Privacy Preservation and Mutual Authentication in RFID Systems

Debadatta Meher
Roll. No. 710CS2036

under the guidance of
Prof. Ashok Kumar Turuk

Department of Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela – 769 008, India

Privacy Preservation and Mutual Authentication in RFID Systems

Thesis submitted in partial fulfillment for the degree of

Master of Technology

in

Computer Science and Engineering

(Specialization: Information Security)

by

Debadatta Meher

(Roll No: 710CS2036)

under the supervision of

Prof. Ashok Kumar Turuk

Department of Computer Science and Engineering

National Institute of Technology Rourkela

Rourkela – 769 008, India

June - 2015

Declaration

I hereby declare that the work presented in this thesis entitled *"Privacy Preservation and Mutual Authentication in RFID Systems"* by **Debadatta Meher** is my own work. The contents referred from valuable resources like journals, articles and published papers are properly referenced.

Debadatta Meher

Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela-769 008, India. www.nitrkl.ac.in

Dr. Ashok Kumar Turuk
Professor

June 1, 2015

Certificate

This is to affirm that the work presented in the thesis entitled *Privacy Preservation and Mutual Authentication in RFID Systems* by **Debadatta Meher** is a record of genuine research work carried out by him, under my supervision and guidance in partial fulfilment of the requirements for the award of the degree of Master of Technology with the specialization of Information Security in the department of Computer Science and Engineering, National Institute of Technology, Rourkela. Neither this thesis nor any part of it has been submitted for any degree or academic award elsewhere.

Place: NIT Rourkela
Date:

Ashok Kumar Turuk
CSE Department
NIT Rourkela

Acknowledgment

I am indebted to Dr. Ashok Ku. Turuk for the kind of help, support and guidance he has provided throughout this project. He has helped me significantly and been a source of information giving me a whole new exposure to this topic. His remarks and guidance has helped me a lot to carry out this project.

I am also thankful to my friends for encouraging and motivating me persuasively. They have been a lot of help for discussing my ideas and opinions and showing their humble appreciation towards my work.

I am thankful to my parents for understanding my nature of work and being with me perpetually.

Debadatta Meher

Abstract

Identification and tracking of devices and objects has always been helpful in many fields like transportation, tele-medicine, business and supply chain etc. Radio Frequency Identification (RFID) tags are petite, wireless devices attached to objects for the purpose of identification and information exchange. RFID systems is composed of tags, readers and an application system. These tags can be identified by a reader and are useful for tracking and monitoring. RFID tags uses Radio Frequency (RF) for wireless communication which renders these tags vulnerable to wireless security attacks. Implementation of RFID systems faces huge challenges regarding privacy as these tags can be uniquely identified and thereby are subject to tracking by an adversary. In this project a new privacy and mutual authentication scheme has been discussed that uses cryptographic algorithms and can be used in RFID systems to overcome the issues with privacy.

List of Figures

List of Tables

List of Algorithms

Contents

Chapter 1

Introduction

Radio Frequency Identification is a process of identifying objects over wireless medium. RFID systems are automatic identification systems that uses electromagnetic waves to transfer data for the purpose of identification. It does not require the object to be visible for identification. RFID systems can identify thousands of objects around a reader's range within fraction of seconds.

RFID technology has surpassed the abilities of traditional barcode system. Barcode system is another form of identifying objects. It requires scanning of the object with precision. Barcode system usually identify the type of an object but it cannot identify these items uniquely. Identifying an object requires human participation for scanning the object with a barcode reader, it is not automated. On the other hand RFID systems are fully automated systems which can work without human interaction. It can identify objects from a distance and doesn't require vision of the object. RFID tags are able to store information regarding the object with some level of security which barcodes cannot.

RFID system also supports ubiquitous services where each object is tagged with RFID tags and can be uniquely identified and tracked by the system. The expansion of market has led to the increase in flow of manufactured goods. The supply chains can be easily regulated and maintained with the use of RFID technology. It can also be implemented in tele-medicine and assist in many day to day activities.

1.1 RFID System

RFID system is composed of three important entities [5]. Any system that has to perform identification has to have some information about objects it identifies. RFID systems stores information in a back-end database that also performs many other operations. The back-end database is also called application system. Objects are tagged with small RFID chips. These chips contain information necessary for identification and each chip can be identified uniquely unlike barcode identification. RFID readers are the devices that identify an object by interrogation and relay the information back to the application system for verification.

Figure 1.1: RFID System

1.1.1 RFID Application System

An application system performs data processing and can be an application or a database depending on the requirements of the RFID system. It is linked with the RFID readers through a secure transmission channel for information sharing. It contains important information regarding the RFID objects.

1.1.2 RFID Reader

RFID readers are also known as transceiver/ interrogator in RFID systems. Readers initiate the identification task. Readers relay the information between tags and

application system.

1.1.3 RFID Tag

Tags are small chips, comparable to a grain of rice, attached to objects that are to be identified by the system. Each tag has a unique identification number initially provided by the system. Tags responds to a reader's query by sending the information stored in it.

1.2 RFID Tags

RFID tags are devices meant for wireless transmission of data. It has a size comparable to a grain of rice, some $0.4mm^2$ [4]. There are various types of RFID tags which can be categorised as active tags, passive tags and semi-active tags [3].

1. Active RFID Tags

   Active RFID tags have the characteristics of a transponder. They have their own power source and transmitter. These tags have a long range for transmission. Active tags operate in UHF radio bands.

2. Passive RFID Tags

   Passive tags do not have their own power source. They use the energy of the interrogating Radio Frequency as their power source. These tags can operate in UHF or LF radio bands.

3. Semi-Active RFID Tags

   These tags have battery assisted power supply. However, they do not have their own transmitter.

1.2.1 Read Ranges

Apart from the distinction of tags based on their power source they are also classified based on their range of operation. The operable ranges for RFID tags are specified by RFID Standards and product specifications. Considering the range of operations, RFID tags roughly operates in four different ranges [4].

1. Nominal Read Range

   This specify the maximum distances within which a reader can scan tag data. For example, a nominal read range of 10 cm is specified by ISO 14443 for contactless smartcards [4].

2. Rogue Scanning Range

   The range of reader extends when equipped with powerful antenna. A rogue reader may be equipped with such technique to exceed the legal limits. This range is maximum for a reader at which it can power and read tag data. For example, ISO 14443 tags can be read from a distance of 50cm by a rogue reader.

