Communications and Network, **2010, 2, 183-186**
doi:10.4236/cn.2010.23026 Published Online August 2010 (http://www.SciRP.org/journal/cn)

An Introduction to RFID Technology

Sanjay Ahuja, Pavan Potti
School of Computing, University of North Florida, Jacksonville, Florida
E-mail: {*sahuja, pavan.potti*} *@unf.edu*
Received March 7, 2010; *revised July* 2, 2010; *accepted July* 30, 2010

Abstract

RFID technology emerged some time back and was not used that much because of lack of standardization and high costs. Latest technologies have brought costs down and standards are being developed. Today RFID is mostly used as a medium for numerous tasks including managing supply chains, tracking livestock, preventing counterfeiting, controlling building access, and supporting automated checkout. The use of RFID is limited by security concerns and delays in standardization. This paper describes RFID technology and its applications in today's world.

Keywords: RFID, RFID Applications

1. Introduction

According to Roy Want in [1], "Radio Frequency Identification Technology (RFID) has moved from obscurity into main stream applications that help speed the handling of manufactured goods and materials". Barcode is still the dominant player in supply chain industries and departmental stores. However RFID is replacing barcode technology and enjoys the major advantage of being independent of line of sight problems and scanning the objects from a distance. It offers the promise of reduced labor levels, enhanced visibility, and improved inventory management. Walmart has been one of the leaders in the large scale adoption of RFID technology [1, 2]. RFID tags have a memory capacity of 16 - 64 Kbytes which is far more than the barcodes (1 - 100 bytes) [3] and can store additional data such as manufacturer name and product specifications.

The initial step of RFID was during World War II, when the British used it to identify whether planes belonged to "friend or foe". Some technical problems resulted in the gunning down of allied planes and since then the use of RFID was limited to Defense and armed forces industries due to the cost factors. New advancements in science and technology have enabled usage in commercial applications. Large institutions, such as the US Department of Defense, have since implemented RFID which is now spreading to other organizations and industries [1]. Walmart is the second biggest user of RFID and investing significant resources to develop its applications.

Security problems still prevailing about RFID technology is the fear that people can easily build RFID readers with lower costs and can read data from an RFID chip without knowledge and maybe even alter the data. For example, someone could use the RFID reader on an inexpensive product and upload the data to a chip that is on an expensive product, thereby getting the latter for a lower price. Another example is about retrieving data from unsecured RFID enabled mobiles.

RFID advantages can be briefly explained as follows:

- Reader can read and write data to RFID tags with out direct contact and no line of sight problem.
- Data from the multiple RFID tags are accessed by the reader by radio waves.
- No maintenance costs; RFID can work under different environments and can be used effectively for over 10 years.
- Fast read and write with the time taken for read/write being a few milliseconds.
- Modern RFID tags are made with very good memory capacities ranging from 16 - 64 Kbytes which is many times more than a typical barcode.
- RFID tags can work with GPRS and has been used for tracking.
- RFID tags can also integrate with other technologies. For example, it is used with wireless sensor networks for better connectivity.

The rest of the paper is organized as follows. RFID principles are discussed in Section 2, Section 3 discusses RFID applications, and Section 4 discusses RFID security and technical solutions. Conclusions are listed in Section 5.

2. RFID Principles

Different types of RFID tags exist, but are broadly classified as active or passive. An active tag requires a power source and is either connected to a powered device or to a battery and is often limited by the lifetime of its source. Being dependent on a powered source puts limitations on Active RFID tags. Cost, size, lifetime make them impractical for regular use. On the other side, Passive RFID is of interest because of the fact they are independent of power source and maintenance.

Passive RFID also have advantages of long life and being small enough to fit into a practical adhesive label. Hence passive RFID tags are used for many applications and this paper focuses more on passive RFID tags. A passive RFID tag consists of mainly three parts: an antenna, a semiconductor chip attached to the antenna, and some encapsulation to protect the tag from the environment. As explained before, passive RFID tags don't carry any powered device and became active only upon exposure to external energy. The RFID reader does the work for activating and communicating with the tag. The passive RFID tag antenna captures energy from the reader and is responsible for communicating the data between tag and reader. Roy Want states in [1], "Two fundamentally different RFID design approaches exist for transferring power from the reader to the tag: magnetic induction and electromagnetic (EM wave capture). These two designs take advantage of the EM properties associated with an RF Antenna – the near field and the far field". Both technologies can transfer enough power to a remote tag, usually the power levels will be in the range of 10μW and 1 mW which is very minimal when compared to regular Intel 4 processor power levels 50W. Near-field is the most common approach used for implementing passive RFIDs, and used for near range communications. It has the physical limitations of range. The range of communication of near field technology depends upon the formula $c/2\Pi ef$ where c is the speed of light and f is the frequency. It has the limitation that frequency of operation increases as the distance decreases. One more limitation is the energy available for induction as a function of distance. These physical limitations have led to far field communication and far field communications depend upon backscattering.

