RFID AUTHENTICATION SCHEME BASED ON DYNAMIC KEY GENERATION

by

Amandeep Singh Sran

Submitted in partial fulfilment of the requirements
for the degree of Master of Computer Science

at

Dalhousie University
Halifax, Nova Scotia
December 2012

DALHOUSIE UNIVERSITY

Faculty of Computer Science

The undersigned hereby certify that they have read and recommend to the Faculty of Graduate Studies for acceptance a thesis entitled "RFID AUTHENTICATION SCHEME BASED ON DYNAMIC KEY GENERATION" by Amandeep Singh Sran in partial fulfilment of the requirements for the degree of Master of Computer Science.

Dated: December 06,2012.

Supervisor: _____

Readers: _____

_____

DALHOUSIE UNIVERSITY

DATE: December 06, 2012

AUTHOR: Amandeep Singh Sran

TITLE: RFID AUTHENTICATION SCHEME BASED ON DYNAMIC KEY GENERATION.

DEPARTMENT OR SCHOOL: Faculty of Computer Science

DEGREE: MCSc CONVOCATION: May YEAR: 2013

_____

Signature of Author

DEDICATION PAGE

The thesis work is dedicated to my Maternal Grandfather S. Pritam Singh Chahal.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

RFID technology has potential for a number of applications in a wide variety of fields. However, there are several challenges that make it difficult for the technology to be widely deployed; one of it being security. Due to severe resource constraints, it makes it difficult to deploy strong authentication schemes on RFID tags. This result in making the system vulnerable to attacks that in turn causes the loss of confidential and private data. In this thesis, we propose an authentication scheme for RFID that is based on the cellular network authentication principle for the reader and the server and dynamic generation of keys coupled with the use of basic logical operation for the tags and the server. The key generation mechanism for tags involves independent generation of keys along with support for forward secrecy and non repudiation. The proposed scheme removes the drawbacks of some of the previous works done in the RFID field.

LIST OF ABBREVIATIONS USED

RFID	Radio Frequency Identification
EPC	Electronic Product code
Wi-Fi	Wireless Fidelity
LF	Low Frequency
KHz	Kilo Hertz
MM	Millimeters
HF	High Frequency
MHz	Mega Hertz
UHF	Ultra High Frequency
SHF	Super High Frequency
GHz	Giga Hertz
AES	Advanced Encryption Standard
AND	Logical and operation
OR	Logical or operation
NOT	Logical negation operation
XOR	Logical exclusive or operation
R-XOR	Rotation with Xor
SHA-1	Simple Hashing Algorithm-1
SHA-256	Simple Hashing Algorithm-256
ID	Identifier or Identification Number
R_{id}	Reader Id
AV	Authentication Vector
R	Reader
T	Tag
T_{id}	Tag Id
DES	Data Encryption Standard
RAM	Random Access Memory

ACKNOWLEDGEMENTS

I gratefully acknowledge the support of my supervisor Dr. Srinivas Sampalli under whose guidance I did my research work. I would also acknowledge the support of my committee members Drs. Nur Zincir-Heywood and Vlado Keselj whose remarks and feedback helped me to improve my work. I would like to give a special mention to Musfiq Rahman, Raghav Sampangi and Monika Lal who helped me through different stages of my research. I acknowledge the support of my family, friends and all my teachers. Above all I would thank WAHEGURU (THE GOD) with whose blessings I am able to complete my research work.

CHAPTER 1: INTRODUCTION

1.1 Overview: Radio Frequency Identification

Radio Frequency Identification (RFID) is an emerging wireless technology which currently has its application in many fields. It is a simple technology that automatically and uniquely identifies an object from a set of objects with the help of radio waves. It finds its applications in many areas, which include, but are not limited to, manufacturing and supply chain, distribution and retail, transportation, access control, military, safety and security, library systems, agriculture, endangered species, sports, emergencies, pharmaceuticals, environment and library systems, etc [1].

Figure 1 shows the basic architecture of an RFID system. It consists of the following components:

- RFID tags i.e. basically a silicon chip with antenna and a small memory that stores a unique identifier known as EPC (electronic product code). This EPC code acts as a key to uniquely identify a record in a database. The dimensions for a RFID tag could be as small as 0.05mm by 0.05 mm.
- RFID reader, i.e., a device capable of sending and receiving data in the form of radio frequency electromagnetic waves. This device is basically used to read the unique EPC from the tag.
- Middleware which acts as a filter to eliminate bad or multiple reads.
- Backend Enterprise Server which stores the information related to the objects being tagged with the help of RFID tags.

The basic setup for a RFID System is that the objects are tagged. These tags store data and they respond to the queries sent by the RFID readers. These readers could be fixed as well as mobile. The data received by the tags is transmitted to the backend server through wired or wireless networks. The middleware is a hardware that helps in pruning the corrupt data so that the processing becomes easy and fast for the backend server. The server processes the request from the reader and sends the information about the object which is tagged to the reader [2].

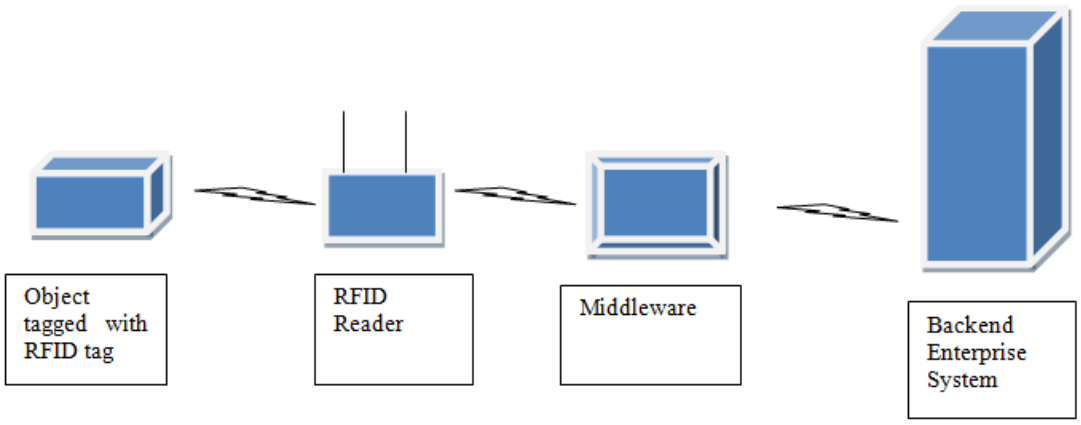

Figure 1 An Overview Of A Typical RFID System

A typical 96-bit EPC (Electronic Product Code) has the following structure [1]:

Table 1 Electronic Product Code Structure

Header (8 Bits)	Domain Manager Number (28 Bits)	Object Class (24 Bits)	Serial Number (36 Bits)

The advantages that RFID technology posses over traditional methods of object identification [1] are as follows:

- No line of sight required for reading the tags.
- The tags can be embedded inside the product and thus they suffer from less damage.
- Tags can withstand harsh environments.
- The data on the tags can be modified.
- The reading distance from the tags can be of the range of several meters.
- Multiple reads for the tags are possible at any given moment of time.
- The read rates are faster and this increases the overall capability of the system.
- RF (Radio Frequency) scanning is hands free.

The catalysts that played a major role in the emergence of the RFID technology [1] was related to cost effectiveness of the tags (as low as few cents per tag), standardization provided by EPCglobal, advancements in application software as well as middleware and integration of RFID with already existing wireless technologies such as Wi-Fi and Sensor Networks.

Table 2 [1] gives brief information about the RFID radio frequencies and the advantages and drawbacks associated with each frequency.

1.1.1 Classification Of RFID Tags

RFID tags are broadly classified as:

- **Active Tags:** These tags are generally powered by a battery of theirs which is limited by a life time period. These tags have a large reading distance and a reader can read them from tens of meters away. They generally operate at a higher frequency range of 433 MHz or 2.45 GHz [1] and have a read rate that is fairly high. A reader can simultaneously read around thousand active tags if they are static and around 10 if they are moving at a

high speed (>100 mph) [1]. These tags not only have a high memory storage space around 1 MB but these tags are capable of performing complex cryptographic operations like hashing functions.

Table 2 An Overview Of The Frequency Range For RFID Systems

Frequency name	Range	Advantages / Drawbacks
Low Frequency (LF)	125-134 KHz	Provides small read distance (few mm) but RFID signal is not affected by the presence of metals or liquids.
High Frequency (HF)	13.56 MHz	Reading distance is of the range of few meters and read signal is little affected by the presence of metals or liquids.
Ultra High Frequency (UHF)	433 MHz	Large reading distances of order of few meters and the RFID signal is affected by liquids and metals.
Super High Frequency (SHF)	2.45 GHZ	The reading distance is in order of 10's of meters.

- **Passive Tags:** These tags are generally energized by the electromagnetic waves of the reader and then utilize these electromagnetic waves to perform basic logical operations and respond to the reader. These tags thus have an unlimited life time. The reading

distance for these tags <5 meters [1]. These tags generally operate at a low frequency of range of few MHz and the read rate for these tags is low. A reader can simultaneously read only few hundred of them if they are static and very few even if they are moving at a very slow speed. These tags have limited memory resources order of few kilobytes and can perform only basic logical operations.

Tags can also be classified on the basis of operations they perform [3]. The **full fledged class** tags can perform complex cryptographic operations like hashing and public key cryptographic functions. These tags are widely used in E-passports. The **simple class tags** support less expensive operations such as random number generators and hash functions. This class tags do not support public private cryptography. The **lightweight class tags** only support simple random number generations but not the hashing functions.

Khan *et al* [4] published the classification of RFID tags based on their EPC global class structure. Table 3 shows the classification of RFID tags.

1.1.2 Classification Of RFID Readers

The RFID readers are classified on the basis of types of tags they intend to read data from. These are broadly classified as:

- **Active Readers:** These readers are basically used to read data from the active readers. These readers generally operate at higher radio frequency in terms of few hundred MHz or even few GHz. They are capable of reading large number of tags simultaneously. These are quite significant in cost when compared to passive readers.

Table 3 Classification Of RFID Tags

EPC Class	Definition	Programming
Class-0 Gen-1	Read Only, Passive Tags	Programmed by Factory.
Class-1 Gen-2	Write Once, Read many, Passive Tags	Programmed once by the user.
Class-1 Gen-2	Write Many, Read Many, Passive Tags	Programmed once by the user.
Class-2	Rewritable Passive Tags with extra functionality like encryption	Re-programmable
Class-3	Semi passive tags that support broadband Communication	Re-programmable
Class-4	Active tags that can communicate to other peers	Re-programmable

- **Passive Readers:** These readers are used to read data from the passive tags. These readers generally operate at a frequency of few hundred KHz to few MHz. These readers are capable of reading only few hundred static tags. These readers are relatively cheaper than the active readers.

Preradovic *et al* [5] provided a review on classification of RFID readers based on power supply, communication interface, mobility, tag interrogation, frequency response, supporting protocols etc. The readers can be classified as:

- Readers Supplied from the power network.
- Battery powered readers.
- Serial RFID readers.
- Network RFID readers.
- Stationary RFID readers.
- Handheld RFID readers.
- Unique frequency response readers.
- Non-Unique frequency response readers.

1.1.3 Challenges For RFID Technology

There are several challenges for RFID technologies that have made it difficult for its widespread acceptance. These include the transmission of information through wireless mechanism and non ability of the tags to perform heavy cryptographic operations due to severe resource constrictions thus resulting in a weak authentication process.

All these problems combined together pose a real challenge for the successful implementation of RFID systems. In most of the approaches, the researchers either exchange the keys for encryption or use a predefined static key for encrypting the data. In few of the proposed schemes, the researchers make use of the mechanism to dynamically generate the keys but it suffers from desynchronization problems.

We present a solution based on dynamic generation of keys through basic logical operations to encrypt the data being sent or received between the tag and reader or tag and the server. Also, for the authentication process between a reader and the server, we make a use of technique similar to the one being used in cellular networks. Our approach also presents the mechanisms to prevent

the desynchronization attacks which are a major area of concern in the event someone makes use of a dynamic generation of keys approach.

