Ensuring Application Specific Security, Privacy and Performance Goals in RFID Systems

Farzana Rahman
Marquette University

ENSURING APPLICATION SPECIFIC SECURITY, PRIVACY AND PERFORMANCE GOALS IN RFID SYSTEMS

by

Farzana Rahman

A Dissertation submitted to the Faculty of the Graduate School,
Marquette University,
in Partial Fulfillment of the Requirements for
the Degree of Doctor of Philosophy

Milwaukee, Wisconsin

May 2013

ABSTRACT

ENSURING APPLICATION SPECIFIC SECURITY, PRIVACY AND PERFORMANCE GOALS IN RFID SYSTEMS

Farzana Rahman

Marquette University, 2013

Radio Frequency IDentification (RFID) is an automatic identification technology that uses radio frequency to identify objects. Securing RFID systems and providing privacy in RFID applications has been the focus of much academic work lately. To ensure universal acceptance of RFID technology, security and privacy issued must be addressed into the design of any RFID application. Due to the constraints on memory, power, storage capacity, and amount of logic on RFID devices, traditional public key based strong security mechanisms are unsuitable for them. Usually, low cost general authentication protocols are used to secure RFID systems. However, the generic authentication protocols provide relatively low performance for different types of RFID applications. We identified that each RFID application has unique research challenges and different performance bottlenecks based on the characteristics of the system. One strategy is to devise security protocols such that application specific goals are met and system specific performance requirements are maximized.

This dissertation aims to address the problem of devising application specific security protocols for current and next generation RFID systems so that in each application area maximum performance can be achieved and system specific goals are met. In this dissertation, we propose four different authentication techniques for RFID technologies, providing solutions to the following research issues: 1) detecting counterfeit as well as ensuring low response time in large scale RFID systems, 2) preserving privacy and maintaining scalability in RFID based healthcare systems, 3) ensuring security and survivability of Computational RFID (CRFID) networks, and 4) detecting missing WISP tags efficiently to ensure reliability of CRFID based system's decision. The techniques presented in this dissertation achieve good levels of privacy, provide security, scale to large systems, and can be implemented on resource-constrained RFID devices.

ACKNOWLEDGMENTS

This work is the result of my PhD studies at Marquette University. During this period, many persons happened to cross my way. It is likely that I may forget some important names. But here I want to shortly recall some of those people who I deeply interacted with and therefore, in a way or another, impacted my dissertation work.

I would like to express my heartfelt gratitude to my supervisor, Dr. Sheikh Iqbal Ahamed. I have learned great things from him in all these years. His critical and invaluable suggestions and guidance have refined and polished my PhD Work.

I'm also grateful to all the dissertation committee members, Dr. Brylow, Dr. Zulkernine, Dr. Madiraju, and Dr. Ahmed, for their invaluable comments and patience during the preparation of this dissertation. I would also like to thank Dr. Stephen Merrill and Dr. Gary Krenz, who helped me a lot to build up my self-confidence during all these years. I am thankful to my fellow UbiComp lab members for their benevolent support and valuable advice, which were very useful to drive the research towards the right direction.

I would like to thank my parents for giving me a wonderful childhood. Their love, trust and support have given me great comforts and encouragements through my entire life. I can never thank them enough. I want to thank my loving sister for believing in me more than I believe in myself. My sincere gratitude goes to my in-laws who were very supportive during every step of my PhD studies. Many thanks must go to my wonderful friends in Milwaukee, West Lafayette, Bangladesh, and everywhere else.

Most of all, my special thanks go to my husband, Md. Endadul Hoque, for his never ending support, for making me believe that I am capable, and for always being there with me. I would like to thank him for encouraging me, helping me, and always "tolerating me!". I can never even have made this journey without his endless support and trust. Finally, thanks to God for what He has done for me.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS AND ELABORATIONS

TERM	ELABORATION
ABAC	Attribute Based Access Control
ACL	Access Control List
CA	Certification Authority
CRFID	Computational RFID
BD	Database
BR	Bit Record
DoS	Denial-of-Service
EDFSA	Efficient Dynamic Framed Slotted ALOHA
EPC	Electronic Product Code
FSA	Framed Slotted ALOHA
IFF	Identify Friend or Foe
MAC	Message Authentication Code
MIM	Man-in-the-Middle
OSK	Ohkubo-Suzki-Kinoshita
P-RBAC	Purpose Based Access Control
PRNG	Pseudo-Random Number Generator
PRF	Pseudo-Random Function
RF	Radio Frequency
RFID	Radio Frequency IDentification
RBAC	Role Based Access Control
SP	Slot Position
UHF	Ultra High Frequency
WISP	Wireless Identification and Sensing Platform

WWII	World War II
XOR	eXclusive OR
XACML	eXtensible Access Control Markup Language

Chapter 1: Introduction

Radio Frequency IDentification (RFID) is an automatic identification technology that uses radio waves to identify objects such as products, animals or persons. Each RFID system has three main components: tag, reader, and database. An RFID reader and an RFID tag communicate via a wireless radio communication channel. The basic idea of RFID technology is an automatic identification technique, which relies on storing and remotely retrieving data about objects we want to manage using RFID tags. Some popular applications of RFID technology are product tracking in a supply chain [Li07], toll payments [Mayes09], military applications and access control [Juels05a], patient recognition in hospitals [Juels05a], automatic vehicle identification [Juels05a], point of sale applications [Juels05a], library book administration [Juels05a], and e-passports [Juels05b].

Near field communication (NFC) [NFC] is a similar technology like RFID with much less capability. NFC is a subset of RFID that limits the range of communication to within 10 centimeters or 4 inches. However, one advantage of NFC is that some mobile phones are being equipped with NFC now-a-days. But this advantage of NFC is overshadowed by its limitations, like: NFC has a very limited range and it cannot be programmed like active RFID tags. Therefore, it cannot be used in applications where the reading range has to be in meters. It cannot be used in many sophisticated applications where the active tag has to be programmed for special purpose. Specially, in most of the healthcare applications (like: pharmaceutical drug tracking, patient specific meal dispatch and such sophisticated application) longer range and tag programming capability is required. Since RFID tags can be read in longer range and it can be programmed for special purpose, it has become popular over the last decade in many real life application areas.

We envision that low-cost RFID tags will be attached to every object in our daily lives, from clothes, books, and pens, to very small objects, such as pins and buttons. Annotating objects around us with tags gives us an enormous advantage in connecting the physical world with the

cyber-world so that people can easily obtain information about the environment and physical objects. We believe that more powerful tags and readers in the future promise many more applications based on how we may use those tags.

Unit cost per tag is a major consideration for RFID tags because some applications need low cost tags. Cost may be a secondary consideration in passports or credit cards because security is paramount and these devices may pass that cost on to the consumer without much concern. In an application like product tagging, cost is paramount, and the cost per tag needs to be low; otherwise, the benefits of RFID are outweighed by the cost.

However, simply integrating RFID technology into the above mentioned applications will not ensure that the needed services are provided adequately, because RFID systems operate untrusted environments, for which adversaries motivated by different purposes may attack the system. Some will block readers from hearing tags. Further, attackers may attempt to hide within a group of authorized users in an attempt to eavesdrop private information. Moreover, privacy is an issue that could hinder the wider use of RFID. Furthermore, privacy will become an even more important issue as RFID technology is pervasively applied. To ensure a wider use of RFID technology, security must be included into any design of applications. In some systems one must make sure the communication between tags and readers is confidential and authenticated, in other systems the information provided by the tags needs to be authenticated and in other systems the access to the RFID systems, including tags, readers and other related equipment should be classified against unauthorized parties.

Securing RFID systems and providing privacy in RFID consumer applications has been the focus of much academic work lately. Due to the constraints on memory, power, computation capacity, and limitations of logic on RFID devices, standard cryptographic primitives are often unsuitable for them. Therefore, researchers focused on developing general authentication protocols based on lightweight cryptographic tools to ensure the security and privacy of RFID systems. However, these generic authentication protocols provide relatively low performance for

different types of RFID applications. There was no validated explanation as to why achieving a generalized security solution with maximum system performance is not possible for all RFID systems. With deeper investigation of existing RFID applications and analysis of authentication protocols, we identified that each RFID application has different underlying research challenges and a different set of performance bottlenecks based on the unique characteristics of the system. One strategy is to devise security protocols such that application specific goals are met and system specific performance requirements are maximized. For example:

1) The main challenge in an RFID based supply chain is to detect counterfeit products at the same time ensure low system response time.

2) Systems like, RFID-based healthcare, e-passports, and office personnel monitoring are more focused on ensuring privacy and maintaining scalability.

3) More sophisticated applications like RFID-installed military networks are more focused on maintaining system survivability without sacrificing system's performance.

All these applications of RFID technology have a different set of research challenges in meeting their system specific goals.

The aim of this dissertation is to make several contributions to address the problem of devising application specific security protocols for the current and next generation of RFID systems so that in each application area maximum performance can be achieved and other system specific goals are met. Since ensuring security is the common goal in almost any RFID system, our major focus has been to develop and implement authentication protocols to solve the identified research issues using lightweight operations like hash functions, XOR operations or pseudorandom number generation.

1.1. Dissertation Focus

In this dissertation, we focus on understanding different research challenges corresponding to four different applications of current and next generation RFID systems, so that

in each application area maximum performance can be achieved and other system specific goals are met. Though there can be numbers of different RFID applications, most of them fall under the umbrella of the four RFID application areas that are mentioned in this dissertation. Therefore, the contribution of this dissertation makes an effort to address the security, privacy and performance goals of many common RFID applications, as well as providing solution to the following research issues of four major specific RFID application areas:

1) Detecting counterfeits in large-scale RFID systems

2) Preserving privacy in RFID based healthcare systems

3) Ensuring survivability of Computational RFID (CRFID) systems

4) Ensuring reliability of system's decision in CRFID based critical systems

1.2. Major Contributions

In this section, we briefly summarize the contributions of this dissertation. In this dissertation, first, we describe the properties of a typical RFID and Computational RFID system in Chapter 2. Next, in Chapter 3, we summarize all the possible attacks that can be launched against RFID systems and how our proposed approaches can defend against those problems. Then, in Chapter 4, we point out the security, privacy and performance goals that should be guaranteed by RFID protocols to defend against various attacks. Throughout the dissertation, we use four different RFID applications as a motivating example of RFID systems with a strong demand for various goals mentioned in Chapter 4. In this same chapter, we also present how these goals are achieved by our proposed four RFID protocols. Then, in Chapter 6, 7, 8 and 9, we present our approaches that propose defense mechanisms against various attacks as well as ensure application specific goals mentioned in chapter 4. Our proposed approaches to ensure security, privacy and system specific goals in four different RFID application areas are as follows:

- **Detecting counterfeits in large-scale RFID systems:** In Chapter 6 we have introduced the concept of batch authentication for detecting counterfeits efficiently. In large-scale RFID

applications (such as supply chain, pharmaceutical industry, etc.), general authentication is used to detect counterfeit products. However, general authentication protocols are mainly per-tag based where the reader needs to authenticate tags sequentially and one at a time. This increases the protocol execution time due to a large volume of authentication data. To solve this issue, we proposed to detect counterfeit tags by verifying the objects in batches. We present a batch authentication protocol named *FTest* to meet the requirements of prompt and reliable counterfeit tag detection. The novel discovery of this work is that the batch authentication can reduce the system response time while performing significantly better than existing counterfeit detection approaches.

- **Preserving privacy in RFID based healthcare systems:** In Chapter 7, we have identified the two major types of privacy preservation techniques that are required in RFID-based healthcare: 1) a privacy preserving authentication protocol is required while sensing RFID tags for different identification and monitoring purposes and 2) a privacy preserving access control mechanism is required to restrict unauthorized access of private information while providing healthcare services using the tag ID. We designed and developed a "*two component based framework*" that makes an effort to address the above mentioned two privacy issues. One component of the framework is a privacy preserving authentication protocol that provides more privacy than the existing approaches when RFID tags are sensed by a nearby legitimate reader. The other component of the framework allows authenticated user access in the information system. This system consists of both the ID of the RFID tag and its corresponding usage history. To the best of our knowledge, it is the first framework to provide increased privacy in RFID-based healthcare systems, using RFID authentication along with access control techniques.
- **Ensuring survivability of Computational RFID (CRFID) systems:** In Chapter 8, we propose a robust authentication protocol to defend against the DoS attack in CRFID systems. Due to the sensing capability of CRFID tags, recently they have been used in many sophisticated applications like physiological signal monitoring in home healthcare systems, enemy move

detection in military battlefield, activity inference, etc. In these types of CRFID applications, an adversary may launch DoS attack by de-synchronizing the tags with the reader. This may jeopardize the survivability of the system. In an effort to address the survivability issues of CRFID systems, we propose DRAP protocol. DRAP allows both tag and reader to communicate successfully with each other and provide service even if the adversary launches De-synchronization or DoS attack.

- **Ensuring reliability of system's decision in CRFID based critical systems:** In Chapter 9 we have studied the problem of monitoring a large set of WISP tags and identifying the missing tags in CRFID-based critical systems. Recently, CRFID tags have been used in many critical applications like monitoring indoor activity, vital signs, sleep quality, and health status remotely. These types of systems make critical decisions based on the data collected from each individual tag in the system and perform collective information analysis. Hence, the absence of any tag data may eventually introduce serious error into the decision making process of the system. To address this, we propose two tag monitoring protocols for WISP based critical systems based on probabilistic methods. Our approach proposes a secure protocol to monitor for missing tags and for collecting sensor values from existing tags only, to reduce system response time of CRFID based critical systems.

- In chapter 6, 7, 8, and 9 we propose four different protocols for four example RFID application areas. Though we have used specific application scenario as a motivating example, most of the RFID systems fall within the category of one of these application types. Figure 1.1 presents a summary of what security, privacy and performance goals are achieved by our proposed protocols.

We emphasize that we do not consider in our work low-level criteria such as gate count or power consumption of tags because, although important, these depend on the implementation of the building blocks. Instead, we focus on the protocols, their efficiency, and the security and privacy level they achieve. The techniques presented in this dissertation achieve good levels of

privacy, provide security, scale to large systems, and can be implemented on resource-constrained RFID devices. From now on we refer to Computational RFID systems as CRFID systems.

Table 1.1 Security, Privacy and Performance goals addressed by our proposed protocols

	Privacy Violation	Access of data	DoS/De-Synchronization	Spoofing	Tracking	Eavesdropping	Scalability	Low response time
Ftest Protocol (Chapter 6)	**X**	**X**	**NA**	**X**	**X**	**X**	**X**	**X**
PriSens Protocol (Chapter 7)	**X**	**X**	**NA**	**X**	**X**	**X**	**X**	**X**
DRAP Protocol (Chapter 8)	**X**	**X**	**X**	**X**	**X**	**X**		**X**
MTD Protocol (Chapter 9)	**X**	**X**	**NA**	**X**	**X**	**X**	**X**	

Assumptions in our Proposed Approaches: For the rest of the dissertation, we consider typical RFID tags that are capable of generating Pseudo Random Number (PRNG), performing simple hash function and XOR operation. From this point on and in the rest of the dissertation, we use Computational RFID and CRFID interchangeably. Like majority of the literature on RFID security, in all of our approaches, we assume that the channel between server and reader is secure. We also assume the physical security of the devices involved, like an intruder not being able to have physical access to the contents of the truck.

1.3. Dissertation Organization

The rest of this dissertation is organized as follows:

- In Chapter 2, we present a brief description of RFID technology. We first discuss the historical perspective of RFID technology. Next in this section, we discuss different components of RFID systems and their constraints. Next, we introduce *Computational RFID* (CRFID) technology.

- In Chapter 3, we start by pointing out the attack objectives and goals of an RFID system attacker. Then we briefly discuss the security requirements of RFID systems and RFID protocols. Next we define different types of adversary. This is followed by a detailed discussion of different types of attacks in RFID systems and attack intentions of an adversary.
- In Chapter 4, we briefly describe the security, privacy and performance goals that should be guaranteed by most RFID applications. We also point out some system specific goals that should be guaranteed by authentication protocols to ensure maximum system functionality. At the end of this section we present a summary of which goals are satisfied by our proposed RFID authentication protocols.
- In Chapter 5, we discuss some classic and some recently proposed RFID protocols that use symmetric cryptography to ensure the identified privacy, security and performance requirements.
- In Chapter 6, we present our motivation for addressing the issue of batch authentication in large scale supply chain. The rest of the chapter presents the details of our proposed protocols (GTest and FTest), analysis, and evaluation results.
- In Chapter 7, we introduce the notion of the two-fold privacy preservation issue in RFID based healthcare systems. The rest of the chapter presents the details of our proposed privacy preserving framework (PriSens-HSAC), security analysis, and evaluation results.
- In Chapter 8, we introduce the issue of survivability in CRFID networks. The rest of the chapter briefly presents the details of our proposed protocol (DRAP), security analysis, and evaluation results.
- In Chapter 9, we introduce the notion of missing tag monitoring in CRFID based home healthcare systems. The rest of the chapter briefly presents the details of our proposed missing tag detection protocol (MTD), security analysis, and evaluation results.

- In Chapter 10, we summarize the contributions of this dissertation, and identify future research directions.

1.4. Publications

In this section, we list out the publications that forms the basis this dissertation.

1.4.1. Publication based on the contributions of the dissertation

- ***The contribution of chapter 4, i.e. the literature survey on attacks on RFID systems forms the base of a paper that we have submitted in Journal of ACM Computing Surveys.***

- ***The proposed methodologies of Chapter 6 have been published and they are as follows:***

Published [Rahman12a]: *Farzana Rahman* and Sheikh Iqbal Ahamed, "Looking for needles in a haystack: Detecting Counterfeits in Large Scale RFID Systems using Batch Authentication Protocol", *In Proc. of IEEE PerCom Workshop on Pervasive Wireless Networking (PWN12)*. Switzerland. 2012. pp. 811 - 816. [Acceptance rate: 20%]

In Press [Rahman12c]: Farzana Rahman and Sheikh Iqbal Ahamed, "Efficient Detection of Counterfeit Products in Large Scale RFID Systems with Batch Authentication Protocols", *Accepted to be published in Journal of Personal and Ubiquitous Computing*, Springer-Verlag. 2012.

- ***The proposed methodologies of Chapter 7 have been published and they are as follows:***

Published [Rahman12b]: *Farzana Rahman* and Sheikh Iqbal Ahamed, "I am not a goldfish in a bowl: A Privacy Preserving Framework for RFID based Healthcare Systems", *In Proc. of IEEE 14th International Conference on e-Health Networking, Applications and Services* (IEEE Healthcom 2012). China. 2012. [*Best paper winner*]

Published [Hoque11]: Md. Endadul Hoque, *Farzana Rahman*, and Sheikh I. Ahamed, "AnonPri: An Efficient Anonymous Private Authentication Protocol", *In Proc. of IEEE*

International Conference on Pervasive Computing and Communications (PerCom 2011), WA, USA. 2011. pp.102-110. [Acceptance rate: 11%]

Under Review: *Farzana Rahman* and Sheikh Iqbal Ahamed, "A Privacy Preserving Framework for RFID based Healthcare Systems", *In a journal*.

- ***The proposed methodologies of Chapter 8 have been published and they are as follows:***

Published [Rahman12d]: *Farzana Rahman* and Sheikh Iqbal Ahamed, "DRAP: A Robust Authentication Protocol to Ensure Survivability of Computational RFID Networks", *In Proc. of ACM Symposium on Applied Computing (SAC 2012)*. Italy. 2012. pp. 498-503.

In Preparation: Farzana Rahman and Sheikh Iqbal Ahamed, "Designing Survivable Computational RFID Systems with Robust Authentication Protocol".

- ***The proposed methodologies of Chapter 9 have been published and they are as follows:***

Published [Rahman12e]: *Farzana Rahman* and Sheikh Iqbal Ahamed, "MonAC: Detecting Missing Tags for Improved Accuracy in Computational RFID based Assisted Environments", *In Proc. of the ACM Symposium on Research in Applied Computation (ACM RACS 2012)*. USA. 2012.

Under Review: *Farzana Rahman* and Sheikh Iqbal Ahamed, "Towards Improving Security and Reliability of Computational RFID based Assisted Environments", *In a journal*.

1.4.2. Other related publications

Notable publications related to this dissertation are as follows: [Ahamed08a, Ahamed08b, Ahamed08c, Ahamed08d, Ahamed08e, Hoque09a, Hoque10a, and Rahman 11].

Chapter 2: Overview of RFID and Computational RFID Technology

The goal of this chapter is to discuss some basics of RFID technology. It starts by highlighting the historical perspective of RFID. Then the technical background of RFID readers and tags are discussed. We also give a description of Computational RFID (CRFID) technology at the end of this chapter.

2.1. Radio Frequency Identification (RFID) Technology

Radio Frequency IDentification (RFID) (Figure 2.1) is the classic pervasive computing technology. At the very beginning, RFID was plugged as the replacement for traditional barcodes and its' wireless identification capabilities promise to revolutionize our industrial, commercial, and medical experiences. What makes RFID unique is that it facilitates information gathering about physical objects easy. Information about RFID tagged objects can be read through physical barriers and from a distance. In line with Mark Weiser's concept of ubiquitous computing [Weiser93, Pervasive1, and Pervasive2], RFID tags could turn our interactions with computing infrastructure into something more ubiquitous than ever before.

Figure 2.1 Different types of RFID tags (Source: [WikiTag])

Unit cost per tag is a major consideration for RFID tags because some applications need low cost tags. Cost may be a secondary consideration in passports or credit cards because security is paramount and these devices may pass that cost on to the consumer without much concern. In

an application like product tagging, cost is paramount, and the cost per tag needs to be low; otherwise, the benefits of RFID are outweighed by the cost. Securing RFID tags and providing privacy in consumer applications, while limiting cost per tag, has been the focus of much academic work. Due to the constraints on memory, power consumption, and amount of logic on RFID devices, standard cryptographic primitives are often unsuitable.

In recent years, numbers of papers have been published providing solutions to RFID security and privacy challenges. One approach to addressing such privacy and security threats is to use a tag authentication scheme in which a tag is both identified and verified in a manner that does not reveal the tag identity to an attacker. However, RFID tags have limited computation power and storage because of the tag cost requirements.

2.2. History and RFID Technology

RFID is an acronym for Radio Frequency IDentification. It designates a large family of technologies and devices all having in common the aim to identify objects or persons with RFID tags. Even if RFID is often thought of as a very new domain, actually it dates back to World War II. British technology IFF (Identify Friend or Foe) was developed in the late 1930s to help the Royal Air Force to distinguish between friendly and hostile aircrafts, and it is the ancestor of RFID technology. Basically, the IFF of WWII and Soviet era systems used coded radar signals to automatically trigger the aircraft transponder in an aircraft identified by the radar. An aircraft responding to an IFF request was then considered a friend, one not responding a foe. This technique was intended to reduce friendly fire. Since then RFID has seen new forms and applications.

Starting in the late 1980s battery powered active RFID devices have been used for automatic toll collecting on motorway (*e.g. Telepass* in Italy). Nevertheless the big revolution, bringing RFID to the attention of common people and media, has certainly been due to the

progresses in miniaturization, which led to very small and cheap tags, well suited to be applied on single packages of products.

2.3. A Typical RFID System Architecture

RFID systems are made up of three main components: RFID tag, RFID reader, and the back-end database. Figure 2.2 illustrates a typical RFID system. In the following subsections, we explain the details of different components of an RFID system.

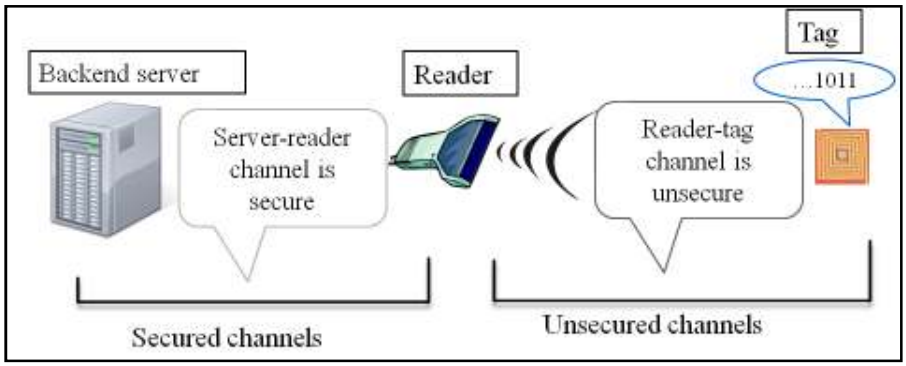


Figure 2.2 Architecture of a simple RFID system

2.3.1. RFID tags or transponder

In an RFID system, each object will be labeled with a tag. Each tag contains a microchip with some computation and storage capabilities and an antenna coil for communication. Tags can be classified according to three main criteria:

A) Memory Type: The memory element serves as writable and non-writable data storage. Tags can be programmed to be *read-only*, *write-once read-many*, or *fully rewritable*. Depending on the kind of tag, tag programming can take place at the manufacturing level or at the application level.

