privacy may be compromised in a number of ways: (1) tags could be read without a person's knowledge because humans can not sense radio signals; (2) tags could be read by unauthorized parties; (3) it is possible to create a database to track associations between tags and owners of tagged items over a long period of time; (4) information exchange between a tag and tag reader could be secretly monitored.

These could 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 which could be used against the owner, or to store extra identifiers in the tags.

The debate over the use of RFID technology has become more commonplace and fervent as the technology has developed. In fact, social reaction to a trial deployment of RFID tags in retail stores surprises many companies [4]. Privacy protection groups are worried that RFID tags attached to such items as clothing could be used to provide specific marketing to the customers of the stores.

To be sure, privacy groups are especially worried about random eavesdroppers accessing the data contained on RFID tags attached the purchased merchandises. However, companies developing RFID technologies and the retailers that use the technologies developed have been quick to point out the impracticality of scanning RFID tags from any real distance. They say that eavesdroppers would have a hard go at reading RFID tags due to the tags with distance [4].

Despite these efforts, privacy groups have been successful in convincing the public that RFID technology might have a lasting negative effect on their rights to privacy. Privacy groups have been so successful, in fact, that some companies have been forced to reconsider their adoption of RFID technologies. For example, Benetton Group, an Italian clothing manufacturer and retailer, received great criticism and scrutiny when it tried to attach RFID tags to its products [32]. Gillette also was the subject of public scrutiny and concern when it decided to buy 500 million RFID tags for use with its products [9].

Clearly, the biggest privacy concern associated with RFID technologies is the ability to track RFID tags. With large corporations, such as ChoicePoint, specializing in the storage and selling of personal data, including buying habits, privacy groups have cause for concern: there is a viable market for data collected by reading RFID tags.

Despite these concerns, there is much to be gained from the adoption of RFID technologies, especially by businesses concerned with improving their bottom line.

Even more 'insidious' organizations might find data collected from RFID tags tempting. Concerns that the government might use RFID tags to track citizens and eavesdrop on citizens' personal habits have gained attention. Specifically, since the terrorist attacks of 11 September 2001, the government has been seeking new and broader ways to track terrorists' habits in the effort to prevent future terrorist attacks. Fears that the government may reach too far into law-abiding citizens are not far fetched. Although Total Information Awareness (TIA) proposal of the U.S. Defense Advanced Research Projects Agency had been recently dropped, the TIA proposal aimed at gathering data from all available sources into a huge database [9].

Certain measures can be taken to protect consumers' privacy, for example: (1) to deactivate the tags at the time of purchase; (2) to partially erase part of the ID on the tag at the time of purchase; (3) to allow consumers to assign passwords to tags so that unauthorized parties could not read the tags because the tags can only be read by those who know the password.

Certain safeguards can be used in conjunction with RFID technologies to prevent malicious and unintended use: (1) *Blocker tags*—tags which are similar in size to conventional RFID tags but are used to block data transmission of RFID tags; these tags can be carried by individuals and block the reception of any other RFID tags by an RFID reader within range of both the blocker tag and the RFID reader; (2) *Kill switches*—kill switches are small, implanted features of RFID tags that allow the tags to be disabled, or killed, when their use is no longer necessary or when concerns of malicious use are afoot; (3) *Opt-in*—opt-in laws and policies would help limit the use of data collected by RFID readers in public places, including stores.

But there are a number of factors that may prevent these measures from being carried out. Some of the factors are: consumers may be unaware of the presence of the tags or be unable or unwilling to deactivate them; or a merchandiser may not want to invest extra funds into reprogrammable tags or may wish to keep the tags for future use [11].

To address the growing concerns about privacy issues connected with the use of RFID, some researchers have proposed an 'RFID Bill of Rights' which adapts the Code of Fair Information Practices to the use of the RFID technology [11]. Some guidelines like this should be accepted across the industries to draw the line between using information collected by using RFID for good purposes and misusing the technology to compromise somebody's privacy. If RFID is to be widely used in many aspects of our lives, this line should be very clear.

Another security feature was proposed to protect manufacturers' goods and information: being able to 'put tags to sleep' while the tagged products are in transit. This can be done by assigning passwords to tags and denying access (read/write/kill operations) to anyone until a proper password is supplied [14].