1.2 Organization of the Report

The second chapter gives a brief overview of the problems related with RFID technology. It is then followed by the literature review organized as the problem the authors tried to solve, their approach, advantages and limitations of their approaches.

The third chapter provides the detailed description of the proposed protocol.

The fourth chapter discusses about the implementation of the proposed protocol in java framework along with the screen shots of the simulation.

The fifth chapter provides the detail about the evaluation of proposed approach, its comparison with other approaches.

The report ends with advantages and the limitation of the proposed approach, concluding thoughts and a bibliography.

1.3 Summary

In this chapter, we gave an introduction of the RFID technology and discussed about the factors that led to its emergence and also the factors that are hindering its progress to be accepted for a widespread use.

CHAPTER 2: BACKGROUND AND RELATED WORK

2.1 Background

2.1.1 Issues With RFID

Apart from all the advantages, RFID systems suffer from several drawbacks which have raised doubts on widespread acceptance of this technology. The first one is that the whole communication takes place through a wireless medium. Thus any information exchanged is open to everyone. This information needs to be secured through cryptographic methods so that a legitimate resource can access this information.

Another problem is that the RFID tags especially the passive RFID tags suffer from severe resource constraints, i.e., in terms of memory as well as computational capability. They cannot perform any heavy cryptographic operations to secure the information they are sending out or any message they are receiving. This puts up a limitation on the tags to perform the authentication as well as encryption operations. The basic function of a passive RFID tag is that it will respond to any query by any reader. In such a scenario it becomes a top priority that only a valid reader should be able to extract any useful information from the tag. Furthermore, the powerful readers can sniff any information on the tags from a very large distance. This also increases the risk for the data at rest being exposed to the adversary. There is always a tradeoff between the security and performance of the RFID systems.

2.1.2 Attacks On RFID Systems

The RFID systems are prone to several attacks. Some of the well known attacks [6] are listed as follows:

- **Physical Layer Attacks:** These generally include attacks on RFID devices itself like permanent disabling the tags through Kill command. They also include temporary disabling through passive interference and active jamming. Apart from this it include physically removing the tag or destroying the tag. For the readers, they involve removal or destruction of readers physically and relay attacks on the readers.
- **Network-Transport Layer Attacks:** In these types of attacks, the adversary tries to find and exploit the weak link in the communication channel. For tags, it involves cloning or spoofing of the unique identifier of the tags. For the readers, these attacks include the impersonation of the rouge readers as valid readers and also they include eavesdropping on the information that is being exchanged between the RFID entities. These kinds of attacks also include the attacks on network protocol known as network protocol attacks.
- **Application Layer Attacks:** These kinds of attacks are generally launched on tags as well as application middleware. The common attacks include unauthorized reading of the tags, modification of data on tags through universal write commands. These also include attacks such as buffer overflow or malicious code injection, which are commonly launched on the Application Middleware.
- **Strategic Layer Attacks:** These attacks include Competitive Espionage, i.e., attacks by the rival competitor in the market, social engineering, i.e., unauthorized tracking of a person through RFID tags. It also includes threats to the privacy of an individual as well as specific targeted security breaches in a system.
- **Multilayer Attacks:** The common type of RFID attacks is not launched on a specific layer of a RFID system but it includes a group of layers so that an attack has a maximum impact and it should result in a total system failure. The common types of multilayer

attacks include attacks through covert channels, denial of service attacks, traffic analysis, crypto tacks, side channel attacks and replay attacks.

2.2 Literature Survey

In this section, we will present an overview of related research work that has already been done in the RFID field. For each research publication, we will first discuss the problem the authors are trying to solve, briefly discuss their proposed approach, and then it will be followed by the advantages and the disadvantages of the proposed approach.

Mubarak *et al* [7] present a review of the RFID system towards security, trust and privacy. According to them, most of the RFID work discusses security and privacy as two different solutions. Their approach presents security, trust and privacy as a one complete RFID solution. This also helped them to sort out the issues related with tag tracking and privacy of the data on the tag [7]. The combination of all the three approaches will help in protecting the data within the system, i.e., when the data is at rest and also when it's within the communication channels [7]. In their approach, they propose the use of a lightweight encryption solution such as modified AES [8] or ECC can be used to encrypt the data [7]. This will help in providing the security aspect of their proposed approach when the data is in motion through the communication channel. In order to provide the security to data at rest, they propose to make the use of Trusted Platform Module (TPM) [9] [10].

Based on their previous work [11] related to mutual attestation and integrity verification, the authors propose to provide the trust component of their proposed protocol. They make the use of process of Attestation which is similar to challenge response protocol between the platform to be

verified and already verified platform [7]. The TPM provides the integrity values that need to be verified.

The privacy part of the proposed approach is given by the use of anonymizer [12] [13]. An annonymizer is a device that annoymizes each tag id when it participates in the communication process. The published work is a first of its kind which has taken into account all the three aspects i.e. security, trust and privacy and presented them as a one solution. The major drawback with this approach is that they did not provide any kind of results or proof of concepts to support their claims. The discussed approach is a theoretical one and has not been implemented. The authors are taking up the best of the already available optimal solutions for each of security, trust and privacy and trying to come up with the optimal global solution. This approach does not always provide with the best solution.

Kim *et al* [14] proposed a lightweight RFID Authentication protocol with a new set of keys generated at each step of the communication process. The problem they tried to address is related to location tracking and user privacy. They make the use of AES for authentication. The symmetric keys are updated with each communication through Random Number Generator generated by the Tag, Reader and the Server. This results in a new set of keys for encryption for each communication. They have assumed that the communication channel between the reader and the server is safe where as the communication medium between the tag and the reader is assumed to be open to attack by the adversary. The proposed protocol is broken into two stages. The first stage is known as the initialization stage. The tag and the server have the same symmetric key at start. The reader and the tag have the same secret number and this would help the tag to authenticate the server.

This approach helps in mitigating several attacks such as eavesdropping, replay attack and location tracking. This is due to the random number generated through the Pseudo Random Number Generator. Since it is not possible to get the previous key and the key changes for new communication, it gets difficult to use the keys to get a pattern. Different messages are transmitted in each communication and also the tag identification is never sent in open. This approach is safe against tag tracking problem.

The major drawback of this approach is that it uses a static number 'm' across all the tags and the readers. This number helps the tag to authenticate reader through a simple encryption XOR operation. This number remains static throughout the life time of the system. If an adversary gets hold of this number, this will eventually lead to compromising the security of the whole system and eventually bring it down. Another problem with the proposed approach is that it suffers from the desynchronization attack. The random number generators are updated with each message assuming that other two entities will also update their random number generators in successive messages. The problem will arise if the message is lost during the transmission or an adversary blocks the messages from reaching the next entity. This will lead to desynchronization of random number generators between the three entities and they would not be able to decrypt the messages being received. This will result in failing to authenticate even a genuine set of readers or tags or both by each other.

Treck [15] *et al* proposed two non-deterministic light weight protocols for security and privacy in RFID systems. These proposed protocols are known as non deterministic because when a reader gets a response from a tag for a challenge, the expected values of the response are not unique nor discrete but they lie in an interval; this puts the calculation overhead on the reader and the backend system. The interval range is predefined and the tag and the reader share a same

secret numbers which remains static. The tag is assumed to store up to four different numbers. These numbers are basically the time stamps of the reader that has inquired the tag. These protocols are suitable for single as well as multiple tag environments. When the reader queries the tag, the tag computes the random number from the given time stamps and concatenates it with the secret number and sends it back to the reader. On receiving the message, the reader calculates the expected response from the given interval and compares the response with received message. If the match occurs, the tag is said be an authentic one.

In the second protocol, the reader sends out the challenge to the tag. The tag checks if the received message is already present in the list of stored numbers. If the challenge is a new one, the tag stores it in its stack, otherwise it is discarded. Based on the received challenge, the tag computes a random number Δr. This random number is basically the difference between any two stored numbers in a tag. It concatenates the obtained result with the already stored secret number s. This result is further XORed with Δr. The reader on receiving this message calculates Δr and then concatenates it with secret number s. This result is Xored with the range of $\Delta r's$ obtained from the set of timestamps the reader has already stored with it. The process continues until the match occurs.

The proposed approach helps in mitigating several well known attacks such as man in the middle, passive eaves dropping and the replay attack.

The major drawback with this approach is the use of time stamps. This is a serious issue if the different readers having different values of time stamps are used to query a same tag. These protocols will face serious issue if they are deployed in a multi tag and a multi reader environment. These proposed approaches may also suffer from a desynchronization attack. These approaches put up a lot of computational strain on the readers. This could potentially

decrease the performance in a scenario where several tags are read by the reader at the same time. Furthermore, the shared secret s remains static throughout the system i.e. it's same for all the readers and the tags. If an adversary gets hold of this shared secret, it will potentially compromise the security of the whole system.

Lopez *et al* [16] proposed an authentication scheme for a low cost RFID tags operating under the EPC global Framework. In 2006, EPC global and the International Organization for standards specified universal standards for low cost RFID tags [16]. The major concern with these specifications was that the security issues were not properly addressed. Konidala *et al* [17] tried to address this issue with their proposed scheme. But Lim an Li [17] [18] showed that a passive eavesdropping attack can be launched on this scheme and thus it could lead to the password recovery if the eavesdropping can be done through multiple sessions and the packets can be reverse engineered. Konidala *et al* [19] tried to mitigate the problem in the extended version of their protocol but it again failed for almost a similar kind of attack. Lopez *et al* tried to mitigate these problems in the third version of the protocol known as M^3 Authentication Protocol. This scheme is basically an extension of Konidala and Kim's scheme. The main focus of the new proposed approach is to provide mutual authentication between the RFID tag and the RFID reader. They have assumed the communication between the reader and the server to be secure. In this scheme they tried to introduce a mix bits function to enhance the security of their proposed scheme.

The proposed scheme is safe against the common attacks such as correlation attack, dictionary attack as well as tag killing attack.

Some of the drawbacks of this approach include sending out the EPC i.e. Electronic Product Code for the tag in open. This is not a good practice as it may lead to tag tracking. Thus it makes

this approach difficult to use in a scenario where there is a lot of emphasis on user privacy. This approach would be really ineffective in a case if user tag tracking is a real issue. The other attacks which it might be prone to includes replay attacks, offline as well as active brute force attacks as well as desynchronization attacks. The authors are aware of the problem with the tag tracking and emphasized that implementing the counter measures may result in higher costs. Another problem with this approach is that it generates a lot of random numbers. This might cause problems in a scenario where passive tags are to be used or there are severe resource restrictions. This is so because it would requires lot more memory as well as power resources to store and manipulate the stored data on the tag. This might in turn slow the performance of the system as a whole.

Sadeghi *et* al [13] proposed an anonymizer based security and privacy for RFID. The problem they are trying to address relates to inability of the tags to perform heavy cryptographic functions. Apart from a RFID tag, RFID reader and the backend server, their approach involves the use of another entity known as the anonymizer. These are the separate devices that are specifically designed to protect the privacy of tags and perform the heavy cryptographic encryption on the behalf of tags [13]. These devices basically take off the computational workload from the tags. This would help in use of better and more secure cryptographic operation for ensuring the privacy and security of the tag data.

The security analysis of the proposed approach shows that the scheme is able to authenticate the legitimate tags. The security analysis is implemented as a proof of concept and validated by the contradiction hypothesis. The proposed security scheme is robust against denial of service attacks. It achieves most of the security, privacy and functional requirements for a practical RFID system [13].

One of the major drawbacks that the proposed approach suffers from is that it opens up a whole new area of attack for the adversary. The adversary can now manipulate the communication between the tag and the anonymizer to corrupt the data. The authors have mentioned this flaw but did not discuss how to mitigate it. Another drawback is that this approach like the most of other anonymizer based approaches, requires the existence of honest anonymizers. Another drawback for the anonymizer based models is that these models could not be compared with each other. Thus an approach which appears to be secure under one scenario might not be as useful in the other scenario [13]. Thus these anonymizer based approaches provide solution only to a specific problem and thus cannot be generalized for a wide scope.

