RESEARCH SURVEY ON MIFARE WITH RFID TECHNOLOGY

S.SRINIVASAN
Assistant Professor, School of Computing,
SASTRA University, Kumbakonam-612001
Tamil Nadu, India
ramuluvasan@rediffmail.com

Dr. C. CHANDRASEKAR
Reader, Periyar University, Selam
Tamil Nadu, India
ccsekar@gmail.com

Abstract: ***A paper that discusses the evolving technology of MIFARE and its potential for replacing the existing RFID technology. Though RFID technology has several advantages there are several technical disadvantages of RFID. As RFID makes use of radio waves they are susceptible to interference and moreover memory is less and is devoid of security. Other problems that can arise include RFID reader collision and RFID tag collision. All of these problems can be solved by using MIFARE technology. MIFARE technology has a greater memory with an option of providing security. In contrast to RFID technology which has 1Mb of memory MIFARE uses 4Mb of memory and several security algorithms can be implemented. Here, we discuss how memory can be used and the security features that can be used in MIFARE technology.***

Keyword: *Memory storage, Security, authentication, MIFARE, RFID*

I. Introduction to RFID with MIFARE

RFID or Radio Frequency Identification is a technology that uses radio waves as a mode of communication to exchange data between the reader and the RFID tag. During the World War II it is used as an espionage tool, it underwent development to become an Identification tool. After significant improvements in micro technology, miniature RFID tags are used widely today in consumer markets to identify items. For example, a grocery store can uniquely identify every item and can give description from the RFID tags. RFIDs have found widespread use in today's world and are expected to be used in many domains including transportation, logistics, mobile transactions, and medicine and emergency services.

MIFARE tags also have the advantage of being read from quite a distance, unlike bar codes, which needs to be shown to the reader. Multiple MIFARE tags can also be read simultaneously thus allowing parallel processing. These characteristics can be used to prevent theft or shoplifting using an alarm that goes off once a specific RFID embedded product moves out of range. MIFAREs typically have two parts: an integrated circuit for processing and storing information and an antenna for sending and receiving signals.

Another source of resistance to the adoption of RFID by many organizations stems from, ongoing privacy concerns. One concern is that RFID tags can be scanned even after they exit the supply chain, and without anyone's knowledge. Anyone with an RFID scanner can conceivably access data encoded on an RFID tag.

In an increasingly fragmented, regulated, and uncertain world, MIFARE technology gives businesses, governments, and consumers a safe, private, and unobtrusive way to keep track of it all. Consumer's benefit from shorter lines at checkout counters, in hospitals, libraries, and gas stations because MIFARE fast tracks them to the front of the queue. The can also benefit from lower prices because of the efficiencies MIFARE brings to the supply chain. Business and institutions are turning to MIFARE technology as they comply with government product-tracking regulations, seeking to limit theft, reduce out-of-stock losses, strengthen brand loyalty, and make interaction with customers a more positive experience. A paper that discusses the evolving technology of MIFARE and its potential for replacing the existing RFID technology

The user in the MIFARE environment is initially required to show the MIFARE tag in front of the MIFARE reader. The MIFARE tag has an antenna that transmits data to the system that sends back a reply adhering to the ISO14443A standard. Since MIFARE handles multiple applications at the same time, the card needs to be selecting properly. The card will send an AT code which determines the type of card selected currently and the reader can then access the particular authenticated block from the card. The signal transmitted between the antenna and the reader is converted into digital format during communication.

MIFARE is a series of chips used in contactless smartcards and proximity cards and is owned by Philips Electronics. It works on the frequency 13.56MHZ and can operate up to 10mm in length. The data transfer rates are high at 106kbit/s. MIFARE is capable of both read/write and are similar to memory cards in operation. It is basically designed for public transmission like automatic entry in gates, personal identification, Asset Tracking, Manufacturing, Supply Chain Tracking etc. MIFARE technology is described under ISO 14443 Type A.