Seven rights are defined in retail products for consumers [34]: (1) know whether a tag is in a product; (2) know when the tag is read; (3) remove the tag when a product is purchased, prohibit merchants' pressure tactics to coerce keeping the tag active, and prohibit reactivation without consent; (4) own and use inexpensive readers to detect tags; (5) access any database accumulating information from a tag; (6) maintain security and integrity of information transmitted from the tag and subsequently stored, with strict regulations on the use of the information by third parties, including governments; and (7) be able to account for everyone in the tag information chain.

However, there are a lot of issues on privacy issues deserved to further research and study.

4.4. Multiple Readers' Interference

If multiple tags are present, anti-collision algorithms should be adopted so that each tag is read-only once. Furthermore, multiple readers may interfere each other if they are in the same field. Neighboring readers cause interference if they communicate the same tag at the same time. The problem of minimizing reader collisions is called *reader collision problem* [35].

In Reference [35], Colorwave, an anti-collision algorithm for reader collision problem, is proposed. Colorwave models readers as an undirected graph, where vertices are readers and edges are collision constraints, for example, two readers connected with an edge collide if transmitting at the same time. Colorwave extends the distributed color selection (DCS) algorithm [35]. Both Colorwave and DCS are two color readers such that each reader has the smallest possible number of adjacent readers with the same color. DCS works as follows [35,36]:

1. A reader transmits only in its color timeslot. If collides, the transmission request is discarded.
2. The reader can randomly reserve a color so that its neighbors have to select different colors. This switch and reservation action is referred to as a 'kick.'
3. Each reader keeps track of what color it believes the current slot to be.

In DCS, the maximum colors variable is fixed [35,36]. A mechanism for dynamically changing the maximum number of colors is also proposed in Colorwave, to which five inputs determine the timing when a reader changes its local value of max colors [35,36]: (1) UpSafe: the safe percentage at which to increase max colors; (2) UpTrig: the trigger percentage at which to increase max colors if a neighboring reader is also switching to a max colors higher than that of this reader; (3) DnSafe: analogs of UpSafe but decrease max colors; (4) DnTrig: analogs of UpTrig but decrease max colors; (5) MinTimeInColor: the minimum number of timeslots before the Colorwave algorithm will change max colors again after initialization or changing max colors. Colorwave is briefly described as follows [35,36]:

1. When a reader reaches a threshold called safe percentage to change its own value for max colors, it reserves a color and lets all neighboring readers know.
2. If exceeding a safe percentage due to local to that reader, the other readers will not have passed their own Trig percentages and will not respond.
3. If the phenomenon causing the collision value to exceed a safe threshold is widespread, neighboring readers will most likely have exceeded their own Trig thresholds, and a kick will ensue.
4. As kicks spread from the initiating reader throughout the entire system, a large portion (or all) of the readers in a reader system may change their value of max colors.

Clearly, the above algorithms cannot work well under the situation when some mobile handheld reader devices exist. Multiple readers' interference is indeed a research issue, which deserved further investigation.

4.5. Security Issues

Compared to other networks, RFID system is relatively secure as an authentication technology and an identification technology. Counterfeiting radio frequency identification chips is difficult. However, a hacker having specialized knowledge of wireless engineering, encoding algorithms, and encryption techniques, still can hack the system. Data on the tag can be defined in different levels of security. Security issues attracted the researchers' attention recently and will become a very hot research topic.

A cloned attack can be carried out if installing a cloned replacement tag that authenticates itself successfully to the reader due to weak authentication or no authentication [37]. Since tags are highly resource constrained, lightweight cryptographic primitives are needed. In Reference [37], five lightweight authentication algorithms are proposed to prevent theft and the cloned attack, but the proposed schemes can be attacked a powerful attacker. There is always a tradeoff between strength of security and complexity. Further research on security issues is needed. Let x denote a random challenge. Let $R \rightarrow T$ denote that the reader sends to a tag, and vise versa. We introduce the five schemes in Reference [37] as follows.

