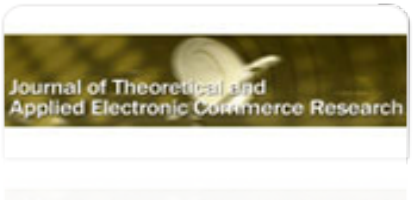

Journal of Theoretical and Applied Electronic Commerce Research

E-ISSN: 0718-1876

ncerpa@utalca.cl

Universidad de Talca

Chile

Ou Yang, Chih-Cheng; Prabhu, B.S.; Qu, Charlie; Chu, Chi-Cheng; Gadh, Rajit

Read / Write Performance for low memory passive HF RFID tag-reader system

Journal of Theoretical and Applied Electronic Commerce Research, vol. 4, núm. 3, diciembre, 2009, pp. 1-16

Universidad de Talca

Curicó, Chile

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 4 / ISSUE 3 / DECEMBER 2009 / 1-16

This paper is available online at
www.jtaer.com

Read / Write Performance for low memory passive HF RFID tag-reader system

Chih-Cheng Ou Yang[1], B.S. Prabhu[2], Charlie Qu[3], Chi-Cheng Chu[4], and Rajit Gadh[5]

University of California, Los Angeles, Wireless Internet for the Mobile Enterprise Consortium (WINMEC), UCLA RFID LAB
[1] ccouyang@winmec.ucla.edu, [2] bsp@winmec.ucla.edu, [3] charlie@winmec.ucla.edu, [4] cchu@winmec.ucla.edu, [5] rgadh@winmec.ucla.edu

Received 17 January 2009; received in revised form 4 May 2009; accepted 5 July 2009

Abstract

Certain applications of passive radio frequency identification (RFID), such as those in healthcare where the patient's name, identification or medical record must be stored, require data within a tag to be encrypted. Encrypted data within an RFID tag has the potential to affect the accuracy or time to read/write the data by the reader. The current research measures and analyzes the effects of encryption, distance of read and delay time between two read/write cycles on the accuracy of the read or write function in an RFID infrastructure. The research also measures and evaluates the time to read/write (R/W) data that is encrypted and compares this encrypted data with unencrypted data.

The data encryption standard (DES) encryption method is used in this research due to the limitation of the tag. A multi-functional interface has been developed for the user to test the performance using a High Frequency RFID reader. The measurements were repeated 1000 times for each R/W test.

The performance of R/W accuracy is not affected in any meaningful way by encryption even though there is an increase in memory requirement from 88 bytes to 128 bytes. The effect of R/W distance shows that the performance decreases with increase in the distance between the reader and the tag.

By inserting a small amount of delay time between different cycles, we can get a significant increase up to 100% accuracy for read function. However, the write accuracy is not affected as significantly as the read accuracy.

The effect of the encryption on the time to write the data on the tag shows that encrypted data group takes 70 ~ 120 milliseconds for the transmission more than the unencrypted data group.

We conclude that while the encryption does not have a significant impact on the accuracy of R/W, the distance and cycle delay does. Also, the encrypted data takes longer to write to the tag.

Key words: RFID, Healthcare, DES Encryption Method, Accuracy, Hashing Algorithm

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 4 / ISSUE 3 / DECEMBER 2009 / 1-16

This paper is available online at
www.jtaer.com

1 Introduction

Currently, the unencrypted data transfer between the RFID reader and the tag is typical of most RFID transmission protocols. However, increasing security demands from industries such as healthcare or homeland security are starting to change this. RFID technology in various applications such as supply chain management, medical specimen tracking for healthcare, border security, library system, and smart shelf, etc., need security for authorized access , [1], [4], [7], [12] – [13], [15], [20], [23], [30], [41] – [42]. Without security protection of transmitted RFID data, inclusion of personal privacy information, confidential information and non-public information, in the transmitted data may not be allowed by the enterprise. Threats of RFID system are eavesdrops, relay attacks, unauthorized tag reads, cloning threats, location tracking, and denial of service from back-end server threats [14], [17], [28] – [29]. Encrypting data that require privacy is therefore essential.

In this research, various authentication and encryption methods for an RFID system have been discussed, presented and analyzed.

Two authentication methods are commonly used. The first method for authentication is to use a central database to authenticate readers and tags [8], [19], [21], [28]. The second method, which has been presented by Tan *et al.,* introduces a new server-less authentication protocol which results in having a simpler infrastructure [34]. However, both methods need persistent connection to the database server or a persistently authenticated third party, limiting when and where it can be used.

While there are a significant number of encryption methods, the two most common and relevant ones have been compared in this research. One encryption method is a recently developed, lightweight method that is called “SASI” [5]. SASI uses only bit-wise operation, such as OR, AND, XOR, etc. to encrypt tag data. While this new approach was originally supposed to have the ability to disallow the tag to be tracked, other researchers have claimed that they have been able to track the tag [22]. This shows the dilemma of securing passive devices/tags.

A second method involves a separate encryption circuit on the RFID tag itself [16]. Instead of a software method, a hardware method can reduce workload of the software protocol thereby making it faster. However, increasing complexity of tag design results in an increased cost of each tag.

RFID in healthcare has recently had significant growth. Privacy, confidentiality and security requirements on confidential information such as patient personal identity or medical conditions are mandated by the law. For example, HIPAA (Health Insurance Portability and Accountability Act of 1996) mandates certain security and privacy of patient data by the healthcare provider (Site 1). Therefore, if patient information is placed within a tag, it must be completely secured and protected. RFID systems can be used in hospitals for patient identification and specimen identification [17], [29]. An RFID wristband is used to identify the patient and also for storing patients’ conditions such as emergency information to simplify the job of the nursing staffs when they are trying to identify a patient and provide proper medical treatment.

Not only does such a system have the potential to alleviate the nursing staff’s workload, but it also decreases the chance of medical errors. Even so, if the information in the wristband is not secure, the data could be furtively stolen or modified wirelessly which could result in serious consequences. Data without encryption could be modified in the tag by replacing the original data via a handheld RFID reader that is operating on the same frequency and protocol.

One way to prevent patient data theft and modification within a tag is to not store any patient information in the tag, but, instead, to only have a tag ID which is a meaningless number to any non-authorized user. To map this tag ID to the patient record, a hacker would need to have access to the back-end database server, which is typically secured, making it difficult if not impossible to steal patient information [43]. However one major disadvantage of this model is that it needs a persistent internet connection between the RFID reader and the back-end database server, which may not be possible in some situations, such as when a patient is not in the hospital. Also, in several hospitals worldwide, Wi-Fi is still not allowed due to its affect on medical equipment within the premises [24].So, for a complete system, the ability to function in a non-connected modality becomes essential.

Encryption of data typically increases data size, and to that effect, two hypotheses have been made:

1. Accuracy of data transmission will be affected. The larger data size will have a higher probability of not completing the transaction in real-world environments, and therefore, accuracy of data transmission on a statistical basis will be impacted.

2. Time to read/write during transmission would be affected. This is also due to the larger size of the data.

In this paper, a symmetric encryption method, DES (Data Encryption Standard), will be used to encrypt unencrypted data, and a MD5 hashing algorithm will be used to verify data accuracy [10]. Different R/W parameters in high frequency passive RFID systems, such as read range, delay time between R/W cycles, time to R/W and accuracy,

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 4 / ISSUE 3 / DECEMBER 2009 / 1-16

This paper is available online at
www.jtaer.com

will be discussed and compared. The research will also describe methods of retransmission and R/W delays so as to achieve 100% accuracy in the R/W function.