B) Power Source: A tag can obtain power from the signal received from the reader, or it can have its own internal source of power. The way the tag gets its power generally defines the category of the tag.

- ***Passive RFID tags.*** Passive tags do not have an internal source of power. They harvest their power from the reader that sends out electromagnetic waves. They are restricted in

their read/write range as they rely on RF energy from the reader for both power and communication.

- ***Semi-passive RFID tags*.** Semi-passive tags use a battery to run the microchip's circuitry but communicate by harvesting power from the reader signal.
- ***Active RFID tags.*** Active tags possess a power source that is used to run the microchip's circuitry and to broadcast a signal to the reader.

C) Computational capability: Based on the computational capacity of RFID tags, there are mainly two types [Song09]: dumb and smart.

- ***Dumb tags:*** A dumb tag has very low computation capacity, and it has a unique identifier that is of a fixed unique length (usually 10 or 16 hexadecimal digits long) value. The memory capacity of a dumb tag is likely to be fairly small (i.e. hundred bytes to 2kBytes).
- ***Smart tags:*** Smart tags have a small processor built within them that has the capability do some cryptographic operation [Laurie07]. They usually have a larger memory capacity (32kBytes or more) compared to dumb tags. Smart tags can perform authentication before allowing access to the stored data. Such a tag can encrypt communications to avoid some major attacks [Laurie07].

2.3.2. RFID Readers or Transceiver

RFID readers are generally composed of an RF module, a control unit, and an antenna element to interrogate electronic tags via RF communication. Readers may have better internal storage and processing capabilities than the tags they interrogate, and they frequently have a connection to backend databases. Complex computations, such as all kinds of cryptographic operations, may be carried out by RFID readers. Figure 2.3 shows an RFID reader.

Figure 2.3 A simple RFID reader (Source: [Reader])

2.3.3. Back-end server

The information provided by tags is usually an index to a back-end server (pointers, randomized *id*s, etc.). This limits the information stored in tags to only a few bits, which is a sensible choice due to severe tag limitations in processing and storing. It is generally assumed that the connection between readers and back-end server is secure, since processing and storing constraints are not so tight in readers.

2.3.4. Constraints on the RFID System

The constraints on the two main components of an RFID system are as follows:

A) Constraints on the tags:

1) Tag is passive: It has no batteries. It can operate just when interrogated by a reader and only for a short time after each interrogation.

2) Tag has limited memory: Each tag has on board only a few kilobits of memory to store its *id* and its secrets. At present the majority of the tags can just save a fixed 96-bit *id*. Nevertheless, we consider more sophisticated tags where some more memory is available otherwise there would be no space for any cryptographic data.

3) Tag has limited computational abilities: Each tag can perform only basic calculations, hash calculations, PRNG, AES 2. Public-key cryptography is quite expensive.

4) Tag provides no physical security: Each tag can be physically opened, thus revealing the complete contents of its memory.

5) Tag communicates up to a fixed distance: The tag-to-reader communication is limited to a few meters, but the reader-to-tag communication could be eavesdropped at a greater distance.

B) Constraints on the reader:

While having constraints on the tag seems quite obvious, it might appear that there is no constraints on the reader side. However, the constraints of the readers are mainly associated with the complexity of the reader-side algorithms. Many RFID systems consist of millions of tags. The main concern on the reader is the number of cryptographic operations needed to identify tags. These identification costs increase if computation intensive cryptographic functions are used. Therefore, to keep the reader's response time moderate, efficient and scalable protocols need to be designed and deployed that take these constraints into account.

2.3.5. Assumptions in Typical RFID Systems

Usually the following assumptions are made about the availability of cryptographic functions in RFID tags.

- There are sufficiently secure hash functions, which are suitable for a low-cost tag.
- There is a sufficiently secure pseudo-random number generator for a low-cost tag.

2.3.6. RFID Standards

As with any technology, lack of standards leads to inefficiencies because customers have to rely on a single equipment provider. Even the well-known EPC standard is not yet fully standardized. Another problem is that frequency regulations are not internationally standardized. EPC Global standardizes different categories of devices, in relation with the technical characteristics and functionalities provided by the tag. Each class includes all the properties of the previous and adds some new. The summary of EPC class is showed in Table 2.1.

Table 2.1 EPC class types

Class type	Specification
Class 0	Read only tags
Class 1	Write once, read many tags
Class 1 Gen 2	Write once, read many tags, UHF Gen 2 protocol
Class 2	Rewritable tags
Class 3	Semi-passive tags
Class 4	Active tags

Class 0: Class 0 tags are the simplest type of tags, where the data, which are usually a simple *id* number (EPC), are written into the tag only once during manufacture. No further updates are possible. These tags announce their presence when passing through an antenna field.

Class 1: Class 1 tags are manufactured with no data written into the memory. Data can either be written by the tag manufacturer or by the user, but only once. After this no further update is possible and the tag can only be read.

Class 2: Class 2 tags allow users to both read and write data into the tag's memory. They are typically used as data loggers and therefore contain more memory space than tags that carry only simple ID numbers.

Class 3: Class 3 tags are just like class 2 tags except that they contain on-board sensors for recording parameters like temperature and pressure into the tag's memory. As sensor readings must be loaded into memory in the absence of the reader, the tags are either semi-passive or active, thus requiring an on-board power source.

Class 4: Class 4 tags are equipped with integrated transmitters. These tags are similar to radio devices, which can communicate with other tags and devices in the absence of a reader.

Presently deployed Gen 1 RFID systems are based on a number of competing protocols, most notably Matric's Class 0 and Alien Technology's Class 1. There is a problem that these protocols are proprietary. Beyond that, they lack the features, reliability and power to adequately serve the growing number of applications, particularly when taking worldwide operability into account. MIT's Auto-ID Center recognized these problems and created a single open standard that would firstly create an environment of interoperability and international regulatory compliance and secondly raise the bar on RFID system performance in a significant way. These two values formed the backbone of the EPC Gen 2 UHF standard. With a single worldwide specification in place, UHF RFID-based systems are expected to become faster, easier to use, less costly to deploy and more robust.

2.4. Introduction to Computational RFID (CRFID) Technology

Table 2.2 Comparison of different technologies [RFID_Journal**]**

	CPU	**Sensing**	**Size (inches)**	**Range**	**Power**	**Lifetime**
WSN (Mote)	Yes	Yes	3.0 x 1.3 x .82 (2.16 in^3)	Any	Battery	< 3 yrs
RFID tag	No	No	6.1 x 0.7 x .02 (.08 in^3)	30 ft	Harvested	Indefinite
CRFID (WISP)	Yes	Yes	5.5 x 0.5 x .10 (.60 in^3)	10 ft	Harvested	Indefinite

Despite many successes of RFID technology and various applications of wireless sensor networks, none of them has led to an approximation of sensing embedded in the fabric of everyday life, where walls, clothes, products, and personal items are all equipped with networked sensors. For this type of deployment, truly unobtrusive sensing devices are necessary. The size and finite lifetime of motes make them unsuitable for these applications. One recent extension of RFID, Computational RFID (CRFID) [Buettner08b, Sample08], which has some exciting sensing capabilities, presents numerous possibilities for many future pervasive computing applications. CRFID combines the advantages of RFID with those of sensor networks. As discussed, two

technologies, wireless sensor networks and RFID, have been widely used to realize real-world applications. But CRFID presents the combination of both of these networks. The comparison of these three technologies is presented in Table 2.2.

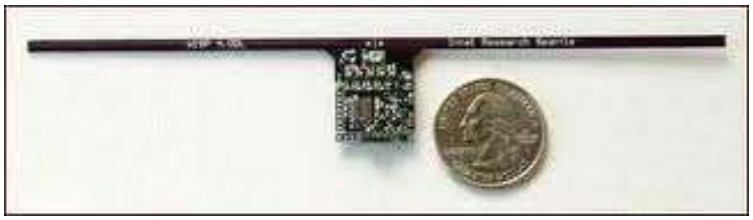


Figure 2.4 Wireless Identification and Sensing Platform (WISP) tag's size (Source: [RFID_Journal])

The Wireless Identification and Sensing Platform (WISP) from Intel Research Seattle [Buettner08, Sample08] is an example of Computational RFID tags. WISPs combine passive UHF RFID technology with traditional sensors. A current WISP is shown in Figure 2.4. WISPs are assembled from discrete components costing at most $25. However, they are intended to be mass manufactured like RFID tags at price points closer to $1 [Buettner09]. WISP is the only RFID sensor node with computational capabilities and that operates in the long range UHF band. In the rest of the chapter, we will use tag or WISP tag interchangeably to refer to a WISP tag.

WISPs combine passive UHF RFID technology with traditional sensors. A current WISP is shown alongside a commercial UHF RFID tag and a common wireless sensor node (mote) in Figure 2.4. WISPs have the capabilities of RFID tags but also support sensing and computation. Like any passive RFID tag, WISP is powered and read by a standard off-the-shelf EPC "Gen 2" RFID reader, harvesting the power it uses from the reader's emitted radio signals.

To an RFID reader, a WISP is just a normal EPC class-1 or gen-2 tag. However, Inside WISP, it has a 16-bit Microcontroller that features an 8 MHz clock rate, 8 kilobytes of memory, and 512 bytes of RAM. The microcontroller also has an analog-to-digital converter within itself. It can perform a variety of computing tasks, including sampling sensors and reporting sensor data back to the RFID reader. WISPs are the first programmable, passive RFID devices. They have used in different types of studies, from energy harvesting experiments [Jiang05] to monitoring

animal behavior [Holleman08, Segawa09]. The main advantage of WISP tags is that they allow us to implement novel security solutions on a live, passive RFID device. One disadvantage of using WISP tags is that they need to be placed within 1-2 meters of the reader.

WISP uses an integrated 802.15.4 radio for communication with readers. WISPs can sense parameters such as light, temperature, acceleration, strain, and liquid level. The WISP harvests energy from a reader and stores this energy in a capacitor. When enough energy is harvested, the WISP powers up and can begin sensing and communicating. However, sensing and communication drain power from the WISP. Though the feasibility of WISPs has been discussed in some research literature, how to harness many such devices to create a WISP sensor network is until now an open question. In near future, sensor networks will consist of multiple WISP tags, RFID tags and one or more readers. Consequently, realizing such a secure full-scale network will require research on both the WISP tag's end and the reader's end.

2.5. Security Challenges and Goals In CRFID Networks

As WISP tag is a combination of RFID and sensor, the security challenges of WISP networks is a combination of those found in RFID networks and traditional sensor networks. To develop useful security mechanisms while borrowing the ideas from the current security techniques, it is necessary to understand these constraints and challenges first. Some of the most important challenges of WISP networks are discussed next.

C1. Communication Medium: Since WISP tags are wireless in nature, a network consisting of WISP tags involves broadcast communication which makes eavesdropping and jamming easier.

C2. Data Conflict: In WISP networks data conflicts may happen even when the channel is reliable. Since the communication may still be unreliable. This is due to the nature of the WISP networks. If many tags reply at the same time, conflicts will occur and the transfer itself will fail.

C3. Constraint Power: WISP tags do not have their own battery or power. This can result in the WISPs losing power in the middle of an operation. WISPs may also need to cooperate with readers for power management.

C4. Data Sensitiveness: In order to decrease the collision rate while replying to reader queries, only the WISP tags with new sensor data need to reply. Therefore, estimating an aggregate property of the data without collecting the data is also a challenge.

C5: Mobility: Establishing secure association in the presence of mobility is challenging. Moreover, if a WISP tag is associated with a human user, tracking the device reveals the user location and mobility pattern which is a severe privacy violation.

C6. Close Proximity: Currently WISP tags can communicate at most up to 4.5 meters of distance. But much future application will demand longer distant communication. Designing security protocols for such applications will be more challenging as it will incur more communication cost. Moreover, such protocols need to ensure the reliability of the collected WISP data.

C7. Asymmetric Identification and Sensing Protocol: RFID tags and WISPs are highly asymmetric in terms of their communication abilities. With RFID and WISPs, readers are able to transmit messages to all tags and tags can send messages to the reader. But, tags can do so only when the reader initiates communication, and tags cannot communicate directly with each other. This makes it difficult to develop efficient protocols for gathering sensor data that changes over time.

C8. Accessibility: Though some WISP tags in the networks may be managed by the owner some of them can be placed in remote and/or hostile locations for the application's purpose. This greatly increases their vulnerability to physical attacks.

C9. Non-Collaborative: Though in most of the WSNs sensors can collaborate among themselves, this feature is totally unavailable in WISP networks. WISP tags can only

communicate with the reader that makes the design of security protocols even harder. This is one of the key reasons for which WSN security protocol cannot be applied in WISP networks.

C10. Various Attacks: The unreliable communication channel makes the security of WISP networks defenses even harder. WISP networks are particularly vulnerable to several types of attacks. Attacks can be performed in a variety of ways, most notably as denial of service attacks, but also tracking, cloning, eavesdropping, Replay attack, privacy violation, physical attacks, and so on.

Usually, in CRFID networks the security goals are classified as primary and secondary [Buettner08a]. The primary goals are known as standard security goals such as Confidentiality, Integrity, Authentication and Availability. However, the secondary goals are identified as Privacy Preservation, Resistance against Tracking, Cloning, Replay attack, Eavesdropping and DoS attack. Figure 2.2 illustrates the relation among the primary and secondary goals of WISP networks. Here the inner nodes correspond to primary security goals and outer nodes correspond to secondary security goals. We establish the relationship among security goals in such a way so that if we want to satisfy a primary security goal (identified by an inner node), we need to satisfy all the secondary security goals (identified by the outer node) belonging to the primary goal.

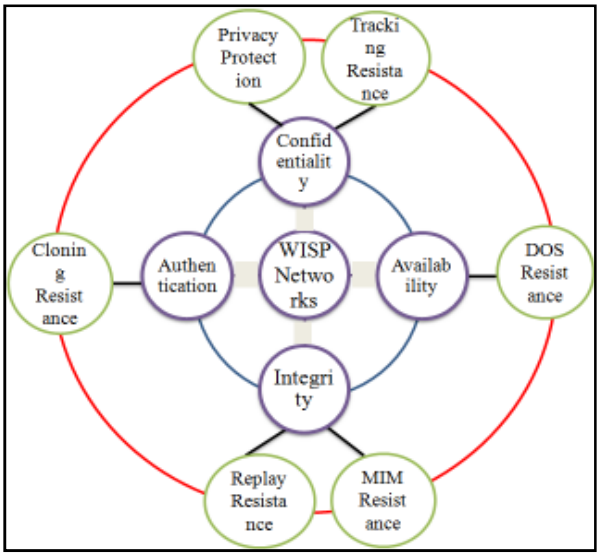


Figure 2.5 Primary and secondary security goals of WISP Networks

2.6. Summary

In this chapter, we discuss the properties and capabilities of different categories of RFID tags. This is followed by the discussion of constraints of tags, readers, and back-end server. We also discuss RFID standards and the details of different types of EPC classes. Finally at the end of the chapter, we discuss the properties of Computational RFID tags and their capabilities.

Chapter 3: Attacks in RFID Systems

Security and privacy concerns are the two major drawback of RFID technology. Security problems in RFID systems can be divided in two categories. The first concerns those attacks which aim to wipe out the functioning of the system. The second category is related to privacy where the problem is information leakage and also traceability.

Apart from the two above mentioned security problems, a great variety of attacks can be identified in RFID systems. Attacks in RFID systems opened the door for the development of both classical and modern security techniques, ranging from signal jamming to challenge-response based authentication. And it is just as likely that RFID will continue to inspire progress in security and privacy research in the future, as it has done for decades. The major goal of this chapter is to discuss the existing weaknesses of RFID systems so that a better understanding of RFID attacks can be achieved.

3.1. Attack Objectives

The objective of each attack in an RFID system can be very different. It is important to identify the potential targets in order to understand all the possible attacks. The target can be the complete system or only a part of the entire system. Most of the literatures focus on protecting the transmitted data. However, while designing the RFID system, additional objectives such as tracking or data manipulation should be addressed. Let us imagine the following example in a department store: an attacker modifies the data of a tag of an item by reducing its price from 200 to 20 ¤. This leads to a huge loss for the store. In this scenario, the data is transmitted in a secure form and the database is not manipulated. However, attack is carried out because part of the system has been modified. Therefore, in order to make a system secure, all of its components should be considered. Neglecting one component could compromise the security of the whole system. As shown in the above example, the attack may be carried out to steal or reduce the price of a single item, while other attacks could aim to prevent all sales at a store.

3.2. Adversary Types

The adversary can be categorized into the following classes:

- ***Weak adversary:*** This type of adversary cannot corrupt any tags.
- ***Strong adversary:*** This type of adversary has no limitations on corrupting tags, and can do anything at its wish.
- ***Forward adversary:*** This type of adversary can corrupt tags under the limitation that once the adversary corrupts a tag, it can do nothing subsequently except for corrupting more tags.
- ***Destructive adversary:*** This type of adversary can do anything after corrupting a tag. However, this statement is true under the limitation that the adversary cannot reuse a tag after corrupting it. Specifically, once a tag is corrupted it will be virtually destroyed. In particular, a destructive adversary cannot observe or interact with a corrupted tag nor can the adversary impersonate a corrupted tag to the reader.

3.3. Classification of Different Attacks

The following section discusses the major classes of attacks that are usually launched in RFID systems.

Modification of data:

This type of attack deals with the alteration of data saved within the memory of the tags. By unauthorized write access, the data stored on the tag can be modified. This attack is only effective if the identifier and security information such as keys remain unchanged. Otherwise this attack leads to denial-of-service. The attack is only possible if additional data along with the identifier are stored at a physical device (e.g. tags or database).

Deactivation of tags:

In this type of attack, the tag is made inoperative by executing a dedicated command or by physical intervention. Depending on the degree of deactivation the identity or the presence of the tag can no longer be determined.

Active jamming:

Although passive interference is usually unintentional, an attacker can take advantage of the fact that an RFID tag listens indiscriminately to all radio signals in its range. Thus, an adversary may cause electromagnetic jamming by creating a signal in the same range as the reader in order to prevent tags from communicating with readers.

Sniffing or tracking:

RFID tags are designed to be readable by any compliant reader. Unfortunately, this allows unauthorized readers to scan tagged items, oftentimes from great distances. This type is attack is called *sniffing* or *tracking* and this is one of the major attacks launched in most of the RFID systems. This type of attack can also be launched by eavesdropping on the wireless channel between the tag and the reader. Tracking of RFID tags allows monitoring of individuals' whereabouts and actions. RFID readers placed in strategic locations (like doorways) can record RFID tags' unique responses, which can then be persistently associated with a person's identity. RFID tags without unique identifiers can also facilitate tracking by forming collections which are recurring groups of tags that are associated with an individual. In such cases, RFID technology also enables the monitoring of entire groups of people. Moreover, tracking attack will also lead to unrestricted access to tag data or tagged object's information. Unrestricted access to tag data can have serious implications and collected tag data might reveal information like medical history which could cause denial of insurance coverage or employment for an individual.

Spoofing or cloning:

In this type of attack, the attackers can create authentic RFID tags by writing appropriately formatted data on blank RFID tags. For example, thieves could retag items in a

supermarket identifying them as similar, but cheaper, products. Tag cloning is another kind of spoofing attack, which produces unauthorized copies of legitimate RFID tags.

Replay attack:

Replay devices are capable of intercepting and retransmitting RFID queries, which could be used to abuse a variety of RFID applications. These types of attacks usually occur in situations where RFID components use a challenge response based protocol. RFID tags and readers usually share a secret and use a challenge response protocol to authenticate their identities. Nevertheless, very often this approach is subject to replay attacks. In a replay attack, an adversary broadcasts a tag's response recorded from a past transaction in order to impersonate the tag to a reader. Typical example of this attack is the unauthorized access to restricted areas by broadcasting an exact replay of the radio signal sent from a legitimate tag to the reader that grants access.

Relay attack:

In a relay attack an adversary acts as a man-in-the-middle. An adversarial device is placed surreptitiously between a legitimate RFID tag and reader. This device is able to intercept and modify the radio signal between the legitimate tag and reader. Subsequently, a momentary connection is relayed from the legitimate tag/reader through the adversarial device to the legitimate reader/tag. The legitimate tag and reader are fooled into thinking that they are communicating directly with each other. To make this type of attack even more sophisticated, separate devices could be used, one for the communication with the reader and one for the communication with the RFID tag. This sort of attack dismisses the assumption that readers and tags should be very close for communication. Additionally, even if communications are encrypted, the attack is feasible because messages are only relayed through a fast communication channel, without requiring knowledge of their contents.

Denial-of-Service (DoS):

This is a type of attack in which an attacker causes RFID tags to reach to such a state from which they can no longer function properly. This results in the tags becoming either

temporarily or permanently out of operation. More precisely, in this attack a tag is attacked with queries from an illegitimate reader. As a result, that tag is not able to respond to a further query from the legitimate reader. In other words, a genuine reader cannot communicate with its legitimate tags. A similar attack is also possible on the reader, but since the tag is much more resource constrained than the reader, they are more susceptible to such attacks than the readers. Such attacks are often intensified by the mobile nature of the tags, allowing them to be manipulated at a distance by covert readers. This type of attack can be a serious threat to the integrity of automated inventory and shipping applications.

Eavesdropping attack

As RFID technology operates through radio channel, so communication can be covertly overheard. In eavesdropping an unauthorized individual uses an antenna in order to record communications between legitimate RFID tags and readers. In this type of attack, the communication between tag and reader over the air interface is intercepted, decoded and interpreted. A passive adversary can eavesdrop on messages between a reader and a tag and can keep records of the messages. The information recorded can be used to perform more sophisticated attacks later. The feasibility of this attack depends on many factors, such as the distance of the attacker from the legitimate RFID devices.

There are two possible distances at which an attacker can listen to the messages exchanged between a tag and a reader. They are:

Forward Channel Eavesdropping Range: In the reader-to-tag channel (forward channel) the reader broadcasts a strong signal, allowing its monitoring from a long distance.

Backward Channel Eavesdropping Range: The signal transmitted in the tag-to-reader (backward channel) is relatively weak, and may only be monitored in close proximity to the tag.

3.4. Attack Intentions

Table 3.1 summarizes various intentions that an adversary might have while attacking an RFID system. An attacker may want to access sensitive information or exploit an RFID system by spoofing an RFID tag. An attacker's intention might be to make an RFID system unavailable.

Table 3.1 Intentions behind attacks in RFID systems

	Privacy Violation	Access of data	DoS	Spoofing
Modification of data		■		
Tag Spoofing		■		
Deactivation of tags		■	■	■
Removal of tags		■		■
Eavesdropping	■			
Jamming		■	■	■
Reader Spoofing	■			

3.5. Attack Addressed by our Proposed Protocols

Table 3.2 Attack intentions addressed by our proposed protocols

	Privacy Violation	Access of data	DoS	Spoofing
Ftest Protocol (Chapter 6)	**X**	**X**		**X**
PriSens Protocol (Chapter 7)	**X**	**X**		**X**
DRAP Protocol (Chapter 8)	**X**	**X**	**X**	**X**
MTD Protocol (Chapter 9)	**X**	**X**		**X**

In this dissertation, we propose four protocols suitable for four different example application areas. These four protocols are also suitable for other application areas that have the same core functionality like our example applications. In Table 3.2 we summarize what attacks

intentions are addressed by our proposed protocols. By addressing the attack intentions, our protocols basically address various attacks mentioned in this chapter.

3.6. Summary

In this chapter, we present the security issues that arise with RFID technology. Firstly a discussion of the attack objectives of an adversary in an RFID system is given. After that, major attacks in RFID systems are identified and discussed. Then, attack intentions of an RFID system attacker are identified. Finally we present what attacks are addressed by our system.

Chapter 4: Security, Privacy and Performance Goals in RFID Systems

In our previous chapter, we have described various attacks that can be launched in an RFID system by an adversary. In this chapter, our aim is to identify the key fact that can ensure the security of an RFID system. Moreover, to ensure widespread deployment of RFID systems, there are three main goals that need to be addressed by the RFID researchers. We have identified, that these three goals are related to security, privacy and performance of RFID system. Usually, most RFID protocols need to guarantee the security goals. For some RFID systems preserving privacy is the major goal and for some other systems ensuring survivability or ensuring low response time is the major goal. Nonetheless, no matter what the major goal is for any RFID systems, providing basic security is a common requirement for every RFID protocol. Next we describe these goals briefly.

4.1. Security Goals in RFID Systems

Security and privacy of data (and of consumers) is one of the major concerns that have hindered the adoption of RFID technology for many applications. The absence of protocols for privacy and security introduce concerns such as scanning and tracking, cloning, eavesdropping, and replay attacks. However, a major problem of designing cryptographically secure RFID protocols is the lack of computational resources on RFID tags. This prohibits the use of common cryptographic operations to enhance privacy and security in RFID infrastructures. Therefore RFID protocol designers need to keep in mind all the challenges to find some new lightweight alternatives. RFID technology may bring spontaneous risks because of the proliferation of RFID tags. We try to point out the security goals that should be guaranteed by a protocol:

- ***Privacy protection*:** A tag cannot be distinguished by an adversary without tampering it and realizing the data stored in the tag.