The main concept behind the anonymizer based approaches [20] [21] [22] [23] is that each tag stores the information which is basically an encrypted text. This text is encrypted using a public key of the reader and remains static. This static data can be eventually used to track the tags. This problem might limit the use of this anonymizer based systems in the scenarios where the privacy of the users are a top priority. Apart from all this, it would include a cost to introduce new entities i.e. anonymizer in the system. This would also put load on the backend system which might have to perform some redundant operations each time because the communication process will involve the use of anonymizer. Also in a large system, the scalability could be an issue based on the cost and the number of anonymizers required to implement the new system.

Qingling *et al* [24] proposed a new security scheme for mutual authentication to eradicate the flaws with earlier proposed solutions. The earlier approaches for the minimalist protocols either had security flaws or did not comply with the standards laid down by EPC CIG2 [24] . The proposed security scheme satisfied the system requirements for a low cost RFID system. It's a minimalist authenticating protocol which conforms to the standards laid down by the EPC CIG2.

The standards dictate that to be a minimalist authenticating protocol it should be a case of just a challenge and a response mechanism [24].

In the proposed approach, during the authentication phase, the reader sends a query to the tag which contains a random number. The tag responds to the reader with another random number. This reader computes a predefined equation based on the random numbers. If the equation holds true for the value sent by the tag, the tag is said to be an authentic tag. After that, using another predefined equation, the server sends a challenge to the tag. Using the challenge as a text, the reader computes a number through a predefined logic to check the authenticity of the server.

The proposed protocol is secure against the attacks such as spoofing attacks, replay attacks, tag tracking through eavesdropping on the communication. It is also robust against a denial of service attack.

The major drawback of the proposed approach is that it uses the two static parameters for the purpose of computation and authentication. These parameters are present in all the tags for a given system. If any of these parameters is exposed by an adversary, this could potentially compromise the security of the whole system.

Burmester *et al* [25] proposed a solution for a lightweight RFID authentication system. The main focus of the proposal relates to the privacy and integrity attacks on the RFID tags which result in compromising the security of the tags. The proposed protocol makes the use of lightweight cryptographic functions such as random number generated from the Pseudo Random Number Generator. The proposed protocol provides a mechanism that supports the session unlinkability [25]. The proposed protocol also complies with the EPC Gen2 platform and it could easily be implemented.

In the proposed solution, the tag and the backend server share a synchronized random number generator. The authentication takes place by exchanging 3 or optimally 5 consecutive random numbers that are generated through the random number generator. The randomness for the random number generator is periodically updated through a predefined mechanism. This mechanism is only known to the reader and when the probability of the random numbers generated by tag being compromised is higher than a certain threshold value [25] , the random number generator is refreshed.

The major security goals that the proposed protocol is able to satisfy are authentication and session unlinkability; for instance two interrogations of a tag cannot be linked to each other. This is made possible through the generation of the random numbers by a random number generator. The other security goals that the proposed approach satisfies include the forward and backward security of the tags. This implies that even if an adversary is able to get hold of the numbers generated by a random number generator through eavesdropping, the captured data should not make any sense to an adversary. This protocol is quite good with providing the randomness. There is a pool of random numbers generated for each tag. There is also a provision for refreshing the random number generator for each tag when it appears that it will compromise the security of the system.

One of the drawbacks of the proposed approach is that it requires a lot of data i.e. at least 5 numbers for each tag to be stored in the backend server. This will require a lot of space in a scenario if there are large number tags that need to be manipulated. Also this will create issues with scalability because it will require a large number of resources to be upgraded if more tags are needed to be added to the system. Another drawback of the proposed approach is that there is no mechanism for the system restore in case if some desynchronization occurs between the

random number generators of the tag and the back end server. If certain messages are lost or blocked on purpose by an adversary, the random number generators for the tag and the backend server might generate a different set of number and this will hamper in authenticating even a valid tag. This approach also suffers from man in the middle attack (integrity concerns) because all the random numbers for authentication are sent in open. If an adversary captures all these numbers and replay them to the backend server posing as a valid tag, there is no way that a backend server can distinguish a valid tag from a cloned tag.

Lethonen *et al* [26] proposed a solution for tag cloning through the use of synchronized secret. The novelty of this approach is that they make the use of a web server to update the shared synchronized secret for the tags. The solution is pretty effective in case of a low cost RFID tags. The tag is updated by a random number each time it is scanned by the reader. These random numbers are supplied by a backend web server. So when a cloned tagged is scanned by a reader, it would raise an alarm in the system about the cloned tag being scanned by the reader.

This approach is pretty effective in recognizing the tag cloning in a lost cost RFID systems deployed over a large area.

The main drawback this protocol seems to suffer from includes the real time delay for updating and then verifying the shared synchronized secret on the web server. This approach will have a serious performance issues especially related to time in a scenario where a reader has to read, verify and then update the synchronized secrets in a bulk such as in case of supply chain management. The issue that the back end server is a web server also brings into picture the place where the proposed system can be deployed. The proposed approach might suffer from serious time delays affecting the system performance. Also another drawback of the proposed system is in terms of scalability. It would require a large number of synchronized shared secrets for a large

number of objects and managing the shared secrets through the web server might become a problem over a period of time. This proposed approach is a prone to denial of service attacks. If a denial of service attack is launched, it might even cause a genuine trigger to raise an alarm even if there is no cloned tag. An adversary can read the tags and produce cloned tags and smuggle them into the system in order to cause unnecessary performance degradation of the system.

Dimitriou [27] proposed a novel idea of having a proxy framework for the RFID systems in order to enhance their security and privacy. In the proposed work, the proxy agent framework which makes the use of a personal device maybe a cell phone to enhance the privacy. This proxy framework will help the user in getting the more control on tags in a sense that it will regulate the release of information by the tag. Apart from this it will also help in controlling and authenticating the requests for information from the tags. The authors basically propose to make the use of a cell phone as a proxy to interact on the behalf of the tag, but there is a mechanism in place which allows only a legitimate user to put the tags under the control of a proxy device.

The security goal that the proposed approach is trying to satisfy is privacy, i.e., it should not be possible to locate a user or identify a user based on the tag. This goal is taken care of by the fact that there is no fixed or static information that is released by the tag which an adversary can eavesdrop on and use it to identify an individual. By providing a control on information release, the proxy helps in satisfying this security goal. In order to prevent a malicious user to issue commands to the tags, the authors have proposed a use of a secret key to validate and issue the commands to the tag. The secret key inside a tag also prevents the tag from being cloned by an adversary. The use of a proxy in a form of a cell phone also helps in enforcing the policy and access controls.

The main drawback of using a proxy in the form of cell phone is similar to use of an anonymizer [13] based approach. This would open up a new area of attacks on the area on communication between the tag and the proxy. There is no way to identify a legitimate proxy device. An adversary can eavesdrop on the communication between the proxy and other entity and then can relay the same information to the other entity. There is no way for the other entity to distinguish between a legitimate and a rogue proxy device. Apart from this there are also issues related to the cost to incorporate the new device and it would put an unnecessary load on the backend server as it would have to perform redundant operations related to the proxy.

Osaka *et al* [28] proposed a scheme for RFID security. They proposed to store the tag id in the server and only provide the tags with the encrypted tag id. The reader sends out a random number along with a query to the tag. The tag on receiving the query performs a logical Xor operation on the random number and a hashed tag id and sends the result to the reader. The reader sends the received result along with the random number to the server. The server performs the authentication for the tag and the reader and then sends backs the information about the tag to the reader.

This scheme provides an advantage of securing the tag ids and thus preventing the unauthorized tracking of the tags. It is quite useful in a scenario where preserving the privacy of the user is very important.

This scheme suffers from a drawback of suffering from denial of service attacks.

We summarize in table 4 the papers that are pertinent to this thesis.

Table 4 Summary Of Papers

Title	Focus	Advantages	Drawbacks
A critical review of RFID systems towards security trust and privacy [7].	Security based on an encryption solution such as AES or ECC or any light weight type of encryption. Trust based on their previous work i.e. the use of Tpm to provide integrity value which can be verified by a remote party. Privacy based on the concept of Anonymizer and Tpm which provide security to data at rest.	The first work of its kind in which they have summarized Security, Trust and Privacy in one research work.	No proof of concept to validate their claims. No tests results to prove their claims of novel system. A set of local optimum solutions does not always gives you a general optimum solution.
Non-Deterministic Light Weight Protocol for security and privacy in Rfid environments [14].	Takes into account the authentication between the tag and the reader.	Helps in mitigating several attacks such as Man in the middle, passive eaves dropping, reply attack.	Uses the time stamp from the reader for challenging the tag which could cause issues if several different readers are used. This could suffer from a de synchronization attack. Puts a lot of strain on the reader for performing calculations. This could potentially decrease the reader performance if it has to read many tags at the same time. The shared secret and the number n are static and potentially could lead to compromising the whole system.
A lightweight Rfid Authentication Protocol using step by step	Takes into account the authentication between the tag, the	Helps to address the issues relating to eaves dropping attack, replay	Uses the static number m in all the three entities. If that is

Symmetric Key Change [15].	reader and the server.	attack and the location tracking. Uses the new key for encryption for each communication which is secure for communication.	compromised it will bring the downfall of the whole system.
Providing stronger Authentication at a low cost to Rfid tags Operating under the Epc global framework [16].	The authentication is between the tag and the reader. It doesn't take into account the backend server.	The new approach tries to mitigate the attacks such as correlation attack on the previous versions of the protocol.	The tag sends its unique Epc number in the open which could lead to tracking of the tag and give arise to a privacy issue. This generates lot of random numbers and puts a lot of calculation strain on the reader and the tag and it may cause some problems if the reader has to read tags at the same time.

2.3 Summary

In this chapter we discussed the problems with the RFID systems, limitations or the resource constraints with the tags and the threats the current systems are facing. In the literature review section, we critically analyzed the research work done in the field so far which included the problems the researchers are trying to address, the advantages offered by their approach and the drawbacks or the attacks the proposed approaches are susceptible. These problems discussed in this chapter forms the basis for the motivation for our proposed work.

CHAPTER 3: PROPOSED SECURITY SCHEME

3.1 Motivation

In a typical RFID system setup, the messages are exchanged over a wireless medium and the tags are not able to perform heavy cryptographic operations. The major challenge is to secure the information being transmitted over the wireless medium and yet apply very basic encryption schemes. The information is transmitted in the air over a wireless medium. Thus it is open to adversary for interception and manipulation. Also the limited resources with the tag forbid us to apply heavy cryptographic operations to encrypt the data being transmitted. With the hand held readers becoming popular in use, it opens up new area of research as well as attacks as the information is being transmitted over the wireless medium. The use of trivial public private key cryptosystems is one of the viable solutions but it generally compromises the performance at the expense of providing security.

Moreover with most of the schemes discussed in literature review either assumed the existence of wired stationary readers or assuming reader and backend server as one entity or simply assuming the communication between the reader and the server is secure. The encryption scheme involving the tags lagged from any scheme that provides dynamic key updating with every frame being transmitted. Most of them advocated the use of a static pre-shared secret number to encrypt the data using the simple logic operations. It is not a good idea in a long run because if an adversary gets hold of the secret number, it may compromise the security of the whole system. If any of the schemes discusses the use of dynamic key generation techniques, they suffer from a specific type of attacks known as desynchronization attacks where if some of the messages are

blocked by the adversary, the dynamic key generators tend to go out of sync and hence putting the whole authentication mechanism out of order.

The problem of exchange of messages with the keys for encryption, inability of the tags to perform complex operations, assumptions for the readers to be static and wired, lack of techniques to dynamically update the encryption keys and not to suffer from desynchronization attacks are few of the limitations of the current techniques.

3.2 Objectives

With the above stated limitations of the existing techniques, we present you a security mechanism that will focus of the following goals:

- Fast and efficient authentication between the tag and server and the reader and the server.
- No key exchange for encryption.
- Independent generation of keys.
- Automatic updating of keys with each new frame.
- Randomness with each set of newly generated keys.
- Robustness against the desynchronization attacks.