2 Literature Review

RFID performance tests of read range, orientation sensitivity and performance variance of same model tags, etc, have already been done [3], [6], [26]. Ramakrishnan verified the performance of EPC-compliant passive ultra high frequency (UHF) tags in reference to different aspects, including measuring maximum distance, read rate, orientation sensitivity, variance in tag performance, read rate in isolation, etc [26]. In this paper, Ramakrishnan concluded that these UHF tags have a maximum read range of 18 feet, three regions operation of different read range, 6 db or even more difference of tags in the same tag model, etc. Arror et al., identified the performance of read distance, near-metal read distance, near-water read distance, frequency-dependent read distance, etc [3]. Another performance test of UHF RFID tags studied the effect of tag orientation and package content shows that only 25% tags are readable with water-filled packaging and 80.6% tags are readable with rice-filled package. The tag orientation performance test shows tags facing outwards and towards the reader antenna have the highest read rate [6].

An RFID system has been proposed and utilized in healthcare for years [18], [39] - [40]. Wang *et al*., demonstrate an actual RFID system applied in a hospital in Taiwan [39]. The demonstration in the hospital is a location-based Medicare service (LBMS) which provides the location of patients, staff and essential equipment. Drug safety of inpatient nursing healthcare is another application of RFID in healthcare [40]. RFID can help track patient information accurately as well as help nurses to provide correct medicine with fewer mistakes. A survey of consumer sentiments towards RFID healthcare technology has been done [18]. In the survey, the public shows interest in utilizing RFID in healthcare for emergency purpose; however, people worry about the privacy issue of having personal information stored in an RFID tag. Therefore, privacy protection and security problems are two of the main concerns before broadly applying RFID in the healthcare industry.

Authentication and data encryption are two important methods for RFID security. There are two common types of the authentication method. The first type is using a central database to authenticate tags [8], [19], [21], [28]. Dimitriou proposed a simple protocol for reader and tag authentication to the database, and this lightweight protocol can prevent cloning or privacy attacks [8]. Lee *et al*., proposed an authentication protocol, Low-Cost RFID Authentication Protocol (LCAP), which uses two one-way hash operations to achieve efficient authentication for a low cost RFID system [19]. The LCAP protocol can prevent leakage of information by allowing a tag to emit information only after authentication by a backend database. The second common authentication method is to use mutual authentication between readers and tags. The second technique does not need a persistent connection to the central database, but instead, it needs to authenticate to a trusted (third) party [34].

Many encryption methods have been presented as being applicable to RFID systems. One of the latest encryption methods for a low-cost RFID system is called SASI (Strong Authentication and Strong Integrity). The SASI encryption method only uses bit-wise operation, such as XOR, OR, AND, to encrypt the data [5]. However, Phan announced that SASI cannot block tracking, one of the original SASI design objectives [22].

Tag circuits can also be designed to encrypt RFID data by adding redundant bits and adaptive frequency rates in the transponder of RFID tag [16]. Such circuit design can reduce the workload of data transmission of RFID system. However, the extra encryption circuit increases the complexity of RFID circuit designs and the overall cost of the tag.

3 Materials

3.1 RFID Reader Module

The RFID reader module used in this research is a Texas Instruments S6500 Long Range High Frequency (operates around 13.56 MHz) Reader Module. The module's part number is RI-STU-650A -- ISO 15693 which is compliant with a relay output and an asynchronous interface which can be configured as RS232 [35]. ISO 15693 is a standard for a vicinity card, which regulates the range up to 1 meter. The module operates at high frequency and is consistent with the tags used in this experiment.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 4 / ISSUE 3 / DECEMBER 2009 / 1-16

This paper is available online at
www.jtaer.com

Figure 1: RFID Reader Module

Figure 2: S6500 Long Range Reader Module

3.2 RFID Reader Antenna

The reader antenna which is connected to the reader module is Texas Instruments Series 6000 Gate Antenna Part Number: RI-ANT-T01A -- Single-loop antenna with transmitting frequency of 13.56 MHz and an output impedance of 50 Ohm [36].

Figure 3: TI Series 6000 Gate Antenna [37]

3.3 RFID Tag

The tags used in this experiment are Zebra's RFID wristbands RFID Z-Band® 4000, Size: 1" x 11“, Memory Size: 128 Bytes [27]. These tags are commonly used in the healthcare field to identify patient information.

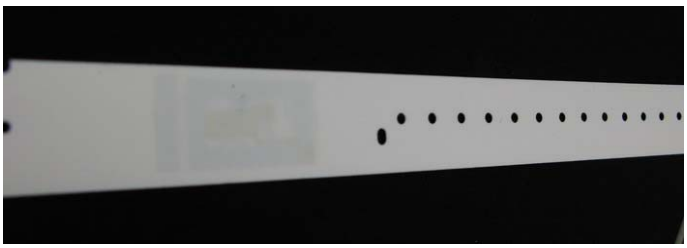

Figure 4: Zebra RFID Tag

Figure 5: Zebra RFID Tag Circuit

3.4 Programming Software:

Microsoft Visual Studio 2005 C# has been used as the development framework because the WinRFID middleware is based on this platform [24], [31] – [33].

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 4 / ISSUE 3 / DECEMBER 2009 / 1-16

This paper is available online at
www.jtaer.com

4 Encryption Method

4.1 Symmetric Encryption Method

The symmetric encryption method, DES, has been used to encrypt and decrypt the data for the tests. However, the Rijndael, Advanced Encryption Standard (AES), is also implemented in the system. The theory behind the symmetric encryption method is that the administrator and the clients both have the same secret key to encrypt and decrypt the confidential data. The most common way to encrypt the data is called Cipher Block Chaining (CBC), which operates as follow [9]:

1. Break the unencrypted data into blocks of same size as the input for the cipher function.
2. Process the first message block.
3. Use XOR of the message block with the “seed” data to create a combined data block.
4. Encrypt the result to produce the first block of cipher text.
5. Process remaining message blocks in turn.
6. XOR the plaintext block with most recently created cipher text block to create a combined data block.
7. Encrypt the combined data block and append the result to the cipher text.

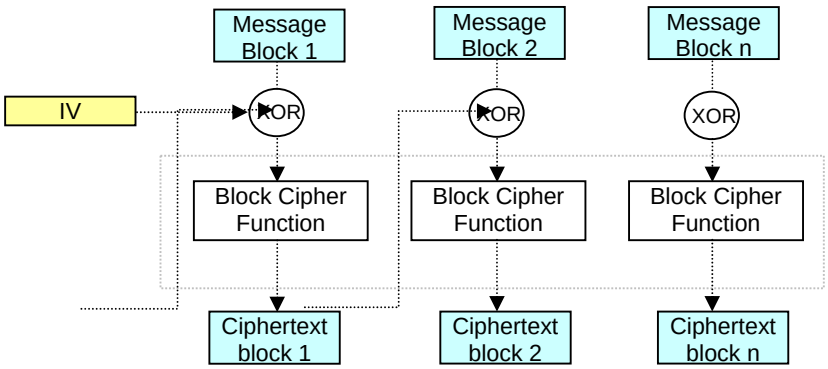

Figure 6: CBC mode [9]

The program allows for the user to choose whether or not to generate a static initialization vector (IV) and DES key. IV and DES key are used as the elements to encrypt the confidential data.