II . Challenges for RFID

While the number of RFID implementations continues to grow at a rapid pace, mass- market adoption of this technology is being hampered by:

- Privacy concerns in the form of clandestine tracking and inventorying of tagged items and security concerns related to authentication of tags and readers (Juels 2006). For individuals, the limited privacy protection in current RFID systems is the major concern, as the article by Zappone (2007) shows. For the corporate executive, the limited privacy protection in many of RFID systems in place today can leave the entire supply chain exposed to industrial espionage, while the security vulnerabilities can lead to counterfeiting and other acts of economic sabotage.

- The high costs of the tags and readers. Current projections are to have tags that cost about 5 US cents each in order to facilitate wider adoption of RFID for tagging individual items. It appears that the target of 5 US cents per tag (Sarma2001) is arbitrary, as our attempts to find an economic justification for this targethave failed and so costs may not be as a big a drawback on wider adoption as some might be claiming.

- The constrained electrical power supply for the mass-market components of the RFID systems; that is the tags. This is directly related to the first two issues above. Low cost tags are for the most part passive; they do not have an on-board power source, they derive their power from the signal sent by the interrogating reader. As a result they generally are, smaller in size, chip-less, easier to manufacture and to apply onto products and require no in-field maintenance. However, they have lower transmission ranges and are cryptographically-weak. Active tags have an on-board power source and, when appropriately configured,address all the weaknesses of their passive counterparts; however they have as weaknesses all the strengths of their passive counterparts.

III . MIFARE ISO 14443

ISO/IEC 14443 is a contact less technology with an operational range of up to about 4 inches (10 centimetres). This 13.56 MHz technology was originally designed for electronic ticketing and electronic cash. For these applications, short read ranges and fast transaction speeds are critical. The same market requirements led ISO/IEC 14443 to be adopted for transit, off-line purchase, and vending transactions. ISO/IEC 14443 products are now starting to move into the physical access control market. The transmission protocol specifies data block exchange and related mechanisms such as data block chaining, waiting time extension and multi-activation

ISO/IEC 14443 uses following terms for components:

- ✓ **PCD:** proximity coupling device (or reader)

- ✓ **PICC:** proximity integrated circuit card
- ✓

Key Features of ISO/IEC 14443

- Operating frequency: 13.56 MHz
- Operational range: Up to 4 inches (10 cm)
- Speed: The ISO standard specifies a speed of 106 Kbps. ISO/IEC 14443 technology (A or B) is now capable of 212 Kbps, 424 Kbps, and 848 Kbps, with higher speeds under discussion by the ISO committee.
- Storage memory available: 64 bytes - 64 Kbytes.
- Security:
    - ✓ Wired logic cards: Authentication mechanisms are available. The only solution for conditional access that is interoperable from multiple sources is the MIFARE encryption unit.
    - ✓ MCU cards: Security mechanisms available in contact smart cards are also available for both ISO/IEC 14443 Type A and Type B (e.g., hardware memory firewalls, sensors, tamper resistance features).
    - ✓ Crypto coprocessors, such as 3DES, AES, ECC and RSA, can be used.
    - ✓ The close proximity of the card to the reader helps limit unintended communication.
    - ✓ Interoperability: Supported through full definition of communication commands in ISO/IEC 14443, part 4.
    - ✓ Vendors: Many [1]

IV . MIFARE Architecture

The MIFARE 4K classic comprises of 4kbtes of EEPROM memory divided into 2 main areas. The first area is made up of 32 sectors of 4 blocks each and the other area consists of 8 sectors of 16 blocks, where each block is 16 bytes in size.

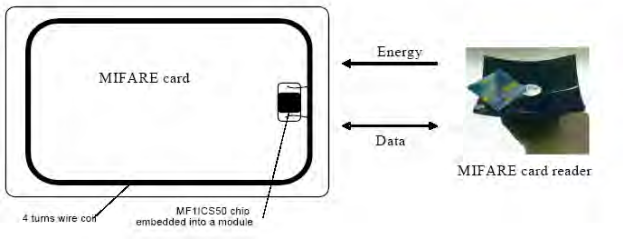

Fig 1. MIFARE Card Reader

In the 1 Kbytes EEPROM version it has 16 sectors, with the 1st sector reserved for *IC manufactured data* and the remaining 15 sectors used to handle 15 different applications. Each sector is separated by unique passwords thus ensuring data integrity between each application.