Apart from the above goals, the proposed scheme should also satisfy the following security goals:

- Confidentiality i.e. no spoofing of the data.
- Non-Repudiation i.e. source cannot deny sending of a message later.
- Forward Secrecy i.e. one should not be able to derive future keys from previous keys.

3.3 Proposed Security Scheme

In this chapter we will discuss in detail the proposed security scheme and the assumptions involved for our security scheme to work efficiently. The proposed scheme has two parts; the first part involves the authentication between the reader and the server. This authentication process is based on the concept similar to the SIM card authentication in a cellular network. The second part involves the authentication between the tag and the server which involves the already authenticated reader helping in exchange of the messages between the tag and the server. This chapter also discusses in detail the key generation mechanism for authentication and encryption between the reader and the server and also between the tag and the server. Apart from this, this chapter focuses on the overall working of the proposed protocol, pseudo code for various mechanisms applied for encryption, authentication and key generation.

3.4 Assumptions

In this section, we will discuss about the assumptions regarding the functionality of the tag, the reader and the server.

- The tags, the readers and the backend server are preloaded with the data before implementation of the RFID system by the manufacturer.
- The pre loaded information for the tags include their tag id, pattern for query message, synchronized pseudo random number generator. This implies that it would have the same seed value for random sequence generation as provided for the corresponding tag id to the server.
- The pre loaded information for the readers include their reader id and a set of authentication vectors.

- The pre loaded information for the servers include tag ids, hashed tag id for the corresponding tag id, reader ids, for each tag id the corresponding value of seed for random sequence generation, reader id and for each reader id the corresponding hashed reader id.
- The tags are able to store one 64 bit key.
- The tags are able to perform simple logical operations such as AND, NOT, OR and XOR.
- The tags are able to perform simple one way hashing operation known as R-XOR i.e. Rotation with XOR.
- The tags are able to perform simple concatenation operation as well as simple comparison operation for the received messages.
- The readers are capable of performing hashing operations such as SHA-1 and SHA-256.
- They are capable of performing heavy encryption operations such as DES or triple DES.
- They are able to perform simple logical operations such as OR, AND etc.
- The message exchange and the operations involving a tag are mostly 64 bit while with the reader they are 128 or 256 bits.
- The backend server holds the information about each object being tagged by the RFID tag and able to perform basic logical operations such as OR, AND, NOT, XOR. Also it is able to perform basic as well as complex encryption and hashing operations.
- The backend server is assumed to be a genuine and safe entity.

3.5 Proposal

3.5.1 Overview

A typical RFID system consists of the objects tagged with RFID tags: a reader to read the information on the tags and the backend server which stores the information about the objects being tagged. In an ideal scenario, the reader reads the tags on the objects; the information (a number) is transmitted from the tag to the reader via wireless medium. The reader forwards the information from the tag to the backend server. This number acts as a unique key to the information in the database about the object. The server verifies the information and sends it back to the reader.

In our proposed approach, the server first authenticates the reader, the authenticated reader then interacts with the tag and with the help of already authenticated reader, the server then authenticates the tag. After authenticating both the entities, the server releases the information about the tagged object to the reader. The figure2 presents an overview of the messages being generated by the tag, reader and the backend server and it also depicts the flow of the messages in the proposed security scheme.

3.5.2 Authentication Between The Reader And The Backend Server

The reader is preloaded with a set of authentication vectors. These vectors are nothing but a randomly generated sequence of 128 bit numbers. The length and the number of vectors may vary from scenario to scenario in which the RFID system is implemented. It is a tradeoff between security and performance.

The information on a reader can be represented by following equation:

$$R = \{R_{id}, AV\{AV_1, AV_2, AV_3, \ldots\}\} \quad \ldots.(1)$$

where,

R_{id} is the reader id.

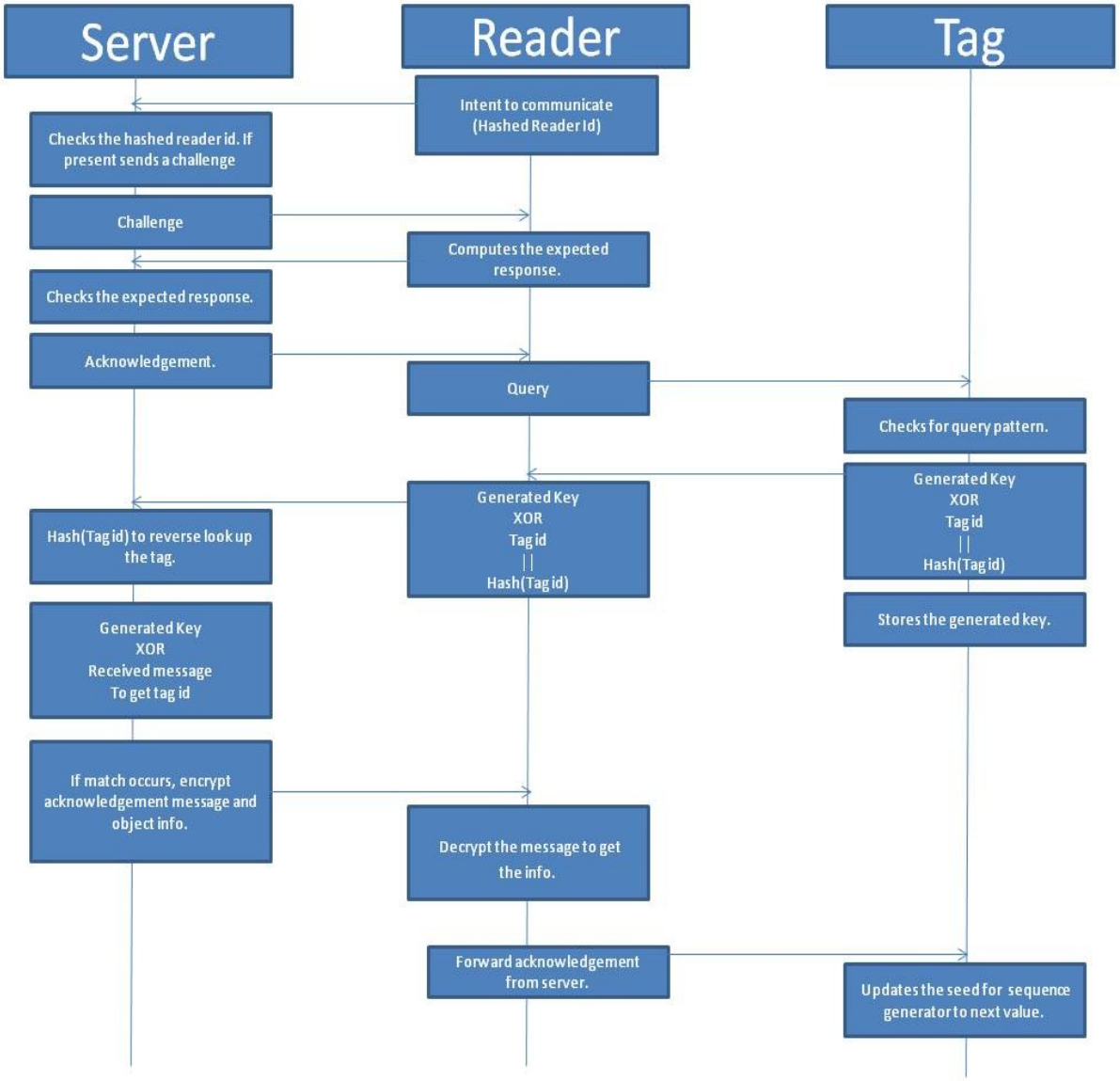

Figure 2 An Overview Of The Proposed Security Scheme

AV represents a set of authentication vectors.

AV_i represents the authentication vectors itself.

The authentication mechanism involves the following steps:

- The reader hashes its reader id using any of the available hashing techniques (SHA-1 or SHA-256) and sends it over to the server.
- The server on receiving the hashed reader id compares it with the set of all hashed reader ids. If the match fails the server does not respond.
- If the match occurs, corresponding to that reader id, the server randomly chooses two authentication vectors from a set of authentication vectors to challenge the reader. The same authentication vector set is available with the reader. The server then waits for the expected response.
- The server concatenates both the authentication vectors and sends them to the reader.
- On receiving the vectors, the reader checks if the authentication vectors are present in its' own vector set and then proceeds to compute the expected response. The expected response is a set of logical operations with the two authentications vectors received as a challenge and the reader id. The figure3 depicts the expected response generation.
- The reader then sends the generated expected response to the server.
- The server verifies the expected response and if the match occurs, authenticates the reader. If the match fails, the server flags the reader as rouge.
- The server sends an acknowledgement message to the reader which is a signal that it may start the tag querying process.

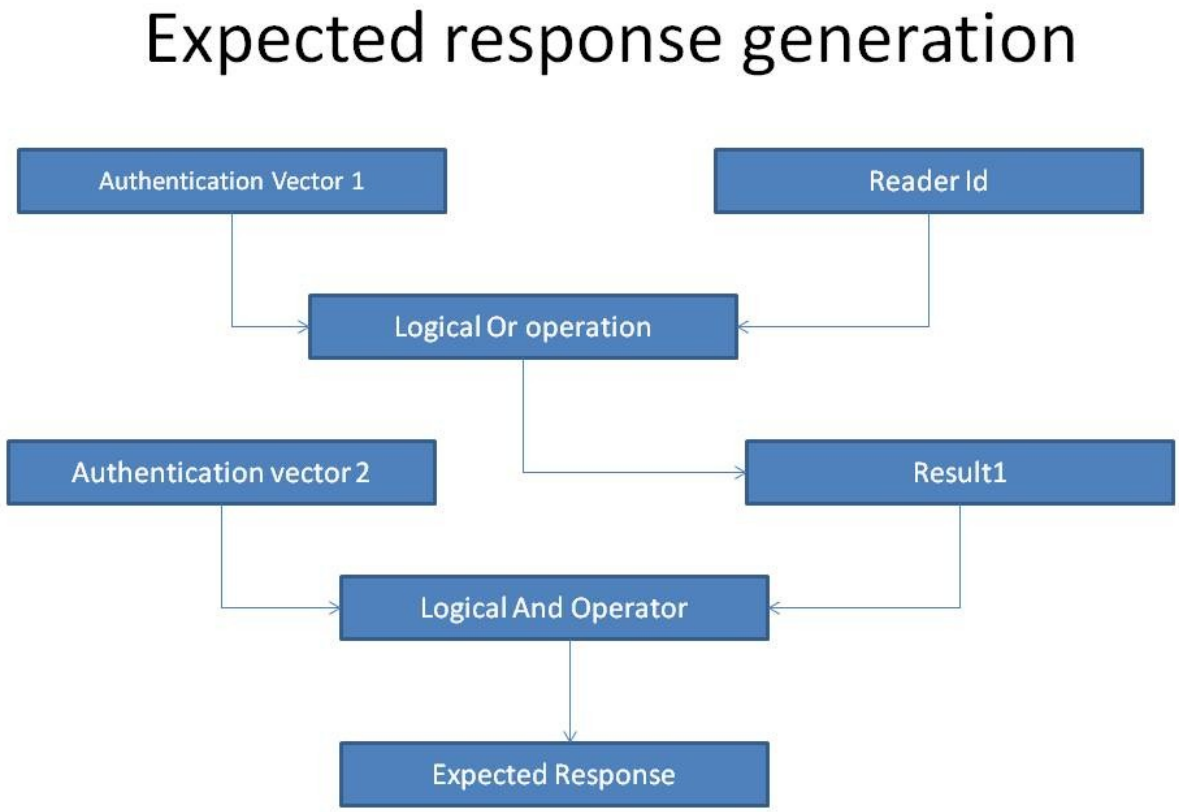

Figure 3 Expected Response Generation Mechanism

Table 5 Algorithm For Expected Response Generation

Algorithm: Generate Expected Response
Input: Authentication Vector1, Authentication Vector 2, Reader ID Output: Expected Response Process: Authentication Vector1 **OR** Reader Id : Result1 Authentication Vector 2 **AND** Result1: **Expected Response.**

Table 6 Algorithm For Reader Authentication

Algorithm: Authenticate the reader

Input: Encrypted Reader Id, Authentication Vector set, Reader Id
Output: success (if reader is authentic)
Fail (if the reader is rogue)
Process: For a Reader R,
Encrypt Reader id using one way Hashing Function (SHA-1 or SHA-256).
After receiving message for reader, For all readers: 1 to n
{
If (encrypted reader id == one in the records)
Send a challenge()
Else
Terminate the connection
}
Send a challenge()
{
Randomly choose two authentication vectors, concatenate them and send them as Challenge reader ().
Wait for Expected_Response()
}
Challenge Reader()
{
Checks for authentication vectors with its own set.
Compute the Expected Response and send it to the server.
}
Expected_Response()
{
Checks if the expected response matches.
If the match occurs, reader is valid.
Else
Reader is rouge.
}

3.5.3 Use Of Authentication Vectors

The Authentication vectors help to provide randomness to the response generation mechanism and enhance the security of the RFID system as a whole. The concept of sending out two Authentication vectors instead of one also helps in generation of the expected response in a more

secure way as it assists in the application of a greater number of operations. The Authentication Vectors are sent as a whole and not as partial parts as it is done in the original 3G Cellular Network Scheme. This is done because if we use a large key length of around 512 bits and the number of readers are also high, this would render it difficult to generate the unique Authentication Vectors in which there is little similarity in the bit pattern. Suppose if we send only a 16 bit or 32 bit part of an Authentication Vector, the chances are high that the bit pattern could match with two or more Authentication Vectors. Another reason is that it would take more time to compare and then verify the small bit patterns with original Authentication Vectors.

