تقنية أنظمة ترددات الراديو الشبكية لحماية وخصوصية الأشـــياء

Networked Radio Frequency identification Systems Security and Privacy Issues

أ. المهدي عبدالسلام عجال ، أ . يونس المهدي قنيدي ، أ. حميدة علي الأســـود
ـ كلية التربية ـ جامعة غريان .

المُلـــــخّص

تقنية تردّدات الراديـــو هي إحدى تقنيات انترنت الأشياء، وأدّى انتشار هـــذه التقنية إلى ظهور بعض المشكلات الخطيرة بما في ذلك مخاوف الأمان والخصوصيـــة ، وهذه التقنية لديها القدرة على تمكين الآلات من تحديد الأشياء وفهم حالتها ، والتواصل واتخاذ الإجـــراءات عند الحاجة لتفادي هذه المشكلات في الوقت الحقيقي . ستناقش هـــذه الورقة مشكلات استخدام التكنولوجيا الحالية وستجري تحليلا للتهديدات لمكونات نظام تحديد التردد اللاسلكي ، ثم تحدد المشكلات- المخاطر ، وتوضّـــح كيف يمكن حل هذه المشكلات والمخاطر أو التخفيف منها.

Abstract

Radio Frequency identification (RFID) is one of the enabling technologies of the Internet of Things. The pervasiveness of this technology has given rise to a number of serious issues including security and privacy concerns. and this technology has the potential to enable machines to identify objects, understand their status, and communicate and take action if necessary, to create real time awareness. This paper will discuss current technology usage issues and conduct a threat analysis of the radio frequency identification system components then identify issues/risks and elucidate how these issues can be resolved or risks can be mitigated.

1- Introduction

Many technologies are available for business to identify, track and audit the assets. These technologies automate the business processes such as collection of data about stock, assets and components with accuracy and speed. Radio Frequency Identification is widely deployed technology in the business which can provide fast, accurate

identification for assets.

RFID consist of technologies which allows short range contact less reading of information from distance and compact data source. RFID tags are the unique ids and contain information about assets such as manufacturer, product type and also have the capability to measure the environmental factors such as temperature. Tags are attached to the assets or individual for the monitoring purpose and a RFID reader collect the information from tag or detect the tag passing through a particular location. The information gathered from this way can pass to the inventory database to perform query or update operations.

The simple example of RFID enabled application is a Teesside University library. Library has attached the RFID tag on each book to keep the record of books issued such as when and who issue the book. Teesside University students cards are RFID tag embedded in it. To borrow a book, a student detail is gathered by the RFID reader which also gathered data from the tags on each book when it scans through the reader. The inventory database will update the information about books and students automatically.

Why RFID technology took 50 years to become common technology

The main reason for this is a cost. The biggest challenge for the electronic automatic identification technologies were to compete with low cost printed barcodes, they must be equal to low cost barcodes or have additional value to cover the cost. RFID is not a cheap technology as compare to the traditional barcode but it is a value added technology and because of this retail industry is adopting this technology at large scale

1-1 Research Objectives

This paper aims to identify the RFID security and privacy issues and search the countermeasures to mitigate these issues. The security and privacy research has the following objectives.

- RFID security objectives
- Investigate the security and privacy issues that inherent in the RFID

system

- Research the potential ability of available countermeasures to resolve those issues
- Evaluate the security algorithms embedded in those countermeasures

This paper provides security requirements when considering deploying the RFID system. Security and private issues of the RFID system are discussed with a description of potential countermeasures to mitigate the issues.

Analysis of algorithms shows that several factors (such as cost, performance, complexity) need to consider when choosing the potential security measures.

2. LITERATURE REVIEW

2.1 RFID as an Enabler of the Internet of Things

A new dimension has been added to the world of information and communication technologies (ICTs): from **anytime, anyplace** connectivity for **anyone,** there is an additional dimension - connectivity for **anything** . Connections will multiply and create an entirely new dynamic network of networks – an Internet of Things [24]. This new IoT will now integrate physical things into the information flows. The IoT includes the overall infrastructure (hardware, software and services) supporting this networking of objects that are active participants in business and information processes, exchanging data including their identities, their physical properties and information 'sensed' from their environment. Identification technologies like RFID allows each object to have a unique identifier that can be read at a distance allowing automatic, real time identification and tracking of individual objects [23].