3. Tag to Reader Eavesdropping Range

   When a reader sends interrogation signals to a tag, the tag responds by transmitting stored information in it. An illegitimate reader can then eavesdrop and collect information transmitted by the tag. The range of such a reader is called tag-to-reader eavesdropping range and can be greater than rogue scanning range.

4. Reader to Tag Eavesdropping Range

   In some RFID systems readers send data specific to tags, like in query base anti-collision protocol the query is part of the tag's ID. Since readers operate at much higher power than tags, they are more susceptible to eavesdropping.

1.3 RFID Standards

The International Organization for Standardization (ISO) has furnished multiple standards that serves different purposes for the implementation of RFID systems. Some of the important standards by the ISO are tabulated below.

Table 1.1: ISO standards

Standard	**Description**
11784	How data is to be structured in tag.
11785	Defines protocols for air interface.
14443	Defines protocols for contactless smartcards
15693	Defines protocols for vicinity cards.
18047	Standards for testing the conformance of RFID tags.
18046	For testing the performance of RFID tags and readers.

The situation for standardization became in jeopardy when Auto-ID center, which developed EPC technologies, created its own air interface protocols for tracking of goods through the international supply chain. The Auto-ID centre rejected the standards proposed by ISO, because the ISO UHF protocol was too complex and unnecessarily increasing the cost of the tags [16]. Auto ID centre developed RFID tags categorized in five classes:

- Class 1: Passive tags that backscatter the signals by a reader. Read only memory that is non-volatile.
- Class 2: Passive tags that backscatter the reader's signals. It has read-write memory of up to 65 KB.

- Class 3: These are semi-passive tags which have built-in battery to support increased read range.
- Class 4: Active tag that has a battery for power supply. It also has a transmitter.
- Class 5: Active tags that are compatible with other class 4 and class 5 tags.

1.4 Singulation

RFID systems are used to identify objects uniquely. It works in wireless media in which readers send out radio signals for communication with tags and the tags respond to these interrogation signals with the information stored in them. For a tag to respond to a reader it needs to be in the range of the reader. If there are multiple tags within the range of a reader, all of them will respond to the reader. Since these tags operate at a common frequency, tag collision occurs. Tag collision is a problem in which multiple tags respond to an interrogation signal of a reader simultaneously and the reader cannot decode the signals because of signal collision [5]. Tag collision prevents a reader from recognizing a tag and thus increases communication overhead. To avoid this problem there are many anti-collision protocols. The anti-collision protocols can be broadly divided into two types [5]

1. ALOHA based protocols (probabilistic protocols)
2. Tree based protocols (Deterministic protocols)

1.4.1 ALOHA based protocols

ALOHA based protocols tend to reduce the occurrence probability of tag collision. In this protocol each tag transmits its ID at a selected time based on the type of ALOHA protocol. However, ALOHA based protocols fails to prevent tag collision completely. They are subject to a serious problem of tag starvation [2]. In tag

starvation a tag is denied from transmitting its ID or roughly speaking it does not get a chance for transmitting.

1.4.2 Tree based protocols

Tree based protocols, on the other hand constructs a tree while identifying tags. They split the set of tags in the reader's vicinity into two subsets at a time and tend to identify the tags in each subset. One of the advantage of tree based protocols is that, it does not suffer from tag starvation problem. In this project a variation of tree based protocol known as AQS is used to avoid the tag collision problem. There are several variations of tree based protocols like Binary Tree protocol (BT), Query Tree protocol (QT), Adaptive Binary Splitting protocol (ABS), Adaptive Query Splitting protocol (AQS). Among the mentioned protocols, best performance is observed in AQS [2] with lesser number of collisions and transmission of bits.

AQS Protocol

This is a MAC protocol used in wireless singulation. In this protocol, a tree is built from the IDs of tags. If the length of tag identifiers is L then the depth of tree is L. The binary tree is built in this manner: The root is labelled **NULL**. For a node having binary label s, the left child of the node has label s‖'0'and the right child of the node has label s‖'1'. Reader sends a request to all tags within its range. Tags acknowledge the reader's request with the first bit of their identifier. If the reader receives '0' bit as the only response, then it concludes that all tag identifiers lie in the left half of the tree and recurses on the left half of the tree. Conversely, a response of '1'causes the reader to recurse on the right half of the tree. If a tag collision occurs, that is, some tags emit '0' bits and others emit '1' bits, then the reader has to recurse on both halves of the tree. The reader needs to perform a depth first search of this tree to identify individual tags.

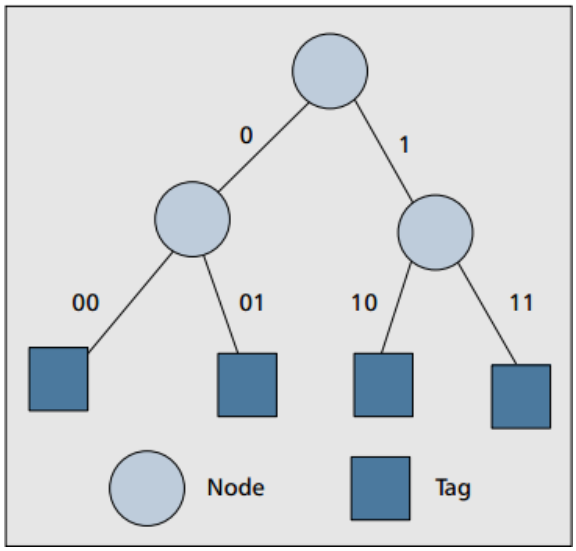

Figure 1.2: AQS Singulation protocol

1.5 Authentication

RFID systems are automatic identification systems in which tagged objects are identified and can be monitored automatically without or with fewer human interaction. General RFID tags respond to any reader's query. The process of identification poses a threat to privacy of individuals. If any reader can identify a tag then it can be tracked down by an adversary, which is known as clandestine tracking. If such tags can be identified without the knowledge of the tag bearer, an adversary can also perform clandestine inventorying.