The differences between DES and AES are the key length and the block size. The comparison of these two methods is shown in Table 1, and the result of the data size change by the two encryption methods is shown in Table 2.

Table 1: Comparison between DES and Rijndael (AES)

Name	Block Size	Key Length
DES	64	56
Rijndael(AES)	128, 192,256	128, 192,256

Table 2: Comparison between two encryption

	Unencrypted Length (Bytes)	Encrypted Length (Bytes)
DES	0~7	12
	8~15	24
	32~39	56
	88~95	128
AES	0~15	24
	16~31	44
	32~47	64
	80~95	128

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 4 / ISSUE 3 / DECEMBER 2009 / 1-16

This paper is available online at
www.jtaer.com

4.2 Asymmetric Encryption Method

An asymmetric encryption function is also embedded in our encryption program. It is known that asymmetric encryption methods provide higher security than symmetric encryption methods. If the unencrypted data length is 88 bytes, the DES symmetric encryption method will generate a 128 bytes encrypted string and the asymmetric encryption method will generate a 172 bytes encrypted string with this program. A longer encrypted text string has higher security but a decreased efficiency and an increased work load.

Any asymmetric encryption method uses a public key to encrypt the confidential message. Then it uses a private key to decrypt back to the original message. The public key is broadcasted to clients who want to encrypt the confidential message, and the private key is only owned by the administrator to decrypt messages. The public key is only used to encrypt messages, and the private key is only used to decrypt the encrypted messages. Public keys and private keys are generated by two random large prime numbers, and the keys require a very powerful computer to have their values reverse engineered.

In our experiment, the sample tags are Zebra's RFID wristbands RFID Z-Band® 4000. Because the memory of this particular tag is 128 bytes, we do not use asymmetric encryption method in our experiment. Even so, the function is embedded in the program to enhance the flexibility of the program for future use. Future tests with larger tags will allow the use of this function for comparison purposes.

4.3 Hashing Algorithm

A hashing algorithm (MD5) is used to determine the data accuracy in our research. It is a common verification code used for interaction between two data streams. The theory of the hashing algorithm is to cut the streaming data into several data blocks. Subsequently, a seed value is used, generated by .NET, to input into the hash function with the first data block to generate the first hash code. After that, the first hash code is put into the hash function with the second data block to create the second hash code, and subsequently, the same process of hashing data blocks with hash code is repeated until the last message data block is processed. With the MD5 algorithm, streamed data is cut into blocks of 512 bit, and the hash code size is 128 bits [10].

The MD5 algorithm is used to determine if the data is modified during transmission, which works as follows. First, the program uses the hashing algorithm to generate a hashing code of data and keeps it in memory. Second, the program generates another hashing code of the data received from the tag. Third, these two hashing codes are compared to determine if the data has been modified.

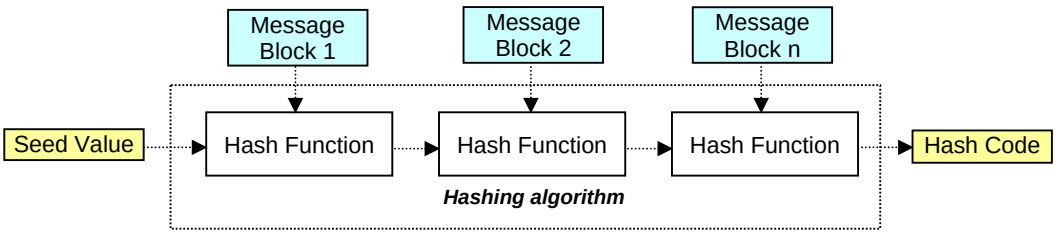

Figure 7: Hashing flow chart [11]

5 Testing Program and Designed Interface

The functions of our program are to encrypt data with assigned encryption methods (e.g. DES, AES or asymmetric), write data to the tag, read data from the RFID tag, decrypt data, automatically measure the accuracy and R/W time in assigned test cycles and generate a test report. Each function and interface will be explained below.

5.1 Interface

The Graphical User Interface of the program is designed for the user to manipulate and set test the parameters of multiple functions, including reading tag ID, encrypting and decrypting data with different encryption methods, writing the data into the tag memory, reading the data from the tag memory, clearing the tag memory, measuring the R/W time, testing sequentially and creating test record files. The following parameters and functions are set by the user:

1. Encryption methods
2. Key values (like encryption key)
3. Number of test cycles

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 4 / ISSUE 3 / DECEMBER 2009 / 1-16

This paper is available online at www.jtaer.com

4. Enabling delay time between cycles

5. Enabling 100% accuracy of write tag

6. Enabling the encryption function

The designed interface is shown in Figure 8.

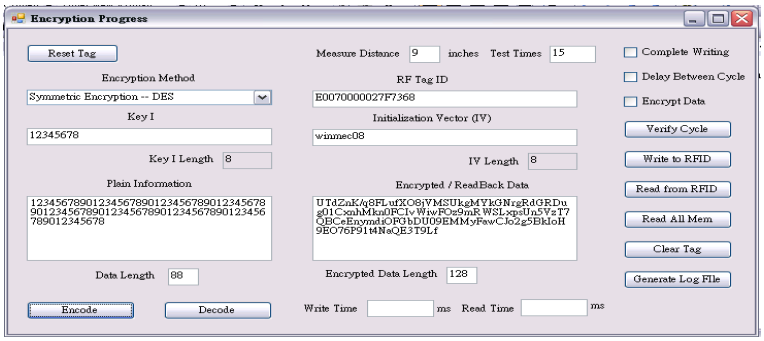

Figure 8: The designed interface and demonstration of verifying a cycle

5.2 Write and Verify Algorithm

The write algorithm contains the following steps:

1. Before transmission of the original data can be sent to the tag, the program first generates the hash code of this data and stores it in its memory.

2. The program writes the original data to the tag after splitting it into blocks of 4 bytes each.

3. If the reader returns a success flag for the write operation, then the program requests the reader to get the actual tag data.

4. The program generates the tag data's hash code and compares it with the original data's hash code to determine if two sets of data match. If the two hash codes match, the write cycle is deemed as a success.

Comparison of the hash-codes allows detection of errors due to a variety of reasons including errors in transmission or reception modes (due to air interface and noise issues), errors due to defective tags, or errors due to problems in readers.