2.2 Security and privacy concerns about the RFID layer of EPC Gen2 networks

for retrieving digital information without physical contact or line-of-sight, that is revolutionizing the manner in which objects and people can be identified by computers [25]. Tagging objects or even people with smart labels (the so called RFID tags) emitting identifying information in form of binary modulated signal, is the way computers can actually understand the

presence of objects. RFID technology is the closest approach to the ubiquitous computing [26] or the future Internet of Things. RFID labels are frequently referred as the next generation barcodes. Although the utility is the same (the identification of an object), RFID offers two main advantages over conventional barcode systems. On the one hand, optical barcodes only indicates the generic product, whereas an RFID tag can identify the item (being able to distinguish different objects from the same product). On the other hand, there is no need of line-of-sight. Thus, while optical arcades must be identified one by one, RFID tags can be read much faster, without human intervention and in large quantities [25, 27].

2.3 Attacking RFID Systems

Press stories about radio-frequency identification (RFID) often give inaccurate descriptions of the possibilities that exist for abuse of this technology. They predict a world where all our possessions will have a unique identification tag: clothes, books, electronic items, medicines, etc. For example, an attacker outside your house equipped with a commercial reader would be able to draw up an inventory of all your possessions, and particular information such as your health and lifestyle could also be revealed. Also, it is said that this technology allows "Big Brother" to know when you are in public places (office, cinemas, stores, pubs, etc.), tracking all your movements and compromising your privacy in terms of your whereabouts (location). RFID technology is a pervasive technology, perhaps one of the most pervasive in history. While security concerns about the possibility of abuse of this pervasive technology are legitimate, misinformation, and hysteria should be avoided. One should be aware that ways of collecting, storing, and analyzing vast amounts of information about consumers and citizens existed before the appearance of RFID technology. For example, we usually pay with credit cards, give our names and address for merchandizing, use cookies while surfing the Internet, etc. In this chapter we give an overview of the risks and threats related to RFID technology, helping the reader to become better acquainted with this technology. Although the privacy issues are the main focus in literature [2–3], there are other risks that should be considered when a RFID system is designed

2.4 Development and Implementation of RFID Technology

Radio Frequency Identification (RFID) is an automated identification technology that uses tags to transmit data upon RFID reader queries. Compared to barcodes identification technology, RFID tags provide a unique identifier, which raises concerns over user privacy, such as clandestine tracking and inventorying [4]. In its original version, a RFID tag responds to a reader query with its fixed unique serial number. This fixed unique serial number enables tracking of tags and the bearers, possibly without the bearers' knowledge or consent. In addition to the unique serial number, some tags carry information about the objects they are attached to. Thus, a retail store or a person owning such tags might be under threat of clandestine inventorying. Enormous research effort has been paid in attempt to solve the problem of consumer privacy and industrial espionage in the RFID world. However, most methods demand heavy or frequent cryptographic operations on RFID tags, which contradict the low cost demand of RFID tags ($0.05-0.10). Typically, a low-cost tag should only store hundreds of bits and have 5K-10K logic gates, only a fraction of the gates can be devoted to security tasks. The trade-off between cryptographic operations and low-cost has become a significant challenge in designing RFID tags, and this challenge has impeded RFID being the replacement of barcode technology for cost sensitive item-level applications, such as in supply chains, libraries and rental shops. To solve this problem, a new RFID structure is proposed. Except the fixed unique serial number, tags carry only the IDs in disguise to avoid eavesdropping and clandestine tracking. The database, on the other hand, is responsible for protecting the information security, integrity and non-repudiation. This chapter discusses and presents the implementation of this passive ultra high frequency (UHF) RFID system, based on EPC Class 1 Generation 2 UHF RFID (abbreviate as Gen 2) protocols [4-5].

2.5 Security in Pervasive Computing

RFID systems are composed of three key elements [24]: the RFID tag, the RFID reader, and the back-end database that associates records with tag data collected by readers. The RFID readers interrogate tags for their contents by broadcasting a radio signal. Tags respond by transmitting back resident data, typically including a unique serial number [14]. The way such communication occurs differs based on the tag type: passive, semi-passive,

and active. Active tags initiate and respond with a stronger signal while passive tag can only respond to the RFID reader's interrogation. The backend IT system is responsible for cross-referencing the RFID tag's ID number with a database record that describes the object to which the tag housed within is attached.

3- RFID System Components

RFID system consists of three main components.