Standard / Memory	Mifare Standard 1k	Mifare Standard 4k
Name	MF1 S50	MF1 S70
EEPROM	1 Kbyte	4 Kbyte

Fig 2. Memory Standards

Anti-collision:

MIFARE is capable of preventing collisions. Since the memory has 15 sectors with each capable of handling a different application, during simultaneous access, the probability of collisions occurring are high. In order to resolve this conflict, an intelligent anti-collision system is present which allows the different cards to operate simultaneously. Anti-collision algorithms are embedded and are part of the technology. The algorithms have an anti-collision loop that allows the unique keys to maintain card information separately.

MIFARE to overcome RFID Security issues

RFID technology has a few security problems. For instance, when a user uses the RFID card for identification, the RFID reader will read the unique number to verify the user's identity. At the same time a relay attacker can also read the information without the user being aware of the relay attack. Since the retrieval of unique numbers takes only a few seconds and there need be no physical contact with the card, the attackers can easily create relay-attacking programs. The relay attacker can then impersonate as the legitimate user and use the identity for malicious purposes.

To resolve this conflict MIFARE uses a three-pass authentication according to the ISO9798-2. The MIFARE data are encrypted during transmission and is protected by a 48-bit key. It generates a random number based on the key and the data is encrypted using it. The encrypted data is then sent to the receiver, which needs to be decrypted first before the original data can be accessed.

The steps in the three-pass authentication include

1. The card reader reads the sector tailor field based on which the card generates a random number that is sent to the reader.
2. The reader then calculates a challenge and replies back with a secret key based on the random number as a response
3. In the third pass, the card solves the challenge and responds to the system. The system then compares its own challenge and verifies the identification.

V. Memory Organization

The Mifare card memory is organized as 8192 Bit EEPROM, which is split into 16 sectors with 4 blocks. One block consists of 16 bytes (1 Byte = 8 Bit). The Mifare card memory organization is as:

Manufacturer Code (Block 0 of Sector 0):

The first block of the memory is reserved for manufacturer data like 32 bit serial number. This is a read only block. It is named as "Block 0".

Data Block (Block 0 to 3 except "Block 0"):

Access conditions for the Data Blocks are defined in the Sector Trailers. According to these conditions data can be read, written, incremented, decremented, transferred or restored either with Key A, Key B or never.

Data blocks are:

(Blocks 1,2 / 4,5,6 / 8,9,10 / 12,13,14 / 16,17,18 / 20,21,22 / 24,25,26 / 28,29,30 / 32,33,34 / 36,37,38 / 40,41,42 / 44,45,46 / 48,49,50 / 52,53,54 / 56,57,58 / 60,61,62).

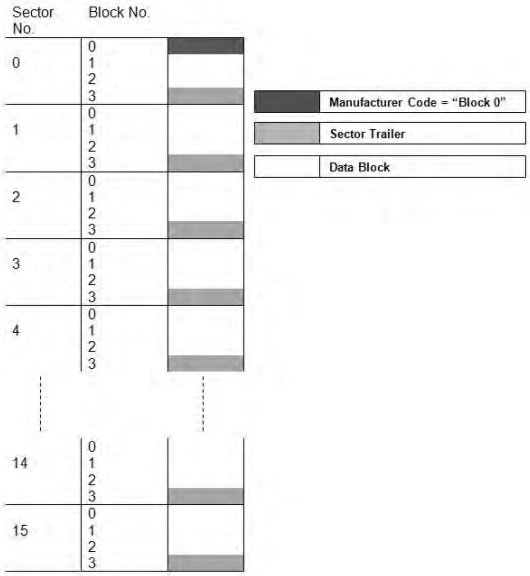

Fig 4.1. Memory Organizations

Sector Trailer:

The fourth block of any sector is the Sector Trailer. The Sector Trailer contains access Key A, an optional Key B and the access conditions for the four blocks of that sector.