- $XOR - with - Two - Keys : R \rightarrow T : x \oplus k_1$ 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 choose 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 $(i-1)$-th run and the i-th run: $(x^{(i-1)} \oplus k^{(i-1)}; k^{(i-1)} \oplus k^{(i-2)})$ 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 the first-time key establishment problem due to limited resource.
- $Subset : R \rightarrow T : x \oplus k$ and $T \rightarrow R : f(x)$, where k is the key, $f(x)$ is a function, and $x = (x_L, x_R)$. The j-th byte of x_R addresses a bit of x_L, and is considered as the j-th bit of the output vector.
- $Squaring : R \rightarrow T : x$ and $T \rightarrow R : k_L \oplus ((k_R + x)^2$ mod $2^n)$, where $k = (k_L, k_R)$ with $2n$ bit length.
- $RSA : R \rightarrow T : x$ and $T \rightarrow R : E(x \wedge k)$, where E is the encryption of RSA and ^ is the bitwise AND
- $KNAPSACK : R \rightarrow T : (d \oplus k, \kappa(x, d))$ 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 κ is a punctured multiplicative knapsack.

The above schemes can be attacked by a powerful attacker. There is always a tradeoff between strength of security and complexity. Further research on security issues is needed.

5. Conclusion

RFID is a very promising and rapidly developing technology with a number of significant advantages over the traditional optically scanned barcode systems and has the potential to replace them in the near future. RFID technologies can significantly improve the bottom line of many businesses and even governments. Many people believe that RFID is going to dominate the market of auto identification systems in a few years. But before this takes place, several important issues have to be successfully resolved, the most important being adequately protecting personal privacy of users and reaching the necessary cost efficiency of RFID equipment, while other issues such as energy efficiency, multiple readers' interference, and security issues, should be further studied and investigated.

References

1. barcodeman.com, 2D Barcodes Explained, accessed April 2005. site: http://www.barcodeman.com/faq/2d.php
2. Allied Business Intelligence, RFID White Paper, 2002.
3. Sarma S. Integrating RFID, ACM Queue, Vol. 2(7), October 2004.
4. Want R. The magic of RFID, ACM Queue, 2004, pp. 41–48.
5. Intermec. Supply chain RFID: How it works and why it pays, 2004.
6. Das R. RFID explained. IDTechEx. Site: http://www.idtechex.com
7. Boss RW. RFID technology for libraries [Monograph]. *Library Technology Reports*, November–December 2003.
8. Ayre LB. Position Paper: RFID and Libraries. *Wireless Privacy: RFID, Bluetooth and 802.11.* Addison-Wesley/Prentice Hall, 2005.
9. Cavoukian A. Tag, You're It: Privacy Implications of Radio Frequency Identification (RFID) Technology, Information and Privacy Commissioner, Ontario 2004, February.
10. Microsoft, Microsoft and RFID, 2004.
11. Schmidt A, Gellersen HW, Merz C. Enabling Implicit Human Computer Interaction. A wearable RFID-Tag Reader, 2000 IEEE.
12. Grønbæk K, Kristensen JF, Ørbæk P, Eriksen MA. Physical Hypermedia: Organising Collections of Mixed Physical and Digital Material. HT'03, August 26–30, 2003, Nottingham, UK, ACM.
13. Garfinkel SL. Adopting Fair Information Practices to Low Cost RFID Systems. The IEEE Ubiquitous Computing 2002 Privacy Workshop.