- RFID tags
- RFID Tag Reader
- REFID Backend Database

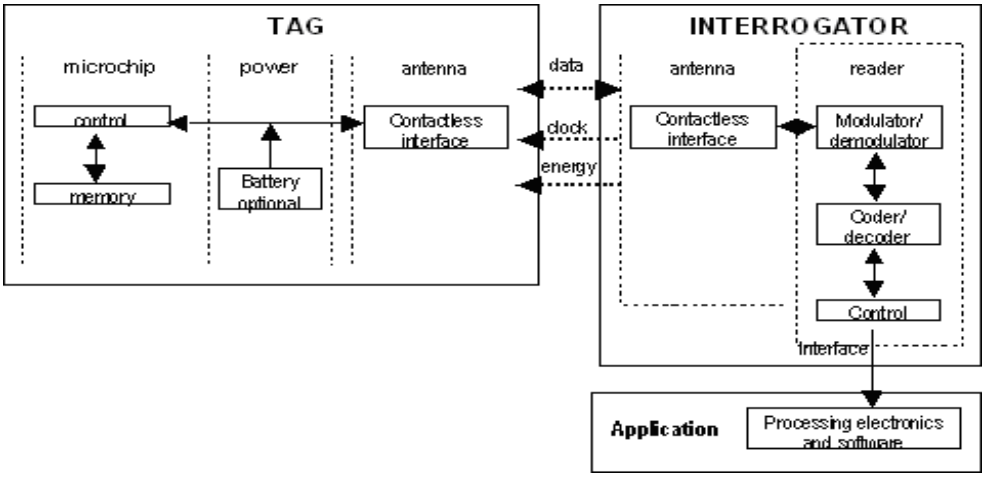


Figure 1. RFID System Components

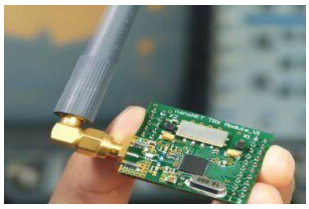
Examples for RFID cards systems :

RFID Tags

RFID is available in many types, but mainly RFID is divided into two main following classes.

3-1 Active Tags

Active tags are heavily dependent on power source they are either directly connected to power source or use the power from integrated battery. The active tags which utilize the power from battery have the limited lifetime because of stored power in the battery and tags have to undergo many read operations. For example aircraft transponder is attached with active tags to identify its national origin. A real active RFID tags are shown in figures 2 and 3.



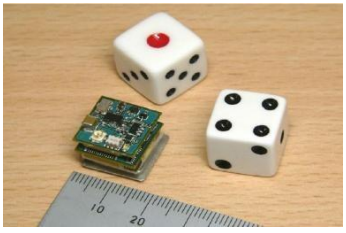


Figure 2. Active RFID tag with a changeable antenna[6] **Figure 3.**Acompact active tag [6]

Active tags are not suitable for retail industry because of the batteries, cost, size and limited lifetime.

3-2 Passive RFID Tags

The passive RFID tags do not require a power source or maintenance. These tags have unlimited lifetime and their tiny size make it possible adhesive label. A passive tags consists of three main components; an antenna, a semiconductor chip and encapsulation. These tags get powered when they communicate with RFID reader. A passive tag is shown in figure 4.

Figure 4. Passive RFID tag[18]

3-3 RFID System Frequency Bands

In addition to active and passive RFID tags, RFID tags can be identity by their radio frequency. There are four radio frequency bands are available for RFID tags ranging from 30 KHz to 5.8 GHz, are low frequency (LF), high frequency (HF), ultra high frequency (UHF) and microwave frequency (MW).

The RFID system requirements determine what range or frequency band is required, because frequency is depended on the application, size of tag and reader range. The use of higher frequency means, higher the data transfer rate but it will increase the RFID system over cost.

The listed below table, RFID frequency bands and read range provide an overview of the characteristics of each RFID frequency band and includes read range, data transfer rates.

Table: RFID frequency bands and read range

	LF	HF	UHF	MW
Frequency	**30 – 300 KHz**	**3 – 30 MHz**	**300 – 1000 MHz**	**2 – 30 GHz**
Read Range	**Up to 1m**	**Up to 1.5m**	**Up to 100m**	**Passive – 3m Active – 15m**
Data Transfer Rate	**Less than 1kbit/s**	**25kbit/s**	**30kbit/s**	**100kbit/s**
RFID Tags type	**Passive Tags**	**Passive Tags**	**Passive Tags**	**Passive and Active Tags**
Applications	**Access control, Animal identification, Inventory control, Vehicle immobilizers**	**Smart cards, Contact-less access and security, Item level tracking, Library books, Airline baggage**	**Logistics case/pallet tracking, Baggage handling**	**Railroad car monitoring, Automated toll collection**

Table Reference[8]

RFID Standards

International Organization for Standardization (ISO) is major contributor for defining the RFID standards. The ISO RFID standards include the following.

- ISO TC 23: Animal Identification
- ISO TC 104: Freight Containers
- ISO TC 204: Road Telematics
- ISO TC 122: Packaging
- JTC 1/SC 17: Integrated Circuit Cards (i.e.: credit cards with embedded tags)

- JTC 1/SC 31: Automatic Identification and Data
- Collection Techniques ("Where's the lost child at the amusement park?")