Clandestine tracking and clandestine inventorying are two major privacy issues regarding the RFID system. The problem becomes serious when the tags serial number also contain some personal information. EPC tags in particular carry information regarding the manufacturer details, class of object etc. [4]. Clandestine tracking can be prevented if the tag confuses the adversary and cannot be traced. This can be achieved if the tag responds with a different identity to each new interrogation by a reader. By changing its identity a tag can avoid tracking issue. Clandestine inventorying can be prevented if the tag only share personal information

with genuine reader. A reader which should be able to validate its authenticity to a tag to obtain information stored in the tag. This can be achieved by authentication of reader to tag.

Privacy can be achieved with authentication. Genuine readers validate themselves to obtain information or to get the ID of a tag. Authentication can be performed using symmetric key protocols or asymmetric key protocols. Privacy problem for symmetric key enabled RFID-tags lies in the challenge of key management. Cryptographically secured authentication or identification of an RFID-tag T_i relies on the symmetric key K_i shared between the tag and RFID-application system.

In various existing schemes, the common operation for authentication include the following two steps:

i. Tag T_i sends E = f_{K_i}(P)
   E : Encryptedtext
   P : Plaintext sent by reader
   f_{K_i} : Encryption function using key K_i

ii. On receiving the encrypted text E from a tag, the reader searches the space of all keys K in the *systems* database for the key K_i
   $E' = f_{K_j}$(P)
   if E' = E, then $T_j = T_i$

This leads to a problem as discussed below:

- Tag identifies itself prior to authenticating reader at all. The tag T_i emits its unique identifier ID_i promiscuously. Privacy in such condition is unachievable, since any reader can learn the tag's ID.

- A reader cannot authenticate a tag unless it has been identified by the reader. If the reader has no knowledge about the identity of tag, it cannot determine which key K_i to use for authenticating the tag.

It is necessary for a reader to identify a tag uniquely so to avoid tag collision. After identifying a tag, the reader can communicate with the tag. However, an RFID-tag, if identified before authentication is subject to tracking and hence, violates privacy. Since, any reader can obtain the tag's ID. Conversely, an RFID-tag cannot be authenticated before identification, because the interrogating reader doesn't know which key to use for authentication.

1.6 Applications of RFID systems

Being an automatic identification system the application domain of RFID system is vast. With the application of RFID system smart cities and smart environments can be created. Use of sensors along with RFID tags can change the way several systems that are operating traditionally like the supply chain management. RFID technology can be used to assist the concept of pervasive computing also known as Internet of Things. The function of identification can be extended to perform tracking of objects. Tracking is the process of observing persons or objects on the move and providing timely information to a system [3].

The most interesting and successful implementation of RFID system include the following:

- Supply chain management
- Production process control
- Object tracking management

Now RFID has been broadly used in the following fields:

- Retail: Supply chain control, Payments and Transactions, Product Management.
- Logistics: Quality of shipment conditions, Item Location, Fleet Tracking.

- Smart metering: Smart Grid, Tank Level, Water flow, Silos Stock Calculation.
- Smart Cities: Smart Parking, Traffic Congestion, Smart Lighting.
- Health care and Telemedicine: Health assistance for aged or disabled people, Patients Surveillance, Vital signs monitoring in high performance centres and fields.
- Military and Defence: Detection of friend or foe, tracking of artillery.

1.7 Motivation

RFID systems supports automatic identification and are helpful for tracking of objects or persons. RFID tags responds to any reader's query and hence expose their identity to the reader. In such a scenario anyone having a reader can track a person or object. Moreover clandestine inventorying can also be initiated. In either case there is a privacy breach. Privacy preservation in RFID systems has been a debate from decades.

There has been a lot of research work going on to eliminate the problem of privacy regarding RFID systems. However the issue of performing identification before authentication and vice-versa has been addressed by a few with a little resolution to the problem. In this project a scheme is presented that aims at preserving the privacy of an object in the RFID system and performing mutual authentication between the reader and tag without disclosing any sensitive information.

1.8 Objective

There are several security challenges regarding RFID systems like DOS attacks, privacy, profiling, eavesdropping and inventory jamming etc. [16]. Our proposed work focuses mainly on the privacy issues regarding RFID systems. The main objectives of the proposed work are as follows:

i. Untraceability: The RFID tags should not be susceptible to tracing.

ii. Identification: Tags should be easily identifiable to a genuine reader.

iii. Mutual Authentication: An RFID reader should authenticate itself to a tag prior to sharing information.

Our proposed scheme will avoid tracing issues by confusing a fake reader. It will also perform identification followed by mutual authentication to verify that the interrogating reader is genuine.

1.9 Organization of thesis

1. Chapter 1: A detailed introduction to RFID systems has been presented. The security issues regarding RFID system are briefly discussed. Application domain of the system is mentioned.

2. Chapter 2: In this chapter we present the literature review where we have discussed existing privacy and authentication protocols for RFID systems.

3. Chapter 3: In this chapter we present our proposed scheme for privacy preservation and mutual authentication.

4. Chapter 4: In this chapter we analyse our schemes in the context of privacy and authentication issues.

5. Chapter 5: We conclude our work in this chapter.

Chapter 2

Literature Review

In [3], Xiaolin et. al. discusses how RFID technology can accompany pervasive computing. They describes the integration of RFID technology with IoT with the help of three layers which are perception layer, network layer, service layer. Perception layer collects all kinds of information from the physical world. The network layer provides an efficient and trusted network infrastructure to large scale industry application. The problems of tag collision and privacy threats in RFID systems are also discussed.

A research survey by Ari Juels in [4] discusses the security and privacy issues faced by RFID systems. Many cryptographic and non-cryptographic approaches are discussed in this survey. The following subsection discusses few approaches for protection of privacy.

1. Non-cryptographic approaches

    i. Kill Tag approach

    This is the simplest and straightforward approach towards protection of privacy. When a product has been purchased by a customer the tag attached to the object is simply disabled by a KILL command. This approach has manifested many issues. It eliminates the usage and advantages of the RFID tag in the product after it has been purchased.

Instead of killing the tag it was also suggested to cause the tag to sleep by giving a SLEEP command. The tag can be woken-up by a WAKE UP signal. However, in such a case any reader genuine of fake, can cause the tag to sleep or wake-up. This requires a scheme in which a reader has to authenticate itself to the tag before sending SLEEP or WAKE UP signals.

ii. Active Jamming approach

The bearer of an RFID tagged object may carry a jammer that actively broadcast radio signals to any nearby reader. This will cause the reader to get stuck during identification. This approach may be illegal as mentioned in [6].