While adding the read step after the write step allows a higher degree of accuracy in the write operation, it is still limited by the accuracy of the read step, and this limitation can not be eliminated in our approach. The logic flow chart of the writing process is shown in Figure 9.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 4 / ISSUE 3 / DECEMBER 2009 / 1-16

This paper is available online at
www.jtaer.com

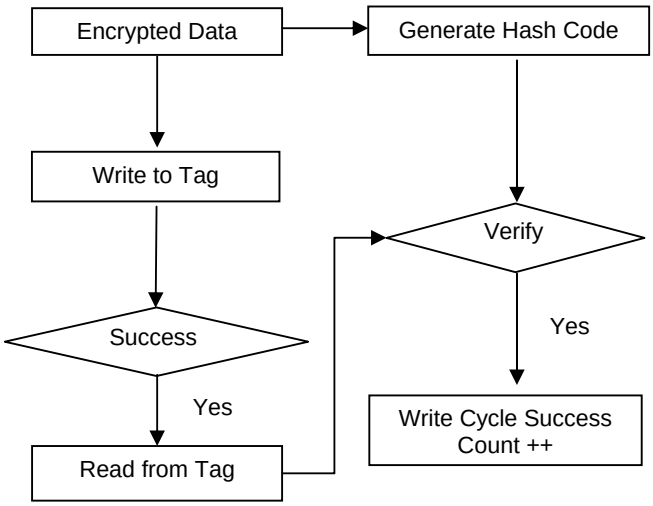

Figure 9: Writing process flow chart

5.3 Read and Verify Algorithm

The read step and its verification have the following steps:

1. The program reads the data from the tag.
2. It compares the hash code of the tag's data and the hash code generated by the original data.

The read process flow chart is shown in Figure 10:

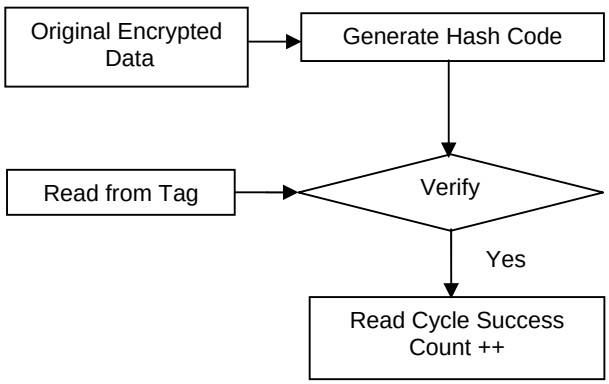

Figure 10: Reading process flow chart

5.4 Statistical Performance for the Verification Function

The goal of the statistical performance in the verification function is to study how the RFID system would perform for an average case if it were to be scaled up for enterprise use. Our program measures the average writing time, the average reading time, the write accuracy and the read accuracy. Before starting the test, the interface requires the user to set test parameters such as distance, test times, encryption method, encryption keys, enabling 100% write success function to tag function and enabling delay time between cycles. General information and test results are generated as a text file.

5.5 Testing Report

The test report is created as a text file automatically after completion of the test. The file name corresponding to a test report is designed to for incorporation within an RFID middleware framework (so as to be able to index it in a database such as that for WinRFID [24]). The file name includes tag ID, measurement distance, encryption method, unencrypted data bytes, encrypted data bytes and test times. An example of this as follows: E0070000027F7368-2-0-88-128-100.txt, where E0070000027F7368 is the tag ID, 2 is the measuring distance, 0 represents using DES

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 4 / ISSUE 3 / DECEMBER 2009 / 1-16

This paper is available online at
www.jtaer.com

symmetric encryption method, 88 is the unencrypted bytes, 128 is encrypted data length and 1000 is the test times. The test report contains the following:

1. General information:
    - Reader Model: The reader TiS6500 is used.
    - Standard: The standard ISO15693 is used.
    - Tag Id: Unique tag id for each RFID tag.
    - Test Distance (inch): Test distance from the reader to the tag shown in inches.
2. Encryption Method Information:
    - Encryption Method: Represents which encryption method is using in the test. 0 represents DES symmetric encryption method. 1 represents AES symmetric encryption method. 2 represents asymmetric encryption method.
    - Key: The key which was set by user.
    - Key Size (Byte): The length of the key.
    - Initialization Vector: Initial vector set by user.
    - IV Size (Byte): The length of initialization vector.
    - Plain Data: Unencrypted data.
    - Plain Data Bytes: The length of the unencrypted data.
    - Encrypted Data Bytes: The length of the encrypted data.
    - Hash Code: Hash code of the encrypted data which was generated for transmission verification.
3. Test Result Information:
    - Test Times: Number of tests.
    - Average Success Write Time (ms): Average successful write time of test shown in milliseconds.
    - Average Read Time (ms): Average successful read time of the test shown in milliseconds.
    - Write Accuracy Rate: The accuracy rate of the writes data in 1000 times.
    - Read Accuracy Rate: The accuracy rate of the reads data in 1000 times.
    - Write Failed Times: Represents number of times the tag failed to write.
    - Read Failed Times: Represents number of times the tag failed to read.

6 Experiment Design and Results

The goal of this experiment (using the program from section 4) is to measure the following:

1. Write accuracy
2. Read accuracy
3. Write time
4. Read time

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 4 / ISSUE 3 / DECEMBER 2009 / 1-16

This paper is available online at
www.jtaer.com

The variables which are the parameters in this experiment are as follows:

1. Whether or not to use an encryption function.

2. Whether or not to use a delay time function.

3. Whether or not to use a 100% write success function. This function is designed to make sure all tags are written successfully by resending data when the write process fails. However, the function should only be used within a capable range of reader to prevent infinite transmissions.

4. Distance between reader and tag. The read distance in this experiment varies from 1 inch to 12 inches since the R/W accuracy drops to zero above 12 inches.

By using different variables, the experiment is separated into two major experiment groups: the unencrypted data group and the encrypted data group. Each major group has four subgroups, and each subgroup will be tested 1000 cycles. Each cycle is defined as a read and a write from each tag once. The settings of each parameter of the four subgroups are as follows:

1. Disable 100% write success function and disable delay function in each cycle (called group NG_ND)

2. Enable 100% write success function and disable delay function in each cycle (called group G_ND)

3. Disable 100% write success function and enable delay function in each cycle (called group NG_D

4. Enable 100% write success function and enable delay function in each cycle (called group G_D)

The following groups are compared:

1. Subgroups of unencrypted data group(with 88 bytes data)

2. Subgroups of encrypted data group performance (with 128 bytes data)

3. Comparison the performance between encrypted data group and unencrypted data group

In the encrypted data group experiment, since the encryption time is less than 1 millisecond, the additional time is negligible compared to the transmission time. Therefore, in the field of RFID for low-memory tags, the effect of encryption computing time on the performance can be neglected.

6.1 Unencrypted Data Group

In the test group of unencrypted data, delay time between each cycle and 100% write success function affects the result significantly. Comparing the NG_ND group to the G_ND group, the write time of the G_ND group is 30 ~ 90 ms greater than the NG_ND group. Comparing the NG_D group to the G_D group, the write time of G_D is 8 ~ 64 ms greater than the NG_D group. The amount of variation depends upon how many writes fail, since the program will re-write to the tag for in order to gain 100% accuracy, which results in the large difference between the writing times. The failed write time is shorter than the successful write time. Comparing the differences between G_D⇔G_ND and NG_D⇔NG_ND, the trends are very similar. Therefore, the delay time function does not affect write time, but the 100% write success function does affect write time. The comparison chart is shown in Figure 11.