3. Applications of RFID

RFID applications are very broad and open in nature. First we discuss daily use applications followed by a case study.

RFID is used as a medium for numerous tasks including managing supply chains, tracking livestock, preventing counterfeiting, controlling building access, supporting automated checkout *etc.* RFID is also used as a means of providing security to differentiate pirated copies of video and audio discs by sticking RFID stickers to the discs.

Another widely popular example for RFID application is RFID based toll gates. Electronic payment of toll collecting using E-ZPass is a wide spread application. E-ZPass tags are RFID transponders attached to the car license plate and sends account information to the equipment built into lane-based or open toll collection lanes. The toll system will charge from a pre-entered credit card or sends a check. A latest enhancement to this technology is sending the bill details instantly to the user's mobile phone. And this technique is also used to track stolen cars and other vehicles by police departments with the use of GPRS and RFID.

Another popular application of RFID is in animal tracking. Using RFID tags to track animals is not a new application, but it has evolved from the usage of detecting of missed cattle to the tracking of its movements and behavior. The RFID tags are even used to control outbreaks of animal diseases. Today technology has transformed into human implantation of RFID tags. RFID based wristbands and clothes embedded with RFID tags are used to track prisoners.

The RFID tags are also used in the health care industry; an RFID tag is used to store the patient's medical history. RFID tag is scanned each time to know the developments and changes of the patient's health condition and medication. RFID tags are often used for medical transactions. RFID tags can also be used in airline industry to track the baggage of the passengers [4]. Walmart is conducting trials to explore a cart integrated with an RFID reader and a wireless mobile computer authorized to make payments as customers add items to the cart. The system displays prices and then authorizes a batch payment when the customer finishes shopping. If a customers RFID mobile is also tuned with credit details, the payment is also done electronically.

Bluetooth is one potential option for providing connectivity, but its usage is hindered by the time it consumes for device discovery and service discovery processes [5]. Salminen *et al* in [5] used RFID technology to enhance Bluetooth connection establishment and compared the results with and without using RFID and showed that their approach dramatically increase the performance. Even though Bluetooth is one of the leading means of communicating between devices, the limiting factor for it is the time it takes for device discovery process. And when the user is looking for a specific service offered by other Bluetooth enabled devices it takes more time and is often unnecessary. So the work in [5] authors suggests that the RFID system be used to as a means to initiate a Bluetooth communication channel between the user's terminal and the services in the environment. Establishing connection between two Bluetooth devices is a two step process. The first step is to search for the devices in its neighborhood called Device

Discovery, and the second step is to look for the available services and their characteristics called Service Discovery. So to decrease the time of communication, Salminen at al in [5] the stored address and the attributes of the provided service in RFID tags so that the Bluetooth connecting device is quickly aware of the services offered by other devices. A typical Bluetooth device takes about 10.24 seconds for connecting with other Bluetooth enabled devices and some times it exceeds that time with multiple Bluetooth devices in the environment. Compared with Bluetooth, RFID takes only a few milliseconds for communication which is much faster. Another research area for RFID is in the field of Wireless Sensor networks which are a mixture of both sensors and RFID tags and are used for better connectivity and communication [6]. RFID is also used for Activity Recognition and Visual Tracking [7].

4. RFID Security and Technical Solutions

4.1. RFID Security

The major and primary security concern of RFID is that anyone can access the RFID data because there is no line of sight problem and be able to gather data. In addition, people are cloning RFID tags and using them just as the way it was done for credit cards before. Preventing effective cloning of RFID tags is still an open and challenging problem. Criminals with RFID readers could scan crowds for high-value banknotes. And terrorists could scan digital passports to target specific nationalities.

Currently the research is on-going on RFID malware [8]. RFID malware can be grouped into three distinct categories: exploits, worms, and viruses. RFID exploits are traditional hacking attacks that are identical to those found on the Internet like buffer overflows, code insertion, and SQL injection attacks. RFID worms and viruses are simply RFID exploits that copy the original exploit code to newly appearing RFID tags. The main difference between the two is that RFID worms rely on network connections whereas RFID viruses do not.

4.2. Technical Solutions

One of the problems of RFID tags is that customers often forget to remove the tags from clothes after purchase and this gives the chance of tracking customers. The better solution is to use EPC kill command as a pro-privacy technology after selling the products. Another alternative to prevent leaking of data from RFID tags is the use of cryptography as measure of privacy. This in turn results in an additional problem of key management and the level of encryption standards and its cost. A different approach is using Tag passwords so that a tag could emit important information only if receives the right password. The dilemma is in the reader having to know the tag identity. Another solution is using a timer based mechanism that the causes the tag to change the password periodically with a predefined mechanism. Another solution is the use of Blocker tags, *i.e.* using two tags and blocker tag creates an RF environment that is hostile to RFID readers. But a simple and effective solution to prevent leakage of data from RFID tags is differentiating the reader with their energy levels. This was based on assumption that criminals will maintain more distance than valid RFID readers and the power levels will be different.