The numbers of Authentication Vectors for the purpose of simulation are kept at 10. The number of Authentication Vectors may vary depending on the scenario in which the proposed scheme is implemented. It would be a tradeoff between the security and the performance if we use higher number s of Authentication Vectors. There would be a time overhead involved in comparing and verifying the Authentication Vectors.

3.5.4 Authentication Of Tag

The tag is preloaded with its tag id and seed for the random number generation. The bit length of this information may vary depending on the type of the tag.

The information on the tag can be represented with the help of the following equation:

$$T = \{T_{id}, Seed, Pattern\} \quad \text{....(2)}$$

where,

T_{id} represents the Tag Id

Seed represents the seed value for the Random Sequence Generator. The value of this seed is in sync with the corresponding value in the server for a given tag id.

Pattern represents the pattern of a query message.

The authentication mechanism involves the following steps:

- The authenticated reader sends out a query message to the tag.
- The tag verifies the pattern of the query message and if the pattern matches, goes on to key generation process to encrypt the tag id. The figure 4 depicts the key generation mechanism.
- The tag encrypts its tag id with the generated key and proceeds to compute the hash of its tag id. The figure4 depicts the hashing process.

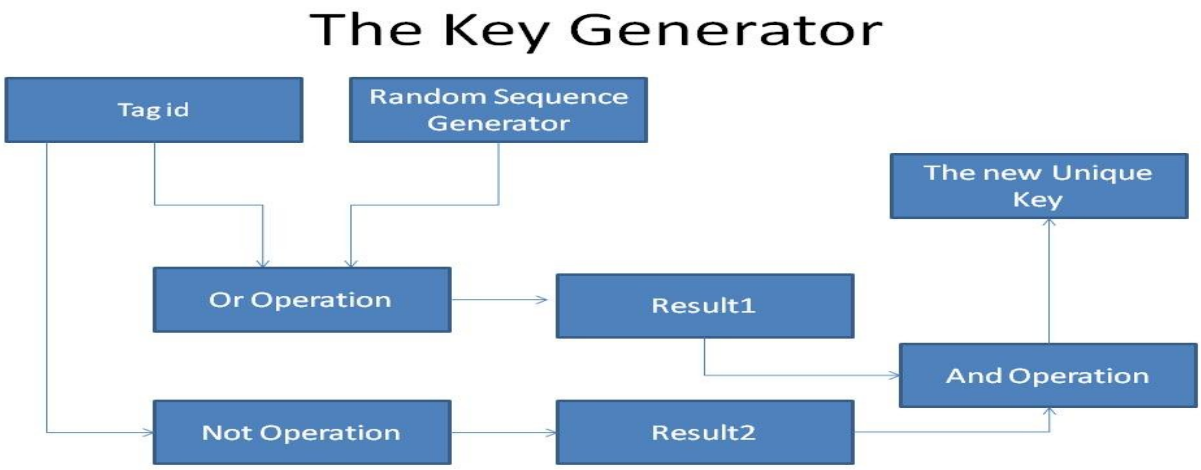

Figure 4 The Key Generation Mechanism For The Tag

- The tag then stores the generated key for encryption in its memory.
- The tag concatenates the encrypted tag id and the hashed tag id and sends it back to the reader.

Table 7 Algorithm For Key Generation For The Tag

Algorithm for Key Generation
Input: Tag Id, Sequence for a random Sequence Generator. Output: A new Unique Key for Encryption Process: Tag Id OR Random Generator Sequence: Result1 Tag Id NOT Operation : Result2 Result1 AND Result2 : **A new Unique Key**

Table 8 Algorithm For Hashing Of Tag Id

Algorithm for Hashing The Tag Id

Input: Tag Id, Initial value of Message digest (MD), size of block (m)
Output: Message Digest of the Tag Id.
Process:
Partition the Tag Id into m-bit block sizes.
Set the initial value of MD to all zeros.
For each small message block
{
Perform 1-bit circular left shift of the Message Digest.
XOR the block with current value of Message Digest.
}

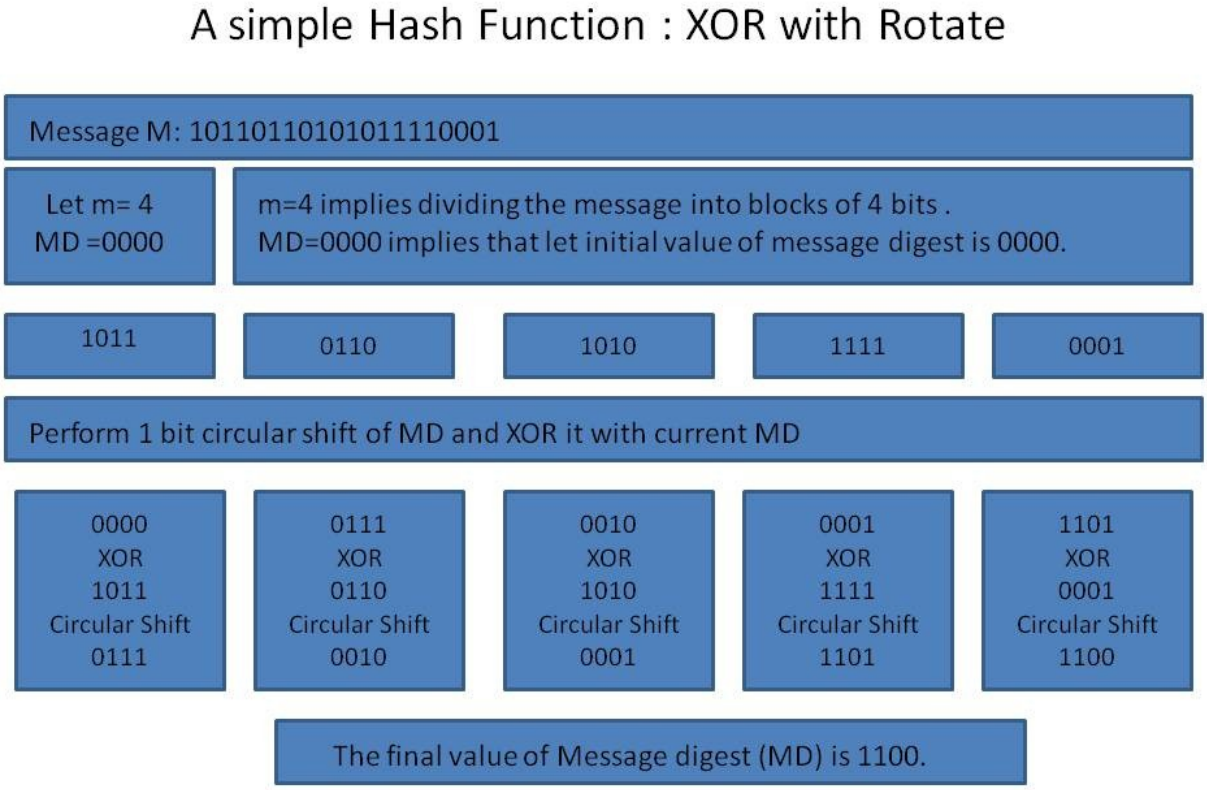

Figure 5 Hash Generation For The Tag Id

- The reader forwards the received message to the server.
- The server on receiving the message gets the hashed tag id part of it and compares it with the already stored values of hashed tag ids. If the match does not occur, it discards the message.
- If the match occurs, the checks for the corresponding tag id. It uses the value of the seed generator to generate the random sequence and proceeds to generate the encryption key through same mechanism as of the tag.

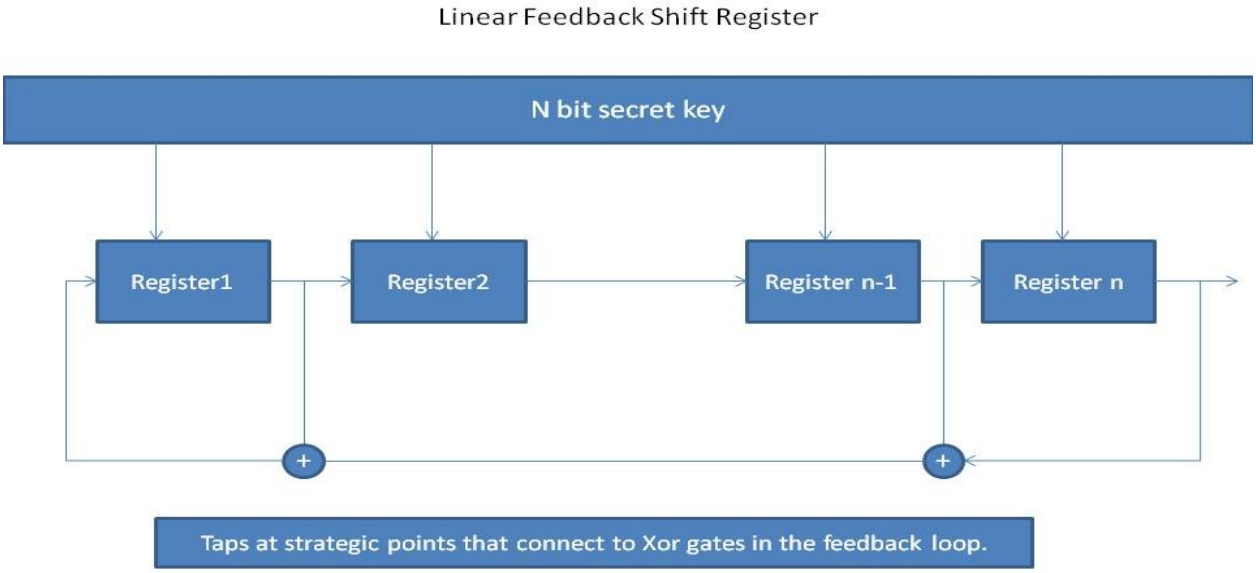

Figure 6 A Generic Overview Of A Random Sequence Generator

- It then uses the encryption key to XOR the encrypted message to get the original tag id. If this matches with the stored tag id, the tag is said to be authentic.
- If the match does not occur, it uses the previous value of seed generator to generate the random sequence and then generate the encryption key. If the match occurs, the server flags that there is some problem because the random sequence generator for the tag is not being updated. The tag is labelled authentic after the second attempt. If the match still does not occur, the tag is not authentic and the value of seed gets set to the original value.
- If the tag is authentic, the server proceeds to compute the acknowledgement message. The acknowledgement message is a unique message which is product of logical OR operation between the tag id and the last key generated by the tag.