- ***Anti-tracking:*** It is tough for an adversary to track a tag if the adversary does not have any information about the tag. But the attacker can track a tag, if the tag replies with a constant response each time it is queried. So protocols should be designed such that a tag neither reveals its id nor replies with constant response.
- ***Anti-cloning:*** In order to clone a tag, an adversary needs to know the secret key shared between a tag and the authorized reader. So, to be secured against cloning attack, protocols should never reveal the shared secret key.
- ***Synchronization*****:** Attacker should not able to update the key used by the tag or the reader to secure the communication.
- ***DoS resiliency*****:** *Denial-of-Service* (DoS) attack means an authorized entity is prevented from accessing its authorized entities. In order to ensure successful communication between a reader and its authorized tags, it should be guaranteed that an adversary cannot desynchronize them.
- ***Susceptible to replay attack:*** Security must be ensured against replay attacks so that an adversary cannot impersonate a legitimate tag by replaying an eavesdropped message.
- ***Forward secrecy*****:** An adversary compromising a tag will not be able to identify the previous outputs of the tag.
- ***Backward secrecy:*** An adversary compromising a tag will be unable to track future transactions even if it has access to the tag's present internal state.

4.2. Privacy Goals in RFID Systems

While RFID has existed for several decades, it is its recent widespread usage that made privacy a major concern for everyone. One of the main concerns of users of RFID systems is user privacy. Since the communication between a tag and reader is unprotected, it can disclose sensitive information about a tag or its bearer, including its location. Two major privacy problems in RFID systems are as follows:

Information Leakage: In a typical RFID system, when a reader queries a tag, the tag responds with its identifier. If unauthorized parties can also obtain a tag ID, then they may be able to request and obtain the private information related to the tag held in the database. For example, if the information associated with a tag attached to person's medical record could be obtained from a server, then the damage would be very serious.

Tag Tracking: If the responses of a tag are linkable to each other or distinguishable from those of other tags, then the location of a tag could be tracked by multiple collaborating unauthorized entities. For example, if the response of a tag to a reader query is a static ID code, then the movements of the tag can be monitored, and the social interactions of an individual carrying a tag may be available to third parties without him or her being aware.

Therefore, RFID protocols should meet the following privacy requirements in order to mitigate the two threats described above.

Tag Information Privacy: RFID systems should be able to resist tag information leakage. To protect against such a attack, RFID systems need to be controlled so that only authorized entities are able to access the information associated with a tag.

Tag reply unlinkability: RFID systems should be able to resist tag tracking attacks. If messages from tags are anonymous, then the problem of tag tracking by unauthorized entities can be avoided.

Though adding privacy protection to RFID tags leads to higher per-tag costs and increased computational cost in the backend system, for some RFID applications (i.e. RFID based healthcare), ensuring privacy is very important. In these types of systems, the cost is outweighed by the need for privacy. Therefore, protocols designed for these types of data sensitive RFID applications needs to ensure privacy and the cost of extra computational complexity.

4.3. Performance Goals

RFID protocols cannot use computationally intensive cryptographic algorithms to provide privacy and security because the low cost of the tags put severe limits on tag side resources. RFID protocols should address the following performance issues [Avoine05, and Weis03].

Scalability:

A protocol is said to be scalable if the number of nodes can be significantly increased without imposing an unacceptable workload on any entity in the network. The interpretation of scalability will vary depending on the context (and the size of the network). Any security protocol deployed in an RFID network should not significantly affect its scalability. In the context of secure RFID systems, we would typically require that the workload on the server, to complete a single transaction, should not be a linear function of the number of deployed RFID tags.

Survivability:

Survivability refers to a system's ability to withstand malicious attacks and support the systems mission even when parts of the system have been damaged. With effective fault tolerance and damage recovery mechanisms in place, a system may still be trustworthy in fulfilling its functions and supporting the system mission. In case of RFID systems, most of the authentication protocols are *request-response* based where the tags and the reader maintain synchronization between them during the protocol execution. Therefore, if any attacker launches DoS attack by de-synchronizing the tags and reader, the system is not able to provide any service. However, in case of some critical RFID applications (i.e. enemy move detection in military battlefield using CRFID technology), it is very important that the system provides minimal service even under attack. Therefore, to ensure system survivability, we need to ensure that the protocols designed for critical RFID systems need to provide service even when it is under attack.

Low System Response Time:

Some of the most famous RFID applications are: asset tracking, supply chain, product identification in warehouse, etc. In all of these applications, products attached with RFID tags

need to be identified in a very quick manner. An identification protocol or authentication protocol may need very small time to identify one particular tag. However, in case of the applications mentioned above, there are usually millions of products in the system that needs to be authenticated on an everyday basis. Therefore, if the protocol is not efficient enough, it might take several hours or days to authenticate all tags in the system which might not be acceptable for the industry owner. So, to increase the popularity of RFID technology and to make RFID systems more efficient, we need to ensure that the designed RFID security protocol can guarantee low system response time

Storage Capacity:

The volume of data stored in a tag should be minimized because of tight tag cost requirements. Therefore, we need to ensure that the designed protocols use very lightweight operations like: hash functions or XOR operations.

Communication:

Since message communication between tags and reader consume much energy and makes an RFID system more vulnerable to various attacks, the number and size of messages exchanged between a tag and a reader should be minimized as much as possible.

Reliability:

Every RFID protocol should guarantee the reliability of the system's decision. Yet, ensuring reliability or decision accuracy of an RFID system has been understudied so far. However, there are some recent RFID applications (i.e. behavior inference using CRFID or physiological status inference using CRFID), where ensuring reliability of system's decision is very important and critical. In these types of applications, the final decision at any state of the system is taken based on the data collected from all the tags. These types of RFID systems depend on all tags' data for collective information analysis and decision making. Therefore, protocols designed for such RFID applications need to ensure that the system will take accurate decision by ensuring system's reliability.

4.4. Goals Achieved by our Proposed Protocols

In this dissertation, we propose four different protocols for four example RFID application areas. Though we have used specific application scenario as a motivating example, most of the RFID systems fall within the category of one of these application types. Figure 4.1 presents a summary of what goals are achieved by our proposed protocols:

Table 4.1 Summary of goals achieved by our protocols

Application Area	Goals achieved by our approach
Supply Chain, Asset Tracking and such applications	1. Ensuring security requirements 2.Counterfeit detection (tag spoof identification) 3. Ensuring low response time
RFID based healthcare or such applications where user privacy is important	1. Ensuring security requirements 2. Efficient privacy preservation (tag information privacy and tag reply unlinkability) 3. Ensuring scalability
Sophisticated critical CRFID applications where system survivability is important (enemy move detection)	1. Ensuring security requirements 2. Ensuring survivability 3. Reducing system response time
Critical RFID applications where decision accuracy is important (physiological status inference using CRFID)	1. Ensuring security requirements 2. Ensuring decision reliability 3. Reducing system response time

\

Chapter 5: Related Work

There have been research initiatives for quite some time now to prevent various attacks in RFID systems and facilitate the expansion of RFID technology. One key research area that focuses on securing RFID systems is the design of secure authentication methodologies. These authentication techniques are designed to defend against various attacks launched in RFID systems while a reader communicates with RFID tags for identification or data retrieval purposes.

5.1. Preliminaries

A variety of authentication protocols have been proposed over the years to secure an RFID system. Many of these protocols use cryptographic functions to protect messages exchanged between an RFID reader and tags and also to perform authentication. Cryptographic techniques can be divided into two main categories based on the nature of the keys used. These two techniques are: symmetric and asymmetric. All the protocols proposed in this dissertation use the symmetric key technique. However, next we briefly describe the two techniques:

5.1.1. Symmetric Key Cryptography

In symmetric key cryptography (or secret key cryptography), the sender and receiver share a common secret key. The precise use of the key will depend on the nature of the protection provided by the algorithm being used. This key can be used to protect the confidentiality and/or the integrity of the message. One widely used symmetric encryption technique is *Hash Functions*. A hash function takes an input of any length and gives as output a short, fixed-length value that is a function of the entire input. The output of the hash function is called hash value. Hash functions must have the one-way property; that is, they must be designed so that they are not only simple and efficient to compute, but also, given an arbitrary output, it is computationally infeasible to find an input that gives the chosen output. It implies that hash functions have to be irreversible.

5.1.2. Public Key Cryptography

In asymmetric cryptography (or public key cryptography), every participating entity has its own key pair. So, there are two keys that work in a pair. One key of the pair is called the "public key" that is publicly available. And the other key of the pair is called the "private key," which is kept secret by its owner. Public key cryptography involves an encryption operation that transforms blocks of plaintext into ciphertext blocks and a decryption operation that reverses this process [Menezes96, Stallings99]. The main difference from symmetric encryption is the way in which keys are used. The public key of the intended recipient of a message is used for encryption and the recipient's private key is used for decryption. A user's public key is made available to anyone who wants to encrypt a message intended for that user; the recipient's private key is used to decrypt the received encrypted messages. Implementing any algorithm involving public key cryptography requires the computation of complex mathematical functions, e.g. involving multi-precision integer or finite field arithmetic [Mitchell03]. As a result, public key encryption schemes tend to be more computationally intensive, and hence slower to compute, than secret key encryption algorithms [Mitchell03]. Tiny RFID tags do not have the computational capability to execute algorithms based on public key cryptography. Therefore, symmetric key cryptography is used for authentication and security purposes in RFID systems.

5.2. Related Works on RFID System Security

An authentication protocol is a defined exchange of messages between two or more parties, with the objective of providing one or both parties with an authentication service. That is, the objective is: 1) for one or both of the parties to verify the identity of who they are interacting with, 2) that the other party is actively involved in the protocol, and 3) that the messages send by the other part are not old messages and maintains integrity. Usually, RFID authentication protocols make use of cryptographic techniques to ensure confidentially and data integrity. In this

section, we present some classic and recently proposed approaches for ensuring the security of RFID systems.

RFID security based research area can be divided into two categories. The first category is protocol based. This category mainly focuses on implementing protocols using secure, lightweight primitives on small RFID tags in order to ensure security and privacy. The second category is hardware based. This category focuses on improving RFID tag hardware so that it can provide additional security primitives. All of our proposed protocols in this dissertation fall in the first category. So we will not discuss the hardware based category. However, interested readers can refer to [Juels05b] and [Rieback07] for more details. In this section, we will mainly discuss the research background related to the protocols based category.

Within the area of the protocol based category, many techniques have been proposed for ensuring RFID security, and the assortment of authentication protocols is quite extensive. Thus we shall avoid a broad review and focus on those works that are related to our contribution. Interested readers may refer to [Juels05b, Juels06 and Avoine12]. Avoine's collection is one of the largest resources on RFID papers available on-line. The protocols scattered throughout the literature of RFID security can roughly be categorized into the following classification (see figure 5.1):

Early Protocols: There are roughly two simple protocols found in early RFID papers: Martin Feldhofer's protocol [Feldhofer03] and Zero Authentication protocols [Engberg04].

Hash Lock Protocols: In later literature, there are many variations of the Hash Lock Protocol ranging from simple to complex. Hash Lock Protocols are a group of protocols based on the hash lock protocol of Weis in [Weis03]. The principle is that if you do not have the right key to fit on the hash lock, you do not get access to the tag and its ID. The Molnar and Wagner [Molnar04] protocol is one of the famous tree based hash lock protocol that is widely used in RFID systems.

Probabilistic Protocols: The cost and size limitations of a tag forces RFID protocols to shift or reduce the workload from tag to reader. A way to do that is to use probabilistic protocols. Probabilistic protocols provide a framework to use weaker encryption primitives. HB [[Hopper00 and Hopper01] and HB+ [Juels05a] protocols are example of such protocols.

Other RFID Protocols: Recently RFID tags have been used in many interesting problems like: tag estimation and object localizing. According to our categorization, these protocols belong to "other" category.

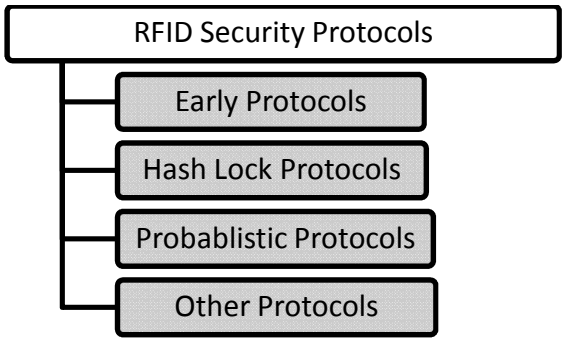


Figure 5.1 Category of RFID security protocols

In the next subsection, we briefly describe some classic hash lock protocols and probabilistic protocols. Following this, we briefly describe some recent protocols for RFID security.

5.2.1. Classic RFID Authentication Protocols

The Weis-Sarma-Rivest-Engels Protocol: Weis et al. [Weis03] proposed an authentication protocol that used a back-end database to perform authentication. In this protocol, an RFID tag replies with a $metaID$ when it is queried by a reader. The reader forwards this $metaID$ to the back-end database, which finds out the real ID of the tag for the reader. An RFID tag replies with the same $metaID$ each time it is queried by a reader. So this protocol is not secured against a tracking attack. This vulnerability hampers the privacy of the tag holder. So the authors proposed a randomized hash lock scheme to solve this problem. In this scheme, a tag replies with $(r,\ ID\ \oplus\ f_k(r))$, when it is queried by a reader. Here, k is the tag's secret, f_k is a

pseudorandom function, and r is a random number generated by the tag. The reader forwards this reply to the secure database, which then searches for the ID/tag secret key pair that matches the reply. Under this scheme, an RFID tag replies with a different value each time it is queried by a reader, as each reply of the tag involves a random number. Weis also introduced in [Weis03] their improved Randomized Hash Lock Protocol, which makes the output of the tag random.

The Tsudik Protocol: Tsudik proposed a protocol, YA-TRAP, in [Tsudik06] that ensures high efficiency at the server side. It is a famous authentication protocol that places little burden on the back-end server. The principle advantage of this protocol is that the central database avoids any real time processing. Authors proposed that YA-TRAP is really advantageous in situations where tag information is processed in batches rather than in real time. The fundamental idea of this protocol is based on a monotonically increasing timestamp, which makes this protocol secured against tracking. But the use of the timestamp makes this protocol unsecured against DOS attack. In this protocol, an RFID tag updates its timestamp based on a value provided by the reader. At the same time, each tag stores T_{max}, where T_{max} is the maximum value that can be reached by the timestamp. When the timestamp reaches T_{max} a tag does not answer to the reader's queries. Hence an adversary can send the tag a large enough timestamp so that it goes beyond T_{max}. Thus it becomes quite easy for a malicious reader to create DOS attack. Although the solution to DOS was proposed in YA-TRAP+ [Avoine05], this protocol still lacks forward secrecy.

The Ohkubo-Suzki-Kinoshita Protocol: Another lightweight protocol is OSK [Ohkubo03]. Ohkubo, Suzuki and Kinoshita proposed that two hash functions H and G are sufficient to provide indistinguishability and forward secrecy. Here, H is a one way hash function and G has a random oracle. According to this protocol, a tag is initialized with a shared secret s_1 and the back-end server maintains a list of tag ID/secret pairs (id, s_i). The tag updates its secret key after each query according to the following formula $s_{i+1} = H(s_i)$. And in response to the

query from a reader, the tag replies $a_i = G(s_i)$. The server on the other hand uses a_i to identify the tag by performing a brute force search through the list of tags. OSK does not ensure scalability. In [Avoine05], Avoine and Oechslin modified OSK, which removed the scalability problem. They introduced a time-memory tradeoff, which reduced the computational complexity for inverting the hash function. Another problem of OSK is that a malicious reader may easily desynchronize a tag— eventually resulting in a DOS attack.

The Henrici-MÄuller Protocol: In [Henrici04], Henrici and MÄuller rely on a one-way hash function to thwart tag tracking attacks. In this solution, a tag responds to a a reader's query with two hash values and updates its stored values after a successful authentication. This solution does not provide a full-degree of anti-tracking since a tag always replies with the same response before it is successfully authenticated. In addition, it does not provide forward security as a strong adversary could derive tag identifiers in previous sessions from the tag's current identifier and the server's random number.

The Molnar-Wagner Protocol: Molnar and Wagner [Molnar04] pointed out that the randomized hash lock scheme does not defend against an eavesdropper. An adversary can eavesdrop on the communication between reader and tag to learn the tag replies. The adversary then uses this information to impersonate the RFID tag to fool a reader. In this protocol, both the reader and tag share a secret (x). Both the reader and tag generate random nonces (r_a, r_b) and share them. By refreshing the random nonces during every instantiation of the protocol, replay attacks through eavesdropping are avoided.

The Hopper-Blum Protocols: Hopper and Blum propose a secure human authentication protocol in [Hopper00 and Hopper01]. Here, $r_A \cdot x$ and $r_A \oplus x$ represent scalar product and exclusive-or (XOR) of k-bit binary vectors r_A and x respectively. The HB protocol relies on the computational difficulty of the Learning Parity with Noise (LPN) problem. It is meant only to be secure against passive attacks, and it is not secure against active attacks. A simple active attack,

where an adversary pretends to be the reader and transmits a fixed r_A to the tag several times can retrieve the value of x. While humans may get suspicious with repeated, failed login attempts if they are actively queried by a computer, a simple tag will blindly reply to active queries. In other words, HB would not protect against skimming attacks.

The HB+ Protocol: An alternative method for RFID authentication is based on a "challenge and response" between a reader and a tag. Juels et. al. [Juels05a] observed that human authentication protocols can be applied to RFID, since RFID tags, like humans, have weak computational capabilities. They introduced the HB protocol, in which a reader issues a new challenge to a tag each time it queries an RFID tag. The tag computes the binary inner product based on the reader's challenge, and returns the answer to the reader. The reader authenticates the tag by verifying the tag response. The HB+ protocol is an improvement over the HB protocol by using an additional binding factor from the tag to defend against an active adversary. Later work by [Piramuthu06], [Gilbert05], [Bringer06] improve on this idea.

The Seo-Kim Protocol 1: Seo et al. [Seo06] proposed a hash function based authentication protocol that ensures high scalability. This protocol is also untraceable. Here back-end server $\mathcal{B}$ has the following four fields associated with each tag: EPC, $h(ID_i)$, ID_i and the access PIN. Each tag saves the last timestamp TS sent by an authorized $\mathcal{R}$ as TS_{last}. Based on its own timestamp TS and shared secret key k, the reader computes $h(k, TS)$ and transmits it to the tag $\mathcal{T}_k$ together with TS. The tag recognizes an authorized reader if TS received from the reader is greater than TS_{last} and replies with $h(ID_i)$. Reader $\mathcal{R}$ forwards $h(ID_i)$ and TS to $\mathcal{B}$ and here the back-end server comes into play. It updates the ID of the corresponding tag and asks the reader to pass on the message to the tag for synchronization. Upon reception of the message, tag $\mathcal{T}_k$ updates its ID and TS_{last}. The most significant contribution of this work is scalability and forward secrecy. Updating ID with a one way hash function ensures forward secrecy. Scalability is ensured in a sense that back-end server needs time complexity $O(\beta)$ to find a tag in a multi tag

environment where β is the number of tags that have same key k within the operating range of a reader. The drawback of this protocol is that ownership transfer requires external intervention.

The Seo-Lee-Kim Protocol 2: Seo et al. proposed another authentication protocol [Seo06b] that ensures high scalability and ownership transfer. It is a lightweight authentication protocol that employs a proxy in addition to the back-end server. The protocol is based on Universal Re-encryption which allows the back-end server to get the tag identifier only after a simple decryption. This decryption requires a constant time, which makes it one of the most scalable authentication protocols. But its application area is restricted because of the use of a proxy. This protocol is best suited for personal use. But it suffers from the problem of traceability and some other security issues such as DOS attack and swapping.

The Tan-Sheng-Lee Protocol: In [Tan07], Chiu et al. proposed a serverless authentication protocol. In this protocol, the reader maintains an access list L_i, which is used for the purpose of tag authentication. And each tag has a secret t that is not shared with anyone. The reader and the tag both know $f(r,t)$, where r is the reader identifier. Here in response to a query from a reader, the tag replies with some of the bits of $h(f(r,t) \parallel n_i \parallel n_j))$ where n_i and n_j are two random numbers generated by the reader and the tag respectively and $h(.)$ is a one way hash function. Since only a legitimate tag can generate $h(f(r,t) \parallel n_i \parallel n_j))$, it works as the tag's certificate to the reader. At the same time, the tag queries the reader with a question string. Only a legitimate reader replies with valid answer string, which introduces the reader as an authorized reader of the tag. The tag releases its data only after confirming that the reader is legitimate. But here again the reader has to do a lot of computation to find out the id of the required tag. But their protocol is not purely and strongly anonymous as they return tag id by performing an XOR operation with a hash value for authentication. Moreover, they didn't propose any technique for ownership transfer.

The Chien-Chen Protocol: In [Chien07], Chien and Chen used a challenge-response protocol to prevent replay attacks. To prevent denial of service attacks, both new key and old key for authenticating a tag are stored in the back-end database. However, a strong adversary can still identify a tag's fixed EPC code and thus identify the tag's past and future interactions after compromising a tag.

5.2.2. Recent Works on RFID Security

In regard to recent RFID authentication protocols, Avoine et al. proposed a group based private authentication scheme in [Avoine07] (later improved by Hoque el.al [Hoque11]) that improves the tradeoff between scalability and privacy by dividing the tags into a number of groups. One major limitation of this protocol is that the level of privacy provided by the scheme decreases as more and more tags are compromised. Molnar et al. propose a new method [Molnar05] that supports delegation in the tag authentication. The tag owner can transfer the ownership to another party for authenticating valid tags. Lu et al. propose a RFID private authentication protocol (SPA) [Lu07], which enables dynamic key-updating for tree-based authentication approaches. A lightweight RFID private authentication protocol, RWP, has been proposed in [Yao09], based on the random walk concept. The analysis results show that RWP effectively enhances the security protection for RFID private authentication, and increases the authentication efficiency from $O(logN)$ to $O(1)$. However, this technique is suitable for tags with high computational power, as the technique requires tags to perform randomized hash functions. Besides these types of deterministic approaches, some RFID applications use probabilistic methods to determine some important features related to the system [Qian08].

In [Hoque09a], Hoque et al. proposed a serverless authentication protocol for RFID systems. But their system is also more focused on defending various attacks without the help of a central database. Moreover, in their system, the reader has to do a lot of computation to find out the id of the required tag. In [Hoque09b], the authors proposed an RFID authentication protocol

that supports not only security and privacy, but also recovery in RFID systems. The protocol can return the desynchronized tags and readers to their normal state, and thus provides robustness. The focus of this system was to defend against various attacks.

Sheng et al. [Sheng09] study a fundamental problem of continuous scanning in RFID systems and designs algorithms based on the information gathered in the previous scanning. Yang el al. [Yang10] proposes a probabilistic approach, SEBA, for fast and reliable batch authentications in RFID application. However, in this protocol, when queried by a reader, tags reply with some bits of their secret IDs. But the drawback of this protocol is that any adversary eavesdropping in the channel may learn the complete IDs of tags over time and launch several successful attacks.

Most of the previous works (i.e. classic protocols) on RFID systems concentrate on collecting the IDs of a large number of tags as quickly as possible. Recently some researchers worked on the *tag-estimation problem*, which is to use statistical methods to estimate the number of tags in a large system [Kodialam06]. Tan, Sheng and Li [Tan08] designed the Trust Reader Protocol (TRP) to detect the missing tags with probability when the number of missing tags exceeds a certain threshold. TRP uses probabilistic methods to choose a frame size that satisfies the system requirements and identifies missing tags.

Another recently studied area of RFID system is the reduction of radio contention during the execution of RFID authentication protocols. Collision is a critical problem in RFID systems when processing a batch of tags. In the literature, tag anti-collision algorithms can be categorized into Aloha based algorithms and tree based algorithms. Aloha based algorithms makes only one tag respond in a slot, in the response of tags, by dividing a time into slot units. On the other hand, tree based algorithms [Lee08] make trees while performing the tag identification procedure using a unique ID of each tag. Aloha based protocols are known for their low complexity and computation, thus making them attractive for use in RFID networks. Examples include Pure, Slotted and Framed Slotted Aloha (FSA) and their variants [Zhen05, and Lee05]. In Pure and

Slotted Aloha [Zhen05], a tag responds after a random delay, and continues doing so until it is identified. Lee *et al.* [Lee05] show that the FSA reader can obtain a maximum identification throughput when the size of the detecting frame equals the number of tags. They propose a dynamic FSA for RFID systems.