Key Management and Multi-functionality:

The desired memory organization makes it possible to appoint different sectors to different applications and to prevent data corruption by using application specific secret keys.

Advantages in using MIFARE

Memory size of the card is higher when compared to RFID and hence a lot more information can be stored as well as other purposes.

The user need not have multiple cards for different purposes, as every MIFARE card is capable of handling 15 applications.

•The 13.56 MHz frequency range allows it to operate up to 4 inches (10 cm).

•It uses a three-pass security and can be thwart relay attacks.

•It is not affected by dust or other harsh environmental factors, which normally affect traditional RFID

•It also has an open architecture platform and is convenient, fast and flexible

•It is both forward and backward compatible.

Problems using MIFARE

RFID is a reasonably established technology and it would take time for people to accept MIFARE as a replacement. MIFARE uses a 32-bit serial number and this is a random number that does not contain a facility code. Hence using another format might result in the system being unable to understand and thus a check has to be done to make sure the control system supports multiple bits formats.

Facility code is an issue in MIFARE. MIFARE doesn't generate facility code and generate only random numbers. There is thus a possibility to generate duplicate packets. To avoid this issue random numbers should be generated only once even among different devices. The data reading rate is also comparatively slow to the proximity technologies.

VI. Conclusion

This study has identified and explained the nature of MIFARE technology evolution with respect to RFID applications. MIFARE technology will open new doors to make organizations, companies more secure, reliable, and accurate. The first part of this paper has explained and described that how the MIFARE Technology differ from RFID technology and its components, and the second part has discussed the main considerations of MIFARE technology in terms of advantages and in its security concern. Our Technology provides more memory for storing the data in authenticated ways. However, there is no doubt in the future that many companies and organizations will benefit from RFID technology.

References:

[1] *A Smart Card Alliance Report Contactless Technology for Secure Physical Access:* Technology and Standards Choices Publication Date: October 2002, Publication Number: ID-02002

[2] International journel Ubiquitous Secure Cash Withdrawal Abdullahi Arabo, Qi Shi and Madjid Merabti School of Computing and Mathematical Sciences Liverpool John Mores University Byrom Street, Liverpool, L3 3AF, UK {a.arabo, q.shi, M.Merabti}@ljmu.ac.uk

[3] NXP Type MF1K/4K *Tag Operation Storing NFC Forum data in MIFARE Standard 1k*/4k Rev. 1.1 — 21 August 2007

[4] J. Schwieren1, G. Vossen, "*A Design and Development Methodology for Mobile RFID Applications based on the ID-Services Middleware Architecture*", IEEE Computer Society, (2009), Tenth International Conference on Mobile Data Management: Systems, Service and Middleware.

[5] B. Glover, & H. Bhatt, *RFID Essentials*, O'Reilly Media, Inc, Sebastopol, (2006), ISBN 0-596-00944-5.

[6] K. Ahsan, H. Shah, P. Kingston, "*Context Based Knowledge Management in Healthcare: An EA Approach*", AMCIS 2009, Available at AIS library.

[7] S. Garfinkel, B. Rosenberg, "*RFID Application, Security, and Privacy*", USA, (2005), ISBN: 0-321-29096-8.

[8] L. Srivastava, RFID: Technology, Applications and Policy Implications, Presentation, International Telecommunication Union, Kenya, (2005).

[9] Application Notes, "Introduction to RFID Technology" CAENRFID: The Art of Identification (2008)

[10] L. Sandip, "*RFID Sourcebook*", IBM Press, USA, (2005) ISBN: 0-13-185137-3.

[11] T. Frank, H. Brad, M. Anand, B. Hersh, C. Anita, K. John, "*RFID Security*", (2006) ISBN: 1-59749-047-4.

[12] Narayanan, S. Singh & M. Somasekharan, "*Implementing RFID in Library: Methodologies, Advantages and Disadvantages*", (2005).

[13] Intermec, "ABCs of RFID: *Understanding and using radio frequency identification*", White Paper, (2009).