- The server then gets the information about the object which is tagged with this particular tag. It encrypts the acknowledgement message along with the information about the object and sends it back to the reader. This encryption depends on the type of algorithm being used between the reader and the server. The algorithm can be DES or triple DES.
- The reader receives the message and decrypts it. It keeps the information part of the message and forwards the acknowledgement part to the server.
- The tag on receiving the message computes its own acknowledgement message and compares it with the received message. If the match occurs, it updates its random sequence generator to a new value for sending out the next message. If the match fails, it keeps the random sequence generator in the previous state.

Table 9 Algorithm For Tag Authentication

Algorithm for Authenticating the Tag

Input: Tag Id, Sequence for a random Sequence Generator.
Output: Success (if the tag is authentic).
Fail (if the tag is rogue).
 	
Process:
Reader sends query to the tag.
If (query message == stored pattern for query message)
{
Accept the query message.
Compute_ message_ to_ send ().

```
}
Else
Discard the query message.
Compute_message_to_send ()
{
Key = Key_Generator ().
Result2 = Hashing_Function ().
Result1 = Key  XOR TagId.
Send Result1 || Result2.
}
```

The server on receiving the message separates the message and checks for the message digest

```
For all tags
{
If (message_digest == saved message digest)
{
Check_the_tag (Remaining Part of the message).
}
Else
{
Dicard the message.
}
}
```

```
Check_the_tag (Remaining Part of the message)
{
Temp = remaining part of the message.
For the corresponding tag id,
Result 1=Key_Generator ().
Result2 = Result1 XOR Temp.
If (Result2 ==Tag Id)
{
The tag is authentic.
Compute_message_to_send.
}
Else
{
Set the value for the seed to random sequence generator to the previous value and
Generate the key.
Temp = remaining part of the message.
For the corresponding tag id,
Result 1=Key_Generator ().
Result2 = Result1 XOR Temp.
If (Result2 ==Tag Id)
{
The tag is authentic.
Compute_message_to_send().
```

```
}
Else
{
The tag is not authentic.
}
Compute_Message_to_Send ()
{
Result1 = Compute_Acknowledgement_Message()
Result2= The information about the object being tagged.
Encrypt Result1 || Result2 and send it to the reader.
}
Compute_Acknowledgement_Message()
{
Temp = Key_Generator ()
Tagid OR Temp.
}
```

3.6 Summary

In this chapter, we discussed the working of proposed scheme is detail, the algorithms used to generate keys for encryption and also the algorithms for authenticating the entities.

In the proposed scheme the server authenticates the reader first and then with the help of authenticated reader, it authenticates the tag. The key generation for authentication is independent and there is no exchange of keys involved.

CHAPTER 4: IMPLEMENTATION OF PROPOSED PROTOCOL

4.1 Implementation Details

In this chapter, we will present the implementation details for various functionalities of the proposed protocol. The proof of concept for the proposed protocol framework is implemented using the program language Java. It is considered a good language to implement the prototypes especially for the cryptographic systems because it has several built in packages such as java.security package. We ran the simulation on a **Dell XPS** machine with 6 GB RAM and a core i7 Intel processor.

The functionality for the tag, reader and the server are represented by the three different files named tag.java, reader.java and server.java. Each file has a detailed description implementing the related functionality for the individual entity. The value for the seeds for Random Number Generators (for each tag and the corresponding tag id with the server) is maintained in the text files. We have assumed the presence of light weight tags capable of performing simple hash operations. We have kept the messages involving the tags as 64 bit messages while the messages involving the readers as 128 bit messages.

4.1.1 Generation Of Tag Id And Reader Id

The tag ids and the reader ids for the implementation purposes are generated with the help of a Random function available with the **java.security package**. These numbers are stored as the corresponding hex values using the variables of the **BigInteger class**. For implementation purposes, the length of the reader id is kept as 128 bits and for the tag; it is kept as 64 bits.

4.1.2 Hashing Function For The Reader

The hashing function for the reader is implemented using an inbuilt class in the java.security package. The class provides a variety of options to choose from for the hashing algorithms such as SHA-1, SHA-256, SHA-512 etc. For the implementation purposes, we have used the SHA-256 algorithm for hashing the reader ids.

4.1.3 Hashing Function For The Tag

As already mentioned in the proposal part, the tag uses the simple hashing algorithm known as R-XOR (Rotate with XOR). So the programmatic implementation for the proposed algorithm is done as there was no available package in the Java language. For the implementation purposes, the length of the message digest is kept to 4 bits.

4.1.4 Authentication Vectors Generation

The authentication vectors used in the process of reader authentication by the server are generated in a similar way as the reader and the tag ids. We made the use of a Random function available in **java.security package** which takes as an input the seed value and also the size in bytes of the resultant number to be generated. For the implementation purposes, the length of authentication vectors is kept to be 128 bits. The number of authentication vectors is kept to be 10.

4.1.5 Random Sequence Generation

For generating the random sequence, we made the use of an inbuilt Secure Random class and its corresponding functions available in the **java.security package**. This class is capable of generating random number up to 64 bit in length. The value for the seed to generate the next

number in the random sequence generation is updated and maintained using the text files. The initial value for each seed is randomly assigned and is in sync with the corresponding tag id on the server side.

4.1.6 DES Algorithm Implementation

For the purpose of encrypting the final message between the reader and the server, we have made the use of DES encryption algorithm. This algorithm is only used as a proof of concept. It could be substituted by any other algorithm. There is an inbuilt package available with Java known as **javax.crypto** which facilitates the use functions related to DES algorithm for key generation and encryption.

4.1.7 Sample Run Of The Implemented System

The following table will present a sample output run for the implemented system. This includes one complete authentication cycle for the tag and the reader until the final message is delivered to the reader and the tag receives the acknowledgement message (updating the seed value for the random sequence generation for the tag).

Table 10 Sample Run For The Proposed Protocol

Sample run of the implementation of proposed protocol
Sending out encrypted reader id #_õ¬˜?õkÉQF½¸½I_šã±^:‰_[žXÅCÇD”Ñ Message recieved by the server: #_õ¬˜?õkÉQF½¸½I_šã±^:‰_[žXÅCÇD”Ñ Processing..... Initial Reader Id Match Found for the Reader With reader Id :1eaf82d6a855979c632a6b8b4d78a0fa Server Sending Field1 (128 bit) and Field2 of an Authentication Vector (128 bit):fbc664d75c8bbccf535cf953e083e721db30384984668b231f9cc8a03fcf4d 21 Message received by the reader:fbc664d75c8bbccf535cf953e083e721 db30384984668b231f9cc8a03fcf4d21 Reader found a match for given fields of authentication vectors:fbc664d75c8bbccf535cf953e083e72 1 & db30384984668b231f9cc8a03fcf4d21 The vector fields are located at index:-1 of the arrays for corresponding vectors Proceeding to Compute Expected response (128 bit) and send to server Reader sending the expected Response:fb4620574c03a887135cc812a08367 21 Message Received by the server:fb4620574c03a887135cc812a0836721 Message computed by the server:fb4620574c03a887135cc812a0836721 The match occurs and hence reader is Authentic Send Acknowledgement to the reader:ffffffffffffffffffffffffffffffff The message received by the reader is:ffffffffffffffffffffffffffffffff The message is valid Sending the query to tag Send a query to the tag(64 bit message):0101010101010101 Query Received by the tag:0101010101010101

```
 The Query Message is valid
 Computing the message to send to the reader
 The random number from Prng:1128768505678981433
 The final generated key for encryption by the
 tag:9008202769287441
 1137990206910443690 1146998409679731131
 The message digest for the tag:81578
 The final message sent from
 tag:1146998409679731131181578messagelength:24
 store the previous key
 Reader forwards the message received from the tag
 to the server:114699840967973113181578

Message received by the server:114699840967973113181578
reverse look up hashed tagid
The message digest for the received message:81578
The encrypted tag id for the received
message:1146998409679731131
The random number from Prng for the
server:5578513376091869413
The final generated key for encryption by the
server:4620702338652864581
The tag id generated by the server:5749685717250701822
The tag has failed authentication for first time
The random number from Prng for the
server:1128768505678981433
The final generated key for encryption by the
server:9008202769287441
The tag id generated by the server:1137990206910443690
The tag is authentic
Computing final message to send
15milliseconds
This field contains the info about tag7
The final message from the
server:VlM/ynxuy5Y4eDnokGBCD6rM6pGBRhzgjm+qLE7ewlI2kBUrrJf4
cMRJr0pWfLSFA7i5PP1PBFAI
YhqsIeyCSQ==
The final message from the
server:VlM/ynxuy5Y4eDnokGBCD6rM6pGBRhzgjm+qLE7ewlI2kBUrrJf4
cMRJr0pWfLSFA7i5PP1PBFAI
YhqsIeyCSQ==
snap the details and forward the acknowledgement to the tag
The information for the tag:This field contains the info
about tag7
Acknowledgement accepted updating the key generator
```

4.2 Summary

In this chapter, we discussed the implementation details of the proposed security scheme. The proof of concept is implemented using programming language Java helped in understanding the working of the proposed security scheme in a better way. This also helped in re designing some of the security aspects that were overlooked during the design phase. This part also helped to strength the way certain functions in key generation were performed.

CHAPTER 5: EVALUATION RESULTS AND ANALYSIS

In this chapter, we will present the results obtained through running the simulation of the proposed protocol in Java framework. The results for the memory or resource complexity would be generic. It implies that based on the type of tags or the readers, the resource complexity may vary through the different scenarios. We also present the detailed performance as well as security analysis of the proposed scheme. We discuss about the limitations that the evaluation in the simulated environment presents when compared to the real network scenario. We conclude this chapter by presenting the comparison of our proposed scheme with some of the already existing schemes.

The proposed scheme is evaluated for the following parameters:

- Performance Evaluation.
- Security Evaluation.

5.1 Performance Evaluation

Performance of the security scheme generally depends on the utilization of resources for its functionality. In this evaluation technique, we evaluate the security scheme based on the number of logical operations it requires and also the memory space needed to execute these operations. This would help in evaluating the computational complexity of the scheme and also helps inestimating the impact of the complexity on the performance of the scheme.

5.1.1 Computational Analysis

The tables below will present the operations and the number of times each operation (frequency) required to be performed (for one full authentication cycle) by the reader and the tag for the successful functionality of the proposed scheme. The operations listed in table 11 are performed depending on the key generation mechanism adopted by the tag. In a scenario, if the tag has successfully received the acknowledgement message and updated its seed value for the random number generation to the next value, it will perform all the operations. In a case if the tag has not received the acknowledgement message, and it gets a query from the reader, it will not go through the process of key generation but it will make the use of the previously stored key. In that case the operations related with the key generation will not be performed. The total number of operations performed in this scenario will be 5. These operations are performed whenever a reader queries a tag.

The table 13 will provide a generic overview of the memory requirements for the reader for the implementation of this scheme.

The table 14 will present a generic overview of the memory requirements for the tag and required for implementation of the proposed security scheme. N represents the size of keys in bits either 64 bits or 128 bits and m represents the size of the message digest. The memory requirement will also depend on the number of operations performed by the tag. The number of operation performed by the tag in turn depends on the condition if it has received an acknowledgement message from the server.

In a scenario, if the tag has received the acknowledgement message, it will perform all the operations. If the tag has not received the acknowledgement message, then the tag will not perform the operations related to key generation and it will proceed to message encryption by

using its previously stored key only. For this particular scenario, the memory requirements will be lower as compared to the amount of memory that is used in a typical authentication scenario.