In the recent past, significant research has been conducted in developing RFID systems to ease the everyday life of humans [Michahelles07, Munishwar09, Zecca09, and Hinske07]. Even recently some research has been performed to devise accurate ways of determining indoor location [Saxena07, Yunhao03]. But all of these works mainly focused on developing the system itself, rather than considering the security and privacy vulnerabilities of installing those RFID systems in practical environments.

5.3. Related Works on Computational RFID (CRFID) Systems

Recently WISP tags have been used in different application areas. For example, it has been used in recognizing daily activities [Buettner09]. In [Buettner09], the authors attached everyday objects (e.g., glass, plate, books) with WISP tags that have accelerometers. Later, daily activities are inferred from the traces of objects that are moved. In [Chaudhri08], WISPs are used for sensing and monitoring exercises involving free weights. The authors embedded WISPs with free weights and body parts. Then the accelerometer sensor readings from the tags are used to infer the exercise being done and the association between the user and the particular weight being used. [Yeager08] presents a wireless neural interface that uses WISPs. It provides the neuroscientists a wireless, battery-free method of monitoring neural signals.

So far, the security aspects of WISP sensor networks have not been explored in literature extensively since the usage of these tags is still a new technology. Recently WISP has been used for RFID and low power wireless security research [Chae07 and Czeskis08]. We are also aware of one result that deals with the backup checkpoint status integrity of WISP [Salajegheh09]. Since WISPs operate intermittently, one problem occurs due to energy constraints in executing

cryptographic computations. Power derived by the sensor from a single cycle of harvested energy might be insufficient to perform a realistic cryptographic operation. CCCP (Cryptographic Computational Continuation Passing) [Salajegheh09] suggests that WISPs can perform demanding computations despite limited energy and power interruptions. The main idea is for a WISP to backup its RAM state just before it loses power (e.g., when the reader leaves). When the reader reappears, the WISP can retrieve its backed up state and resume unfinished operations, without having to re-start from scratch.

By using the 3D accelerometer of WISP tags, Saxena et al. developed a motion detection system that also works as a means to ensure security [Saxena10]. According to the authors, accessing a personal RFID device fundamentally requires moving it in some manner. Determining whether or not the WISP tags are in motion helped the authors to provide enhanced security and privacy. The made the WISP tags to respond only when it is in motion, instead of doing so promiscuously.

Hoque et al. [Hoque10b] proposed a sleep monitoring system based on the WISP tags. Their developed system does not require any additional action from the users outside their daily routines. By attaching WISP tags to the bed mattress, accelerometer data are collocated from WISPs and then reported back. They have shown that their system accurately infers fine-grained body positions from accelerometer data collected from the WISPs attached to the bed mattress.

By adding a super-capacitor to the WISP, the authors of created a wirelessly re-chargeable data logger that can read and log temperature data for 24 hours away from a reader and then report back the data and recharge when it is in range of a reader [Yeager08]. However this work again falls into the category of hardware based improvements of WISP tags.

The founders of WISP tags maintain a repository [Intel] of new research techniques that have been conducted on WISP Network Security. It provides information on the entire WISP related literature that has been proposed so far. But, most of these works focus on the improvement of hardware or power aware parameters of WISP sensor network.

5.4. Summary

In this section, we have reviewed a number of classical and recently proposed RFID authentication protocols. We have also discussed relevant related work on CRFID systems.

Chapter 6: Efficient Detection of Counterfeits in Large Scale RFID Systems

The International Chamber of Commerce estimates that counterfeit goods make up seven percent of world trade, with the counterfeit market being worth 500 billion USD in 2004 [Juels05a]. Counterfeiting has an impact on the rights holder, the country where counterfeiting takes place, and it causes social costs. Counterfeit goods, whether of clothes, medicines or CDs, cost hundreds of billions of US dollars globally every year. The effects of these crimes range from loss of company revenues to threats to public health and safety. Many companies already use anti-counterfeiting measures like holograms to reduce counterfeiting and product piracy. A drawback of existing anti-counterfeiting measures is the low achievable degree of automation when checking the originality of a product. Radio Frequency Identification, or RFID, helps to address this problem, and provides the possibility to implement secure protection mechanisms [Pollinger08].

A very good example of a large scale system that needs secure and efficient anti counterfeiting techniques on everyday basis is the pharmaceutical industry. It is one such market that is constantly fighting battles against counterfeiting (which make up to 7% of all pharmaceutical products in the international supply chain). Since pharmaceutical products are consumed by humans, any mistake during manufacturing may cause serious harm to people's health and even lead to death. The importance of drug authenticity is obvious. In the United States, the Food and Drug Administration (FDA) has been considering the use of RFID tags to prevent counterfeit pharmaceutical products [Pollinger08]. Radio Frequency Identification, or RFID, helps to address this problem and provides the possibility to implement extensible, secure protection mechanisms. In fact, many RFID enabled anti-counterfeiting solutions have been already introduced in logistics, retailing, passports, etc. Because RFID has the capability of capturing and relaying data, it is what the pharmaceutical industry is looking towards to improve quality, reduce costs, and improve patient safety.

The RFID tags are typically low-cost and pervasive devices, being attached to products or objects to enable the identification of those objects. A tag has small microchip and an antenna on board. The reader can collect the IDs of tags via RF signals, without the need of line of sight. As an effective automatic processing measure, RFID offers several attractive features over barcodes, such as non-optical proximity, and rewritable ability.

A common technique of RFID enabled anti-counterfeiting is that the manufacturer stores a serial number K (or termed as *secret key*) for each tag. The secret key is also stored in the central authentication server. During authentication, an RFID reader challenges a tag for its validity, and the tag replies with its encrypted or hashed serial key. This encrypted message is passed to the server for validity checking. If the serial number is valid, the product to which the tag is attached is declared as genuine. During this process, however, an adversary can eavesdrop in between the channel, and the learned information can be used to create a counterfeit tag. To address this issue, many efficient and private authentication protocols have been proposed in the literature. Weis et al. [Weis] propose an authentication scheme based on Hash Lock. The search complexity of Hash Lock is $O(N)$, where N is the total number of tags in the system. To improve the search efficiency, tree-based approaches [Dimitriou06, Lu07, Hoque11] convert the verification process to a Depth-First-Search in a key tree to reduce the search complexity to $O(\log N)$. However, the reader still needs much more time to authenticate products in a large supply chain.

To solve the problem of RFID based counterfeit detection, we propose to authenticate tags in batches. However, if we apply a straightforward private authentication technique, the protocol execution time will still be very high. If we consider this problem from a different perspective, we see that it is not always necessary to ensure the genuineness of every single product in a batch. In fact, even in the genuine products, there can be some products that are shipped as defectives from the manufacture. So it is acceptable if we guarantee that the percentage of counterfeit products is sufficiently small.

6.1. Our Major Contributions

At this point, we summarize our contributions −

- We propose to verify the validity of a batch of tags using statistical inference based sampling in a protocol named *GTest*. However, it is not efficient since it requires high execution time and large volume of authentication data.
- To solve the problems of efficient batch authentication, we propose *FSA based authentication protocol (FTest)* that uses a variation of Farmed Slotted Aloha [Zhen05] technique.
- To compare the performance of GTest and FTest protocols with a per tag authentication protocol, we measure their execution time in a simulated RFID environment.

6.2. Motivation

When detecting product counterfeiting in large systems, existing approaches can be impractical since tags needs to be authenticated one at a time. It may seem at first that the problem of counterfeit tag detection can be solved by using any RFID tag identification or authentication protocol, simply by allowing the reader to interact with the tags of the batch. However, this deterministic process will be very time consuming since reader needs to authenticate each and every tag of the batch to determine its validity. The situation will be even worse if there are large numbers of tags in the system. Such low authentication efficiency is unacceptable in practice especially in large scale supply chain. Therefore, we need batch authentication not only to increase efficiency but also to prevent counterfeiting. To address this issue, we propose a batch authentication protocol that is scalable, efficient as well as able to prevent product counterfeiting within a user defined tolerance level. Due to this protocol, mass authentication along the supply chain can be possible, and the cost of maintaining integrity of supply chains can be significantly reduced. Eventually it may increase health security, company revenues, social awareness and global trading concerns.

6.3. Background

In this section, we discuss how Framed Slotted Aloha (FSA) and Tree based authentication protocol works.

6.3.1. Tree Based Authentication Protocol

In tree based hash protocol [Nohl06, Lu09, Avoine05], the tags are organized in a secret key tree where each tag is assigned to a leaf of the tree. Secret keys are associated with each branch of the tree. Each tag (each leaf) receives all the secret keys along the path from the root to itself. If the tree has L levels, each tag stores L keys. The key tree as a balanced tree and therefore, if the branching factor is α, the $log_\alpha N$ will be equal to L. Each tag has only one key that is not shared with any other tag of the system. Figure 6.1 shows a balanced key tree with $N = 8$ and $\alpha = 2$.

According to this protocol, the reader queries a tag with a nonce n_r. Upon the reception of the nonce from the reader, the tag replies to the reader with

$$h(k_0, n_r), h\left(k_{l_1}, n_r\right), h\left(k_{l_1,l_2}, n_r\right), \dots, h\left(k_{l_1,l_2,\dots,l_L}, n_r\right),$$

where each $l_i \in \{1, \dots, \alpha\}$, $1 \le i \le L$ and $h(.)$ is a hash function. After receiving the response, the reader first finds a match with the first hash value of the response by hashing with all the keys of level 1. Whenever the reader obtains a match, the reader starts to search for the second hash value of the response by hashing with all the keys at the next level of the sub-tree rooted at the node where the reader has found the match. The reader repeats this step until it reaches a leaf. Thus, the reader's complexity is reduced to $O(\log_\alpha N)$. In the worst case, the reader has to search with all the α keys at each level of the tree and the complexity becomes $\alpha \log_\alpha N$.

The major drawback of this approach each tag must transfer 4 hash values to the reader at each authentication. As we discussed before, such a large volume of data is a major bottleneck preventing us from accelerating the batch authentication.

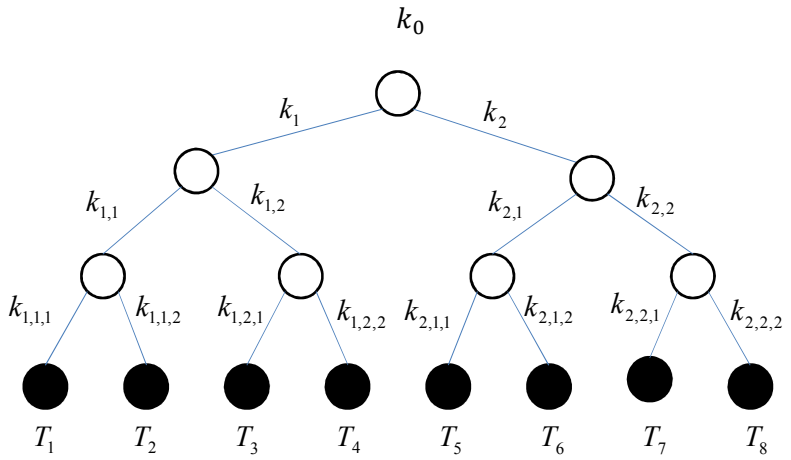


Figure 6.1 A secret key tree for the tree based hash protocol with N=8 and α=2

6.3.2. Framed Slotted Aloha

Aloha based protocols are important because they reduce the probability of occurrence of tag collision. In case of pure slotted Aloha, tags select their response time arbitrarily. In slotted Aloha [Zhen05], tags select the timeslot randomly and reply at the beginning of the timeslot to avoid overlapping of transmissions. Framed Slotted Aloha (FSA) algorithm can be used to identify a batch of tags. The protocol uses a fixed frame size and does not change the size during the process of tag identification. In FSA, the reader offers information to the tags about the frame size (f) and the random number (r) which is used for a tag to select a slot number in the frame. Each uses a hash function $h(x)$, which is used to choose the slot number. After receiving f, each tag selects $h(id \oplus r)\ mod\ f$, as its slot number. The reader then sequentially scans every slot in the frame. In each slot, if a tag's slot number equals zero, it will send its id to the server immediately. Otherwise, the tag reduces its slot number by one. Since a tag cannot sense the signals replied from other tags, there are three types of slots from the reader's perspective − slots with no reply, single reply, or multiple replies. We define these slots as empty slot, single-reply

slot, or collision slot respectively. Slots can also be characterized as *multi-bit response slots* and *single-bit response slots*. Since the frame size of FSA is fixed, its implementation is simple but it exhibits low efficiency of tag identification. For example, if there are too many tags, no tag may be identified since the slots experience high collision. On the contrary, many slots wasted if the number of tags is small. Our FTest protocol is partially dependent on the concept of FSA.

6.4. System Model and Problem Formulation

6.4.1. Problem definition

In our system, we assume that each object is attached with an RFID tag that has a unique *id* (e.g. *secret key*). We define the set of tags as population. These tags are divided into batches or groups of equal size. Suppose, N is the total number of tags in the system and τ is the number of groups. So, the group size is $n = \frac{N}{\tau}$.

The number of tags in a batch, n, is known in advance. We define a batch of tags as valid if no counterfeit tag is detected, otherwise this batch is considered as invalid. In our system, each batch is associated with a unique key that we refer to as a *group key*. In addition to each tag's own secret key id_i, every tag shares this group key with other members of the given group. Figure 6.2 shows the group organization of the tags where $N = 8$ and $\tau = 4$. The k_i's are the group keys, where $1 \leq i \leq \tau$.

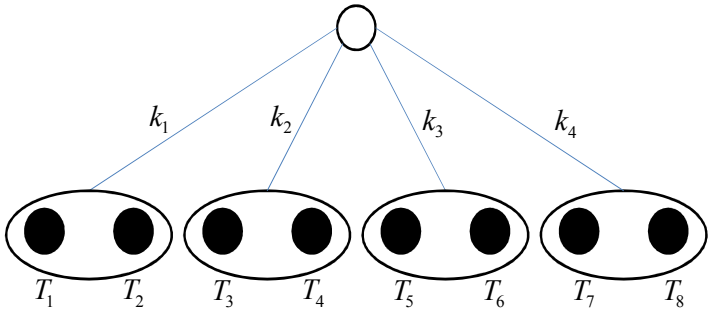


Figure 6.2 Group organization of the tags for the batch authentication protocol, with N=8 and τ =4

6.4.2. Architecture of the system

There are mainly four components in the system:

Issuer: The issuer initializes each tag during the deployment and also authorizes the reader access to the tags. We can think of the issuer as a certificate authority (CA).

RFID Tag: Each RFID tag is denoted as T. The issuer assigns a unique key id_i and a group key k to the ith tag T_i of the system. The use of group key will be explained later.

Table 6.1 Database structure of the authentication server

Group Key	Tag Key	Tag Name
k_1	id_1	T_1
	id_2	T_2
	…	…
	id_i	T_i
…	…	…
k_n	id_{j+1}	T_{j+1}
	….	….
	id_N	T_N

Reader: A reader (R) connects to the authentication server through a high speed network. Here, we assume the communication channel between the reader and the backend server is secured. The reader receives all the secret information by the issuer during the deployment.

Server: The authentication server maintains all the group keys and N secret keys corresponding to N tags in the database. The server also knows which tag belongs to which group by maintaining a database like Table 6.1. The server has powerful computing capability.

6.4.3. Preliminaries and Assumptions

We assume that the reader and all the tags in the system has the knowledge of XOR operation and $h(.)$, an irreversible one way hash function to protect the integrity of the message. The outputs of $h(.)$ cannot be linked back to its input so that an adversary cannot link back the

tag ids. There are many efficient hash functions in the literature. The hash $h(.)$ does not need to be a cryptographic hash function. In order to keep the tag's hardware simple a cyclic redundancy check (CRC) function which is already found in existing RFID tags can be used as $h(.)$. Communication between the reader and the tags is time-slotted. The synchronization between the clocks of the tags and reader is done by "start" signal of the reader. The reader uses a 'slot start' command to start a slot. Our protocols are request-response based protocol, in which the reader issues a request in a time slot and then zero, one or more tags respond in the subsequent time slots. We assume that RFID reader is able to distinguish the three types of slots mentioned earlier. All the notations related to our system are shown in Table 6.2.

Table 6.2 Summary of notations

Symbol	Meaning
$T*$	Set of RFID tags
R	RFID Reader
N	Number of tags in the population
n	Number of tags in a batch
τ	Number of batch in the system
$h(.)$	One way hash function
Δ	Counterfeit threshold
n_s	Sampling size

6.4.4. Protocol goals

The goal of a server is to accurately and efficiently determine the validity of a batch of tags. It may seem at first that the problem of counterfeit tag detection can be solved by using any RFID tag identification or authentication protocol, simply by allowing the reader to interact with the tags of the batch. However, this deterministic process will be very time consuming since reader needs to authenticate each and every tag of the batch to determine its validity. The situation will be even worse if there are large numbers of tags in the system. To solve this issue, we design a probabilistic protocol to solve the batch authentication problem by using a variation

of FSA based tag detection algorithm. We call our protocol probabilistic since FSA itself is a probabilistic protocol. It will provide a provable probabilistic guarantee for valid batches of tags ensuring the percentage of potential counterfeit products is less than counterfeit threshold (Δ). Δ is a system parameter defined by the user in advance. We guarantee a batch is valid if there are no more than $n * \Delta$ counterfeit tags in the batch. Note that it does not mean that the batch will be declared as valid if the number of counterfeit tags is lower than $n * \Delta$. Even if there is only one counterfeit tag in the batch, it will still be declared as invalid.

6.5. Group Test (*GTest*) Batch Authentication Protocol

In this section, we present a batch authentication process called *Group Test (GTest*) that uses statistical inference to determine the validity of a batch of tags. The concept of GTest is to reduce the cost of detecting counterfeits in large populations which is believed to contain a small proportion of defectives by drawing sample from the large population randomly. If GTest protocol is applied to products of batches in a large supply chain, then there may be no interest in knowing which products are defective. The purpose may instead be to accept or reject the batch or to estimate the number of counterfeit products it contains. Therefore, it is useful to know the probability distribution of the number of counterfeit samples.

6.5.1. GTest Protocol Design

GTest protocol operates in two phases − *1) Group identification* and *2) authentication*. In the first phase, the reader queries the tags with a nonce n_r. The tags, then, replies the following encrypted message with probability 0.5

$$h(k_i \parallel n_r)$$

Here, k_i is the group key in which the tag belongs. Now the reader tries all the group keys to decrypt this message. If the reader finds the right group key that correctly decrypts the message, then the reader can learn the identification of all the tags corresponding to that group by online querying the database of the server. This process of tag identification is much efficient

than per tag based identification since the reader do not need to query each individual tag of the batch. The reader will, then, start the authentication process by randomly selecting m tags as samples and collecting the authentication data from them. Next the reader forwards these data to the server. GTest declares this batch of tags as invalid if the server can detect one invalid or counterfeit tag.

6.5.2. Protocol Analysis

According to the statistical inference based on sampling, we can estimate the proportion of individual samples that are defective when they have been taken at random from a large population. If n individual samples are combined t at a time to give m pooled samples, then the number of counterfeit pooled samples follows approximately the binomial distribution $\mathcal{B}(m, \delta_t)$, where

$$\delta_t = 1 - (1 - \delta)^t = probability\ that\ a\ pooled\ sample\ is\ positive$$

Here, δ is the probability that an individual sample chosen at random from the entire population is defective. Suppose, that our complete population of tags (i.e. N tags) contains n_c counterfeit tags. Therefore,

$$\delta = n_c/N$$

A pooled sample is assumed to be invalid if and only if it includes at least one individual counterfeit sample. Then the probability that exactly η of the pooled samples may be invalid is given by

$$f(\eta|n_c) = \binom{m}{\eta} \sum_{i=0}^{\eta} (-1)^i \binom{\eta}{i} \binom{N-n_c}{n-(\eta-i)t} \Big/ \binom{N}{n-(\eta-i)t} \quad \text{...(3.1)}$$

where, $\max\left(0, m - \frac{(N-n_c)}{t}\right) \leq \eta \leq \min(m, n_c)$

In equation 1, when η is zero, we derive −

$$f(\eta|n_c) = \binom{N-n_c}{n} \Big/ \binom{N}{n} \quad \text{... ... ... (3.2)}$$

Equation 3.2 refers to the hypergeometric probability since the absence of counterfeit among the n individual samples is equivalent to the absence of positive pooled samples.

Now that we know that the number of counterfeit tags follows the hyper-geometric distribution, we define random variable X to refer to the number of counterfeit products in a batch. Suppose, in a batch with n tags we sample n_s at a time. Then the pdf of X will be:

$$f(X|n\Delta) = \frac{\binom{n\Delta}{X}\binom{n(1-\Delta)}{n_s-X}}{\binom{n}{n_s}}$$

Here, $E[X] = n_s * \Delta$. However, using GTest protocol, if we want to identify the validity of a batch, reader needs to read a high amount of data. For example, with n = 100000, n_s = 1000 and $\Delta = 0\%$ (meaning that every counterfeit tags need to be detected), reader needs to read $1000 * 20 * log_2^{100000} =$ 3.1 M byte of data which will take high response time. Therefore, to decrease the protocol response time we propose a more efficient protocol in the next section.

6.6. Framed Slotted ALOHA (*FTest*) based Batch Authentication Protocol

In this section, we propose *FTest* protocol which is dependent on a variation of *Frame Slotted ALOHA technique*. We consider an RFID reader R, and a population of N RFID tags denoted as $T*$. Table 6.3 summarizes the notations for FTest protocol.

Table 6.3 Notations for FTest protocol

Symbol	Meaning
SP	Slot position within frame
RV	Response Vector generated by the reader with the replies of tags
RV_s	Response Vector generated by the server
rem	Set of tags that are removed from the authentication initialization phase to reduce collision slot

6.6.1. FTest Protocol Design

FTest has three phases − 1) *Group identification*, 2) *Authentication initialization* and 3) *Counterfeit detection*. The group identification phase is similar to the one mentioned in GTEst batch authentication protocol. The other two phases are discussed next. The entire process is illustrated in Figure 6.3.

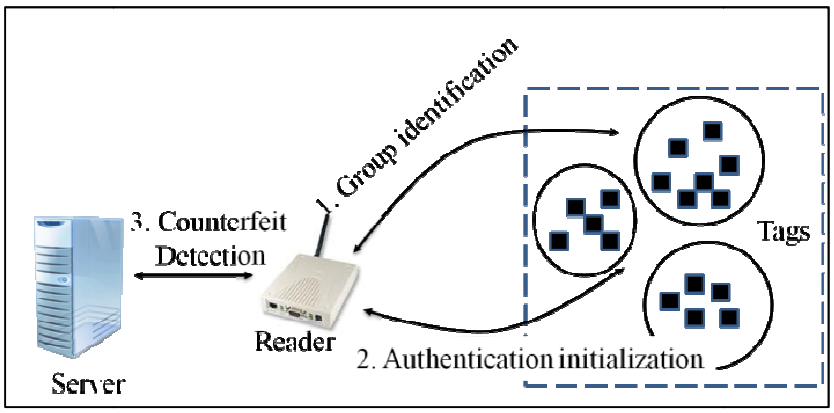


Figure 6.3 Authentication process of FTest protocol

Authentication initialization: After identifying a group of tags using the group identification mechanism mentioned in GTest protocol, the authentication phase is initialized. Reader simply starts the authentication by sending "*start authentication*" command to the server and by receiving a frame size f and random number r. The reader broadcasts the f and r received from the server in the first step. The frame consists of f short-response time slots right after the request. Each tag uses the random number *r* and its key *(id)* to hash to a Slot Position, SP, between $[1, f]$ where

$$SP = h(id, r) \bmod f$$

The tag transmits a short response at that slot (ex. 1 bit). Therefore, the time duration of all slots in our approaches is very short. After the frame ends, the reader abstracts the responses in the frame as a Response Vector (RV). RV is a vector in which each element is related to a slot in the frame. There are three types of elements in an $RV-$ 0, 1, and $collision$, representing empty slot, single reply slot, and collided slot, respectively.