3-4 RFID Tag Reader

RFID tag reader is basically a radio frequency (RF) transmitter and receiver, which is controlled by a microprocessor. The RFID reader uses the antenna to capture the data from tags and pass to the database for processing.

3-5 RFID Backend Database

RFID reader has the networking capabilities such as wired Ethernet or wireless Ethernet that connects the reader with backend database. The backend database performs the various function that including matching, tracking, inventory and storage of tags information. It is also performing the alert function for inventory management systems for example the re-order event is trigger for retailer or an alert is trigger to the guard for security applications.

4-5 Adoption of RFID

RFID are being used in many different ways to create the value. RFID has so many applications and can be adopt according to the industry requirements. Mainly industries have divided RFID applications into following categories.

Automotive

Auto makers are integrating the RFID for anti-theft immobilizer. It enhances the security and convenience into an automobile by using the RFID.

Animal Tracking

Animal farms are using RFID tags to meet the requirements of export regulations and audit the livestock of animals. RFID tags help to track the wild animals for ecological studies and return the lost pets to their owner.

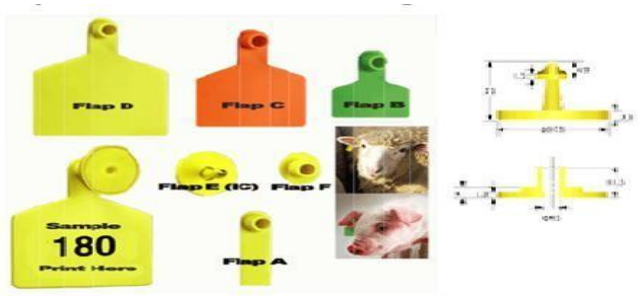


Figure 5. Animal RFID tags [10]

Asset Tracking

Hospitals and pharmacies are using the RFID tags to meet the strict accountability legislation.

Supply Chain

PC World and Tesco have adopted the RFID for inventories control, reduce out-of- stock-losses, and stop shoplifting and speedy customer services through check-out points

Figure 6. Example of bar code and RFID tags [11]

E Passports

The UK government has start issuing he RFID enabled passports to increase the security of UK citizens travel documents. The passport is embedded with RFID tag that can wirelessly send passport and biometric information to an RFID reader.

Figure 7. RFID in UK Passport [12]

Elderly Health Care

RFID are playing the vital role in social care homes, by tagging the key objects such as drugs, food items, appliances and embedding small RFID tags in gloves can monitor daily person's habits and caretaker can monitor these attributes remotely.

Immigration Tracking

RFID can be used for immigrants tracking, such as identify them, their location or if they are still in country after their permissions have been expired.

Contactless Payment Cards

Contactless payment is a new feature on payment cards (such as debit, credit or pre-paid) which make purchases quicker and convenient for both retailers and customers. The contactless cards use the RFID which transmit financial transaction wirelessly. [9]

Figure 8. RFID enabled contactless card [13]

5- RFID Security Objectives

RFID security objectives involve three basic following concepts.

5-1 RFID Confidentiality

This provide the assurance that only authorised people share and access RFID resources and data.

The confidentiality objectives within the RFID system include:

- Tag data should be protected from unauthorised access
- The algorithms that create RFID tag-IDs cannot be reverse engineered
- Communication medium of RFID system should be secure

5-2 RFID Integrity

This provides the assurance that data is not modified and it's from genuine resource. The integrity objectives within the RFID system include:

- RFID tag is protected from unauthorised modification
- Duplication of RFID tags are protected
- Where multiple tags are present its need to ensure they do not cause loss of RFID system integrity

5-3 RFID Availability

This provides the assurance that authorised people are able to access the RFID system when it's needed.

The availability objectives include the following.

- RFID system is operational 24 hours a day, 7 days a week

- Tags do not cause the RFID system availability
- Backend database server should available for multiple RFID reader access

6 Security Issues in RFID System

The widespread applications of RFID technology have created the threats to security and privacy of individuals and organizations. A numbers of privacy and security risks need to mitigate before adopting the RFID technology by individual and organizations.

RFID tags are not intelligent devices and considered as dull devices, they can only listen and respond to the signal without caring who sends the signal and there is a risk of unauthorized access and modification of tag data. The unprotected RFID tags are vulnerable to many security issues. Broadly these security issues can be divided into following categories:

- Tag Access
- Tag Collision

6-1 Tags Access

RFID system is vulnerable to many kinds of attacks. These attacks can be categorised as follow.