Table 11 An Overview Of Number Of Operations For The Tag

Serial Number	Logical Operations Performed By the Tag	Frequency
1	Random Number Generation	1
2	Logical OR	1
3	Logical NOT	1
4	Logical AND	1
5	Logical XOR (Encryption)	1
6	Mathematical Hash	1
7	Concatenation	1
8	Comparing Acknowledgement	1
9	Comparing the query message	1
Total Number of Operations		**9**

Table 12 An Overview Of Operations Performed By The Reader

Serial Number	Logical Operations Performed By the Reader	Frequency
1	Hashing its reader id	1
2	Comparing Authentication Vectors	2
3	Logical OR	1
4	Logical AND	1
5	Decryption	1
	Total Number of Operations	**6**

Table 13 An Overview Of Reader Memory Requirements

Serial Number	**Data on the Reader**	**Memory Requirements**
1.	Authentication vectors	N x m
2.	Result1 (Logical OR)	N x 1
3.	Result2 (Logical AND)	N x 1
4.	Hashing	Algorithm Dependent
5.	Final Decryption	Algorithm Dependent
	Total	N x m + 2N + 2 AD*

** AD=Algorithm Dependent.*

Table 14 An Overview Of The Tag Memory Requirements

Serial Number	Data on the Tag	Memory Requirements
1	Tag Id	N x 1
2	Random Number	N x 1
3	Result1 (Logical OR)	N x 1
4	Result2 (Logical NOT)	N x 1
5	Result3 (Logical AND)	N x1
6	Result4 (Encryption (Logical XOR))	N x 1
7	Hashing	2N + N/m + 1
8	Final Message to send	N + N/m
9	Pattern for query message	N
10	Storing Final Key	N
11	Flag Bit	1
	Total	11N+ 2N/m + 2

If we use **64 bit** keys, and message digests as **4 bits** for the tags, the total memory required would not be more than **738 bits**. Furthermore, if we use **128 bit** keys and message digests as **4 bits,** the total memory required would not be more than **1474 bits**.

If for the readers we make the use of the **128 bit** key length and **10** authentication vectors, the memory required to store the initial information and the intermediate results would be **1536 bits**. For **256** bit key length and **10** authentication vectors it would be **3072 bits**. For **a 512 bit** key length and **10** authentication vectors, it would be **6144 bits**. Apart from this memory space, there would be an additional requirement of memory for the implementation of hashing the reader id and final decryption of message from the server. This would totally depend on the type of algorithm used and it would be the order of few Mega Bytes. The readers now days are quite powerful in terms of memory as well as computational capabilities. So it would not be an issue to implement the proposed scheme with the readers.

5.1.2 Time Analysis

The figure 5 presents an overview of the time analysis for the proposed security scheme. The time analysis is done by running the proposed protocol in java framework on a **Dell XPS** machine with 6 GB RAM and an Intel core i7 processor. The analysis presents the relative time taken to perform a particular operation (such as, expected response generation and decryption of tag message by the server) with respect to minimum time taken to perform a similar operation. The time analysis only presents the information about time taken to compute the message. It does not take into account the time taken to send the message over the communication medium.

Time Analysis of the Protocol								
Message/Frame Number	Encrypt Reader Id by the reader(milliseconds)	Compare Reader Id by the server (milliseconds)	Expected response by the reader (milliseconds)	Expected response check by the server (milliseconds)	Decrypt tag message by the server (milliseconds)	Final Message Encrypt by the server (milliseconds)	Final Message Decrypt by the reader (milliseconds)	Total Time (milliseconds)
1	x	3.2x	1.8x	1.8x	3.2x	39.6x	39.0x	90.0x
2	x	3.0x	1.8x	1.8x	3.4x	39.4x	38.4x	89.0x
3	x	3.4x	1.8x	1.6x	3.2x	38.4x	38.6x	88.2x
4	x	3.0x	1.8x	1.8x	3.4x	38.8x	39.6x	89.8x
5	x	3.4x	1.6x	1.6x	3.4x	40.0x	38.2x	89.6x
6	x	3.2x	1.6x	1.8x	3.4x	38.6x	38.8x	88.8x
7	x	3.0x	1.8x	1.8x	3.0x	39.0x	39.4x	89.0x
8	x	3.4x	1.8x	1.6x	3.4x	38.4x	39.0x	89.0x
9	x	3.4x	1.6x	1.8x	3.0x	39.4x	40.2x	89.4x
10	x	3.0x	1.6x	1.8x	3.4x	39.6x	38.6x	89.0x
11	x	3.2x	1.6x	1.6x	3.4x	40.2x	39.2x	90.2x
12	x	3.0x	1.8x	1.8x	3.4x	38.4x	39.2x	89.0x
13	x	3.2x	1.6x	1.6x	3.0x	40.6x	39.8x	91.2x
14	x	3.0x	1.8x	1.6x	3.0x	39.0x	40.4x	90.0x
15	x	3.4x	1.6x	1.6x	3.4x	38.8x	39.0x	89.0x
16	x	3.2x	1.8x	1.8x	3.2x	39.2x	38.8x	89.8x
17	x	3.2x	1.6x	1.8x	3.4x	38.4x	40.2x	89.8x
18	x	3.4x	1.6x	1.6x	3.2x	40.6x	40.6x	92.4x
19	x	3.2x	1.6x	1.8x	3.0x	39.8x	39.8x	90.4x
20	x	3.4x	1.6x	1.6x	3.2x	39.8x	38.8x	89.8x
Average	x	3.19x	1.7x	1.7x	3.19x	39.3x	39.28x	89.67x

Figure 7 Time Analysis For The Proposed Scheme

5.2 Security Evaluation

In this section, we present the security analysis of the proposed scheme with respect to the security goals as well as we will present a brief overview of the proposed security system against well-known attacks.

5.2.1 Security Goals

- Confidentiality implies that there should be no snooping of the message being exchanged over the wireless medium. The encryption of each message being transmitted with the help of dynamically generated keys for each frame provides a confidential wireless medium for the exchange of the message.

- Authentication implies that you are who you say you are [1]. The server first authenticates the reader and a legitimate reader can access the information from the tag which is turn is again authenticated by the server. The final acknowledgement message also plays a role of the legitimate server identifier for the tag because only an authentic server would be able to produce the final acknowledgement message.
- Non-Repudiation implies that a source should not be able to deny the message that was sent [1]. The hash of the tag id sent with the final message from the tag acts as a digital signature for the tag. The updating of keys with every frame ensures that a valid entity would be able to update the keys and encrypt and decrypt the messages being exchanged.
- Digital Signatures for the tag are provided by the hashed tag id message and for the server, it is provided by the final acknowledgement message it sends to the tag for updating its seed for the Random Sequence Generator.
- Forward security implies that even if an adversary is able to decrypt the previous message, it should not compromise the next message. In our proposed security scheme, the keys for exchange of messages between the server and the tag as well as the reader and the server are updated with each message being transmitted. So even if an adversary is able to get hold of the previous keys, it would not be possible to crack the next keys. The element of randomness is provided by the Random Sequence generator for the generation of each key.

5.2.2 Security Attacks

In this section, we will present a discussion on the performance of our proposed security scheme when it is subjected to some well-known attacks for RFID systems.

- **Eavesdropping:** In this kind of an attack, an adversary snoops on the messages being exchanged between the various entities over the wireless medium. The adversary may use this information to extract any related information or apply reverse engineering to extract a pattern for the encryption keys. The exchange of messages over the wireless medium and availability of strong readers to sniff the information being exchanged makes it almost impossible to prevent this kind of attack. But this attack will be futile if we present garbled or encrypted data to an adversary which makes it impossible for him to derive any useful information.

  In the proposed scheme, the tag ids, reader ids or any important information related to the entities are never sent in open without encryption or hashing. The use of dynamically updated keys for encrypting the subsequent messages will make it impossible for an adversary to get or derive any useful information from the data available that would help in introduction of rogue entities into the system.

- **Desynchronization Attack:** In this kind of attack, an adversary may choose to jam or drop certain messages which help in updating of the seeds for random sequence generators. It implies that two entities involved in the communication may not know about the latest updated state of each other.

  In our proposed scheme, the updating of the seed generator for the tag takes place with the help of an acknowledgement message. This message is always unique for each communication which prevents it from being replicated by the adversary. If this message is lost, the tag will not update the random sequence to the next value but it will use its previously stored key to encrypt the subsequent messages. When the server finds out

about the desynchronization, it resets its seed generator to previous value and also generate an alert about the messages being dropped or an attack being launched.

- **Replay Attack:** In this of attack, an adversary may use the previous messages from the communication between the entities and try to replay them to the respective entities after some time. It may use a message from a tag to the server and try to send it to the server acting as a legitimate reader to get some information about the object that is tagged with the respective tag. This attack is generally performed after the eavesdropping attack.

  In our proposed scheme, if an adversary tries to replay the messages from the tag to the server acting as a rogue reader, it will at best get an encrypted message (encrypted using DES technique) which would be hard to crack. If it tries to replay the acknowledgement message to the tag to de synchronize its random sequence generator, the tag would recognize it because after one update with a certain pattern, it changes a flag variable which prevents its updating twice.

- **Man in the middle attack:** In this type of attack, an adversary might assume the role of an intermediate entity. It will behave as a legitimate entity to the other communicating entity. It may assume the role of a tag for the reader and vice versa. It is similar to hijacking the communication session. The flow of information takes place through the rogue entity and it might be able to modify any part of the information flowing through it.

  In our proposed scheme, if the rogue entity tries to modify any information, this would eventually result in dropping of the packets and forcing the entities to raise an alarm about some kind of attack happening in the RFID system. If the rogue entity only chooses to relay the information back and forth, it might not be detected but in that case the rogue entity will not get any useful information.

- **Tag Cloning:** In this kind of attack, an adversary is able to get all the information stored on the tag through combination of reverse engineering, eavesdropping and any faults in the security scheme. The adversary then uses this information to manufacture a cloned tag which will act as a legitimate tag and perform almost all the operations performed by a legitimate tag. This kind of attack has quite a devastating effect where there is access control in place based on RFID cards.

  In our proposed security scheme, at no point either the reader ids or the tag ids are sent in open. The keys for encryption are updated with each frame and also there is forward security in place. So it is very hard for an adversary to analyze or get any information about the tags and use that information to clone the tags. But on the other hand if an adversary is able to get hold of the tag physically and able to replicate the circuit, then it is very difficult to distinguish a genuine tag from a cloned tag.

- **Tag Tracking:** In this type of attack, the tag can be tracked or located by an adversary when it sends out the information to the queries. This can be used to track the person or an object which is tagged with the object.

  In our proposed approach, the information sent out by the tag is encrypted but if an adversary launches a denial of service attack first and then tries to access tag again and again the tag will give away same information again and again until its seed generator is updated by a legitimate reader. So our proposed approach is partially prone to tag tracking attack under some specific circumstances.

- **Denial of Service:** In this kind of attack, an adversary tries to exploit the limited resources for the various entities by sending out too many messages causing a traffic

overflow over the network. An adversary may jam the whole communication flow making it impossible to send out any message between the entities.

In our proposed security scheme, if an adversary launches a denial of service attack through jamming the signals, there is little that could be done about it.

5.3 Simulation v/s Real Network Scenario

In this section, we will discuss the limitations that simulation of the proposed security scheme present as compared to the analysis on a real network scenario. First of all, it is difficult to simulate the message exchange scenario over the wireless network. This limits us to get the actual data about the time it takes for the message to travel across the wireless medium. Under the simulation method, we are not able to take into account the messages that are dropped because of network traffic congestion. In a simulation environment, it is assumed that the messages are transferred with 100% success rate which is not the case in a real network scenario.

It is also difficult to simulate the actual behavior of the tag in a simulation environment. As implementation of our proposed scheme requires the use of custom manufactured tags, it is difficult to predict their behavior in a simulated environment. If we assume a real network scenario, the tag will take much more time as compared to the server to perform the same operations because of the resource constraints. If we reproduce the tag in a simulation, it takes the same amount of time for the tag as well as the server to perform the same operations. This limits us to perform the time analysis for the tag which is a significant bottle neck issue in analyzing the performance of the security scheme when applied to a real network scenario.

In the simulation, it is difficult to analyze the scenario in which various kinds of attacks (such as Man in the middle attacks) are launched on the proposed security scheme. We simulated them by manually modifying the messages and performing the qualitative analysis.

One of the major drawbacks that the RFID technology suffers from is the absence of a universal framework for analyzing the security schemes.