2. Cryptographic approaches

i. The Hash-Lock approach

In this approach a tag is locked with a value y, and it is unlocked by presentation of a PIN value x such that y=h(x) for a standard one-way-function h. This approach itself violates privacy as stated in [6]. After a tag has been locked, a reader require to know its meta-ID y, so that it can give the PIN value x for unlocking the tag. Thus the tag is still exposed to tracking issue with its meta-ID.

Juels et. al. in [6] discussed a blocker tag approach for privacy in RFID systems. They call this approach as selective blocking approach. This approach exploits the tree walking singulation protocol to provide privacy. A blocker tag has been proposed in this scheme that simulates the IDs of all the tags in a certain zone marked as private zone. This approach has limitations for practical implementations. Use of a blocker tag prevents clandestine inventorying. This approach requires the RFID tag to be within the communication range of the blocker tag.

In [13] Ari Juels proposed an authentication scheme for privacy which is called as minimalist cryptography approach. In this approach tags bear a set of pseudonyms

which is used for authentication. A tag responds with a different pseudonym with each successive interrogation. The tags does not respond with the same pseudonym twice during its lifetime. The pseudonyms are updated by a reader upon requirement. An adversary may clone a tag by collecting the pseudonyms stored in a legal tag. To avoid the cloning issue Juels proposes that tags throttle their tag emissions.

Weis et. al. [8] proposed a new scheme for authentication in RFID systems. In this approach, an RFID tag generates a random nonce value R and computes the hash of it using a hash function stored in the tag. Upon receiving the tuple $\langle h(K_i, R), R\rangle$, the reader performs an exhaustive search to get the key from the database. The major problem with this approach is the key search which is linear to the number of tags in the system. Practically, if there are many tags in the system then, identifying any one of them can be prohibitively costly.

Ohkubo et. al. [9] used synchronization approach for authentication of tags and readers. The main purpose of the scheme is forward privacy. In this approach the system synchronizes its state with that of the tag. Every tag T_i maintains a counter C_i that is incremented with every reader's interrogation. Upon interrogation the tag outputs a hash value of the counter. A genuine reader knows the approximate current value of the counter as the tag is synchronized with the system.

OSK protocol is a single round protocol for authentication. This protocol uses two one-way hash functions G and H. These hash functions are stored in the tag as well as the system's database. Initially all tags share an exclusive secret with the system. For each tag let the secret starts with S_i. When a reader sends a request to the tag, the tag computes $E = G(S_i)$ and updates the secret to $S_{i+1} = H(S_i)$. The reader receives E and performs an exhaustive search for each tag k. After identifying a tag T_k the system also performs $S^k_{i+1} = H(S^k_i)$ and stores it in the database. The tag and system both updates the shared secret S with each interrogation. Both the reader and system are synchronized. This scheme is susceptible to de-synchronization attack. Apart from desynchronization attack the

protocol takes too long to identify a tag as identification of a tag is linear to the number of tags in the system.

Ryu et. al. in [7] implemented public key encryption algorithm to strengthen the security and support privacy in RFID systems. Their authentication has a layout of two phases. The first phase is key generation phase in which the system generates public key (P_k) and private key (S_k). The system also produce a set Δ that is stored in a tag. The set Δ is generated as follows $\Delta \leftarrow \{\alpha_1 = E_{Pk}$ (ID$\|$ r_1), ..,α_m= E_{Pk}(ID$\|r_1$)$\}$. The authentication process consists of three rounds which mutually authenticates both the reader and tag. This authentication system only supports private tags. Public tags are not considered in their scheme. A reader cannot detect whether a tag has been queried by a fake reader in past. In such case it becomes difficult for the system to decide when to update the stored Δ set.

2.1 Summary

In this chapter, we have discussed various proposed schemes for privacy and authentication. Because of limit on the computational capability of RFID tags the security and privacy schemes faces a lot of challenges. Non-cryptographic schemes are favoured for passive RFID-tags whereas lightweight cryptographic protocols are being implemented in active RFID-tags.

Chapter 3

Privacy Preserving Mutual Authentication

From the introduction to the topic and literature review one can clearly infer that privacy is a major concern in RFID systems. There are many proposed ideas to preserve privacy by implementing cryptographic and non-cryptographic schemes. Some of these schemes are not practically implementable while some are too much resource intensive.

3.1 Proposed Scheme for privacy

In this chapter we present a cryptographic scheme that uses the power of asymmetric key protocol to preserve privacy in RFID systems. This is scalable and can be implemented practically. This scheme is inspired from the work in [7]. Our proposed scheme is an improvement over their proposed work in several ways that are discussed in the next chapter where we evaluate our proposed scheme.

3.1.1 Assumptions

There are certain assumptions made by our scheme regarding the RFID system like:

1. All RFID tags has a special **STATUS WORD**, which is of specific length chosen by the system. The tags are capable of computing hash value with a stored hash function **H**. Tags can generate random values. Each private tag contain a set of serial numbers **S** referred to as pseudo-ID set, which can be updated by an authentic reader. This set of serial numbers are used as identifiers for the tag.

2. The communication link between an RFID reader and application system is secure.

3. The application system stores the actual identifier (ID) for each tag along with important information. Since, the communication channel between readers and application system is assumed to be secure, both can be treated as a single entity.

3.2 RFID System

Our proposed scheme describes the RFID system in terms of its three important entities, that is, RFID tags, RFID readers and an application system.

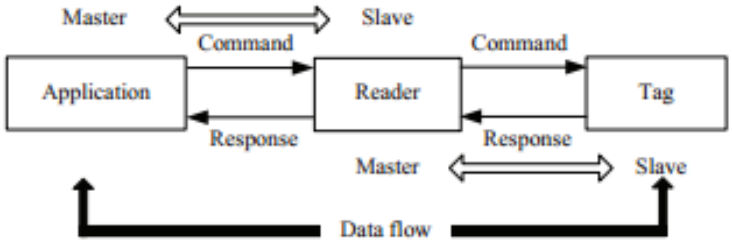

Figure 3.1: RFID System

The features of the RFID entities are as follows:

1. RFID Application System: The application system is the core of the RFID system. It performs several tasks as mentioned below.