We modify the slot picking behavior so that instead of having a tag pick a slot and return its *id*, we let the tag reply with 1 bit of information signifying that the tag has chosen that slot. In other words, instead of the reader receiving

$$\{\dots \mid id1 \mid 0 \mid \dots \mid collision \mid 0 \mid 1 \mid \dots\},$$

where, 0 indicates no tag has picked that slot to reply, and collision denotes multiple tags trying to reply in the same slot, the reader will receive:

$$\{\dots \mid 1 \mid 0 \mid \dots \mid random\ bits \mid 0 \mid 1 \mid \dots\}$$

Algorithm 1: *Algorithm executed by RFID tags*

Receive (f, r) from R
for each tag T_i (where i = 1 to N)
    compute $SP_i = h(id_i, r) \bmod f$
end
while R broadcasts Slot Position (SP)
    if ($SP == SP_i$)
        return 1 in $RV[SP_i]$
end

Figure 6.4 Algorithm executed by tags in FTest protocol

Algorithm 2: *Algorithm executed by reader R*

Define RV of length f
Initialize all entries of RV to 0
for Slot Position $SP = 1\ to\ f$ **do**
    Broadcast SP and listen for reply
    if ($no\ reply$)
        continue
    else if ($reply! = collision$)
        $RV[SP] = 1$
    else $RV[SP] = collision$
end
return RV to the server

Figure 6.5 Algorithm executed by reader in FTest protocol

Algorithm 3: *Counterfeit Detection*

assign $total\_counterfeit\_tag$ = number of counterfeit tag detected during per tag authentication

while ($total\_counterfeit\_tag/n < \Delta$|entire RV checked)

if ($RV[i] == 0$ & $RV_s[i] == 0$) *continue*

else if ($RV[i] == 1$ & $RV_s[i] == 0$)

assert *counterfeit detected*

$total\_counterfeit\_tag$ ++

else if ($RV[i] == collision$ & $RV_s[i] == 1$)

assert *counterfeit detected*

else continue

end

Figure 3.6 Counterfeit detection process in FTest Protocol

This is more efficient since the tag id is much longer than the bits transmitted. However, this approach is still inefficient because the information carried in the collision slot is totally unused. To utilize the collision slot, we turn it into a single reply slot by removing one of the two tags from this phase.

Suppose two tags T_i and $T_j$map to the same slot position. We remove the tag (T_i) from this phase so that it does not transmit any short response. Hence, another tag (T_j) corresponding to this slot has a singleton slot which allows it to be authenticated.

This situation can be made more efficient by turning each $p - collision$ (p tags mapped into one slot) slot into a singleton slot by randomly removing $p - 1$ tags. All the tags that are removed using this process are instructed to keep silent in this phase and they are authenticated in the next phase. We refer to this set of tags as rem. In counterfeit detection phase, the reader authenticates those tags after another to verify their validity.

The authentication protocol is shown in Figure 6.4, 6.5, and 6.6. Each tag in the set executes Algorithm 1 (see Figure 6.4) independently. The reader executes Algorithm 2 (see Figure 6.5) to generate the RV and return it to the server.

Counterfeit detection: In this phase, first the server starts the detection process by challenging the tags belonging to rem with a nonce n_r. The tags, replies the following encrypted message: $h(id \parallel n_r)$.

The server considers those tags as valid for which it can find legitimate ids able to generate the corresponding hash values. Tags that cannot authenticate it selves are considered as counterfeit tags. After this per tag authentication process is over, server starts to verify the validity of RV. Since the server knows all the keys of the tags corresponding to that batch, it can use those keys for reconstructing the RV. The server knows the locations of the empty, singleton and collision slots. If such reconstructed response vector exists, which we name as RV_s, the server deterministically accepts the batch of tags as valid. Otherwise, the batch is invalid. Because a counterfeit tag has no valid key, its corresponding reply is not expected. So if a slot is supposed to be empty but the server finds it singleton, then the server asserts the existence of counterfeit tag. If a slot is supposed to be singleton, but the server finds a collision, then at most one tag of that slot is valid and it is also an indication of the existence of counterfeit tag. Otherwise, the server goes to the next slot position. After the checking ends, if there is no counterfeit tag detected, the batch will be accepted as valid.

Since our goal is to declare a batch invalid if the percentage of counterfeit tags exceeds counterfeit threshold Δ, we incorporate that parameter in our counterfeit detection process. This detection process will not continue if the number of total counterfeit tags in the batch to the number of total tags in the batch is greater than Δ. This will significantly reduce the number of rounds in the counterfeit detection protocol since the entire RV does not need to be checked. It will also reduce the response time of the entire protocol. For example, suppose n = 1000, number of counterfeit tag detected during per tag authentication is 35. Number of counterfeit tags detected during the first 70 rounds of counterfeit detection protocol is 15. Then,

$$total\_counterfeit\_tag\ /n = \frac{50}{1000} = 0.05$$

If $\Delta = 5\%$, then the counterfeit detection protocol will stop after 70th round. With n = 100000, n_s = 1000 and $\Delta = 0\%$, FTest reads 0.03 M byte of data per batch.

6.6.2. Protocol Analysis

- In FTest protocol, we assume that all tags in a batch, both legitimate and counterfeit, will reply at least once in the frame. However, the counterfeit tags may reply more than once to introduce more collision and we name this type of attack as "*collision attack*". Additionally, the counterfeit tags may not reply at all to hide their identity and we name this attack as "*concealing attack*". It is very hard to defend against concealing attack and it is out of the scope of this work. We can identify the collision attack by comparing the RV (response vector returned by the reader) and RV_s (response vector generated by the server for genuine tags only). There can be following types of distinguishable situations that indicate the existence of collision attack:
- When $RV_s[i] = 0$ and $RV[i] = 1$, there should be no genuine tags replying in this slot. But the result shows one tag has chosen this slot. So, this tag must be a counterfeit.
- When $RV_s[i] = 0$ and$RV[i] = collision$, there should be no genuine tags replying in this slot. But the result shows more than one tags of this batch has chosen this slot. This also ensures that there are counterfeit tags in the system.

When $RV_s[i] = 1$ and$RV[i] = collision$, there should be only one genuine tag. But the result shows more than one tags has chosen this slot. It implies that at most one tag replied in this slot is genuine and the rest are counterfeit.

6.7. Security Analysis of FTest Protocol

6.7.1. Attack Model

The goal of an adversary in our system is to install counterfeit tags in the system. Evidently, this fake tag can let a fake object to be identified as an authentic one. We assume $\hat{A}$ is

an adversary who can eavesdrop in between the channel and can use the learned information to create counterfeit tags and install them in the system. Each counterfeit tag is denoted as $\hat{T}$. The attacker may try to track genuine tags of the system. We also assume that genuine tags and reader cannot be compromised by the attacker. In our system, the following oracle-like construction exists:

- $\boldsymbol{\mathcal{O}_{Eavesdrop}(R, T, t)}$: The adversary eavesdrops to listen to the communication between R and one of its tag T.
- $\boldsymbol{\mathcal{O}_{Impersonate_R}(R, T, M, t)}$: The adversary impersonates a reader R by sending a message M to the tag T.
- $\boldsymbol{\mathcal{O}_{Impersonate_{WT}}(R, T, M, t)}$: The counterfeit tag T impersonates a genuine tag in a protocol session at time t and sends a message M to the reader R.
- $\boldsymbol{\mathcal{O}_{Query}(T, t)}$: The adversary queries a tag $\boldsymbol{T}$ to learn information during a communication session at time t.
- $\boldsymbol{\mathcal{O}_{Receive}(U, M, t)}$: The adversary receives a message M from an entity U (e.g., either T or R) at time t.

6.7.2. Security Analysis

In this section, we analyze our proposed authentication protocol against different types of attacks. For every attack, we first describe how the attack is performed by an adversary. Then how our protocol protects against the attack is explained. R and T_i are referred to as a legitimate reader and legitimate tag. Each attack and defend, as a whole, have three phases:

Phase 1. *Learning phase:* This phase represents pre-attack preparations. Adversary, $\hat{A}$ uses non-destructive oracles such as $\boldsymbol{\mathcal{O}_{Eavesdrop}(R, WT, t)}$, $\boldsymbol{\mathcal{O}_{Query}(WT, t)}$, $\boldsymbol{\mathcal{O}_{Impersonate_R}(R, T, M, t)}$, and $\boldsymbol{\mathcal{O}_{Receive}(U, M, t)}$ on a set of target tags and reader to learn information related to them.

Phase 2. *Attacking phase:* $\hat{A}$ starts to attack by creating counterfeit tag ($\hat{T}$) and installing them in the system.

Phase 3. *Defend Phase:* Our protocol is designed in such a way so that it can defend against majority of the attacks performed by the fake tag $\hat{T}$.

Since the defend phase is different for each attack, we discuss this phase for following attacks:

- ***Collision Attack***

Learning and Attack Phase: Under this attack, $\hat{A}$ queries a set of valid tags with different (f, r) using $\boldsymbol{\mathcal{O}_{Impersonate_R}(R, T_i, M, t)}$ oracle to collect replies from the genuine tags. Using this learned information she creates fake tags and installs them in the system. From then on, the fake tags will try to attack the system with their responses.

Defend Phase: In collision attack, a counterfeit tag emits replies in multiple slots for disturbing the distribution of slots in the RV. In fact, our approach is very immune to such attack, since generating more meaningless replies is equivalent to increasing the ratio of counterfeit tags, which helps to increase the probability of detecting counterfeit tags.

- ***Privacy Violation Attack***

Learning Phase: Under this attack, $\hat{A}$ repeatedly queries T_i with different (f, r) using $\boldsymbol{\mathcal{O}_{Impersonate_R}(R, T_i, M, t)}$ oracle to collect replies from the existing tags.

Attacking phase: $\hat{A}$ execute $\boldsymbol{\mathcal{O}_{Receive}(U, M, t)}$ oracle to learn replies from the tags and create a response vector. The goal of the attacker is to learn the ids of different tags.

Defend Phase: Our protocol can preserve the privacy of individual RFID tag since none of the tags reply their id. Therefore, the adversary cannot infer ids from the replies of the tags.

- ***Tracking Attack***

Learning Phase: Here, $\hat{A}$ tries to track T_i over time. $\hat{A}$ succeeds if it can distinguish WT_i from other tags over time.

Attacking phase: Under this attack, $\hat{A}$ repeatedly queries T_i with different (f, r) using oracle $\mathcal{O}_{Query}(T_i, t)$ to learn about the slot picking behavior of the tags. Then the adversary executes oracle $\mathcal{O}_{Receive}(U, M, t)$ to receive replies from the tags. The goal of the attacker is to get a consistent reply that may become a signature of T_i.

Defend Phase: FTest protocol is resistant against tracking. Let an adversary $\hat{A}$ eavesdrops on the transaction between a reader *R* and the genuine tags. So $\hat{A}$ knows the queries and replies but $\hat{A}$ cannot reverse compute the replies. The adversary can certainly be sure that a communication has taken place. However, it cannot Figure out which tag replied in which slot since it do not have ids of the tags. Moreover, the slot picking behavior of the tags changes with the change of f and r. Therefore, the outputs of all the tags seems to be pure random to the adversary $\hat{A}$.

- ***Eavesdropping Attack***

Learning Phase: $\hat{A}$ executes the oracle $\mathcal{O}_{Eavesdrop}(R, T_i, t)$ and later uses this information to launch different attacks (ex. replay attack).

Attacking phase: $\hat{A}$ learns every information exchanged between *R* and T_i. The goal of $\hat{A}$is to use the data to impersonate a fake tag.

Defend Phase: Our protocol is powerful against this attack. In our protocol $\hat{A}$ will not be able to find out the expected reply of the tags. In each pass, all tags will pick a different slot based on the random number sent by the reader. $\hat{A}$ can only observe the communication but it cannot link the outputs of the two parties. It cannot even launch replay attack by replaying previous messages since the slot picking nature of the tags changes with f and r.

6.7.3. Evaluation Results

We evaluate the efficiency of GTest and FTest Protocol based on the metric − *execution time*. To compare the performance of both protocols we also simulate a *Per Tag Authentication*

(PTA) protocol to identify the validity of batches. PTA is a deterministic approach, which authenticates all tags to detect the validity of a batch. The accuracy of PTA is certainly 100% but its efficiency is very low. There are plenty of Per Tag Authentication protocols in literature [Dimitriou06, Lu07, Hoque11, Hoque09a, and Hoque09b]. We use AnonPri [Hoque11], a group based authentication protocol as PTA. In our simulation, the authentication server is implemented on a high performance Dell PC. We use java for protocol simulation where we use SHA-1 as the hash function (returning 160 bits) in all three protocols. We also use MySQL to store secret keys for the simulated tags. In our simulated RFID environment, we have considered two systems with $N = 2^{16}, \tau = 8, 16, 32, 64$ and $N = 2^{20}, \tau = 512, 256, 128, 64$. We deliberately introduce 1% to 4% randomly generated counterfeits into the dataset. We have run the simulation for 100 times and reported the average.

Execution time metric determines the time required for interaction between the reader and tags. This metric tells us the processing time of a protocol to determine the validity of tags when we need to identify all the counterfeit tags in each batch. Since every bit almost consumes the same transmission time which equals $25\mu s$ [EPCGLOBAL] on average, we measure the execution time by multiplying the size of transmitted data (in bits) with $25\mu s$. For all protocols, we consider the tags uses SHA-1 hash function. Therefore, in GTest protocol, the length of data replied by tags is 160-bits [Neill08]. The total size of data used for group identification equals $160 * n/2$ (since tags will reply with probably 0.5). Now to verify a batch with n tags, suppose that n_s tags are sampled and the length of random numbers equals 160 bits. The size of authentication phase will equal $(160 + 160) * n_s\ bits$, since reader will challenge with a random number (160 bits) and tags will reply with their hashed response (160 bits). So, the total data size of GTest protocol will be:

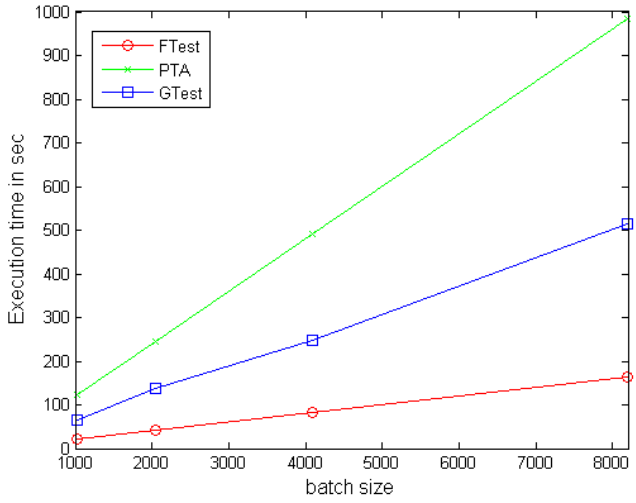
$$d\_size_{GTest} = \left(160 * \frac{n}{2} + (160 + 160) * n_s\right) bits$$

For PTA protocol, the reader needs to check all the group keys and this has to be done for all the tags of the batch. Therefore, the data size will be

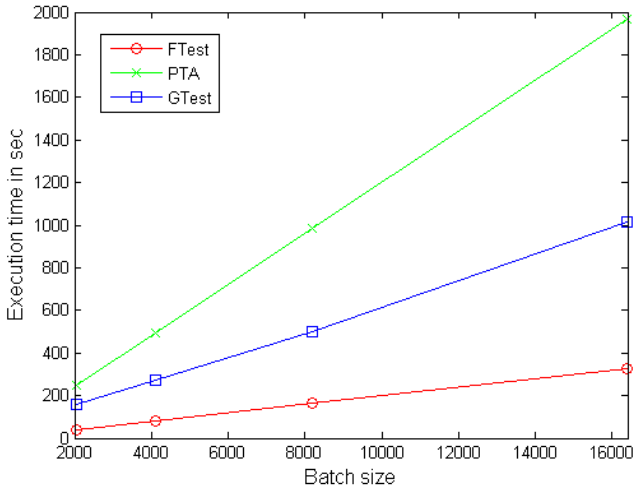
$$d\_size_{PTA} = (160 * n + (160 + 160) * n)\ bits$$

On the contrary, the data transferred in FTest one random number and f replies. Since each echo is in the same size (1bits), the total size:

$$d\_size_{FTest} = \left(160 * {}^{n}/_{2} + (160 + 1) * (n - n_{rem}) + (160 + 160) * n_{rem}\right)\ bits$$



(a) Execution time of FTest, GTest, and PTA when N =2^{16}



(b) Execution time of FTest, GTest, and PTA when N =2^{20}

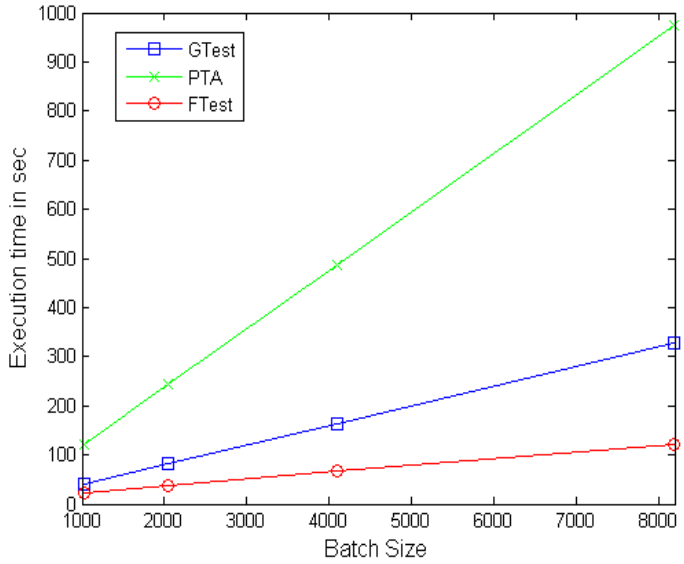
Figure 6.7 Comparison of execution time of FTest, GTest and PTA protocol

Figure 6.7(a) and 6.7(b) shows the execution time of our two protocols. The figure shows that GTest performs better than PTA and FTest performs the best. We can see that FTest protocol significantly reduces the execution time. For system with $N = 2^{16}$, FTest reduces almost 800 sec than PTA for the largest batch. And for system with $N = 2^{20}$, FTest reduces almost 1700 sec than PTA for the largest batch. . And for system with $N = 2^{20}$, FTest reduces almost 1700 sec than PTA for the largest batch (see Table 6.4).

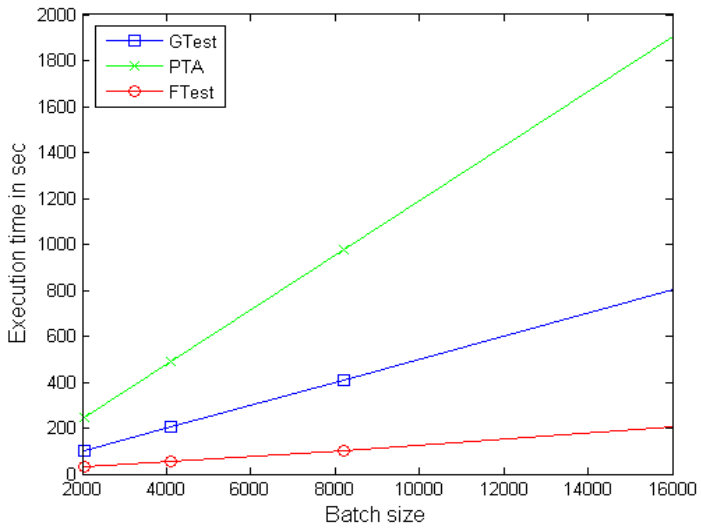
Table 6.4 Performance comparison table

N	Ftest savings over PTA [6]
2^{16}	≈ 800sec
2^{20}	≈ 1700sec

Figure 6.8(a) and 6.8(b) shows the execution time of our two protocols when $\Delta \approx 3\%$. By $\Delta \approx 3\%$, we mean that the protocol will consider a batch invalid if it can identify at least 3% of the tags as counterfeit. At that point, the protocol will declare the entire batch as invalid and will stop executing further. The figure clearly shows that, with $\Delta \approx 3\%$, FTest is the most efficient protocol. We can see that out approaches, especially FTEst protocol significantly reduces the execution time. FTest with $\Delta \approx 3\%$ saves almost 85 sec for largest batch size.



(a) Execution time of FTest, GTest, and PTA when $N = 2^{16}$ and $\Delta = 3\%$



(b)

(b) Execution time of FTest, GTest, and PTA when N =2^{20} and $\Delta = 3\%$

Figure 6.8 Comparison of execution time for FTest, GTest and PTA protocol with $\Delta = 3\%$

6.8. Goals Satisfied by FTest Protocol

The motivating example of RFID application for this chapter is to identify counterfeit tags in large scale RFID systems efficiently. The goal of such a system is to identify counterfeit tags, ensure low system response time as well as provide basic security like confidentiality and authentication. FTest protocol is able to achieve all these goals with very low response time compared to the existing work.

6.9. Summary

Detecting counterfeit tags in large scale RFID systems is a very significant but underrated research issue. Most of the existing RFID authentication methods used for counterfeit detection require a pre-identification process, and suffer from high scanning cost and communication cost. We believe that an efficient, secure and fast counterfeit detection protocol may have good impact on the deployment of many large scale RFID systems. In this chapter, we present an efficient batch authentication protocol (FTest) to detect product counterfeiting in RFID enabled systems.

Our simulation results show that our FTest can perform significantly better than per tag authentication protocols.

6.10. Publication

- ***Published:*** *Farzana Rahman* and Sheikh Iqbal Ahamed, "Looking for needles in a haystack: Detecting Counterfeits in Large Scale RFID Systems using Batch Authentication Protocol", *in Proc. of IEEE PerCom Workshop on Pervasive Wireless Networking (PWN12)*. Switzerland, March, 2012.
- ***In Press:*** *Farzana Rahman* and Sheikh Iqbal Ahamed, "Efficient Detection of Counterfeit Products in Large Scale RFID Systems with Batch Authentication Protocols", *Accepted to appear in Journal of Personal and Ubiquitous Computing, Springer-Verlag*, 2012.

6.11. Acknowledgement

This research is awarded by Computational Sciences Summer Research Program (CSSRP) Fellowship for summer 2011 by Marquette University.

Chapter 7: Privacy Preservation in RFID based Healthcare Systems

RFID technology can provide a number of benefits to the healthcare industry. This technology can improve overall safety and operational efficiency because it operates without line-of-sight while providing immense capabilities. In fact, RFID can contribute to create the hospital of the future by improving patient care and safety, optimizing the workflows, reducing the operating costs, and reducing costly thefts. There are a number of ongoing trials and studies at hospitals and healthcare centers around the world utilizing and integrating RFID into their hospital information systems. One study estimates that the market for RFID tags and systems in healthcare will rise rapidly from $90 million in 2006 to $2.1 billion in 2016 [Harrop08]. Primarily, this will be because of *Item Level Tagging* of drugs and *Real Time Locating Systems* for staff, patients and assets to improve efficiency, safety and availability and to reduce losses [Harrop08].

By attaching RFID tags to different entities in healthcare industry (people and objects), RFID technology can provide tremendous automation in identification, tracking, monitoring and security control measures. These capabilities directly affect the major issues currently experienced by healthcare organizations while helping to drive down costs [BlueBean]. Some of the most promising RFID based systems that are already being successfully tested (or deployed) are: patient identification and monitoring, patient's drug usage monitoring, surgical instrument tracking and locating, newborn identification, hospital personnel identification and tracking, blood bag tracking, detecting pharmaceutical counterfeit, avoiding theft of medical equipment, tagging of meal plateaux to ensure patients get the appropriate diet, ensuring proper identification of laboratory specimens, and restrict access to high threat areas of the hospital to authorized staff, etc.

In a patient identification system of an RFID based hospital, every patient is identified using an RFID tag installed wristband [Wessel05]. A reader is used to identify the ID of the tag

which allows the system to identify the patient uniquely. It also allows doctors, nurses and other hospital personnel to access the medical information of the legitimate patient from the server, using the tag ID. The ID can also be used to access various healthcare services, for example, identifying and dispatching prescribed medicine for a particular patient.

In spite of several ongoing researches on RFID based healthcare systems [Chen10, Turcu09], there are still some significant research challenges regarding privacy that need to be addresses. First, RFID tags can be read at a small distance, through materials, even without the knowledge of its owner. Second, if the communication between tags and readers is performed in wireless environment, any unauthorized reader may try to track the tag to access the user's private information. Third, data collected from RFID tags can potentially be used by multiple users (doctors, nurses, pharmacists and etc) and multiple organizations to provide various healthcare services. Fourth, the ID of the RFID tags along with its Electronic Medical Record (EMR), collected over a period of time, may expose significant private information of user such as: trace of personal health information, clinical history and financial information. In conclusion, RFID technology has not really seen its true potential in healthcare since above mentioned four privacy concerns are not properly addressed by the existing techniques.

7.1. Our Major Contributions

In this chapter, we make an effort to address the above mentioned challenges with following contributions:

- From the four privacy concerns mentioned in the introduction, we point out two major privacy concerns in RFID based healthcare systems: *privacy concerns in RFID sensing* and *privacy concerns in RFID based healthcare service access*.
- We propose a framework (PriSens-HSAC), consisting of two major components, each component respectively addresses one of the above mentioned two privacy issues.

- The PriSens component proposes a group based anonymous authentication protocol to solve the tradeoff between the scalability and privacy problem of RFID sensing. Our idea is to preserve privacy in RFID sensing based on the premise that adversary cannot break unlinkability with probability better than random guessing.
- The HSAC component proposes a privacy preserving healthcare service access mechanism to maintain user's privacy while accessing various healthcare services.
- We also present the evaluation of the framework by measuring the level of the achieved privacy.