Eavesdropping Attacks

RFID tags do not have the processing power to communicate with RFID readers in encrypted form. The radio signal transmitted from the tag and reader is a clear unencrypted signal which can be detect several meter away by other radio receivers. The unauthorised user can intercept the transmission and can read the RFID tag data.

Research in the USA has prove practically eavesdropping attack on RFID embedded credit card, the credit card information, such as the cardholder's name and account information could be read from the distance of meter, if RFID tag data is not properly encrypted. [18]

Figure 9. Eavesdropping Attacks [15]

Counterfeit RFID Tag Attacks

This is the physical attack on RFID tags; in counterfeit attacker make the duplicate of

legitimate RFID tags through cloning. Some inherited attributes of RFID tags make them vulnerable to this attack. For example low cost RFID tags do not save the tag identifier in encrypted form that can be read for duplication. An attacker can gain the access on tag identifier number and generate a false tag with same identifier number.

Replay Attacks

The counterfeit tags cause damage to the integrity of RFID system. Counterfeit attacks also facilitate the replay attacks, in which attacker simulate the legitimate RFID tag signal receiver and sender. Replay attacks on big scale can lead to a Denial of Service (DoS) attack in which counterfeit tags are replayed to RFID readers in huge amount of requests.

Denial of Service (DoS) Attack

The attacker can flood RF signals with noise to cause disturbance in the RFID transmission. The attacker can also consider the power attack in which he/she can change the power of RFID tags to damage them. Some attacker they are not interested in RFID tag data, but can launch (DoS) attacks against RFID System.

6-2 Tags Collision

When numbers of RFID tags are communicating with the RFID reader, there are chances when RFID reader try to read only single tag and

multiple tags respond simultaneously to reader query, in result this will cause interference in the communication. This inference is called collision, when collision occurs RFID tags are unavailable to respond RFID reader query.

7- RFID System Security Countermeasures

The countermeasure can implement to deal the RFID security issues; the main purpose of these security measures is to protect the objective of RFID system (confidentiality, integrity and availability). For example, countermeasures counterfeit tags provide guarantee of confidentiality and integrity of RFID tag data and to achieve this protection encryption can be included in tag contents to prevent from disclosure or modification.

There are numbers of solution available to protect the security of RFID system; broadly these can be categories to the following areas.

Password Protection

Use of strong passwords can protect the tag data from unauthorized read and write. All tags should have different passwords otherwise tag data become public. But the problem is, if all RFID tags have the different passwords then there may be need of millions of passwords and RFID reader has to access the database for each RFID tag password.

Encryption

Encryption is a technique which main purpose is to scramble the RFID clear data into secret code. Encryption process is based on mathematical algorithms which encrypt or decrypt the RFID data. The two kinds of encryption techniques can be implement through public (asymmetric) key and symmetric key. The RFID system based on symmetric key encrypt and decrypt the RFID data with one known key. RFID system relies on asymmetric key uses the two different keys to perform the encryption and decryption functions.

Both encryption techniques provide RFID tag data confidentiality, authentication and integrity. But the management of the encryption techniques is an overhead and costly. RFID tags embedded with encryption still cannot stop the physical attacks which can also lead to

the RFID tag cloning.

Hash Based Access Control

In this countermeasure, Hash equips RFID tags reserved the small portion of memory for temporary meta ID and will use to locked or unlocked RFID tags data[17] . To lock a RFID tag, hash of random keys are store as the tags meta ID, i.e. meta ID □hash (key). This can be done over the RF channel or a physical contact of RFID tags. When RFID tags are in locked state it's only respond to its meta ID and does not perform the any other functions. To unlock a RFID tag, RFID reader queries the meta ID from the tag and search for appropriate key in backend database and transmits the key to the tag. The RFID tag compare the hashed key with stored meta ID, if both values are matched it unlocks the tag and enable all the read and write function on the tag.

RFID Reader Integrity Protection

RFID Readers can reject the tags replies, if there is inconsistency in response times or signal power levels which do not match the tags attributes. This can protect the tags spoofing attacks, if used in passive tags.

RFID readers and tags can be designed to use predefined random frequencies associated with each other. RFID readers can change the frequencies randomly to protect the unauthorized access and eavesdropping on the RF (radio frequency) transmission. In addition, data transmission between reader and database backend requires the verification of the reader's identity. To ensure the information validity passed between reader and tags authentication countermeasures can be implement between reader and backend database.

8- Privacy Issues in RFID System

RFID system privacy issues are divided into two main following categories.

RFID tag data privacy

This refers to protect the personal information hold by RFID tags and in backend database. There is a risk present when unauthorised user gain the access to RFID system, further privacy issues can rise if

someone re-write the tags data.