(a) Generation of private key and public key for the RFID system based on the chosen public key encryption algorithm, i.e. RSA, El-Gamal etc.

(b) Executes all database operations. The database is a part of the application system. All the important information like the identifiers of tags, keys are stored in the database.

(c) Generation of Identifiers for public and private tags. It also generates keys for the private tags.

(d) It verifies the authenticity of a tag based on the data received from a reader.

2. RFID Reader: The reader acts as a relay object between the application system and an RFID tag. It is used for interrogating an RFID tag. The information received from the tag is sent back to the application system to verify the tag's authenticity. A reader performs the following tasks:

   (a) It is responsible for singulation of the RFID tags.

   (b) It also detects whether an RFID tag has been interrogated by a fake reader in the past.

   (c) A reader can update the set of IDs **S** stored in an RFID tag.

   (d) It executes the authentication protocol and relays the data back to the application system for authenticating an RFID tag.

3. RFID tag: Tags are tiny microchips attached to objects and may contain important information about the objects. RFID tags has the following features:

   (a) It responds to a reader's interrogation.

   (b) Each tag has a unique identifier set **S** provided by the RFID application system. A tag uses one of the identifier from the set for identification during an interrogation.

(c) A special set of bits that defines the status of an RFID tag is stored in each tag. In our scheme we call it as **STATUS WORD** (SW). The length of **SW** can be set-up based upon implementation. In our scheme the length is set to be of 8 bits.

(d) A tag can update its **SW** after interrogation.

3.2.1 Significance of STATUS WORD

In this scheme we introduce a special sequence of bits termed as **STATUS WORD**. The length of the sequence can be changed depending on implementation, however, in this scheme we have implemented it with 8 bits for simplicity. The SW of a tag indicates the status of that tag. It tells the reader whether it is a public tag or a private tag. The SW can also give information to the reader whether the tag has been interrogated by a fake reader in the past. It is helpful getting such information when privacy is to be preserved. The reader is able to determine when to update the identifier set S of a tag based on the information from the SW. The SW also tells the tag which identifier to use during an interrogation for identification. Thus, SW plays a major role in preserving privacy of a tag.

Figure 3.2: STATUS WORD

This scheme also supports the use of public tags. All public tags have a single ID and their SW is set to "00000001". The length of ID for public tags is smaller than the length of pseudo-ID for private tags. Each private tag contain a set of pseudo-IDs **S** and initially their SW is set to "10000001". This indicates that the

Table 3.1: Specification of bits in SW

BIT	STATUS	Description
1	0	Tells the readers that the tag is a public tag
1	1	Tells the reader that the tag is a private tag
2	0	Tells the reader that the tag is normal
2	1	Tells the reader that the tag has been interrogated by a fake reader which failed to authenticate itself
3-8	.	Tells the tag which pseudo-ID to use for identification. E.g. "000001"indicates first pseudo-Id to use as ID.

tag is private and informs the tag to use the first identifier from the ID set. This also tells the reader that the tag has not been queried by a fake reader.

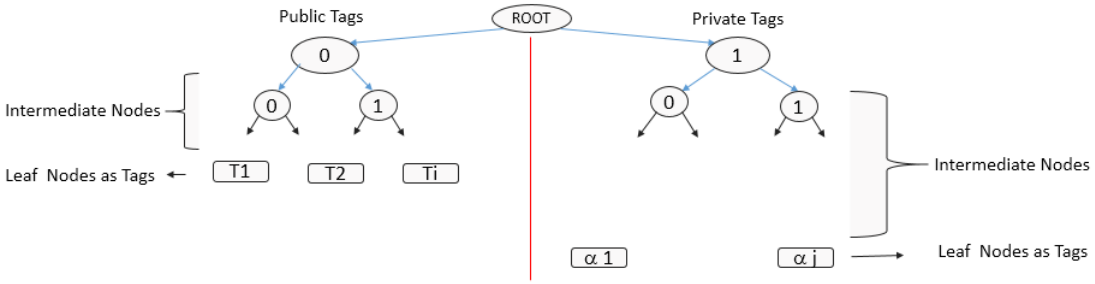

Figure 3.3: Representation of public and private tags

3.2.2 Phases of the proposed scheme

The proposed scheme works in three phases. These phases are explained below.

1. Phase 1: Set-up Phase

   In this phase the RFID application system performs key generation and tag deployment. The key generation task is performed only once. The system

generates public and private keys according to the chosen asymmetric key cryptographic protocol like RSA. Deployment of tags is a complex process in which each tag is given a unique set of IDs referred to as S.

(a) Key Generation: Public Key (P_k)
Private Key (S_k)

(b) Tag Deployment: The tags are assigned unique serial numbers. Public tags can be deployed normally. Their serial number serves as ID for identification. Status Word is set as "00000001".
Private tags are deployed according to the following steps:

i. For each private tag T_i with serial number ID_i, generate a set of random numbers R.

$$\mathrm{R} = \{\ r_1, r_2, \ldots, r_j\ \}$$

ii. Compute the ID set **S**.

$$S_i = \{\ \alpha_1\ ,\ \alpha_2\ , \ldots\ ,\ \alpha_j\ \}$$

Where $\alpha_j = \mathrm{E}(\ ID_i \parallel r_j\ ,\ P_k)$
j $<2^6$, as 6 bits of SW are used for indexing the pseudoID for tag.

iii. The status word of private tags are set to "10000001"

iv. Generate a random key K_i for the tag T_i.

v. The tuple (S_i , K_i) is stored in the tag T_i.

vi. The tuple (ID_i , K_i) is stored in the *systems* database.

2. Phase 2: Protocol execution

This phase of the scheme is executed when a reader tries to get information about a tag. In this phase two tasks are performed. First a reader identifies the tags in its range and then authenticates the tags with which it wants to exchange information.

(a) Identification: Reader broadcasts a signal requesting the tags in its range to identify themselves. The tags responds to the reader's request with

their serial ID. Since all the tags operate at a common frequency and responds to the reader at the same time, tag collision occurs if there are multiple tags in the reader's range. A tree based anti-collision protocol known as AQS [2, 12] is used for singulation of RFID tags. This protocol has been discussed in Chapter 1. After singulation of tags the reader has the serial-ID of each tag in its range. This ID information can be used by the reader to communicate with a tag avoiding tag collision.