In the read time comparison, most of the distance tests show similar times. However, at a distance of 10 inches, NG_ND takes a longer time to read. For a distance of 6 inches, the G_D group requires a longer read time. The two peak time value discrepancies are probably due to errors in the equipment. However, the trends of the four groups are similar. The comparison charts of read time are shown in Figure 12.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 4 / ISSUE 3 / DECEMBER 2009 / 1-16

This paper is available online at
www.jtaer.com

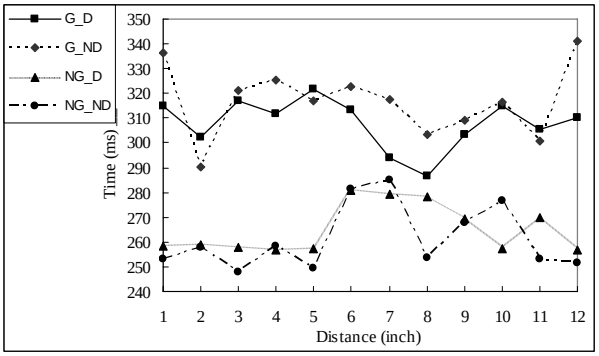

Figure 11: Write time comparison of unencrypted data group

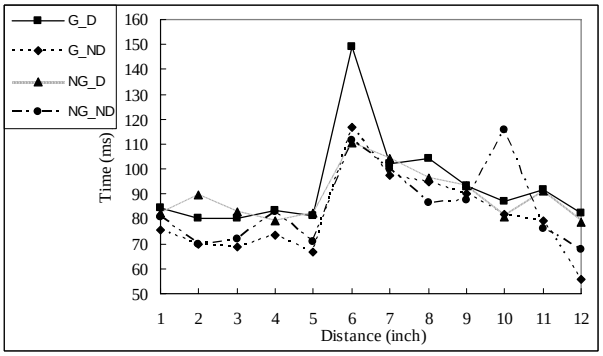

Figure 12: Read time comparison of unencrypted data group

Comparing write accuracy between NG_D and NG_ND, the difference ranges from 1% to 7% with very similar trends. The highest write accuracy of NG_D can reach 94% at a distance of 6 ~ 7 inches, and the lowest write accuracy is 73% at a distance of 12 inches. The highest write accuracy of NG_ND can reach 93% at distance of 6 inches, and the lowest write accuracy is 76% at a distance of 12 inches. Based on the above information and the comparison chart (Figure 13), it can be concluded that the delay function does not improve write accuracy.

Comparing read accuracy, the NG_D and G_D groups reach 100% read accuracy due to the delay function. In the NG_ND and G_ND groups, the two groups have similar trends. Read accuracy of NG_ND is from 82% ~ 98%, depending on the measuring distance. In G_ND group, the read accuracy is from 72% ~ 99%, depending on the measuring distance. However, the lowest read accuracy of two groups both occur at a measuring distance of 12 inches, and the best read accuracy is at, approximately, 6 ~ 11 inches. By the comparing the data, the 100% write success function does not affect read accuracy significantly. The comparison chart is shown in Figure 14.

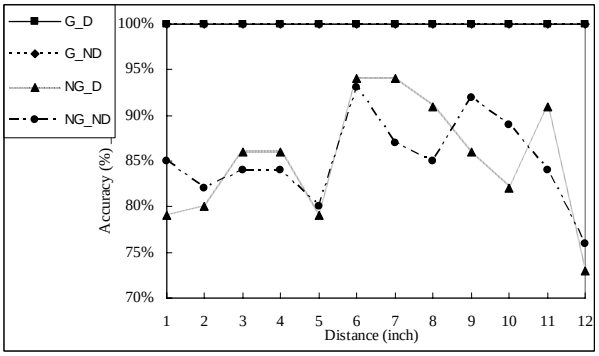

Figure 13: Write accuracy comparison of unencrypted data group

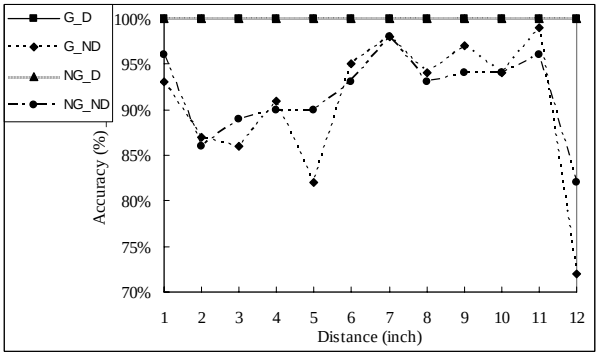

Figure 14: Read accuracy comparison of unencrypted data group

6.2 Encrypted Data Group

The second part of the test studies the data group encrypted by the symmetric method of DES. When encrypting the 88 bytes of unencrypted data, the data size increases to 128 bytes in order to fit the maximum memory capacity of Zebra tag.

Comparing the NG_ND and G_ND groups, the write time difference is small and the trend difference is similar to that of the unencrypted data group. The write time of G_ND in the encrypted data group is 25 (1 inch) ~ 118 (9 inches) ms more than the NG_ND group, and the difference in level is related to the measuring distance. In the comparison of NG_D and G_D, the write time of G_D has 14 (1 inch) ~ 95 (12 inches) ms more than NG_D. The write time trend of 100% write success groups, G_ND and G_D, seems to increase with read distance. The comparison chart is shown in Figure 15.

By comparing the read time? between delay groups and non-delay groups, delay groups take more time to read the data from the tag. The delay group, G_D, is 20 ms slower than G_ND at read distance of 7 inches, from 109 milliseconds to 89 milliseconds, and has similar read time at 3 and 9 inches. The difference between NG_ND and NG_D is not as large as the differences in the 100% write success function groups. The non 100% write success

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 4 / ISSUE 3 / DECEMBER 2009 / 1-16

This paper is available online at www.jtaer.com

function group also has a saw tooth shaped distribution in the read time test. The comparison chart is shown in Figure 16.

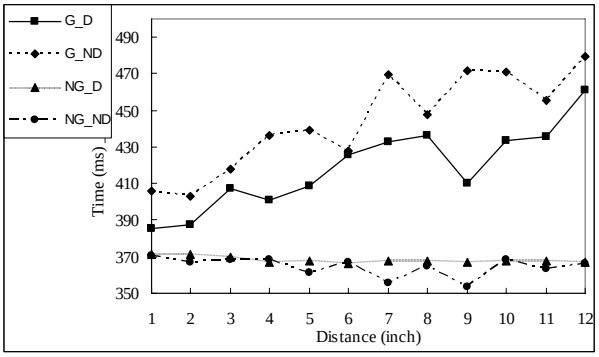

Figure 15: Write time comparison of encrypted data group

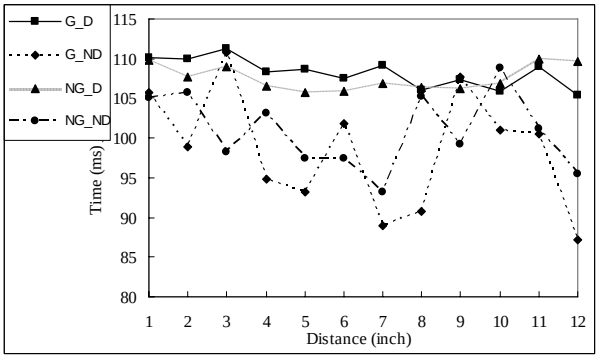

Figure 16: Read time comparison of encrypted data group

By comparing the write accuracy between NG_ND and NG_D, both of the write accuracies drop to their lowest levels at 9 inches, 68% and 74%, respectively. The best write accuracy only reaches ~ 92% at a read distance of 1 ~ 2 inches. Furthermore, the write accuracy trends of these two groups are similar. The write accuracy of both groups drop from a read distance of 1 inch to 9 inches and then bounce back at 10 inches, and therefore, this trend is different from the unencrypted data group. Other groups, G_ND and G_D, both reach 100% write accuracy by program help, using retransmission data method. The comparison chart is shown in Figure 17.