5.4 Comparison With Other Schemes

In the section, we will present a brief comparison of proposed scheme with the other schemes and how our scheme overcomes some of the limitations of those past schemes. We will mainly focus on the security vulnerabilities and security goals for comparing the schemes.

Kim *et al* [14] approach suffers from desynchronization problem as well as they use a static pre shared secret to generate the starting keys. The pre shared secret remains static throughout. Another problem is that they make the simple random generator to generate the keys. There is no provision for digital signatures to support non –repudiation. Our proposed approach overcomes the desynchronization problem as well as there is no pre shared secret to start generating the keys for each communication. The key changes for each communication. Moreover in our approach, the key generation mechanism is more complex. The use of tag id itself also imparts more authenticity to key generation and use of random sequence generator provides randomness and hence enhances security. The use of hashed tag ids and unique acknowledgement messages act as a digital signatures for the tag and the server and support non-repudiation.

Treck *et al* [15] proposed scheme suffers from use of different readers to query the tags because it uses the time stamps for authentication. Also their approach suffers from use of static pre shared secret to generate the messages for authentication. There is no provision to support non-repudiation and forward secrecy of the keys. Our proposed approach supports the use of multiple readers to read any tags. There is no static pre shared secret and there is a provision to support non-repudiation and forward secrecy of keys.

Lopez *et al* [16] proposed scheme suffers from desynchronization attacks and tag cloning attacks. Under the proposed approach, the tag sends out the EPC for the tag in open without any encryption which might lead to certain security issues. They have no provision for non-repudiation as well. In our proposed approach, we have provisions to safeguard from desynchronization attacks as well as against tag cloning attacks. Our proposed approach also supports non repudiation.

Table 15 Comparison With Other Proposed Security Schemes

Security Goals	**Our Proposed Approach**	**Kim *et al***	**Treck *et al***	**Lopez *et al***
Authentication	✓	✓	✓	✓
Confidentiality	✓	✓	✓	✓
Non Repudiation	✓	X	X	X
Forward Secrecy	✓	X	✓	✓
Use of Multiple Readers	✓	✓	X	✓

Prevention against attacks	**Our Proposed Approach**	**Kim *et al***	**Treck *et al***	**Lopez *et al***
Desynchronization attacks	✓	X	✓	X
Replay Attacks	✓	✓	✓	X

5.5 Summary

In this chapter we evaluated our proposed approach for security and performance. We also presented a brief overview on how our proposed approach overcomes the drawbacks of some

earlier proposed security schemes. We discussed the limitations of the evaluation in a simulated environment as compared to the evaluation done in the real network scenario.

CHAPTER 6: DISCUSSION AND CONCLUSION

In this chapter we would discuss about the advantages and limitations of our proposed approach. In conclusion section we would discuss how our proposed approach satisfy the goals we set out at the start. In the last section we would briefly discuss about the scope of future work that can be carried out on our proposed security scheme.

6.1 Discussion

In this section we would briefly discuss the advantages and the limitations of the proposed security scheme.

6.1.1 Advantages Of The Proposed Security Scheme

- **Secure:** The proposed scheme uses complex yet basic logical operations to generate the keys for authentication for tags. It makes the use of a novel approach based on 3G Cellular networks to authenticate the readers. There new updated keys are used for encryption of messages makes it difficult to break the security. This also helps in limiting the introduction of rogue entities in the system.
- **Generic:** The proposed scheme provides flexibility for the use of different key lengths for the messages for the readers and the tags and also with the number of authentication vectors as well as the length of the message digest which acts as a digital signature for the tags.
- **Modular:** The proposed scheme implementation is based on the block model. The various modules are implemented as individual blocks. This gives the flexibility to change them according to the system requirements without having any effect on the system as a whole.

- **Scalable:** The proposed security scheme only stores limited information on the server side and there is no restriction based on multiple readers able to access the same tag multiple times. This property makes our proposed security approach easy to expand in case new tags and the readers are added into the current implemented system.

6.1.2 Limitation Of The Proposed Approach

- **Customized Tags:** In order to implement our security scheme, the owner needs to get the RFID tags custom made from the manufacturer. These tags will comply to the specific designing of gates and data storage in order to function according to the proposed mechanism.
- **Tag Tracking:** Under very special circumstances that includes the launch of several attacks together; an adversary is able to track the tags because it will give our same information until it is queried by a legitimate reader which will update its key seed generator to a new value.
- **Tag Cloning:** Our proposed approach suffers from the drawback of Tag Cloning attack. If an adversary is able to get hold of the tag and replicate the circuit, it makes it very difficult to distinguish the original tag from the cloned tag.
- **Evaluation:** We have implemented our security scheme as a proof of concept and analyzed the related data in the simulated environment. This limited us from obtaining several results like time delay caused when the message in travelling from one entity to the other and also a realistic scenario in which messages are dropped because of traffic congestion.

6.2 Conclusion

We presented an authentication scheme which uses the concept of cellular networks to authenticate the readers and dynamically updated keys to authenticate the tags as well as encrypt the data being sent out from the reader and the tag to the server. It also achieves the objectives of no key exchanges, generation of independent keys for encryption and authentication, dynamically updated new keys for each communication frame being exchanged. It provides the automatic updating as well randomness to new keys that are generated. Our scheme is also robust against the most common type of attack with the dynamic updating key generation system known as the desynchronization attacks. The proposed scheme also ensures that the security goals like Confidentiality, Authentication, and Non Repudiation are met. The scheme also ensures the forward secrecy of the generated keys.

6.3 Future Work

In this section we discuss the opportunity to expand on the ideas our current work in the future. The main points to be focused on are as follows:

- Optimizing resources for the tags.
- More complex yet logically simple key generation mechanisms for the tags.
- Introducing more randomness to make the scheme more robust against tag tracking attacks under some special conditions.
- Expanding the whole scheme or modular parts of the proposed scheme to other resource constrained networks.
- Using the advanced Java simulators to get the results regarding message drops during traffic congestion and also calculating the time taken for the message to travel between various entities.

6.4 Summary

In this chapter, we discussed the advantages and limitations of the proposed approach and how our scheme satisfies the security objectives, and described possible avenues for future work.

BIBLIOGRAPHY

[1] S. Sampalli, *Emerging Technologies RFID Security (CSCI 4174, Handout 16),* Halifax, 2011.

[2] R. Want, "An Introduction to RFID Technology," *IEEE Pervasive Computing,* vol. 5, no. 1, pp. 25-33, 2006.

[3] H. Y. Chein, "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.

[4] M. A. Khan, M. Sharma and P. R. Brahmanandha, "A survey of RFID tags," *International Journal of Recent Trends in Engineering,* vol. 1, no. 4, pp. 68-71, May 2009.

[5] S. Preradovic and N. C. Karmakar, "RFID READERS-A Review," *4th International Conference on electrical and Computer Engineering ICECE 2006,* pp. 19-21, December 2006.

[6] A. Mitrokotsa, M. R. Rieback and A. S. Tanenbaum, "Classifying RFID attacks and defenses," *Information Systems Frontiers,* vol. 12, no. 5, pp. 491-505, 2010.

[7] M. F. Mubarak, J.-l. A. Manan and Y. Saadiah, "A Critical Review on RFID System towards Security, trust and Privacy (STP)," *7th International Colloquium on Signal Processing and its Applications,* pp. 39-44, 2011.

[8] M. Feldhofer, S. Dominikus and J. Wolkerstorfer, "Strong Authentication for RFID Systems using the AES Algorithm," *Workshop on Cryptographic Hardware and Embedded Systems-CHES,* vol. 3156, pp. 357-370, August 2004.

[9] A.Tomlinson, "Introduction to the TPM," *In Smart Cards, Tokens, Security and Application, Springer,* pp. 155-172, 2008.

[10] D. Challener, K. Yoder, R. Catherman, D. Safford and L. V. Doorn, "A Practical Guide to Trusted Computing," *IBM Press,* 2008.

[11] M. F. Mubarak, J. A. Manan and S. Yahya, "Mutual Attestation Using TPM for Trusted RFID Protocol," *2nd Interenational Conference on Network Applications, Protocols And Services-NETAPPS.,* September,2010.

[12] A. R. Sadeghi, I. Visconti and C. Wachsman, "Location Privacy in RFID Applications," *Privacy in Location-Based Application,* Vols. 5599 of LNCS, Springer,Heidelberg, pp. 127-150, 2009.

[13] A. R. Sadeghi, I. Visconti and C. Wachsamann, "Anonymizer-Enabled Security and Privacy for RFID," *CANS 2009,* Vols. 5888 of LNCS, Springer, Heidelberg, pp. 134-153, 2009.

[14] K. Kim, K. Chung, J. Shin, H. Kang, S. Oh, C. Han and K. Ahn, "A Lightweight RFID Authentication Protocol USing Step by step Symmetric Key Change," *Eighth IEEE International Conference on Dependable, Automic and Secure Computing,* pp. 853-854, 2009.

[15] D. Treck, P. Jappinen, J. Stefan and Lappeenranta, "Non-Deterministic LightWeight Protocols For Security And Privacy In RFID Environments," *RFID and Sensor Networks:Arcgitectures, Protocols, Security and Integrations. Auerbach Publications,* 2009.

[16] P. P. Lopez, T. L. Lim and T. Li, "Providing Stronger Authentication at a Low-Cost to RFID Tags Operating under the EPCglobal Framework," *IEEE/IFIP International Symposium on Trust, Security and Privacy for Pervasive Applications,* pp. 159-166, December 2008.

[17] D. M. Konidala and K. Kim, "RFID Tag- Reader Mutual Authentication Scheme Utilizing Tag's Acess Password," *The 2006 Symposium on Cryptography and Information Security,* 2006.

[18] T. L. Lim and T. Li, "Addressing the Weakness in a LightWeight RFID Tag- Reader Mutual Authentication Scheme," in *Proceedings of IEEE Globecom 2007,*, November 2007.

[19] D. M. Konidala, Z. Kim and K. Kim, "A simple and cost effective RFID Tag- Reader Mutual Authentication Scheme," in *Proceedings of International Conference on RFID Security*, July 2007.

[20] A. Jules and R. Pappu, "Privacy Protection in RFID enabled banknotes," *FC 2003,* Vols. 2742, Springer, Heidelberg, pp. 103-121, 2003.

[21] P. Golle, M. Jakobsson, A. Jules and P. Syverson, "Universal re-encryption for mixnets," *CT-RSA2004,* Vols. 2964, Springer,Heidelberg., pp. 163-178, 2004.

[22] J. Satio, J. C. Ryou and K. Sakurai, "Enhancing privacy of universal re-encryption scheme for RFID tags," *EUC 2004,* Vols. 3207, Springer, Heidelberg, pp. 879-890, 2004.

[23] G. Ateniese, J. Camenisch and B. de Medeiros, "Untraceable RFID tags via insuvertible encryption," in *12th ACM Conference on Computer and Communications Security*, NewYork, 2005.

[24] C. Qingling, Z. Yiju and W. Yonghua, "A Minimalist Mutual Authentication Protocol for RFID System & BAN Logic Analysis," *ISECS International Colloquium on Computing, Communication, Control and Management-CCCM '08.,* vol. 2, pp. 449-450, August 2008.

[25] M. Burmester and J. Munilla, "A flyweight RFID Authentication Protocol," *Workshop on RFID Security-RFIDSec'09, Leuven, Belgium.,* July 2009.

[26] M. Lethonen, D. Ostojic, A. Iilic and F. Michahelles, "Securing RFID systems by detecting tag cloning," *&th International Conference on Pervasive Computing - Pervasive 2009,* Vols. 5538 of LNCS, Nara, Japan, pp. 291-308, May2009.

[27] T. Dimitriou, "Proxy Framework for Enchanced RFID Security and Privacy," *Fifth Annual IEEE Consumer Communications & Networking Conference - CCNC 2007, Las Vegas, Nevada,USA,* January 2008.

[28] K. Osaka, T. Takagi, K. Yamazaki and O. Takahashi, "An Efficient and Secure RFID Security Method with Ownership Transfer," *International Conference on Computational Intelligence and Security 2006,* vol. 2, pp. 1090-1095, November 2006.