(b) Authentication: To exchange information with a private tag, both the reader and tag needs to be mutually authenticated. Reader has the serial-ID of each tag in its range after identification process. Authentication is performed in four steps discussed below.

i. Step 1: Reader generates a random nonce (R_R) and send it to the tag T_i with serial-ID α_i.

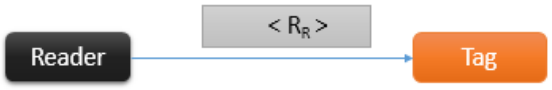

Figure 3.4: Packet 1

ii. Step 2: A tag performs the following operation after receiving a nonce (R_R) from a reader.

A. Computes the hash of $Auth_T$ using its own key k and the stored hash function H.

$$Auth_T = H_k\ (\alpha \parallel R_R)$$

B. Generates a random nonce value R_T.

C. Sends the tuple $<Auth_T, R_T>$back to the reader.

iii. Step 3: The reader performs the following task to authenticate the tag under interrogation.

A. Performs the decryption using the private key of the system (S_k).

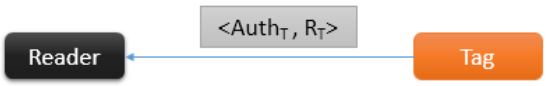

Figure 3.5: Packet 2

$$D(\alpha, S_k) = ID \parallel r$$

B. Parses the decrypted value up to L bits to get the actual ID of the tag as stored in the database of the system.

C. Retrieves the key from the system and computes the hash value using the stored hash function H.

$$Auth_T{}' = H_k(\alpha \parallel R_R)$$

D. Compares the hashed value with $Auth_T$. If the values are equal then the tag is genuine and authenticated to the reader. If the values are not equal then the tag is not a valid tag and the authentication process halts.

$$Auth_T{}' = Auth_T$$

then, the tag is authenticated

else unsuccessful authentication

E. The reader computes $Auth_R$ and sends it back to the tag for mutual authentication.

$$Auth_R = H_k(\alpha \parallel R_T)$$

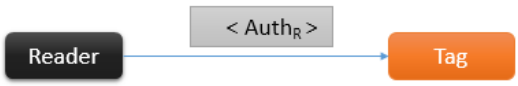

Figure 3.6: Packet 3

iv. Step 4: In this step the tag verifies the authenticity of the reader. The tag computes $Auth_R{}'$ and matches it with $Auth_R$. If the values are equal then the reader is also authenticated to the tag.

$$Auth_R{}' = H_k(\alpha \parallel R_T)$$

then tag and reader are mutually authenticated

else unsuccessful authentication

3. Phase 3: Update

   This step is necessary for preserving privacy. An update is performed based on conditions. The condition may be a successful authentication or an unsuccessful one.

   (a) Successful authentication: The tag updates its SW so that the index represented by SW[3-8] is incremented by one.
   e.g.: initially SW = "10000001"
   After successful authentication it is updated to "10000010"

   (b) Unsuccessful authentication: The tag updates its SW so that the index is incremented by one, as shown in the previous example. It also sets the second bit of the STATUS WORD.

   SW = "11000010"

   When the second bit of SW is set, it indicates the reader that the tag has been queried by a fake reader. The reader updates the identifier set S of the tag to preserve privacy.

3.3 Summary

In this chapter, we presented our proposed scheme for preserving privacy in RFID systems by describing the four phases. Our scheme uses public key encryption algorithm (e.g. RSA) and a hash function for the purpose of mutual authentication. This scheme does not impose burden on the tag to perform cryptographic encryption/decryption.

Chapter 4

Evaluation of proposed scheme

4.1 Implementation

The scheme is implemented using java. MySql database is used as the back-end database to store the information about tags. The implementation contain four important classes which are RFIDTags, Reader, Server, Env. RFIDTags and Reader class are analogous to tags and readers in the RFID system where as server is analogous to application system. Env class is the module which creates an environment where readers interrogate tags. It assumes that tags are static and are within the range of the reader.

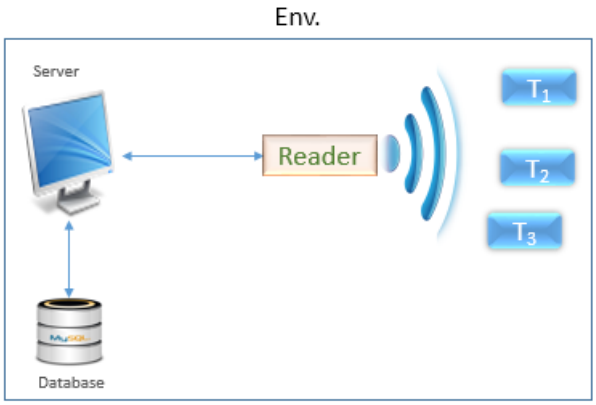

Figure 4.1: RFID system environment

We have used the tree-walking singulation protocol to resolve the issue of tag collision during identification of RFID tags. There are many tree based singulation protocols out of which we have used the AQS singulation protocol because it has lesser number of transmissions compared to all other protocols. It also has lesser number of collisions. The algorithm for Tree Generation is presented below:

Algorithm 1: Tree Generation Algorithm

Result: Returns a binary tree

Data: root, pref, next_bit

```
if pref == NULL then
    if next_bit == 0 then
        Add a node to the left of root with label 0;
    else
        Add a node to the right of root with label 1;
    end
else
    Traverse tree from root according to bits in the pref reaching a node N;
    if next_bit == 0 then
        Add a node to the left of N with label pref || 0;
    else
        Add a node to the right of N with label pref || 1;
    end
end
pref = pref || next_bit;
```

The singulation algorithm is presented below:

Algorithm 2: Singulation Algorithm

Result: Returns a tree where each leaf node is a tag-ID

Data: A, root, L

```
1  pref = NULL, stack[L] = empty, top = -1, coll_bit = -1, next_bit = 0, len =
   pref.length;
2  for all elements in A do
3      if A[i][len] != next_bit then
4          top = top+1 ;
5          push pref || coll_bit to stack ;
6      end
7  end
8  while top != -1 do
9      if len < L then
10         if pref matches prefix of A[i] then
11             next_bit = A[i][len+1] ;
12             Repeat steps 2-6
13         end
14     else
15         pref = stack[top];
16         next_bit = last bit of stack[top];
17     end
18     root = Generate(root, pref, next_bit);
19 end
```

Table 4.1: Notations used in algorithm

Notation	Definition
A	Array of addresses of tags within the range of a reader.
root	Root of the tree which is constructed by the walking tree singulation protocol
L	Length of ID of a tag
$\|\|$	Concatenation operator

4.2 Challenges and Security Attacks

RFID systems faces two important challenges regarding privacy which are clandestine tracking and clandestine inventorying as mentioned in [4]. Our scheme satisfies the requirements to avoid both these problems. The tags responds with different IDs in successive interrogations which confuses the reader and avoids tracking. Our scheme also has a layout for authentication mechanism that prevents illegal readers from obtaining personal information stored in tags.