Comparing read accuracy between groups of G_ND and NG_ND, the read accuracy of G_ND is 82% (12 inches) ~ 99% (9 inches and the read accuracy rate of the group of NG_ND is 88% (7 inches) ~ 99% (8 inches). A disparity of the write accuracy result is that the two groups show good read accuracy around 8 ~ 9 inches. By adding delay time between cycles, NG_D and G_D groups reach 100% read accuracy at every distance. The comparison chart is shown in Figure 18.

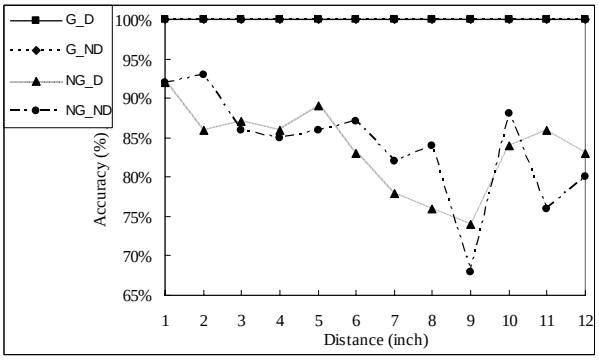

Figure 17: Write accuracy comparison of encrypted data group

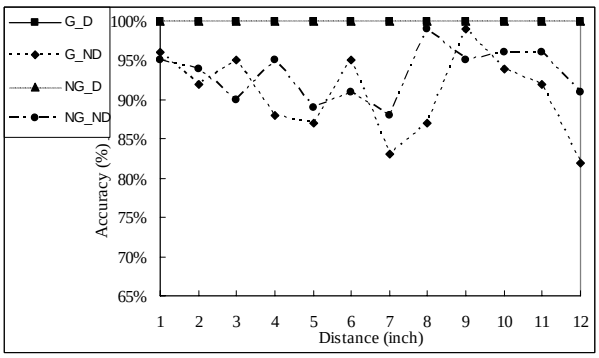

Figure 18: Read accuracy comparison of encrypted data group

6.3 Comparison between unencrypted data and encrypted data

Due to the longer data length of the encrypted data group, compared to the unencrypted data group, the write and read times are also longer. By comparing NG_ND of each group for R/W time difference, the write time of the encrypted data group takes 68 ms (12 inch) ~ 116 ms (10 inches) more than the unencrypted data. The read time of the encrypted data group is 36 ms (2 inches) slower than the unencrypted data group. However, at 6, 7, 10 inches, the unencrypted data group unexpectedly takes longer to read than the encrypted data group. The unencrypted group takes up to 14 ms, at 6 inches, longer than the encrypted group. The comparison is shown in Figure 19 and Figure 20.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 4 / ISSUE 3 / DECEMBER 2009 / 1-16

This paper is available online at
www.jtaer.com

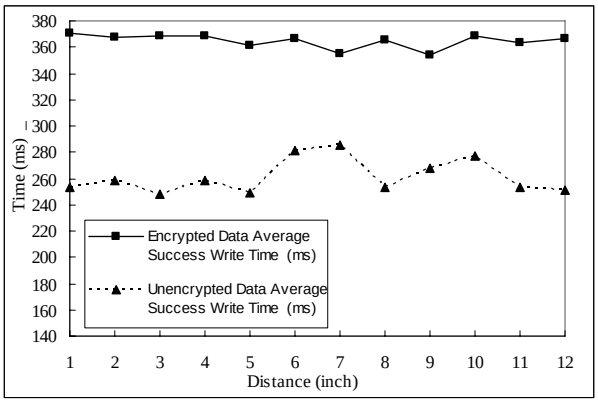

Figure 19: Write time comparison between encrypted data group and unencrypted data group

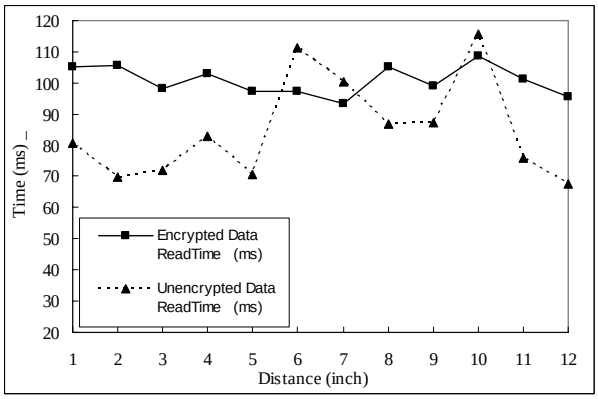

Figure 20: Read time comparison between encrypted data group and unencrypted data group

Focusing on the accuracy test of NG_ND of the two groups, the write accuracy of the encrypted data is better than the unencrypted data for read distance of 1 ~ 5 inches. The biggest difference between the two data groups is 11%, from 93% to 82%, at a read distance of 2 inches. From a distance of 6 ~ 11 inches, the unencrypted data group has better write accuracy than the encrypted data group, and the difference can go as high as 24%, from 92% to 68 %, at 9 inches. The write accuracy comparison chart is shown in Figure 21.

In the comparison of read accuracy, the biggest difference between the two groups is the unencrypted group having 10% higher accuracy than encrypted group, from 98% to 88%, at a read distance of 7 inches. However, by comparing the trends of the two groups, distinguishing the effect of larger data length is not possible, shown in Figure 22.

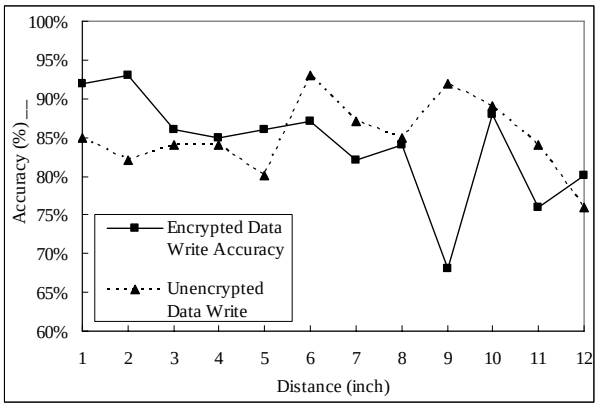

Figure 21: Write accuracy comparison between encrypted data group and unencrypted data group

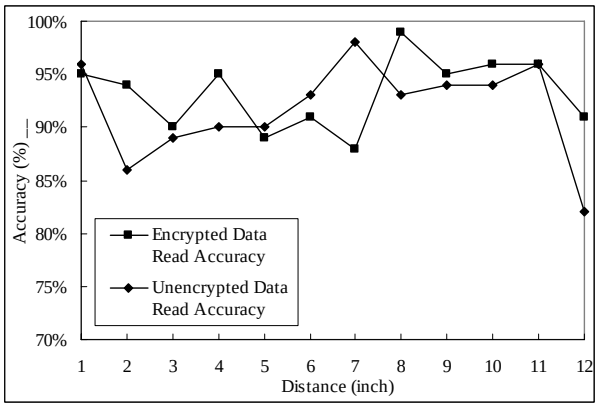

Figure 22: Read accuracy comparison between encrypted data group and unencrypted data group

7 Discussion

In these tests, the conclusion that can be made is that read accuracy and write accuracy are not significantly affected by encryption. However, the trend of the write accuracy is that it reduces as the distance increases. The data indicates that read accuracy does not drop with distance as significantly as does write accuracy. Nevertheless, at a distance of greater than 12 inches, read and write accuracy both drop dramatically to zero.