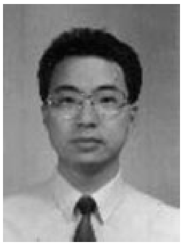
14. Philipose M, Smith MR, Jiang B, Mamishev A, Roy S, Sundara-Rajan K. Battery-Free Wireless Identification and Sensing, 2005 IEEE.
15. Noonan G, Cheyne M, Robertson I. RFID in the Supply Chain: A Balanced View. Business Briefing Paper, Amcor Australasia and Hewlet-Packard, 2004.
16. Nucleus Research Note E21. Five points to consider in your RFID project plan, 2004.
17. Gillette Confirms RFID Purchase, *RFID Journal*, January 7, 2003.
18. Weir J. RFID Tags and IT Services, *IDC Study*, Framingham, MA: International Data Corp., #MS01K, April 2003.
19. Electronic Privacy Information Center. Radio Frequency Identification (RFID) Systems. Washington, D.C., August 11, 2003, p. 3.
20. Perkowitz M, Philipose M, Fishkin K, Patterson DJ. Mining models of human activities from the web, 2004.
21. Bridgelall R. Enabling mobile commerce through pervasive communications with ubiquitous RF tags, 2003.
22. Using RFID's In The Investigation Of Motor Vehicle Accidents, http://rfid2vin.com, 2005
23. Chin LP, Wu CL. The Role of Electronic Container Seal (E-Seal) with RFID Technology in the Container Security Initiatives. In *Proceedings of the 2004 International Conference on MEMS, NANO and Smart Systems (ICMENS'04)*.
24. Schindler E. Smaller, Faster, Cheaper, Quieter. So What Else Is New?, NetNews, June 2004.
25. Grønbæk K, Kristensen JF, Ørbæk P, Eriksen MA. Physical Hypermedia': Organising Collections of Mixed Physical and Digital Material, HT'03, August 26–30, 2003, Nottingham, UK.
26. Yong P, Arlander P, Begovich M, Blomstrand M. 2004 Athens 'Diskos'—Olympic Voting Kit. CHI 2004, April 24–29, 2004, Vienna, Austria.
27. Lampe M, Strassner M, Fleisch E. A Ubiquitous Computing Environment for Aircraft Maintenance. In *Proceedings of SAC04*.
28. Sokoler T, Edeholt H. Physically Embodied Video Snippets Supporting Collaborative Exploration of Video Material During Design Sessions, NordiCHI October 2002, Århus, Denmark.
29. Automation. RFID in Manufacturing: A practical guide on extracting measurable value from RFID implementations in plant and warehousing operations, 2004.
30. Noonan G, Cheyne M, Robertson I. RFID in the Supply Chain: A Balanced View. Business Briefing Paper, Amcor Australasia and Hewlet-Packard, 2004.
31. IDTechEx. An Introduction to RFID and Tagging Technologies, 2002.
32. Chlamtac I, Petrioli C, Redi J. Energy-conserving access protocols for identification networks. *IEEE/ACM Transactions on Networking* 1999; **7**(1): 51–59.
33. Boone B, Whalen M. Benetton Unites with RFID: IDC Predicts Low Adoption in Retail Until 2005, *IDC Flash*... #29131. Framingham, Massachusetts: International Data Corporation. March 2003.
34. Pottie GJ. Privacy in the global E-village. *Communications of ACM* 2004; **47**(2): 21–23.
35. Waldrop J, Engels DW, Sarma SE. Colorwave: An anticollision algorithm for the reader collision problem. In *Proceedings of IEEE ICC 2003*.
36. Waldrop J, Engels DW, Sarma SE. Colorwave: A MAC for RFID reader networks. In *Proceedings of IEEE WCNC 2003*.
37. Vajda I, Buttyán L. Lightweight Authentication Protocols for Low-Cost RFID Tags, 2nd Workshop on Security in Ubiquitous Computing, in conjunction with Ubicomp 2003.

Authors' Biographies

Yang Xiao worked at Micro Linear as an medium access control (MAC) architect involving the IEEE 802.11 standard enhancement work before he joined Department of Computer Science at The University of Memphis in 2002. Dr Xiao is an IEEE Senior member. He was a voting member of 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* (WCMC), *EURASIP Journal on Wireless Communications and Networking*, and *International Journal of Wireless and Mobile Computing*. He serves as a (lead) guest editor for *International Journal of Security in Networks* (IJSN), Special Issue on 'Security Issues in Sensor Networks' in 2005, as a (lead) guest editor for *EURASIP Journal on Wireless Communications and Networking*, Special Issue on 'Wireless Network Security' in 2005, as a (sole) guest editor for (Elsevier) *Computer Communications Journal*, special Issue on 'Energy-Efficient Scheduling and MAC for Sensor Networks, WPANs, WLANs, and WMANs' in 2005, as a (lead) guest editor for (Wiley) *Journal of Wireless Communications and Mobile Computing*, special Issue on 'Mobility, Paging, and Quality of Service Management for Future Wireless Networks' in 2004, and as a (lead) guest editor for *International Journal of Wireless and Mobile Computing*, special Issue on 'Medium Access Control for WLANs, WPANs, Ad Hoc Networks, and Sensor Networks' in 2004. He serves as a referee/reviewer for many funding agencies, as well as a panelist for NSF. Dr Xiao's research areas include wireless LANs, wireless PANs, wireless MANs, wireless WANs (cellular networks), and ad hoc and sensor networks. His research interests are security/reliable communications, medium access control, mobility/location/paging managements, cache access and replacement policies, quality of service, energy efficiency, and routing in wireless networks and mobile computing.