RFID tag location privacy

This refers to protect the individual information by physical location and movement. Mobile tracking system or GPS can identify the physical location of the RFID tags, once the physical location is identified this can be use for data mining and other value added services.

Unauthorised access to RFID tags may compromise the tags data privacy, even appropriate security countermeasures are in place for example encryption cannot protect the individuals been tracked through tag responses, a traffic analysis attack could violate the location privacy.

Privacy objectives for RFID system are as follow.

- Protect the data privacy of individual or object tags
- Protect the location privacy of individual or object tags
- Give confidence to individuals and organisations that RFID system privacy is being protected [20]

In UK and Europe the RFID system privacy protection are based on following same fair information practices.

- Openness and transparency
- Purpose specification
- Collection limitation
- Accountability
- Security safeguards [20]

9- RFID System Privacy Countermeasures

9-1 Kill Tag

The kill command deactivates the RFID tags permanently. The kill command physicaly disconnects or short circuit the RFID tag. This make sure RFID tags are not detected any more and protect the privacy of individuals.

However, there are some implications with kill command. For instance if Teesside University library smart-cards are embedded with RFID chips which requires the continue access to library. If library permanently de-active the smart-cards then library need to issue new

smart-cards every time which is overhead and costly.

9-2 Faraday Cage

The Faraday cage is made of metal or foil which has the ability to block the radio signals at specific frequencies and can protect the RFID tags from being detected.

It is very difficult to wrap the foil around RFID tags which are used by pets and individuals.

9-3 Active Jamming

In active jamming, high power radio frequency signals are broadcast to disrupt the operation of any nearby RFID readers. This can also disrupt the functionality of another RFID system.

Using of active jamming signal is illegal and subject to the government regulations. If the active jamming signals are too high it can disrupt the other RFID system where privacy is not concern.

The listed below Security and Privacy issues table show the relationship between RFID systems security objectives and common security issues and their corresponding countermeasures.

9-4 Table: Security and Privacy Issues [16]

Security Issues	**Security Objective Impacted**	**Countermeasures**
Counterfeit Attacks	**Confidentiality Integrity**	**Encryption Passwords Faraday Cage**
Replay Attacks	**Confidentiality Integrity**	**Faraday Cage Encryption**
Eavesdropping Attacks	**Confidentiality**	**Encryption Faraday Cage Active Jamming**

10 Evaluation

10-1 Analysis of the privacy and authentication countermeasures To evaluate the RFID privacy and authentication algorithms the listed below four factors were considered.

10-1.1 Cost and Complexity

The memory size of the RFFID tags and the number of the gates required by the algorithm determine the cost and complexity. The cost is associated with application area of RFID tags which measures how much resource the algorithm will use. According to the needs of application size of the memory can be reduce for the algorithm and the number of logic gates.

When designing the RFID algorithms, there is need to write simple algorithms that requires small amount of memory and logic gates. For example, for the SHA-1 algorithm approximately 4200 logic gates are required where as lighter hash algorithm required approximately 1700 logic gates [21], it also make the algorithm less complex than the SHA-1 algorithm.

10-1.2 Performance

The performance of the RFID algorithm can be measure in time taken by the each message round trip, the time to access the data from database server and to read and write the data to the tag.

To improve the performance, it is important to reduce the size and the number of the messages in the algorithm. For example, public key algorithms can be used for the small messages and secret key algorithms can be used for large messages. This will maintain the performance of RFID system.

10-1.3 Availability

The use of RFID system on large scale has made it critical system for the businesses which must be available all the time such as RFID system in supply chain.

Therefore, the RFID system must be available during the execution of the algorithm.

10-1.4 Anonymity

RFID tags must have anonymity to protect them from illegitimate

tracking. The algorithms must generate the random numbers and refreshed frequently to protect them from illegitimate tracking.

The mentioned above four categories were applied to evaluate the RFID security algorithms and divided into two following parts

11 Privacy Countermeasures Analysis

11-1 Minimalist: According to the [22], if more memory is required to store the list of pseudonyms codes, the RFID tags communication cost will increase as a cost per session. But the performance of the protocol will be better because the computation will be performed by the RFID tags such as comparisons and XOR operations.

In addition, Minimalist use two different exchange identifiers and refresh the pseudonyms after the authentication, which protect the denial of service attacks and illegitimate tracking. As a result this algorithm provides availability and the anonymity features.

11-2 Re-encryption scheme and universal re-encryption: The re-encryption scheme and universal re-encryption use the public key algorithms which are costly algorithms and required the more memory on the RFID tags. These algorithms perform the complex operations which required number of logic gates.