Though our major motivation in this chapter is to enhance the privacy of users in an RFID based healthcare system, our proposed PriSens-HSAC framework addresses all the security and privacy requirements mentioned in Chapter 3. This framework has scope not only in the healthcare industry, but also in other applications where the privacy of the tag bearers is an important issue.

Organization of the chapter: The rest of the chapter is organized as follows. Section 7.2 presents the motivation of our work. In section 7.3, we present relevant related work. In section 7.4, we discuss the privacy issues of RFID tag sensing in healthcare setting. In this section, we also discuss the privacy issues in RFID based healthcare service access. In section 7.5, we present the details of our framework. Then we present the group based anonymous authentication protocol (PriSens) in section 7.6. The architecture of HSAC is presented in the same section. In section 7.7, we present the evaluation of our framework.

7.2. Motivation

7.2.1. RFID in Healthcare

With the deployment and use of RFID technology in the healthcare domain, there are increasing privacy concerns regarding the technical designs of RFID systems. The potential benefits of RFID technology have been accompanied by threats of privacy violations [Juban04].

These threats pertain to the potential risks of unauthorized data access, misuse of patient data, and the capabilities of permanently saving and linking information about individuals through temporal and spatial extension of data collection activities. While RFID technology can improve the overall quality of healthcare delivery, the benefits must be balanced with the privacy and security concerns. The use of RFID introduces a new set of risks: Security risks are associated with the possible failure of the RFID system under various security attacks, i.e. tracking, eavesdropping, and denial of service, while the threat to privacy reside in the capabilities to permanently save and link information about individuals through temporal and spatial extension of data collection activities. Although concerns about information privacy are not unique to the healthcare domain, health related information can be perceived as more personal and more sensitive. Due to the highly personal and sensitive nature of healthcare data, both healthcare providers and patients can be expected to resist further digitalization though the usage of RFID technology until security and privacy protections is in place.

There are different kinds of RFID applications that allows healthcare professionals to avoid errors or risks that could endanger the patient safety. Usually, RFID based sensing activities related to healthcare can be divided in two types:

Direct sensing activity: These activities refer to various identification and monitoring systems. Some of the most promising RFID based direct sensing activity that are already being successfully tested (or deployed) in a number of hospitals are: hospital personnel [Wessel05], patient and newborn identification and monitoring [Wessel05], patient's drug usage monitoring [Yao10], surgical instrument tracking and locating [Rivera08], and blood bag tracking [Yao10].

Indirect inferred activity: These activities basically refer to those systems that use direct sensing activity data to infer important information. For example, detecting pharmaceutical counterfeit, avoiding theft of medical equipment, the tagging of meal plateaux to ensure that patients get proper diet according to their treatment, allergies and tastes and etc.

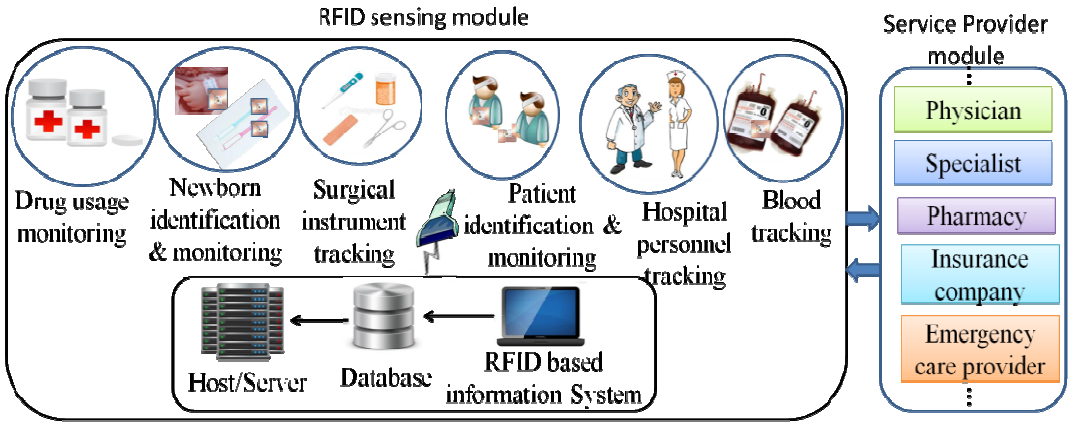


Figure 7.1 An RFID based ubiquitous healthcare system

Figure 7.1 illustrates a simple architecture of an RFID system in healthcare. It has two individual modules:

1) *RFID Sensing Module* - consisting of all the RFID identification and monitoring systems.

2) *Service Provider Module* - consisting of all the systems that uses legitimate RFID identification data to provide various healthcare services (ex. physician's diagnosis, prescription, medicine usage chart, specialist's opinion, insurance verification, appropriate medicine dispatch, and etc).

Some simple example scenario of RFID tag usage in healthcare area can be as follows:

Medicines' authenticity tracking: Ensuring the origin of medicines is essential to guarantee their quality. RFID tag based identification and authentication methods can guarantee the origin of medicines, especially in pharmaceutical supply chains. Electronic Product Codes (EPC) (e.g. a serial number) in RFID tags are used to track each individual medicine along the supply chain. Each EPC/RFID tag is attached to a drug unit. Thus, it is possible to track every individual drug unit and to verify its authenticity.

Patients' drug dispatch: Usually, in case RFID based hospitals, a patient is identified using RFID installed wristband [Wessel05]. The medical information of the legitimate patient is then pulled up from the central database and passed onto the physician's PDA which is a part of

the service provider module. The physician's system may suggest medicine based on diagnosis and the pharmacy system may use the prescription to dispatch proper medicine for the patient.

Financial Transactions: Depending on the health care system, patients must pay for the service that they receive. In addition, health care providers must be able to verify that a given patient is covered under a particular plan, what specific procedures, lab tests, and whether dependants are covered. In this case, RFID can be used to identify patients using wristbands [Wessel05] which can pull up all those information in seconds for hospital bill calculation.

Patients' disease monitoring: Wide varieties of methods have been used to identify patients when they are in hospitals. One of the most popular methods is based on using a wristband in which a bar code is printed. However, recently the barcode based bracelets has been replaces by RFID tag based bracelets [Wessel05]. In some chronic diseases, continuous monitoring of patients is very important. RFID technology could be used to send information from patients to a control system. The control system could activate an alarm based on the received data.

7.2.2. Two Fold Privacy Preservation

It is evident that in RFID based healthcare systems, the privacy concerns are twofold: *privacy concerns in RFID sensing* and *privacy concerns in RFID based healthcare service access*. Therefore, to address this problem we need to have twofold privacy management mechanism in place:

1) *A privacy preserving authentication protocol is required while sensing RFID tags. This protocol will preserve privacy when different identification and monitoring process are executed in "RFID sensing module" of Figure 7.1.*

2) *A privacy preserving access control technique is required while receiving services from "service provider module" of Figure 7.1 to ensure that user preferred privacy level is achieved.*

To address the two above mentioned privacy problems in RFID system, we propose a privacy preserving framework (PriSens-HSAC) in this chapter. With this privacy mechanism in place, the true potential of an RFID based healthcare system can finally be exploited. The widespread adoption of such privacy preserving RFID based healthcare system will open doors for various assisted care, remote health monitoring, and elderly care systems. Eventually, it may help to ensure quality healthcare facilities, longer life expectancy, reduced death rate, and preserve patient's privacy.

7.3. Background Study

The HSAC component of the framework uses P-RBAC [Dafa-Alla05]. There are plenty of role based access control (RBAC) techniques in the literature. In [He05], the authors propose an enhanced role based access control mechanism for hospital information systems but they did not consider any privacy issues. Purpose based access control (PBAC) models also have been proposed to protect sensitive data [Byun05, Yang07], but the purpose is difficult to define. Jin et al propose a framework for e-Health systems [Jin09], which supports patient-centric selective sharing of virtual composite e-Health data using different levels of granularity. However, it focuses on the framework only and does not discuss a detailed approach for policy definition and management. Attribute based access control (ABAC) adopts XACML [Godik03] to define policies, and transform them into access control lists (ACLs). However, commercial DBMS kernel cannot support XACML and thus existing ABAC module in databases are implemented in an on the fly basis. This brings high performance degradation for the database.

The major component of PriSesn-HSAC framework is PriSens which is an RFID authentication protocol. Several authentication protocols have been proposed to secure RFID systems against major attacks and details of such related works are presented in Chapter 5.

Our proposed PriSens-HSAC framework provides higher level of privacy and security in terms of RFID sensing. The framework provides more privacy in RFID based healthcare system

by proposing a better privacy preserving authentication protocol and by using P-RBAC while accessing healthcare services. To the best of our knowledge, PriSens-HSAC is the first framework to provide increased privacy in RFID based healthcare systems through the usage of RFID authentication along with access control technique.

7.4. Privacy Concerns in RFID Systems

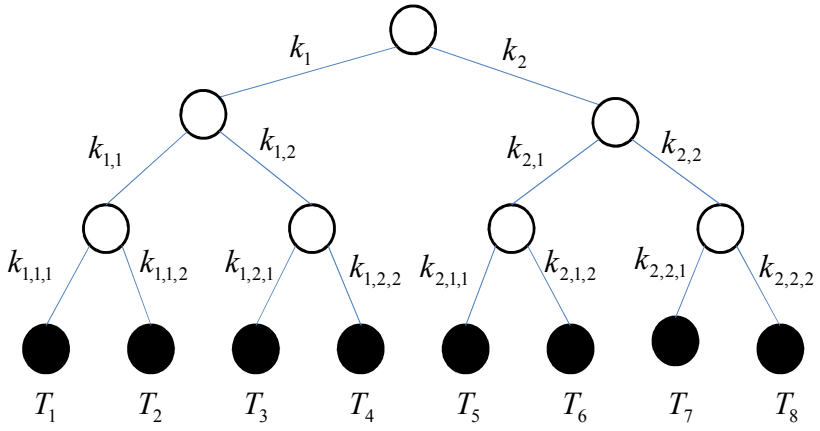
7.4.1. Privacy Issues in RFID Sensing

Ensuring strong privacy in RFID sensing imposes a higher complexity on the reader. Conversely, improving efficiency may hamper some privacy. Here, our main focus is on the tradeoff between privacy and scalability of RFID systems. Public key cryptography would be a better candidate to solve the problem between privacy and scalability. In this approach, the tag would encrypt its message using the public key of the reader so that only the real reader would be able to decrypt the message and identify the tag. But public key encryption is too expensive for low cost tags. In this chapter, we consider the low cost tags which are capable of doing symmetric key encryption, in which keys are shared between the tag and the legitimate readers. First, we outline how the tree based hash protocol provides scalability but sacrifice some privacy. Then, we describe how the group based protocol provides improved scalability as well as a higher level of privacy. Finally, we point out the privacy problem of this group based protocol. Our main focus, here, is on this major problem of tradeoff between privacy and scalability of RFID systems.

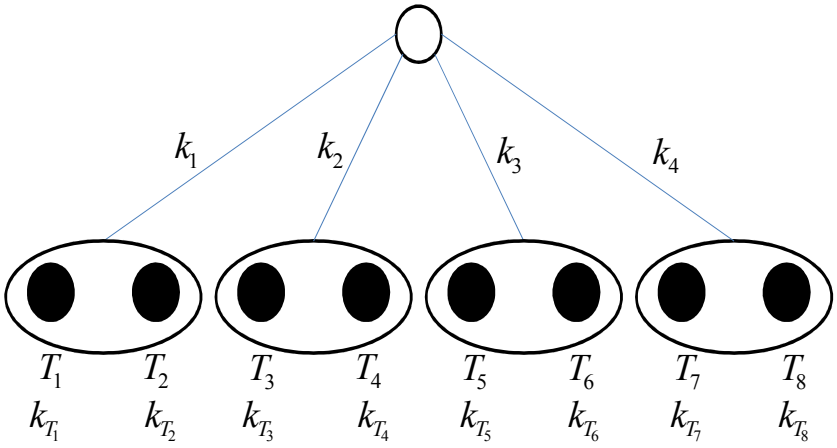
Molnar and Wagner [Molnar04] first proposed a *tree based hash protocol* for RFID systems to reduce the search complexity of the reader from $O(N)$ to $O(\log_{\alpha} N)$, where α is the branching factor at each level of the tree. But this approach achieves better scalability at the cost of some privacy loss of the tags [Nohl06]. Figure 6.2(a) shows a balanced key tree with $N = 8$ and $\alpha = 2$**.** Suppose the tag T_3 in Figure 6.2(a) becomes compromised. All the tags of the system are partitioned into three disjoint sets. The adversary can now uniquely distinguish the tag T_4 and identify the tags T_1 and T_2 as a unique partition. All the remaining tags (T_5, T_6, T_7, T_8) form

a single partition because the tag T_3 shares no key with them. Therefore each tag of this partition (T_5, T_6, T_7, T_8) is anonymous among these four tags. The privacy provided by this scheme diminishes as more and more tags are compromised.

Avoine et al. [Avoine07] proposed a *group based authentication protocol* to address the privacy problem of the tree based hash protocol. According to this protocol, tags are divided into γ disjoint groups of equal size. Figure 6.2(b) shows the group organization of the tags where $N = 8$ and $\gamma = 4$. This protocol reduces the complexity of both the reader and the tag. The tag always has to perform two encryptions. In the worst case, the reader has to perform $\gamma + 1$ encryptions. In addition, each tag needs to store only two keys for the authentication. The group organization of this protocol improves the level of privacy. For instance, if the tag T_3 is compromised, the adversary can uniquely identify only the tag T_4 (see Figure 6.2(b)). The adversary cannot uniquely distinguish the other tags $T_1, T_2, T_5, T_6, T_7, T_8$. Each of these tags remains anonymous among these six tags. Like other protocols, this protocol also has some limitations. There is a tradeoff between the number of groups and the group size. To address this problem, we propose an efficient anonymous private authentication (PriSens) scheme that improves the privacy protection by keeping the reader's complexity moderate. This protocol is specifically suitable for healthcare since its goal is to achieve automation and preserve privacy.



(a) Tree based hash protocol with N=8 and α=2



(b) Group based protocol, with N=8 and γ=4

Figure 7.2 Two privacy preserving RFID authentication protocols

There are several authentication protocols that have been proposed [Hoque11, Hoque 09a, Hoque09b, Avoine05, Avoine07, and Dimitriou06] for RFID systems to secure them against major attacks. However, all those protocols can preserve minimal user privacy at the cost of large reader complexity. The reader complexity increases with large number of tags is the system. Moreover, the level of privacy provided by the scheme decreases as more and more tags are compromised. Therefore, we identify that there is a tradeoff between privacy preservation and scalability in RFID authentication. To address this problem, we propose an anonymous private authentication (PriSens) protocol that improves the privacy protection in RFID sensing by keeping the reader's complexity moderate. This protocol is specifically suitable for healthcare industry since RFID based healthcare systems since its main goal is to preserve privacy while achieving automation. In our approach, each tag is assigned a couple of identifiers. A single tag shares some of its identifiers with some members of its group. Thus this protocol prevents tracking by increasing the uncertainty of the adversary.

7.4.2. Privacy Issues in RFID based Healthcare Service Access

The ID of the RFID tag identified by PriSens, may need to be shared with physicians, pharmacy, insurance company and emergency care providers to access various healthcare

services. This information, collected over a period of time, may expose significant private information such as trace of personal location, personal health information and etc. To address this, we propose a privacy preserving access control technique to restrict unauthorized access of patient's private information.

7.5. Architecture of PriSens-HSAC Framework

To solve the two major privacy issues in RFID based healthcare systems, we propose PriSens-HSAC, a framework consisting of two major components. One component is PriSens that proposes a group based anonymous authentication protocol to solve the tradeoff between the scalability and privacy of RFID sensing in healthcare. PriSens provides more privacy and achieves better efficiency than existing RFID authentication protocols. The second component is HSAC that proposes a privacy preserving healthcare service access mechanism to maintain user's privacy while accessing various healthcare services. HSAC follows the concept of role based access control mechanism to restrict unauthorized access to private data. The architecture of the framework is shown in Figure 7.3.

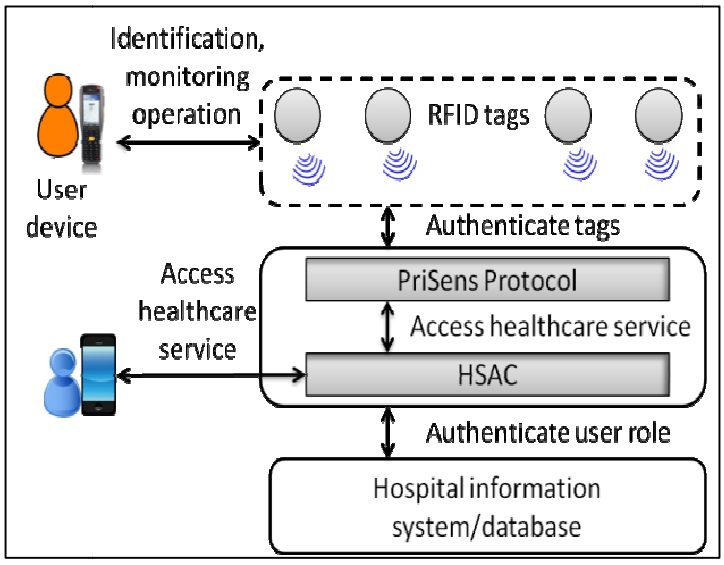


Figure 7.3 Architecture of PriSens-HSAC framework

When any RFID based identification or monitoring operation takes place in a healthcare system, the reader as well as tags in concern executes PriSens protocol to preserve user privacy. It is important to notice that PriSens can preserve privacy and defend against attacks launched by the outsider adversary. For example, if any unauthorized reader tries to launch any attack in the RFID information system of the hospital or tries to violate user privacy (by tracking the user), PriSens can defend against the launched attacks and provide better privacy compared to the other existing protocols [Molnar04, Avoine07]. If any unauthorized user wants to access any healthcare service (ex. access patient's medical history using the ID of the tag), HSAC will not allow the user to access that service using a privacy aware role based access control mechanism [Dafa-Alla05]. Therefore, it is evident that PriSens component will run in tags and reader. But HSAC component can be executed in user's mobile devices, central server or any other machines that uses ID if the RFID tag to access healthcare related services.

7.6. Overview of PriSens-HSAC Framework

In this section we describe the two components of Prisens-HSAC framework in detail.

7.6.1. Details of PriSens (Group based Anonymous Authentication Protocol for RFID Sensing)

In this section, we will describe the details of PriSens Protocol.

1) Privacy Characterization in PriSens

In literature several different notions of privacy have been proposed so far. Some authors mention *information privacy* as the privacy of RFID systems. This privacy notion is the act of preventing a tag from disclosing its product information [Ohkubo03, Weis03]. But protecting information privacy keeps tags traceable. Therefore, it is a weak notion of RFID privacy. Some define *unlinkability* as the strong notion of RFID privacy [Nohl06, Chatmon06]. Unlinkability means the inability to distinguish between the responses from the same tag and the responses from different tags of the system. Providing unlinkability ensures strong privacy when the

adversary cannot distinguish between two tags with a probability better than random guessing [Juels07]. In our protocol, we protect privacy of the tags by providing unlinkability between two tags of the system.

The level of privacy obtained by any protocol can be measured using the *anonymity set*. *Anonymity* has been proposed in the context of mix-nets in [Diaz02]. Mix-nets are used to make the sender (and the recipient) of a message anonymous. The anonymity set is defined as the set of all potential senders (recipients) of the message. Anonymity is defined as being not identifiable among a group of entities, i.e., the members of the anonymity set. A higher degree of anonymity is achieved with an anonymity set of larger size. Perfect anonymity is achieved if anonymity set contains all the members capable of sending (receiving) messages in system.

2) System Model of PriSens

In our protocol, tags are divided into groups of equal size. Suppose, N is the total number of tags in the system and τ is the number of groups. So, the group size is $n = \frac{N}{\tau}$. Next, we define the components and parameters of our system.

Issuer. The issuer initializes each tag during the deployment by writing the tag's information into its memory. The issuer also authorizes the reader access to the tags. Even each group receives its unique group key and a pool of identifiers from the issuer.

Group. Each group has a n number of tags. The issuer assigns a unique group key k_{G_i} to the ith group G_i of the system. This key is shared between the members (tags) of this group. Each group also receives the following pool of identifiers from the issuer $\xi_i = \{ID_{i,1}, ID_{i,2}, \dots, ID_{i,M}\}$, where, $1 \leq i \leq \tau$ and M is a system parameter. The pools of any two groups do not share any identifier, i.e., $\xi_i \cap \xi_j = \emptyset, \forall i \neq j$. Each tag of the group G_i is assigned a couple of identifiers from ξ_i by the issuer.

Tag. All the tags of the system are divided into τ groups. Each tag receives the shared group key of the group that the tag belongs to, a unique secret key that is known only to the

reader and the tag itself, and a set of identifiers from the pool of identifiers of the group. Suppose, the tag T_j belongs to the group G_i. This tag possesses the group key k_{G_i}, the unique secret key k_{T_j}, and a set of identifiers Ω_{ij}. Each key is of θ bits, where θ is the security parameter of symmetric key encryption. We define the Ω_{ij} as follows

$\Omega_{ij} = \{ID_{i,j_1}, ID_{i,j_2}, \dots, ID_{i,j_m}\}$, where,

each ID_{i,j_x} is chosen randomly following uniform distribution from the pool ξ_i and $j_x \in \{1,2, \dots, M\}$, where $1 \leq x \leq m$

$ID_{i,j_x} \neq ID_{i,j_y}$, for all $x \neq y$

m is also a system parameter and $M > m$.

The identifiers are assigned to the tags in such a way that at least one identifier of a tag is shared with at least two other members of the same group. So, we can say for the tag T_j,

$$\exists p, q\left[ID_{i,j_x} \in (\Omega_{ip} \cap \Omega_{iq})\right],$$

where p,q are any two members of G_i and $p \neq q$.

Reader. The reader is connected to the backend server. We assume the communication channel between the reader and the backend server is secured. From now on, we denote the backend server as the reader. In our system, the tag is the prover and the reader is the verifier. The reader receives all the secret information by the issuer during the deployment. The issuer issues the reader a set of secret information for each group in the system $\psi = \{\langle k_{G_i}, \sigma_i\rangle | 1 \leq i \leq \tau\}$, where k_{G_i} is the secret group key and σ_i is the mapping of the identifiers of the pool ξ_i with the secret keys of tags. Formally,

$$\sigma_i = \{\langle ID_{i,x}, \pi_x\rangle | 1 \leq x \leq M \text{ and } ID_{i,x} \in \xi_i\},$$

where π_x is the set of secret keys of tags associated with the $ID_{i,x}$. π_x can be defined as an empty set if no tag is associated with the $ID_{i,x}$ or it can be a set of size at least one. Formally,

$$\pi_x = \begin{cases} \{k_{\omega_1}, k_{\omega_2}, \dots\}, & \text{where } \omega_* \in \{T_1, T_2, \dots, T_N\} \\ \emptyset, & \text{otherwise} \end{cases}.$$

System parameters. Since each tag receives m identifiers randomly chosen from the pool of M identifiers, according to the ID distribution strategy, we can say that each tag has at least one identifier common with at least two group members. The probability that each tag shares at least one identifier with at least two group members is

$$P_{share} = 1 - \left(\frac{\binom{M-m}{m}}{\binom{M}{m}} \times \frac{\binom{M-2m}{m}}{\binom{M}{m}} \right) = 1 - \frac{\left((M-m)!\right)^3}{(M!)^2 (M-3m)!}$$

where $M \geq nm$. For example, we consider an RFID system of 1000 tags divided in 10 groups. 100 tags are in each group. For simplicity, we assume M = 100 and m = 10. Then the probability that each tag shares at least one identifier with at least two group members is $P_{share} =$ 96.87%.