4.2.1 Security Attacks

There are many known security attacks on RFID systems, some of which are eavesdropping, desynchronization, spoofing, replaying. We analyse our scheme against each of these security attacks.

Eavesdropping

Tags responds to reader's request with a pseudo-ID which is encrypted with RSA by the application system and stored in the tags. An adversary listening to the transmissions cannot decrypt the pseudo-ID to get the actual ID. Mutual authentication is solely based on one-way hash function. Based on the difficulty of inverting an OWF, it prevents an illegal reader from getting any information

regarding the key of a tag.

Desynchronization

This attack is a major concern in hash based RFID mutual authentication protocols [11]. Desynchronization attack is possible in authentication protocols where the tag and application system shares a common secret and updates that secret with each successful authentication. In this scheme the application system and tags do share a secret, that is the secret key k_i for tag T_i, but the system and tags are not synchronized. There is no synchronization information stored in the application system about the tag apart from the secret key and tag's ID.

Spoofing

In this attack an adversary A impersonate a legal tag. An attacker cannot rewrite or replace tags and pass the authentication process successfully. The tag's information may be modified by an attacker but the tag cannot validate its authenticity as discussed below:

Table 4.3: Notations and Definitions

Notation	Definition
S	Legal set of Pseudo-ID
S´	Tampered set of pseudo-ID
k	Legitimate key
k´	Tampered key

The information stored in the tag, which is (S, k), can be modified

S = $\{\alpha_1, \alpha_2, .. , \alpha_m\}$

S´= $\{\alpha'_1 , \alpha'_2 , .. , \alpha'_m\}$

In this case the hash value $Auth_T$ as mentioned in chapter 3 doesn't match $Auth'_T$ as computed by the reader. The reader will know that the tag is not a legal instance.

Replaying

In this attack an adversary gathers information from a session of authentication and tries to get further information using it later. The proposed scheme is not susceptible to reply attack because for each authentication session a new random nonce is generated. $Auth_T$ sent by attacker will not match $Auth'_T$ computed by the reader.

4.3 Complexity Analysis

We used Adaptive Query Splitting (AQS) [2, 12] protocol for avoiding tag collision during tag identification. AQS makes the least number of collisions and has the least number of transmitted bits as compared to other anti-collision protocols. The authentication mechanism requires three transmissions, two from the reader and once from the tag. Searching the key in the database is of constant time as it requires only one decryption operation to get the actual ID of a tag from its pseudo-ID.

Table 4.5: Comparison of Authentication Schemes

Scheme	$Reader_{time}$	Tag_{time}	$Reader_{space}$	Tag_{space}	Comm.
WSRE [4]	O(N)	O(1)	O(N)	O(1)	O(1)
MSW [7]	O(logN)	O(logN)	O(1)	O(logN)	O(logN)
OSK [7]	O(N)	O(1)	O(N)	O(1)	O(1)
Our Scheme	O(1)	O(1)	O(1)	O(m)	O(1)

i. $Reader_{time}$: Time taken by an RFID-reader to obtain key of the tag once it is identified with its pseudo-ID α.

ii. Tag_{time} : Time taken by an RFID-tag to authenticate itself to a reader.

iii. $Reader_{space}$: Space requirement for the reader to authenticate an RFID-tag.

iv. Tag_{space} : Space requirement for the tag to get authenticated by an RFID-reader.

v. Comm. : Number of communications between reader and tag during the authentication session.

Justification regarding the claims of our scheme

$Reader_{time}$ **O(1)** : Reader performs only one decryption operation to obtain the key of a tag from the database. Hence, the retrieval of key is of constant time, independent of the number of tags in the RFID-System.

Tag_{time} **O(1)** : A tag performs only two hashing operations for authentication, independent of the number of tags.

$Reader_{space}$ **O(1)** : A reader uses the pseudonym (α) obtained from singulation to authenticate a tag. The length of the pseudonym is same for all private tags chosen by the system.

Tag_{Space} **O(m)** : A tag is required to store its pseudo-ID set S, hash values and nonce. Tag space depends on the size of S, i.e. m.

$Comm.$ **O(1)** : A total of three transmissions are required for mutual authentication.

We compared our scheme with OSK. $Fig.4.2$ shows the result of authenticating a group of tags and $Fig.4.3$ shows the result of authenticating a single tag. It can be

clearly concluded that the proposed scheme takes lesser time to authenticate large number of tags as compared to OSK. Further, our proposed scheme authenticates a tag in constant time.