The delay time between cycles only affects read accuracy and does not show obvious affects on write accuracy. By adding the delay time, the results show that the reader is able to finish the previous reading instruction before starting the next one. This improvement in read accuracy is significantly beneficial when one is developing a middleware-based approach (such as WinRFID [24]) because the middleware can use this information to create policies that can ensure high quality of read that would otherwise be impossible if left to the reader itself.

In the write test, the program invokes the write capability of the reader, which in turn performs one write followed by one read. This makes the write command inherently different from the read command since it waits to get a confirmation (which is a read). Therefore, the delay time function does not have a significant impact on this test.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 4 / ISSUE 3 / DECEMBER 2009 / 1-16

This paper is available online at
www.jtaer.com

The encrypted data test group that was 128 bytes has 40 bytes more than its unencrypted counterparts – an increase of 45%. The encryption time is negligible (< 1ms.) compared to the increase in the transmission time of the larger data size. In our comparison, the encrypted data group takes 70 ~ 120 milliseconds more for the transmission than the unencrypted data group for the write function which is an increase of 24% ~ 49%. In the read time comparison tests, most encrypted data groups take longer to read than their unencrypted counterparts. However, the tests also show that the unencrypted data group takes longer than the encrypted data group for certain distances. The apparently inconsistent results are most likely due to instability of the RFID reader.

Encryption of RFID tag data is still important and necessary; nevertheless, encryption of tag data can cause longer read/write time. The test result shows the encrypted data takes 70 ~ 120 milliseconds for the writing transmission more than unencrypted data. Therefore, encryption of tag data is still potentially viable for commerce used because encryption of tag data can enhance security while only slightly increasing R/W time. The transmission time could be reduced if different hardware settings are used, such as choosing a different reader or tag. Security and privacy protection are two of the main issues to solve before RFID is broadly applied in healthcare, and this experiment shows that application of an encryption method in a RFID system to enhance security and privacy protection is still beneficial.

8 Conclusion

Certain applications of passive RFID, such as those in healthcare, where the patient's name, I.D. or medical records must be stored, require the data within a tag to be encrypted. Encrypted data within an RFID tag has the potential to affect the accuracy or time to read/write the data by the reader. This study measured and analyzed the effect of encryption, distance of read and delay time between two read/write cycles on the accuracy of the read or write function in an RFID infrastructure. The research also measured and evaluated the time to read/write encrypted data and compared that with the time to read/write unencrypted data.

According to the test results, the performance of write and read cycles is a function of the distance between the reader and the tag and the delay time. However, encryption does not affect read accuracy and write accuracy significantly, even though the data is larger. Nevertheless, the encryption function does affect R/W time due to having more data. In our research, read accuracy may be improved to 100% by inserting a certain amount of delay time between cycles.

Write accuracy of 100% can be achieved by our program; however, the write time will increase from 10ms to 100ms. This range of 10 to 100 ms is dependent upon the measuring distance. If encryption is required, then, in general, longer read and write time is necessary. Nevertheless, in the encryption data group experiment, since the encryption time is less than 1 ms, it is negligible compared to the transmission time. Therefore, in the field of RFID for low-memory tags, the effect of encryption computing time on the performance can be neglected.

Using asymmetric encryption, one can use larger memory tags (since low memory tags can only incorporate the data increase allowed by symmetric encryption). Future research could be performed to completely characterize relationships between the use of asymmetric/symmetric encryption and tag type (low/high memory, passive/active, HF/UHF, etc). The current research establishes a baseline for the development of this entire genre of research.

According to the results of the experiment, encryption of RFID tag data increases the transmission time and does not affect the accuracy of read/write. However, the encryption method is still potentially viable for the healthcare industry. Privacy protection and security issues are two of the main concerns of broadly applying a RFID system to healthcare, and encryption can solve most of the problems while still keeping the efficiency of the RFID system. Therefore, an appropriate encryption method and a related RFID infrastructure need to be developed in order to apply the system in a healthcare setting, where it can be used to prevent medical mistakes and reduce the costs of labor.

Another area of future research is the development of an optimization scheme which would automatically select the best encryption method given a particular set of RFID requirements for a given application and industry. For example, if homeland security department is using RFID-enabled passports with UHF passive tags containing minimum of 64Kb of data [25], it would be desirable to find the most optimum encryption method that is also optimal in read reliability and read distance. Such requirements present natural possibilities for extending the current research.

Acknowledgments

We would like to gratefully acknowledge the support and the help of the WINMEC (Wireless Internet for Mobile Enterprise Consortium) center, UCLA RFID Lab, Arunabh Chattopadhyay, Kirby Chiang, Siddartha Mal and other students, researchers associated with these institutions.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 4 / ISSUE 3 / DECEMBER 2009 / 1-16

This paper is available online at
www.jtaer.com

Websites List

Site 1: Overview HIPAA - General Information, Centers for Medicare & Medicaid Services
http://www.cms.hhs.gov/hipaaGenInfo/