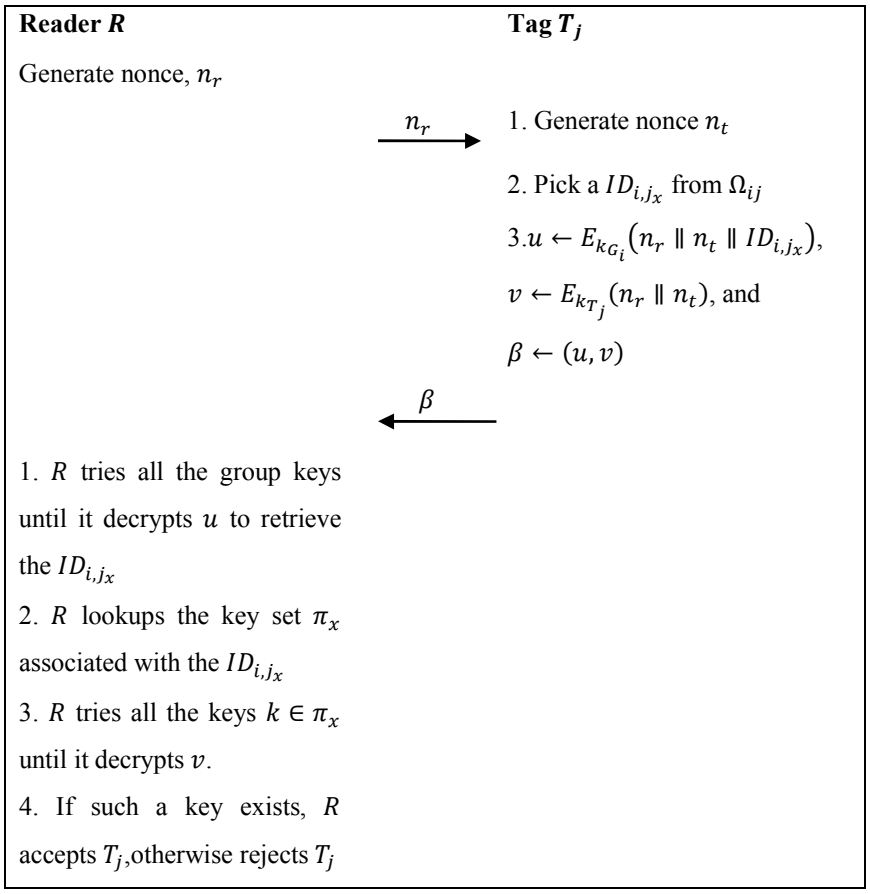


Figure 7.4 The PriSens protocol

3) Brief Overview of PriSens

We describe our protocol briefly in this section. The reader starts to query the tag with a nonce n_r. Upon the reception of the query, the tag generates another nonce n_t. Suppose the reader interrogates the tag T_j. In the second step, the tag picks an identifier, say ID_{i,j_x}, from Ω_{ij}. Then the tag computes β as shown in Figure 7.4. Here, $E_k(.)$ denotes symmetric key encryption with key k. The tag replies with the β. Now the reader searches all the group keys until it finds the correct one that properly decrypts the first part (u) of the response. If the reader retrieves the identifier ID_{i,j_x} that the tag used in its response, then the reader tries to decrypt the second part (v) of β with the potential set of secret keys (π_x) associated with ID_{i,j_x}. After finding the right secret key, the reader can uniquely identify the tag T_j. Sharing some identifiers of a tag with other members of the group provide unlinkability even if any tag is compromised by the adversary.

7.6.2. Details of HSAC (Privacy Preserving Healthcare Service Access Mechanism)

Unauthorized disclosure of health related information can have serious consequences like: refusal of employment, seclusion from family or community groups and personal embarrassment. Once information has been disclosed, the damage cannot be undone so to earn user trust it is important that unauthorized disclosure is prevented. Also to prevent any kind of insider attack in the RFID based hospital information system, unauthorized access of sensitive data should be prevented. A major concern in RFID based healthcare system is how to protect user privacy when the RFID identification data, i.e. patient's private information are increasingly passed around and accessed by a large number of people such as doctors, nurses, technicians, and researchers. This information, collected over a period of time, may expose significant private information such as: trace of personal location, medical history, treatment history, and even financial information. One measure is to use access control technique which requires that only authorized entities or users with a legitimate request satisfying related policies or laws can access sensitive information.

1) Access Policy Requirements for Healthcare Privacy

In modern day healthcare systems, most of the organizations are internetworking their systems, increasing the potential for unauthorized access. Since there are countless individual scenarios, circumstances and relationships, the access control framework must be flexible and highly expressive. The framework needs to ensure that a user's access policy can be recorded and enforced in a manner that reflects their understanding of who they want to have access and who they don't want to have access. This will typically involve *allowing* or *disallowing* consent to groups or roles. In order to restrict access of certain information to only certain people, allowing or disallowing access to certain roles needs to be included too. To employ allowance and disallowance of consent or access rights *explicit denial* of access to particular role is necessary.

2) Brief Overview of of HSAC

Role based access control (RBAC) [Ferraiolo92] is a popular security model. Due to its flexibility, RBAC model has been widely applied to healthcare information systems [Becker04, Bhatti06]. In this research work, we propose HSAC, a privacy preserving healthcare service access mechanism. The architecture of HSAC is shown in Figure 7.5. HSAC propose to preserve user preferred privacy while accessing healthcare services using Privacy-aware Role Based Access Control (P-RBAC) [Dafa-Alla05]. The adoption of a model like P-RBAC in a RFID based healthcare seems justifiable since healthcare is a complex environment which deals with various user roles in multiple organizations. Classical RBAC, does not support role roaming among different organizations. Furthermore, in order to protect privacy in healthcare sector, not only the content of EMR but also some meta information about EMRs, e.g., the creators, owners are required for privacy protection. However, the main feature of P-RBAC lies in the complex structure of privacy permissions that reflects a structured ways of expressing privacy rules. Moreover, aside from the data and the action to be performed on the data, in P-RBAC, privacy permission explicitly states the intended purpose of the action along with the conditions under which the permission can be granted and the obligations that are to be finally performed. It helps

in verifying that the access control policies of the healthcare organization are compliant with privacy regulations. Moreover, in HSAC, we allow users to have preferred privacy configuration by including user defined privacy policies along with the organizational privacy policies.

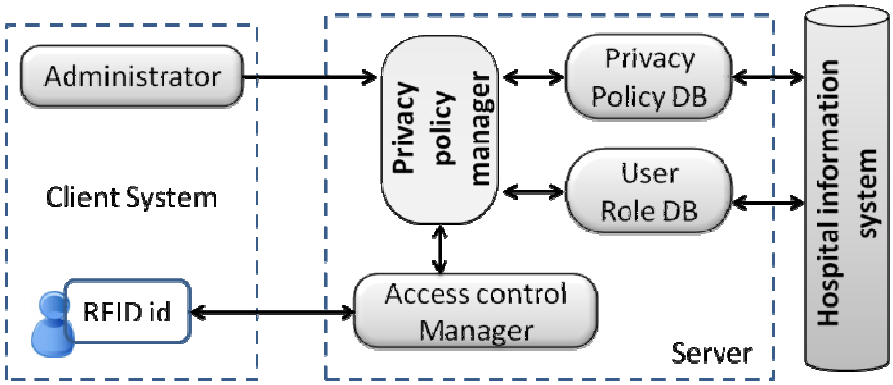


Figure 7.5 The architecture of HSAC

In HSAC, the administrator can define and manage traditional privacy policies related to the access of various data as well as user preferred privacy policies. For example, some doctor may not want anyone else to view her patient's medical diagnosis without her permission. All these policies are broken down into unit privacy policy and unit user role by the Privacy Policy Manager (PPM). The unit policy and unit role are stored in Privacy Policy DB (Database) and User Role DB (Database). The User Role DB module also contains a role hierarchy. For example any information that can be viewed by the nurse must be accessible by the doctor too. But only a part of information visible to nurse may be accessible by the pharmacist, who only needs to know which drug to dispatch for which patient. Moreover, the pathologist only needs to know the *lab test name,* and the accounts section of the hospital needs to know the breakdown of costs for various services provided to the patient. It is hard to develop a generalized role hierarchy since it may differ for different institutions. However, such a role hierarchy can be defined by the administrator based on the preference and organization requirements. Whenever, a user requests for some healthcare service using the ID of the tag, the Access Control Manager (ACM) locates policies defined by the PPM. The PPM then brings up the requested information by querying

stored unit policies and merging them for the particular user role. If ACM detects any violation of any unit privacy rule for a particular role, the service request is denied.

7.7. Evaluation

Though our framework consists of two major components, the main privacy preservation is done by the PriSens component while identifying a tag via radio frequency channel. HSAC is able to preserve privacy by restricting unauthorized access given that HSAC follows a proper implementation of P-RBAC technique and privacy policies are properly defined. Therefore, it is more significant to evaluate the privacy achieved by the PriSens component. In this section, first we evaluate PriSens protocol using formal security analysis. Then, we measure the level of privacy achieved by PriSens as a function of the total number of compromised tags. We also evaluate PriSens by assessing the memory and search complexity of the protocol and by comparing it other classic protocols.

7.7.1. Security and Privacy Analysis of Prisens

In this section, we formally prove that our protocol preserves data privacy and provides unlinkability. In addition, we analyze the preservation of privacy in some attack scenarios where some of the tags of the system are compromised by the adversary $\hat{A}$.

Attack Model: One of the major goals of an adversary in any RFID system is to infringe the tags' privacy by means of tracking. In this work, an adversary is denoted as $\hat{A}$. We assume $\hat{A}$ as an active adversary who has full control over all the communications between the tag and the reader. She can not only eavesdrop, but also intercept, modify and even initiate authentication session. The adversary can, for example, impersonate a tag and communicate with the valid reader. Even the adversary can query a valid tag and learn the tag's response. Our assumptions also include that the adversary can control a number of readers and tags. Each reader and tag controlled by the adversary are denoted as $\hat{R}$ and $\hat{T}$, respectively. $\hat{R}$ is unauthorized to have access

to any real tags since $\hat{R}$ has no secret information like the real reader R. Similarly, $\hat{T}$ is not valid as it does not have the secret and identifying information of a valid tag. However, the adversarial reader $\hat{R}$ can communicate with a valid tag. Even the fake tag $\hat{T}$ can communicate with a legitimate reader. In both cases, the ultimate goal of the adversary is to track any tag of the RFID system. We assume that the adversary, the adversarial reader, and the adversarial tag have polynomially bounded resources. In addition, the adversary can launch physical attacks. However, the hardware based defenses against physical attacks are beyond the scope of this work. We also assume that the reader cannot be compromised.

1) Information Privacy:

Theorem 1. PriSens preserves information privacy with respect to the adversary $\hat{A}$.

Proof. Let us assume $\mathcal{O}_{pick}$ provides the adversary $\hat{A}$ with a tag T. $\hat{A}$ transmits this tag to the oracle $\mathcal{O}_{encrypt}$ with a nonce n_1. Then $\mathcal{O}_{encrypt}$ provides $\hat{A}$ with the response β.

Now, $\hat{A}$ selects a ID. To break data privacy, $\hat{A}$ should tell if $\beta$is produced using the ID. This implies that $\hat{A}$ has to identify the input of the encryption by just learning the cipher text. $\hat{A}$ can succeed in two cases. First, if she can retrieve the inputs from the output of the random oracle. But this contradicts with our assumption that the inputs of a random oracle are computationally intractable from the output of the oracle. Second, if $\hat{A}$ knows the secret keys of the tag T. Without tampering the tag T, if $\hat{A}$ can determine the keys by learning the cipher texts, this again breaks the semantic security of the symmetric key cryptography. Therefore $\hat{A}$ can break data privacy with probability no better than random guessing. Thus it proves data privacy property of Definition 1. ■

2) Unlinkability:

Theorem 2. PriSens provides unlinkability with respect to the adversary $\hat{A}$.

Proof. Let us assume $\mathcal{O}_{pick}$ provides the adversary $\hat{A}$ with two tags T_0, T_1 from the same group. These two tags go into the learning phase. $\hat{A}$ transmits T_0, T_1 to $\mathcal{O}_{flip}$ which outputs the response β_b.

Now, to break unlinkability, the adversary $\hat{A}$ has to tell the value of b. We assume that the adversary's guess is right. In other words, the adversary can determine whether the response β_b is produced by T_0 or T_1, given the learned responses from both the tags. The responses of a tag cannot be a signature of the tag because according to our protocol, a nonce on the tag side makes each response different from all the previous responses originated from the same tag. Therefore, we can say that the guess is right because the adversary knows the keys (the group key and the secret key) stored on these two tags. Without tampering the tags T_0, T_1, the adversary has to determine the keys stored on these tags by just observing the cipher texts. But this contradicts with the semantic security of symmetric key cryptography. Therefore, the adversary can break unlinkability with no better approach than random guessing. Thus it proves the unlinkability property of Definition 2. ■

3) Physical Attack:

Under this attack, we consider that the adversary $\hat{A}$ can compromise any tag with a probability of $\frac{1}{N}$. Whenever a tag T_j becomes compromised, the adversary learns all private information stored on the tag T_j. Therefore, the adversary can now decrypt u of each response β originated from the other members of the group G_i. Thus, $\hat{A}$ can learn the identifier that a tag is using to produce its response by decrypting the u. We discuss the aftereffect of this attack with an example and demonstrate how PriSens provides unlinkability even if the adversary realizes the identifiers used in the responses.

We consider a group G_i of four tags T_1, T_2, T_3, and T_4. Suppose the adversary compromised the tag T_3 as shown in Fig. 4. Now the adversary learns the group key k_{G_i}, the tag secret key k_{T_3} and a set of identifiers $\Omega_3 = \{1,2,3,4\}$. From now on, the adversary can decrypt u

part of all the responses originated from T_1, T_2, and T_4 with the group key k_{G_i}. But, the adversary still cannot decrypt v part of these responses since she does not possess the secret keys of these tags. With this learned information (k_{G_i} and Ω_3), the adversary tries to track the other tags of this group. Since the adversary can decrypt u of each responses, she can learn the identifier underlying the cipher text u. In other words, she can discover which identifier has been used to produce a response. The arrow in the Figure 7.6 represents that the responses of the authentication sessions (after T_3 is compromised) are transmitted from the tags (T_1, T_2, T_4) to the reader. The identifiers used in these responses are shown on above the arrow. Each identifier is shown in plaintext since the adversary can retrieve the identifier by decrypting u of β using k_{G_i}.

According to our protocol, even if the adversary comes to know about the identifier used in a response, she cannot conclude which of the potential tags is the sender of this response. In our example, the adversary discovers the identifier 2 is used two times, but she cannot be certain which of these tags (T_1, T_2, T_4) is the originator(s) of these responses. Though T_3 shares the identifier 2 with only T_1 and T_4, however, the adversary has no knowledge about the parties with whom T_3 is sharing which of its identifiers. Even the adversary does not know how many of the identifiers of Ω_3 are being shared. So, under this scenario, the anonymity set of the potential senders of a given response seems to be 3 to the adversary. Therefore, when the adversary compromises one tag from the group of n uncorrupted tags, PriSens forms an anonymity set of size 1 and another anonymity set of size $(n-1)$ from the group instead of n anonymity sets of size 1 like the group based authentication [Avoine07]. This is the noticeable partition that improves the level of privacy provided by PriSens. Because, the remaining $(N-n)$ tags of the system forms the other anonymity set which is same under both the protocols. Thus PriSens prevents adversary benefit from tracking by compromising a tag.

We now consider the case of compromising multiple tags of the same group. In the above scenario, even if $\hat{A}$ compromises either T_1 or T_4 after compromising T_3, the adversary cannot be

certain whether T_2 has identifier 2 in Ω_2 or not. Therefore, the size of anonymity set is still 2, i.e., $n - c$, where c is the number of compromised tags of the group. If $\hat{A}$ compromises T_2 instead of T_1 or T_4, the size of anonymity set is still 2 (i.e., $n - c$). Therefore, we conclude that the anonymity set, formed from a group that is under physical attack, is of size $(n - c)$, where n is the group size and c is the number of compromised tags of the given group.

PriSens provides protocol-level privacy only. In real world, there are many possible side channels. If tags emit distinct "radio-fingerprint", then no protocol-level privacy countermeasures can prevent privacy infringement [Avoine05].

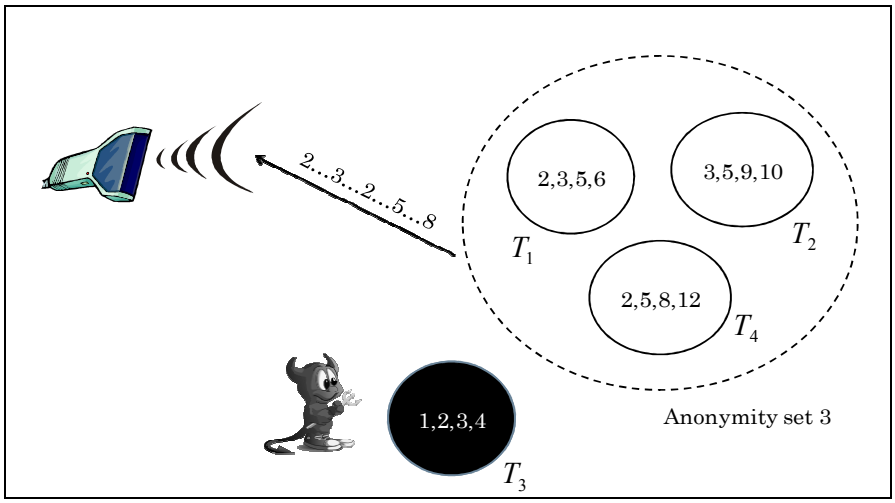


Figure 7. 6 Aftereffect of a physical attack on PriSens, where T_3 is compromised by the adversary

7.7.2. Evaluation of PriSens by Measuring Privacy

We consider two privacy metrics for the measurement of privacy. First, our privacy measurement technique is based on anonymity set like the privacy metric used by Avoine et al. [Avoine08]. Second, we identify the amount of information disclosed by a scheme as another metric presented in [Nohl06]. This metric is based on Shannon's information theorem [Shannon48].

7.7.3. Measurement of Privacy Based on Anonymity Set

The level of privacy of an RFID system, achieved by a scheme, at a given time, is a function of the total number of compromised tags at that time. When some tags are compromised, the set of all tags are partitioned such that the adversary cannot distinguish the tags belong to the same partition, but she can distinguish the tags that belong to different partitions. So, these partitions become the anonymity sets of their members. The level of privacy based on anonymity set, $\wp$, can be measured as the average anonymity set size [Avoine08].

$$\wp = \frac{1}{N}\sum_{i}|P_i|\frac{|P_i|}{N} = \frac{1}{N^2}\sum_{i}|P_i|^2$$

where $|P_i|$ denotes the size of partition P_i and $\frac{|P_i|}{|N|}$ is the probability that a randomly chosen tag belongs to partition P_i.

According to PriSens, a similar kind of partitions is formed when tags become compromised. If c_i is the number of compromised tags within group G_i, then the set of the tags within this group is partitioned into c_i anonymity sets of size 1 and another anonymity set of size $(n - c_i)$. If $\mathbb{C} = \{c_i | c_i$ is the total compromised tags within $G_i\}$ is the set of compromised groups, $|\mathbb{C}|$ is the total number of compromised groups, and $C = \sum_{each\ c_i \in \mathbb{C}} c_i$ is the total number of compromised tags, the level of privacy $\wp$ achieved by PriSens can be expressed as

$$\wp = \frac{1}{N^2}\left(\left(n(\tau - |\mathbb{C}|)\right)^2 + \sum_{\text{each } c_i \in \mathbb{C}} (c_i + (n - c_i)^2)\right)$$

where N = total number of tags in the system

n = total number of tags within a group

τ = total number of groups in the system.

7.7.4. Measurement of Privacy Based on Information Leakage

We measure the information leakage in bits based on Shannon's information theorem [Shannon48]. If we have a group of tags of size S and the adversary divides this group into two disjoint subgroups of size $S/2$, then 1 bit of information is disclosed out of $\log_2 S$ bits. Extending this concept from two subgroups of equal size to two subgroups of different sizes, where $\frac{S}{a}$ tags are in one subgroup and the remaining tags $\left(1-\frac{1}{a}\right)S$ are in another subgroup, we can measure the average amount of information disclosed in bits as follows

$$I = \frac{1}{a}\log_2(a) + \frac{a-1}{a}\log_2\left(\frac{a}{a-1}\right).$$

In general, if the adversary splits N tags of the system into k disjoint partitions, then

$$I = \sum_{i=1}^{k} \frac{|P_i|}{N} \cdot \log_2\left(\frac{N}{|P_i|}\right)$$

where $|P_i|$ denotes the size of partition P_i. According to our protocol, if $\mathbb{C} = \{c_i | c_i \text{ is the total compromised tags within } G_i\}$ is the set of compromised groups, $|\mathbb{C}|$ is the total number of compromised groups, and $C = \sum_{each\ c_i \in \mathbb{C}} c_i$ is the total number of compromised tags, the amount of information leakage in bits I can be expressed as

$$I = \left(\frac{n(\tau-|\mathbb{C}|)}{N}\log_2\left(\frac{N}{n(\tau-|\mathbb{C}|)}\right)\right) + \sum_{\text{each } c_i \in \mathbb{C}}\left(c_i\left(\frac{1}{N}\log_2 N\right) + \frac{(n-c_i)}{N}\log_2\left(\frac{N}{(n-c_i)}\right)\right)$$

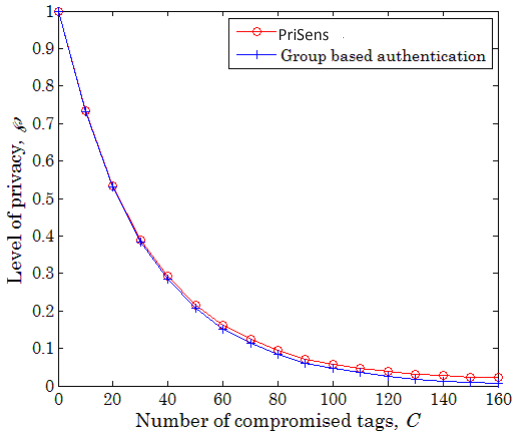
where, N, n , and τ bears the same meaning mentioned before.

7.7.5. Experimental Results

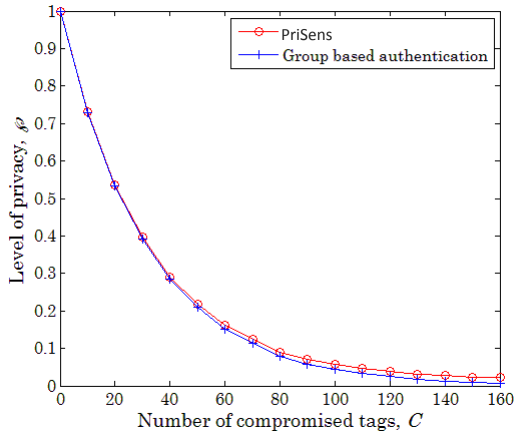
We have compared both the protocols, PriSens and the group based authentication, using a Matlab simulation. The experiment results establish that the level of privacy provided by PriSens is higher than that of the group based authentication. Our comparison is based on the two metrics presented above, the level of privacy (based on anonymity set) and information leakage.

We have come up with a conclusion same as [Nohl06] that the information leakage describes the privacy threats better than the anonymity set.

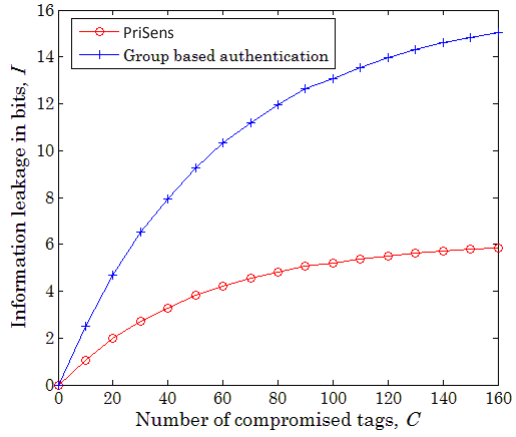
In our simulation, we have considered two systems with $N = 2^{16}, \tau = 64$ and $N = 2^{20}, \tau = 64$. Tags are selected to be compromised with a uniform random distribution. The number of compromised tags ranges from 0 to 160. We have run the simulation for 100 times and computed the average $\wp$ achieved by PriSens and the group based authentication as a function of the total number of compromised tags C (Figure 7.6(a)-(b)).



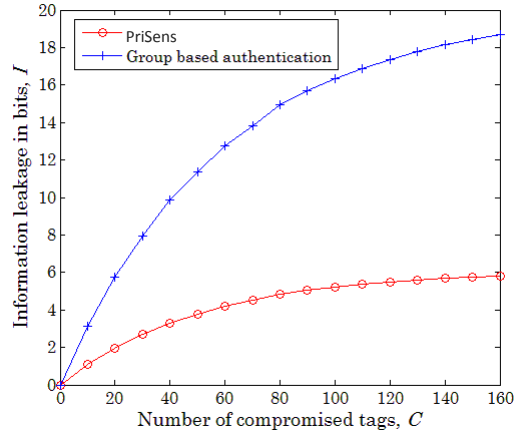
(a) Level of privacy based on anonymity set, with $N = 2^{16}$ and $\tau = 64$



(b) Level of privacy based on anonymity set, with $N = 2^{20}$ and $\tau = 64$



(c) The amount of information leakage, with $N = 2^{16}$ and $\tau = 64$



(d) The amount of information leakage, with $N = 2^{20}$ and $\tau = 64$

Figure 7.7 Experimental results of PriSens against the group based authentication

The small increase in the level of privacy achieved by PriSens is visible when the total number of compromised tags becomes more than 30. During the simulation, we have also computed the average amount of information leakage I, for both the protocols, as a function of the total number of compromised tags C (Figure 7.7(c)-(d)). The plots depict that a significant amount of improvement in privacy protection is achieved by PriSens. With the increase in the total number of compromised tags C, the average amount of information disclosed by the group based authentication is quite higher than the information disclosed by PriSens.