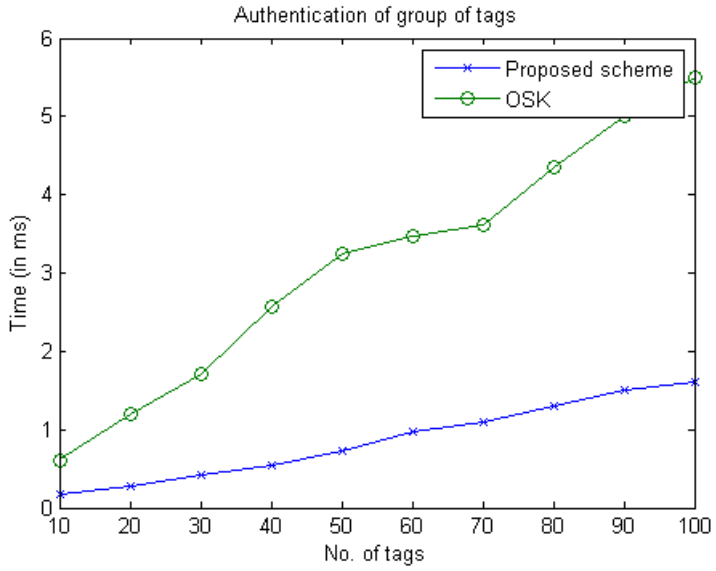

Figure 4.2: Authenticating a number of tags

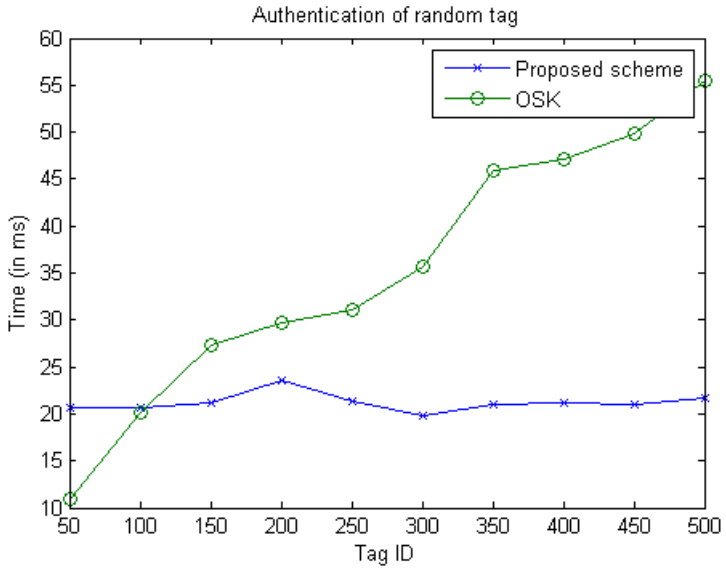

Figure 4.3: Authenticating a single tag

4.4 Summary

In this chapter we analysed our scheme against probable security attacks in RFID systems. Our scheme has an advantage that a tag can inform a genuine reader about a fake interrogation in the past. This helps the reader to change the pseudo-ID set S of the tag to avoid tracking. The key management problem is solved with a key search in constant time.

Chapter 5

Conclusion

This thesis deals with preserving privacy in RFID systems. The scheme proposed in this thesis avoids the issues of traceability, eavesdropping and desynchronization which are of a major concern in RFID systems. Traceability of tagged objects or person by illegal reader is a major challenge in RFID systems. Therefore, we have presented a layout of mutual authentication scheme that authenticates a reader before sharing sensitive information stored in the tags. The tags avoids tracking by confusing the reader by responding with different pseudo-ID in each successive interrogation. A genuine reader can track an object or person by identifying the attached tag, but a fake reader cannot.

Our proposed scheme uses public key encryption algorithms for preserving privacy in RFID systems. The RFID tags doesn't have to bear the burden of computation regarding encryption/decryption. The only resource intensive operation to be performed by a tag is hashing and generating random numbers.

Scope for Future Research

In our proposed scheme the only resource intensive task performed by an RFID tag is computing a hash function. Light-weight hash functions will surely reduce the burden of a tag.

Bibliography

[1] Myung, Jihoon, and Wonjun Lee. "An adaptive memoryless tag anti-collision protocol for RFID networks." In IEEE INFOCOM, vol. 5. 2005.

[2] Myung, Jihoon, and Wonjun Lee. "Adaptive splitting protocols for RFID tag collision arbitration." In Proceedings of the 7th ACM international symposium on Mobile ad hoc networking and computing, pp. 202-213. ACM, 2006.

[3] Jia, Xiaolin, Quanyuan Feng, Taihua Fan, and Quanshui Lei. "RFID technology and its applications in Internet of Things (IoT)." In Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on, pp. 1282-1285. IEEE, 2012.

[4] Juels, Ari. "RFID security and privacy: A research survey." Selected Areas in Communications, IEEE Journal on 24, vol. 2 (2006): 381-394.

[5] Sarma, Sanjay E., Stephen A. Weis, and Daniel W. Engels. "RFID systems and security and privacy implications." In Cryptographic Hardware and Embedded Systems-CHES 2002, pp. 454-469. Springer Berlin Heidelberg, 2003.

[6] Juels, Ari, Ronald L. Rivest, and Michael Szydlo. "The blocker tag: selective blocking of RFID tags for consumer privacy." In Proceedings of the 10th ACM conference on Computer and communications security, pp. 103-111. ACM, 2003.

[7] Ryu, Eun-Kyung, and Tsuyoshi Takagi. "A hybrid approach for privacy-preserving RFID tags." Computer Standards & Interfaces 31.4 (2009): 812-815.

[8] Weis, Stephen A., Sanjay E. Sarma, Ronald L. Rivest, and Daniel W. Engels. "Security and privacy aspects of low-cost radio frequency identification systems." In Security in pervasive computing, pp. 201-212. Springer Berlin Heidelberg, 2004.

[9] Ohkubo, Miyako, Koutarou Suzuki, and Shingo Kinoshita. "RFID privacy issues and technical challenges." Communications of the ACM 48, vol. 9 (2005): 66-71.

[10] Molnar, David, Andrea Soppera, and David Wagner. "A scalable, delegatable pseudonym protocol enabling ownership transfer of RFID tags." In Selected Areas in Cryptography, pp. 276-290. Springer Berlin Heidelberg, 2006.

[11] Kim, Hyunsung. "Desynchronization attack on hash-based RFID mutual authentication protocol." Journal of Security Engineering 9, vol. 4 (2012).

[12] Myung, Jihoon, and Wonjun Lee. "Adaptive splitting protocols for RFID tag collision arbitration." In Proceedings of the 7th ACM international symposium on Mobile ad hoc networking and computing, pp. 202-213. ACM, 2006.

[13] Juels, Ari. "Minimalist cryptography for low-cost RFID tags." In Security in Communication Networks, pp. 149-164. Springer Berlin Heidelberg, 2005.

[14] Jia, Xiaolin, Quanyuan Feng, Taihua Fan, and Quanshui Lei. "RFID technology and its applications in Internet of Things (IoT)." In Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on, pp. 1282-1285. IEEE, 2012.

[15] Piramuthu, Selwyn. "Protocols for RFID tag/reader authentication." Decision Support Systems 43, no. 3 (2007): 897-914.

[16] http://www.rfidjournal.com/