Senhua Yu received his M.Sc. degree in Computer Science from University of Memphis, TN 38152 U.S.A. in August 2003 and is currently a Ph.D. student in Department of Computer Science at University of Memphis. His research interests are in wireless networks, artificial intelligence, and bioinformatics. He is also with University of Tennessee Health Science Center, Memphis, TN 38163 U.S.A. where he is IT Analyst II at the Center for Neurogenetics, Department of Anatomy and Neurobiology. He is currently working on Internet Video Microscope project and Mouse Brain Library. Previously he worked in Intelligent Security Systems

Research Lab (ISSRL) at University of Memphis where he was a research assistant with the responsibility of the development and applications of a new general purpose algorithm *Mulitlevel Immune Learning Algorithm* (called MILA). Mr Yu is a student membership in International Society for Genetic and Evolutionary Computation (ISGEC) and also received his B.Sc. degree and the M.Sc. degree in biology from Nanjing Normal University, China, in 1994 and 1997, respectively. He published more than 10 journal papers in the area of Computer Science and Biology.



Kui Wu received his Ph.D. in Computing Science from the University of Alberta, Canada, in 2002. He then joined the Department of Computer Science, University of Victoria, Canada, where he is currently an assistant professor. His research interests include mobile and wireless networks, sensor networks, network performance evaluation, and network security. He has been actively serving as a TPC member in several international conferences, such as Globecom, ICC, LCN, IPCCC, and ADHOC-NOW, and as a reviewer for several international journals, such as *ACM WINET*, *ACM MONET*, *IEEE/ACM Transactions on Networking*, *IEEE Transactions on Parallel and Distributed Systems*, *IEEE Transactions on Wireless Communications*, *Wiley WCMC*, and *Elsevier Computer Networks*. He co-chaired the first IEEE LCN workshop on network security.

Qiang Ni received his B.Eng., M.Sc. degrees, and Ph.D. from Huazhong University of Science and Technology (HUST), Wuhan City, China in 1993, 1996, and 1999 respectively. He is currently a faculty member in the Electronic and Computer Engineering Division, School of Engineering and Design, Brunel University, West London, U.K. Between 2004 and 2005, he was a senior researcher at the Hamilton Institute, National University of Ireland, Maynooth. From 1999 to 2001, he was a post-doctoral research fellow in the multimedia and wireless communication laboratory, HUST, China. He visited and conducted research at the wireless and networking group of Microsoft Research Asia Lab during the year of 2000. From September 2001 to May 2004, he was a research staff member at the Planète group of INRIA Sophia Antipolis, France. Since 2002, he has been active as a voting member at the IEEE 802.11 wireless LAN standard working group. He has served as Technical Program Committee (TPC) member/session chair for a number of international conferences on wireless communications and networking. His current research interests include communication protocol design, performance analysis, cross-layer optimizations and security issues for wireless networks, vertical handover and mobility management in mobile networks, and adaptive multimedia transmission over hybrid wired/wireless networks. He has authored/co-authored over 40 international journal/conference papers, book chapters, and standard drafts in this field. He is a member of IEEE.

Christopher Janecek is an undergraduate student of Department of Computer Science, The University of Memphis, TN, 38152, USA.

Julia Nordstad is working towards her Bachelor's degree in Computer Science at the University of Memphis (Memphis, TN). Her main interests include database systems and different technologies used for web applications development. This summer she worked at the Computational Neurodynamics Lab at the FedEx Institute of Technology/ The University of Memphis as a research assistant. She has previously been a student member of the Society of Women Engineers and Xplor International.