Other requirements of these algorithms are lot of computation on backend database server side which will cause the slow response from the database server and will take time to write the encrypted text on the tags chip, this affects the performance of algorithms.

However, these algorithms protect anonymity of the tags identifier by re-encryption scheme.

11-3 Authentication Countermeasures Analysis

11-4 Peris-Lopez Algorithm: The base of this algorithm is Miniamlist algorithm which means the conditions are apply to this algorithm that is costly. This algorithm does not require the high computational power by the RFID tags end or backend database server side and achieve the high performance. One drawback of this algorithm is resynchronisation attack [1] which affects the availability of system which cannot be guaranteed all the time.

This algorithm uses four keys to protect the anonymity of the tag identifier.

11-5 SSG Algorithm: This algorithm requires the small size of the memory on tag with small number of logic gates in comparison with other security algorithms.

12 Reflection

The adoption of RFID system has changed from basic identification system to more advanced and complex systems. The traditional RFID system allows a business to track, monitor, utilise and inventory control the business assets with some limitations.

The advanced RFID such as IOT and NFC also known as smart or super RFID system in which RFID tags can be made active, which means regardless of assets tagging these active RFID system collect the data for the business. This approach is called asset communication, where RFID tags communicate with each other and provide some information to the neighbor RFID tag. The modern RFID tags is not just being read for identification purpose, it's about making the RFID tags intelligent so it can work for its user.

The modern RFID system consists of miniature and power efficient electronics which can bring the opportunity of tele-operation and tele-presence (the ability to monitor and control object from distance). This is the future of RFID system development.

The future development of RFID system is more focus on controlling and monitoring the assets from far distances and more intelligent which will also communicate with the end users, but it also have to be smart and processes information themselves. The advanced technologies such as virtual reality and remote access have made the complex future of RFID identification technologies because tagged assets are in large scale and collection of variable data.

In this research report the RFID based mobility for blind people area is considered that future RFID can develop into The visually impaired people have the limited perception of the surrounding environments and they are not aware of unsafe situations. To provide the safe mobility to blind people a future research has been started on assistive

based on RFID system by Joint Research Centre (JRC) of the European Commission.

The research aim is to develop the electronic stick for the blind people based on low- frequency RFID reader and embedded with Bluetooth module for data communication. This will provide secure navigation. The electronic stick will be connected with personal digital assistant via Bluetooth and will perform the navigation logic operations and will play the real time audio messages to direct the blind people. The performance of this algorithm is very good because it transfer the message quickly between tags and backend database server. Same like Persi-Lopez algorithm, this algorithm is vulnerable to resynchronisation attack which affects the availability of RFID system. The algorithm has the ability to change tag identifier after the authentication.

12-1 Randomized Hash Locks: This is costly solution because of its length key list mathematical algorithm. This algorithm cannot protect the DoS attacks but it can protect the tags from illegitimate tracking.

13 Conclusion

In this research paper researches focused on the potential security and privacy issues and countermeasures for a different type of security vulnerabilities present in the RFID system. The wide range adoption of RFID system has increase interest in society because RFID system change the way industry and business manage their assets and RFID system has begin the influence in individual daily life. As discussed above, the RFID application has increased across a variety of industry such as logistics, manufacturing, retail and health. The application requirements are vary according to the industry but security and privacy requirement is same for all kind of industries when adopting the RFID system. While RFID system bring the convenience there are security risks are also present in the RFID system.

The main purpose of security is to protect the RFID security objectives i.e. confidentiality, integrity and availability. Individuals adopting the RFID system, demands the security of personal privacy from both

technical and social aspects. The privacy issues are critical and demand a comprehensive and effective technique that can guarantee individual privacy while preserve the RFID system benefits. While there are several countermeasure are available to protect the RFID system security and privacy but now one provides the complete protection. Privacy and authentication algorithm embedded to RFID tags provide the security to some extent but it make tags more complex and costly. Understanding RFID security today will help in the development of secure ubiquitous computing systems in the future. Identifying built in security or privacy threats of RFID systems can help for to meet regulatory, legislation and compliance requirements and privacy rights of individuals.

References

[1] Li, T. & Wang, G. (2007). Security Analysis of Two Ultra-Lightweight RFID Authentication Protocols, *Proceeding of the 22nd IFIP TC-11 Int'l Information Security Conference*, Vol. 232, Springer, pp. 109-120.

[2] L. Bolotnyy and G. Robins. Physically unclonable function-based security and privacy in RFID systems. In *Proceedings of PerCom'07*, pp. 211–220. IEEE .