References

[1] J. Al-Kassab, and W.-C. Rumsch, Challenges for RFID cross-industry standardization in the light of diverging industry requirements, IEEE systems journal, vol 2, no. 2, pp. 170-177, June 2008.
[2] Apples for Health. (2002, November). Nursing shortage a crisis in US hospitals. [Online]. vol. 4, no. 23. Available: http://www.applesforhealth.com/HealthyFeatures/nscush4.html.
[3] S. R. Aroor, and D. D. Deavours, Evaluation of the state of passive UHF RFID: An experimental approach, IEEE System Journal, vol. 1, no. 2, pp. 168-176, december 2007.
[4] S. Bureau, B. S. Prabhu, and R. Gadh, Radio frequency identification: Beyond the myths. A case for health care, Academy of Management, Anaheim, California, 2008.
[5] H.-Y. Chien, SASI: A new ultralightweight RFID authentication protocol providing strong authentication and strong integrity, IEEE Transactions on Dependable and Secure Computing, vol. 4, no. 4, pp. 337-340, 2007.
[6] R. H. Clarke, D. Twede, J. R. Tazelaar, and K. K. Boyer, Radio frequency identification (RFID) performance:The effect of tag orientation and package contents, Packaging Technology and Science, vol. 19, no. 1, pp. 45-54, 2005.
[7] T. Coltman, R. Gadh, and K. Michael, RFID and supply chain management: Introduction to the special issue, Journal of Theoretical and Applied Electronic Commerce Research, vol. 3, no. 1, pp. iii-vi , 2008.
[8] T. Dimitriou, A lightweight RFID protocol to protect against traceability and cloning attacks, in SecureComm, 2005.
[9] A. Freeman, and A. Jones, Programming .NET Security, O'Reilly, 2003, pp. 341.
[10] A. Freeman, and A. Jones, Programming .NET Security, O'Reilly, 2003, pp. 310.
[11] A. Freeman, and A. Jones, Programming .NET Security, O'Reilly, 2003, pp. 307.
[12] R. Gadh. (2005, April) RFID: Moves beyond supply chain mandates. Computerworld Article. [Online]. Available: http://www.computerworld.com/mobiletopics/mobile/story/0,10801,100886,00.html?SKC=mobile-100886.
[13] R. Gadh, and B. S. Prabhu, Radio frequency identification of katrina hurricane victims, IEEE Signal Processing Magazine, pp. 182-184, 2006.
[14] S. L. Garfinkel, A. Juels, and R. Pappu, RFID privacy: an overview of problems and proposed solutions, IEEE Security and Privacy, vol. 3, no. 3, pp.34-43, 2005.
[15] J.-L. Hou, and C.-H. Huang, Quantitative performance evaluation of RFID applications in the supply chain of the printing industry, Industrial Management and Data System, vol. 106, no 1, pp. 96-120, 2006.
[16] M.-L. Hsia, and O. T.-C. Chen, Low-complexity encryption using redundant bits and adaptive frequency rates in RFID, IEEE Circuits and Systems, ISCAS 2007, IEEE International Symposium, pp. 1601-1604, May 2007.
[17] A. Juels, RFID security and privacy: A research survey, IEEE Selected Areas In Communicastions, vol. 24, no. 2, pp. 381-394, 2006.
[18] J. E. Katza, and R. E. Riceb, Public views of mobile medical devices and services: A US national survey of consumer sentiments towards RFID healthcare technology, International Journal of Medical Informatics, vol. 78, no. 2, pp. 104-114, February 2009.
[19] S.-M. Lee, Y. J. Hwang, D. H. Lee, and J. I. L. Lim, Efficient authentication for low-cost RFID systems, in ICCSA, 2005.
[20] Z. Li, R. Gadh, and B. S. Prabhu, applications of RFID technology and smart parts in manufacturing, in Proceedings of DETC04: ASME 2004 Design Engineering Technical Conferences and Computers and Information in Engineering Conference, 2004.
[21] M. Ohkubo, K. Suzuki, and S. Kinoshita, Cryptographic approach to privacy-friendly tags, in RFID Privacy Workshop, 2003.
[22] R. C.-W. Phan, Cryptanalysis of a new ultralightweight RFID authentication protocol—SASI, IEEE Transactions on Dependable and Secure Computing, vol. 6, no. 4, pp. 316-320, 2009.
[23] S. Prabhu, C. Qiu, B. Schmitt, C.-C. Chu, and R. Gadh, SpecimenTrak: an RFID system for tagging and tracking anatomical specimens, in The 25th Annual Scientific Session of the American Association of Clinical Anatomists, Toronto, 2008.
[24] B. S. Prabhu, X. Su, H. Ramamurthy, C.-C. Chu, and R. Gadh, WinRFID – A middleware for the enablement of radio frequency identification (RFID) based applications, in Mobile, Wireless, and Sensor Networks, Wiley-Interscience, 2006, pp. 313-336.
[25] P. Prince.(2005, October). United States Sets Date for E-Passports, RFID Journal. [Online]. Available: http://www.rfidjournal.com/article/view/1951/1/1.
[26] K. N. M. Ramakrishnan, Performance Benchmarks for Passive UHF RFID Tags, M.S. Thesis, College of Engineering, Guindy - Anna University, Chennai, India, 2003.
[27] Zebra. (2008, December) RFID Wristbands. [Online]. Available: http://www.zebra.com/id/zebra/na/en/index/products/supplies/rfid_supplies/rfid_wristbands.html.
[28] M. R. Rieback, B. Crispo, and A. S. Tanenbaum, The evolution of RFID security, IEEE Pervasive Computing, vol. 5, no. 1, pp. 62-69, 2006.

[29] P. Rotter, A framework for assessing RFID system security and privacy risks, IEEE Pervasive Computing, vol. 7, no. 2, pp. 70-77, 2008.
[30] P. Rotter, B. Daskala, and R. Compano, RFID implants: Opportunities and challenges for identifying people, IEEE Technology and Society Magazine, vol. 27, no. 2, pp. 24-32, 2008.
[31] X. Su, C.-C. Chu, B. S. Prabhu, and R. Gadh, On the identification device management and data capture via WinRFID1 Edge-Server, IEEE System Journal, vol. 1, no. 2, pp. 95-104, 2007.
[32] X. Su, C.-C. Chu, B. S. Prabhu, and R. Gadh, Service organization and discovery for facilitating RFID network manageability and usability via WinRFID middleware, in WTS 2008, Cal Poly Pomona, Pomona, California, 2008.
[33] X. Su, C.-C. Chu, B. S. Prabhu, and R. Gadh, On the utilization and integration of RFID data into enterprise information systems via WinRFID, in Proc. ASME 27th Comput. Inf. Eng. Conf. (CIE) , 2007.
[34] C. C. Tan, B. Sheng, and Q. Li, Secure and serverless RFID authentication and search protocols, IEEE Transactions on Wireless Communications. vol. 7, no. 4, pp. 1400-1407, 2008.
[35] Texas Instrument. (2008, December) S6500 Long Range Reader Module. [Online]. Available: http://www.ti.com/rfid/shtml/prod-readers-RI-STU-650A.shtml.
[36] Texas Instruments. (2008, December) RFID Series 6000 Gate Antenna. [Online]. Available: http://www.ti.com/rfid/shtml/prod-ant-RI-ANT-T01A.shtml.
[37] Texas Instruments. (2008, December) RFID Antenna. [Online]. Available: http://www.ti.com/rfid/graphics/productImages/ant-t01a.jpg.
[38] G. Tsudik, YA-TRAP: Yet another trivial RFID authentication protocol, in PerCom, 2006.
[39] S.-W. Wang, W.-H. Chen, C.-S. Ong, L. Liu, and Y.-W. Chuang, RFID application in hospitals: A case study on a demonstration RFID project in a Taiwan hospital, System Sciences, in HICSS '06. Proceedings of the 39th Annual Hawaii International Conference, vol. 8, pp. 184a-184a, 2006.
[40] F. Wu, F. Kuo, and L.-W. Liu, The application of RFID on drug safety of inpatient nursing healthcare, in the 7th international conference on Electronic commerce table of contents, vol. 113, 2005, pp. 85–92.
[41] Y. Xiao, X. Shen, B. Sun, and L. Cai, Security and privacy in RFID and applications in telemedicine, IEEE Communication Magazine, vol. 44, no. 4, pp. 64-72, April 2006.
[42] J. Yagi, E. Arai, and T. Arai, Parts and packets unification radio frequency identification (RFID) application for construction, Automation in Construction, vol. 14, no. 4, pp. 477-490, 2005.
[43] L. Zhang, H. Zhou, R. Long, and F. Yang, An improved approach to security and privacy of RFID application system, in IEEE Wireless Communications, Networking and Mobile Computing Conf., 2005, pp. 1195-1198.