For details on RFID security protocols, readers are referred to [9,10].

5. Conclusions

RFID is still in a developing phase and more is in the pipeline in terms of new applications. Among applications already developed, RFID tags are being used in clothing for billing and security purposes. RFID tags are embedded inside animals for tracking purposes. RFID tags embedded in uniforms can be used to know the number of hours an employee spends to complete a particular task. There are several associations that are protesting against the use of RFID to track people fearing the impact on people's social life and privacy. Clearly the extent to which use RFID is to be used is still an open debate.

A lot of research on RFID tags is ongoing including on embedding these with other devices, especially mobile devices. RFID manufacturers and users are looking for proper standardization and regulation of RFID. As prices fall further and technological improvements continue to occur, RFID technology is expected to become economically and technically more viable and impact our daily lives as more applications are developed.

6. References

[1] Roy Want, "An Introduction to RFID Technology," *IEEE CS and IEEE ComSoc,* Vol. 5, No. 1, Santa Clara, 2006, PP. 25-33.

[2] Ron Weinstein, "RFID: A Technical Overview and Its Application to the Enterprise," *IT Professional*, Vol. 7, No. 3, June 2005, pp. 27-33.

[3] Klaus Finkenzeller, "RFID Handbook," 2nd edition, John Wiley & Sons, Ciudad Real, 2003.

[4] Badri Nath, Franklin Reynolds, Roy Want, "RFID Technology and Applications," *IEEE CS and IEEE ComSoc*, Vol. 5, No. 1, 2006, pp. 22-24.

[5] Timo Salminen, Simo Hosio and Jukka Riekki, "Enhancing Bluetooth Connectivity with RFID," *Proceedings of the Fourth Annual IEEE International Conference on*

Pervasive Computing on Pervasive Computing and Communications, Pisa, 2006, pp. 6-41.

[6] Lei Zhang and Zhi Wang, "Integration of RFID into Wireless Sensor Networks: Architectures, Opportunities and Challenging Problems," *Proceedings of the Fifth International Conference on Grid and Cooperative Computing Workshops*, Hunan, 2006, pp.463-469.

[7] N.Krahntoever, J.Rittscher, P.Tu, K.Chean and T.Tomlinson, "Activity Recognition Using Visual Tracking and RFID," *Proceedings of the Seventh IEEE Workshop on Applications for Computer Vision*, Vol. 1, New York ,2005, pp. 494-500.

[8] Melanie R.Rieback, Bruno Crispo and Andrew S.Tanenbaum, "RFID Malware," *IEEE Security and Privacy*, Vol. 4, No. 4, 2006, pp. 70-72.

[9] Hyun-Seok Kim, Jeong-Hyum Ob and Jin-Young Choi, "Security Analysis of RFID Authentication for Pervasive Systems using Model Checking," *Proceedings of the 30th Annual International Computer Software and Applications Conference*, Vol. 2, Chicago, 2006, pp. 195-202.

[10] Hyun-Seok Kim, Jung-Hyun Oh, Jin-Young Choi and Jin-Woo Kim, "The Vulnerabilities Analysis and Design of the Security Protocol for RFID System," *Proceedings of the Sixth IEEE International Conference on Computer and Information Technology,* Seoul, 2006*,* p.152.

[11] Simon L.Garfinkel, Ari Juels and Ravi Pappu, "RFID Privacy: An Overview of Problems and Proposed Solutions," *IEEE Security and Privacy*, Vol. 3, No. 3, Massachusetts, 2005, pp.34-43.

[12] Fred Niederman, Richard G.Mathieu, Roger Morley, and Ik-Whan Kwon, "Examining RFID Applications in Supply Caching Management," *Communications of the ACM*, Vol. 50, No. 7, July 2007, pp. 92-101.

[13] Zoltan Nochta, Thorsten Staake and Elgar Fleisch, "Product Specific Security Features Based on RFID Technology," *Proceedings of the International Symposium on Applications and the Internet Workshops*, Phoenix, 2005. pp. 4-75.

[14] Ramaswamy Chandramouli, Tim Grance, Rick kuhn, and Susan Landau, "Security Standards for the RFID Market," *IEEE Security and Privacy*, Vol. 3, No. 6, McLean, 2005, pp. 85-89.

[15] Katina Michael and Luke McCathie, "The Pros and Cons of RFID in Supply Chain Management," *Proceedings of the International Conference on Mobile Business*, Sydney, 2005, pp. 623-629.

[16] Melanie R.Rieback, Bruno Crispo and Andrew S. Tanenbaum, "The Evolution of RFID Security," *IEEE Pervasive Computing,* Vol. 5, No. 1, 2006, pp. 62-69.