[3 S. Spiekermann and H. Ziekow. RFID: A 7-point plan to ensure privacy. In *Proceedings of ECIS'05*, Regensburg, Germany, 2005.

[4] Jin Li, Cheng Tao, "Analysis and Simulation of UHF RFID System", in proceedings of the 8th International Conference on Signal Processing, 2006.

[5] EPC™ Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz~960 MHz Version 1.0.9. 2-5 RFID Privacy Issues in Healthcare.

[6] http://www.intechopen.com/books/deploying-rfid-challenges-solutions-and-open- issues/rfid-applications-in-cyber-physical-system

[8] Wyld, D. C. (2006). RFID 101: The next big thing for management, Management Research News, Vol. 29, No. 4, pp. 154-173, ISSN: 0140-9174.

[9]Core RFID (2011), *RFID Identify, Assign, Track & Audit.* Available at: http://www.corerfid.com/Files/White%20Papers/032%20Introduction%20To%20RFID.pdf (Accessed: 18 November 2013).

[10] RFID Infoteck (2013), *Passive Tags (low Frequency).* Available at: http://www.rfidinfotek.com/detail/rfid-animal-tag-iso-1178411785/381.html (Accessed: 15 December 2013).

[11] Systech International (2013), *IDS Packaging – White Paper*. Available at: http://www.idspackaging.com/common/paper/Paper_249/Securing%20the%20Pharm aceutical%20Supply%20Chain.htm (Accessed: 10 December 2013).

[12] rfidiot.org (2013), *Passport Chip*. Available at: http://rfidiot.org/passport-chip-full.png (Accessed: 10 December 2013).

[13] RFID Blog (2013), *Tagged: contactless.* Available at: http://www.rfid-blog.com/?tag=contactless (Accessed: 10 December 2013).

[14] Weis, S. A., Sarma, S. E., Rivest, R. L., & Engels, D. W. (2004). Security and privacy aspects of low-cost radio frequency identification systems. Security in Pervasive Computing 2802, 50-59.

[15] Dr. Amir Moradi (2013), *Chair for Embedded Security*. Available at:

[16] Smart Border Alliance (2003), *RFID Security and Privacy White Paper.* Available at: http://www.dhs.gov/xlibrary/assets/foia/US-VISIT_RFIDattachE.pdf (Accessed: 5 January 2014).

[17] Garfinkel, S.L., Juels, A. and Pappu, R. (2005) 'RFID privacy: an overview of problems and proposed solutions', *Security & Privacy, IEEE*, 3(3), pp. 34-43.

[18] Mouza, Bani and Chan (2010) *Smart RFID Security, privacy and Authentication.* Available at:

http://www.intechopen.com/download/get/type/pdfs/id/8855 (Accessed: 03 December 2013).

[19] S. A. Weis, S. E. Sarma, R. L. Riovest, and D. W. Engels, (2004), "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems", In D. Hutter et al. (Eds.): Security in Pervasive Computing 2003, LNCS, volume 2802, Springer- Verlag, pages 201.

[20] Smart Border Alliance (2013), *RFID Security and Privacy White Paper.* Available at: http://www.dhs.gov/xlibrary/assets/foia/US-VISIT_RFIDattachE.pdf

[21] Jian Shen, Dongmin Choi, Moh, S. and Ilyong Chung (2010) 'A Novel Anonymous RFID Authentication Protocol Providing Strong Privacy and Security', *Multimedia Information Networking and Security (MINES), 2010 International Conference on.* , pp. 584-588.

[22] Juels, A. (2004). Minimalist cryptography for low-cost RFID tags, *proceeding of Int. Conference on Security in Communication Networks – SCN 2004*, LNCS 3352, Amalfi, Italy, Springer-Verlag, pp. 149-164.

[23] Future networks and the internet: Early Challenges regarding the "Internet of Things," Commission Staff Working Document, Brussels, 29 September 2008, SEC (2008)2516.

[24] Internet Reports(2005): The Internet of Things – Executive Summary, International Telecommunication Union (http://www.itu.int/osg/spu/publications/internetofthings/Internetof Things_summary.pdf) Retrieved June 30, 2010.

[25] L. Buttyan and J. Hubaux,(2008). Security and Cooperation in Wireless Networks. Cambridge University Press, 2007, available at http://secowinet.epfl.ch/.

[26] D. C. Ranasinghe and P. H. Cole,(2010). Networked RFID Systems and Lightweight Cryptography, Chapter 3. Springer, Nov. 2008, ch. Networked RFID Systems, pp. 45–58.

[27] A. Juels,(2005) "RFID security and privacy: A research survey," IEEE Journal on Selected Areas in Communication, vol. 24, no. 2, pp. 381–394, Feb. 2006.