In Figure 7.7(c) ($N = 2^{16}$), when C becomes 160, the group based authentication discloses about 15 bits out of 16 bits of information, while PriSens discloses about 6 bits of information. The group based authentication discloses 56.25% more information than PriSens in a similar setup.

Figure 7.7(d) ($N = 2^{20}$) shows that the group based authentication reveals almost 19 bits out of 20 bits of information and PriSens reveals around 6 bits of information. This time the group based authentication discloses 65% more information than PriSens. Based on the simulation results, we can conclude that the information disclosed by the group based authentication increases with the size of the system; however, PriSens shows consistency in the information leakage in both the cases. Information leakage is a better metric to demonstrate the privacy threats in RFID systems than anonymity set. Though the improvement in $\wp$ provided by PriSens against the group based authentication is not significant, however, we can say that PriSens provides better privacy protection than the group based authentication, based on the results of the amount of information disclosed by these two protocols.

7.7.6. Memory and Search Complexity Analysis of PriSens

Search Complexity: According to PriSens, the reader's complexity is slightly increased than the group based scheme [Avoine07]. After receiving the response $\beta = (u, v)$ from a tag T_j, the reader searches for the correct group key to decrypt u. In the worst case, the reader has to

perform this operation τ times. If such a group key exists, the reader can retrieve the identifier ID_{i,j_x} from u. Now, the reader has to search for the tag's secret key to identify T_j by decrypting v properly. The reader searches a key space of size $|\pi_x|$. Therefore, in the worst case, the reader's total complexity is $\tau + |\pi_x|$. In the best case, the size of π_x is 3 and in the worst case, it can be n, size of the group. But in the group based scheme, the reader's complexity in worst case is $\tau + 1$. Nevertheless, PriSens is much better than the other schemes where the worst case reader's complexity is N, the number of total tags in the system. To provide improvement in privacy protection, we have to sacrifice this small increase in the complexity of the reader. Since readers are more powerful than tags, they can handle this increase in search complexity.

Memory Complexity: According to PriSens, tags need to store m number of identifiers along with the group key and the unique secret key. Though tags have limited resources, however, the increase in memory requirement is acceptable than the increase in computation and communication complexity. A smart RFID tags have memory capacity of 32kBytes or more [Laurie07]. Even RFID tags with extended memory capacity are available at the market [Fujitsu08]. All these tags can store the information required for PriSens.

7.7.7. Comparison of Security Requirements with existing Work

Table 7.1 presents the summary of security and privacy goals satisfied by PriSens protocol. This table also summarizes the comparison of PriSens with other relevant existing work. Here, N is the number of tags in the system.

Table 7.1 comparison of existing techniques

	Complexity	**Cloning Resistance**	**Tracking Resistance**	**Privacy Protection**
[*Ohkubo03*]	O(N)	Yes	Yes	Yes
[Weis03]	O(1)	No	No	No
[Molnar04]	O(logN)	Yes	No	Yes

[Avoine07]	[1]O(γ)	Yes	Yes	Yes
[Avoine05]	$O(N^{2/3})$	Yes	No	Yes
[Dimitriou05]	O(logN)	Yes	No	Yes
[Henrici08]	O(1)	No	No	Yes
[Molnar05]	O(logN)	No	No	Yes
[Tan07]	O(N)	Yes	Yes	Yes
PriSens	[2]$O(\tau + \lvert\pi_x\rvert)$	Yes	Yes	Yes

1. γ is the number of groups in the system.

2. In the best case, the size of π_x is 3 and in the worst case, it can be n, size of the group.

7.8. Goals Satisfied by PriSens Protocol

The motivating example of RFID application for this chapter is to preserve privacy in RFID based healthcare or such systems where user's privacy is the most important issue. The goal of such a system is to preserve privacy efficiently as well as provide basic security like confidentiality, unlinkability, and authentication. PriSens protocol is able to achieve all these goals since it discloses much less information than the existing works.

7.9. Summary

In this chapter, we propose a "two component" based framework PriSens-HSAC that provides increased privacy for RFID based healthcare systems. The PriSens component provides better privacy compared to the existing RFID authentication protocols while identifying an RFID tag in healthcare setting. The HSAC component restricts unauthorized access of patient's private information by using P-RBAC mechanism. Our evaluation clearly illustrates that the adoption of this framework will allows RFID based healthcare systems to preserve user privacy.

7.10. Publication

- ***Published:*** *Farzana Rahman* and Sheikh Iqbal Ahamed, "I am not a goldfish in a bowl: A Privacy Preserving Framework for RFID based Healthcare Systems", *in Proc. of IEEE 14th International Conference on e-Health Networking, Applications and Services (Healthcom 2012)*. China, October, 2012. [*Best paper winner*]
- ***Published:*** Md. Endadul Hoque, *Farzana Rahman*, and Sheikh I. Ahamed, "AnonPri: An Efficient Anonymous Private Authentication Protocol", *in Proc. of IEEE International Conference on Pervasive Computing and Communications (PerCom 2011)*, WA, USA, March 2011. pp.102-110. [Acceptance rate: 11%]
- ***Under Review:*** *Farzana Rahman* and Sheikh Iqbal Ahamed, "A Privacy Preserving Framework for RFID based Healthcare Systems", *In a journal*.

7.11. Acknowledgement

The initial work of this research is awarded by Computational Sciences Summer Research Program (CSSRP) Fellowship for summer 2012 by Marquette University. This Privacy preserving framework will be used for deployment by Prof. Ji-Jiang Yang of Tsinghua University (China) in a healthcare project.

Chapter 8: Ensuring Survivability in Computational RFID based Systems

In the past decade there has been a substantial effort to realize the vision of original ubiquitous computing applications. Particularly wireless sensor networks (WSNs) based on mote sensing have been applied to many real-world problems. Despite many successes, WSNs have not led to sensing devices embedded in the fabric of everyday life, where everything is equipped with networked sensors. For this type of deployment, truly unobtrusive sensing devices are necessary. For the last few years, it is argued that Radio Frequency Identification (RFID) technology has a number of key attributes that make it attractive for such applications. RFID is mainly used for automated identification of objects and people. However, this technology is limited to only identifying and inventorying items in a given space [Ma10]. Future RFID applications will require tags that can also perform minimal sensing, computation, and storage. One recent innovation of powerful RFID is *Computational RFID (CRFID)* [Buettner08b, Sample07] that presents exciting possibilities for future ubiquitous computing applications [Holleman08, Jiang05, and Segawa09]. In this chapter, we explore the survivability issue of CRFID systems. One example of CRFID tags is Wireless Identification and Sensing Platforms (WISP). WISP tags present the combination of capabilities of WSNs and RFID networks.

Authentication is a key technique that can be used to defend against typical attacks on CRFID systems. However, as WISP tags have sensor data along with its *ID*, the chosen authentication technique needs to be different from the ones currently used in RFID systems.

Usually CRFID systems are used in sophisticated applications like: enemy move detection in military battlefield, volcanic activity measure, etc [Buettner08a]. In these types of applications, the main goal of the system is to provide service constantly. However, in CRFID systems an adversary may de-synchronize tags and readers to create DoS attack and to threaten system's survivability [Buettner08a]. Survivability refers to a system's ability to withstand malicious attacks and support the system's mission even when parts of the system have been

damaged. With effective fault tolerance and damage recovery mechanisms in place, a system may still be trustworthy in fulfilling its functions and supporting the system mission. In this chapter, we address the problem of ensuring survivability in CRFID based sophisticated applications without sacrificing system's performance.

8.1. Our Major Contributions

The main contributions of this chapter are:

- To address the survivability issue of CRFID systems, here we propose DoS attack resistant Robust Authentication Protocol (*DRAP*) for WISP networks.
- This protocol detects DoS attack and recovers from the attack so that the tag and the reader can get back to their synchronous state.
- To prevent DoS at the link layer, we also propose to use the Enhanced Dynamic Framed Slotted ALOHA (EDFSA) [Lee05] technique at the link layer during communication. Here, our concept is to reduce the collision rate so that optimum system efficiency can be achieved.
- We measure the performance of the DRAP protocol and present the evaluation results.

Organization of the chapter: The rest of the chapter is organized as follows: in section 8.2 describes our major motivation to address survivability issue of CRFID based systems. We propose the DRAP protocol in Section 8.3. This section also includes the system architecture, DoS attack technique in CRFID systems, existing defend mechanisms, attack models, adversary goals and details of DRAP protocol. In section 8.3, we perform the security analysis of DRAP protocol. Section 8.4 describes our simulation technique and analysis of simulation results.

8.2. Motivation

For simple RFID systems, the data of interest is simply each tag's identity. However, for WISP networks, it is difficult to develop efficient protocols for gathering sensor data that changes

over time. WISP tags with new sensor data must wait until they are interrogated by a reader. This increases the likelihood of many devices wanting to use the bandwidth limited channel at the same time. However, the standard RFID strategy of identifying and then communicating with each device is wasteful as only some devices would have relevant data. Moreover, most of the RFID authentication protocols are challenge response based and they need multiple rounds of message exchange in order to verify the legitimacy of both parties (verifier and prover, i.e. reader and tags). As WISP tags have sensor data associated them, communication can be reduced by not authenticating the tags that do not have new sensor data. One technique to reduce communication is to reduce the number of message exchanges by identifying and authenticating those tags only that have new sensor data. Because of all these differences, the trivial RFID protocols securing RFID network cannot be applied to WISP sensor network.

As a motivating example, let us consider a CRFID system where WISP tags are deployed in a battlefield. Quick response time along with survivability is very important in such systems. A reader might have hundreds of WISPs in its field of view. Because all the WISPs share a single reader channel, the update rate per tag would be very low if every tag were simply queried for sensor data sequentially. However, at any given moment, only a few objects would typically be in motion and therefore producing non-trivial sensor values. For this type of situation, protocols have been designed which gives highest priority to sensors with new data [Saxena10]. But an adversary can send a bulk of dummy messages with dynamic new sensor values which would appear as a legitimate packet to the reader. This scenario may lead to Denial of Service (DoS) attack. DoS attack can also be launched in these types of systems by de-synchronizing the tags and readers. DoS attacks are not addressed by most of the authentication protocols because it is not possible to cope with all kinds of DoS attacks. DoS attacks may also occur because of some communication failure. For example, due to the radio jamming of the channel between the tag and the reader, a communication failure may happen and the tag and reader may become desynchronized which may eventually result in DoS attack. However, defending against DoS due

to radio jamming is out of the scope of this research work. In the application layer, the underlying problem of DoS attack is tag collision. These collisions occur when more than one WISP tag reflects their data at the same time. As a result the reader searches all the tags in interrogation (shown in Figure 8.1) zone.

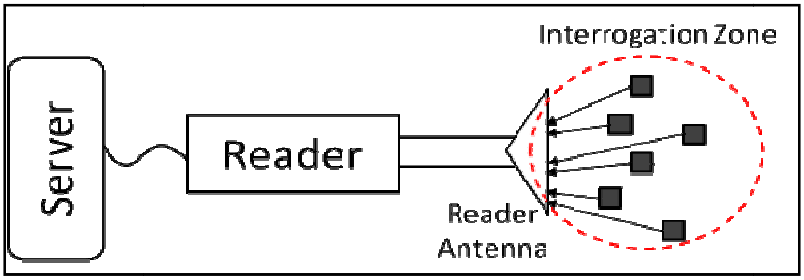


Figure 8.1 Collision by the tags in interrogation zone

Therefore, our focus is to investigate a feasible solution to detect the DoS attack and recover the system to maintain system survivability without sacrificing system's survivability. We also minimize the tag reply collision at the link layer by using EDFSA based communication technique.

8.3. DoS Attack Resistant Authentication Protocol (DRAP)

8.3.1. Our Approach to Ensure Security and Survivability

In order to be secure against the major attacks of WISP networks, we design a mutual authentication protocol. However, in order to prevent the DoS attack in the link layer, we need to reduce the number of tag collisions at the link layer. Tag anti-collision algorithms can be categorized into ALOHA based algorithms and tree based algorithms. Tree based algorithms [Myung06] make trees while performing the tag identification procedure using a unique ID of each tag. On the other hand, ALOHA based protocols are known for their low complexity and computation, thus making them attractive to be used in WISP networks. Examples include Pure, Slotted and Framed Slotted ALOHA (FSA), and their variants [Zhen05]. In Pure and Slotted ALOHA, a tag responds after a random delay, and continues doing so until it is identified. Lee, et

al. [Lee05] proposed enhanced dynamic framed slotted ALOHA for efficient RFID tag identification. The MAC protocol for WISP systems is based on Framed Slotted ALOHA. To increase the system efficiency and also to reduce collision rate, we propose a technique based on Efficient Dynamic Framed Slotted ALOHA (EDFSA) [Lee05] as the underlying layer's communication technique.

8.3.2. Goals of Different Actors

Adversary goals. In WISP based systems, an adversary may perform several attacks like tracking, cloning, eavesdropping, replay attack and DoS attack. DoS attacks cover not only the adversary's attempt to subvert, disrupt, or destroy a network, but also any event that diminishes a network's capability to provide a service. This attack may also include de-synchronization of tags and readers of the system. In WISP networks, several types of DoS attacks in different layers might be performed. At the physical layer the DoS attacks could be jamming and tampering. At the link layer, the attack could involve collision. At the application layer this attack could be performed by malicious flooding and de-synchronization.

Our Goals. Our goal is to design an authentication protocol to ensure systems' survivability in the event of de-synchronization between tags and readers. Our authentication protocol prevents the DoS attack from application layer perspective and makes the system survivable. The EDFSA based communication technique allows us to minimize the effect of DoS attack by reducing the collision rate.

8.3.3. System Architecture of WISP Networks

The architecture of a WISP tag based system is shown in Figure 8.4. There are three main components in WISP network.

Issuer: The issuer initializes each tag during the deployment and authorizes the reader access to the tags. We can think of the issuer as a certificate authority (CA).

WISP Tag: Each WISP tag in the system is denoted as WT. The issuer assigns a unique key k_i to the ith WISP tag WT_i of the system. Each tag contains a 3-tuple consisting of a secret K_i, an identifier ID_i, and new activity threshold Δ. In our protocol, we consider a sensor data as new if the difference between the data at current timestamp and at previous time stamp is greater than Δ.

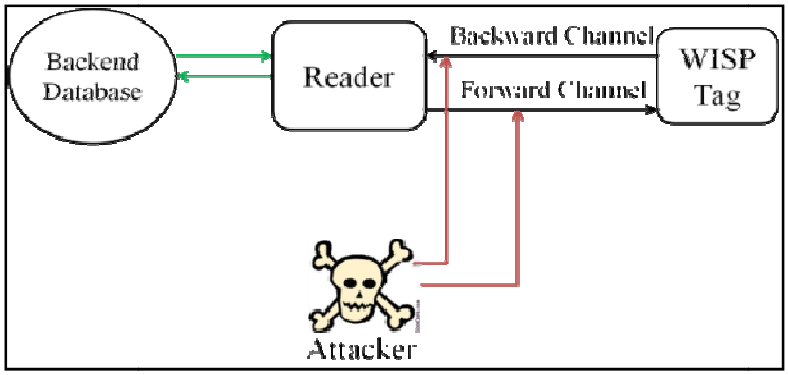


Figure 8.2 System architecture of WISP based systems

Reader: The reader is assumed to be connected to the backend server. We assume the communication channel between the reader and the backend server is secured. From now on, we denote the backend server as the reader. The reader receives all secret information by the issuer during the deployment. For each tag, the reader has a 4-tuple, composed of the secret number K_i, the secret number of the last successful session $K_{i_{prev}}$, the tag identifier ID_i and the previous sensor value $\mathfrak{D}_{prev}$. Initially, all $\mathfrak{D}_{prev}$ are assigned to zero. The reader contains a list of all valid tags that take the following form,

$$R_{database} = \begin{Bmatrix} \langle K_{1_{prev}}, K_1, \mathfrak{D}_{prev_1} : ID_1 \rangle \\ \cdots \quad : \cdots \\ \langle K_{N_{prev}}, K_N, \mathfrak{D}_{prev_N} : ID_N \rangle \end{Bmatrix}$$

where there are N number of WISP tags in the systems. We assume that the reader and all the WISP tags in the system has the knowledge of $\mathcal{h}(.)$, an irreversible one way hash function to protect the integrity of the message. In our protocol, we use SHA-2 as $\mathcal{h}(.)$, and its output is 256 bits. The outputs of $\mathcal{h}(.)$ cannot be linked back to its input, and as a result an adversary cannot

link back the tag *ID.* All the entities of the system can generate pseudorandom number using a generator $P(.)$ based on its *seed*. Initially, the data of tag and reader are in sync, and $K_{i_{prev}}$, equals K_i. We also assume that each tag (WT_i) can perform encryption of their sensor value with their key K_i by using an encryption function $E_{K_i}(.)$. Similarly, the reader can perform decryption the same key (K_i) but by using a decryption function $D_{K_i}(.)$.

8.3.4. Threat Model

We assume that an active adversary has full control over all the communications between the tag and the reader. Our assumptions also include that the adversary can control a number of tags but cannot corrupt a reader. The adversary can install a fake reader in the environment which we call an adversarial reader. We denote the adversary as Å. Each reader and tag controlled by the adversary are denoted as $\hat{R}$ and $\widehat{WT}$, respectively. $\hat{R}$ is unauthorized to have access to any real tags since $\hat{R}$ has no secret information like the real reader R. Similarly, $\widehat{WT}$ is not valid as it does not have the secret and identifying information of a valid tag. However, the adversarial reader $\hat{R}$ can communicate with a valid tag. Even the fake tag $\widehat{WT}$ can communicate with a legitimate reader. We assume that by programming a WISP tag appropriately, such that the sensor value > threshold (Δ), an adversary can create a fake tag $\widehat{WT}$ that can impersonate as legitimate tag in the system. Here, the adversary's goal is to create as many collisions as possible so that the valid tags do not get a chance to reply. We also assume that the adversary, the adversarial reader, and the adversarial tags have polynomially bounded resources. In our system, the following oracles represent the adversary's actions to attack tags.

$\boldsymbol{\mathcal{O}_{Eavesdrop}(R, WT, t)}$: The adversary eavesdrops within a channel at session t between R and one of its communicating tags WT.

$\boldsymbol{\mathcal{O}_{Impersonate_R}(R, WT, M, t)}$: The adversary impersonates a reader *R* in a protocol session *t* and sends a message *M* to the tag WT.

$\mathcal{O}_{Impersonate_{WT}}(\boldsymbol{R, WT, M, t})$: The adversary impersonates a tag WT in a protocol session *t* and sends a message *M* to the reader *R*.

$\mathcal{O}_{Query}(\boldsymbol{WT, t})$: The adversary queries a tag $\boldsymbol{WT}$, to learn information, during the communication protocol session t.

$\mathcal{O}_{Receive}(\boldsymbol{U, M, t})$: The adversary receives a message *M* from an entity *U* (e.g., either *WT* or *R*) during the execution of session *t.*

8.3.5. Our Protocol (DRAP)

The protocol operates as shown in Figure 8.2. At first, the reader sends a request accompanied by a random number n_r. If the tag has a new sensor value, it computes α_i with another random number n_i, generated by itself, and K_i. Next WT_i executes encryption function E_{k_i} on $(\hbar(ID_i) \oplus \mathfrak{D}_{new})$ to generate β_i. Here, to enhance security, WT_i encrypts the XOR of $\hbar(ID_i)$ and new sensor value ($\mathfrak{D}_{new}$) rather than encrypting only the sensor value. Finally, the tag replies with $\alpha_i$for authenticating itself, $n_i$to help the reader to produce the same pseudorandom number and β_i to retrieve the new sensor value. Now, the reader checks the validity of α_i by computing $P(K_i \oplus n_r \parallel n_i)$ for each tag in the database. If the reader finds a match, it can be sure of the validity of the tag.

Then the reader checks if the sensor value sent by the tag is old. WT_i does this by checking if the difference of new and old sensor value is greater than Δ. If it is old, it might be an indication of an adversary trying to launch DoS attack by using previous sensor values (Since a valid tag replies only when it has a new sensor value).

If the sensor value is new, the reader updates $K_{i_{prev}}$ and $\mathfrak{D}_{prev}$. And then α_j is generated by using the next seed that is the hashed secret number $h(K_i)$. If the reader fails to find any match in the first search strategy, it changes the scheme of search by replacing the K_i with the $K_{i_{prev}}$ of all the tags in the database. Upon realizing any match, the reader only generates α_j.

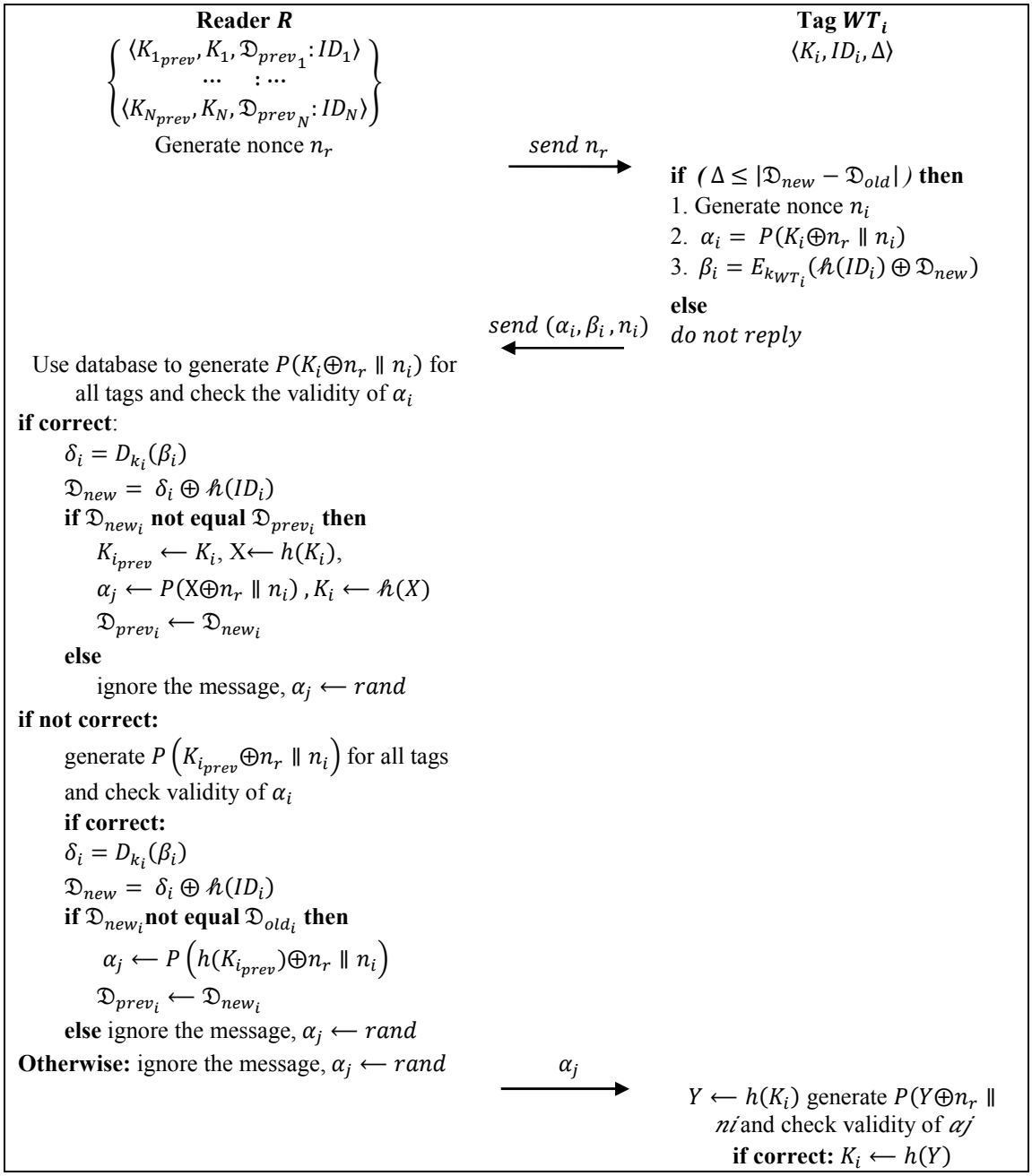


Figure 8.2 DRAP protocol

In fact, this step is to provide the robustness to the protocol by recovering any tag from out of order to be in synchronization with the reader. In both the cases, the reader replies with α_j. If α_i is not valid, the reader simply ignores the message and replies with a random number *rand*. However, this *rand* keeps the protocol consistent by preventing an eavesdropper to acquire any

knowledge about this session. Finally, it is the tag's turn to authenticate the reader by verifying α_j. If α_j is valid, the tag updates its secret number. Otherwise the tag discards the message.

8.3.6. Communication Protocol

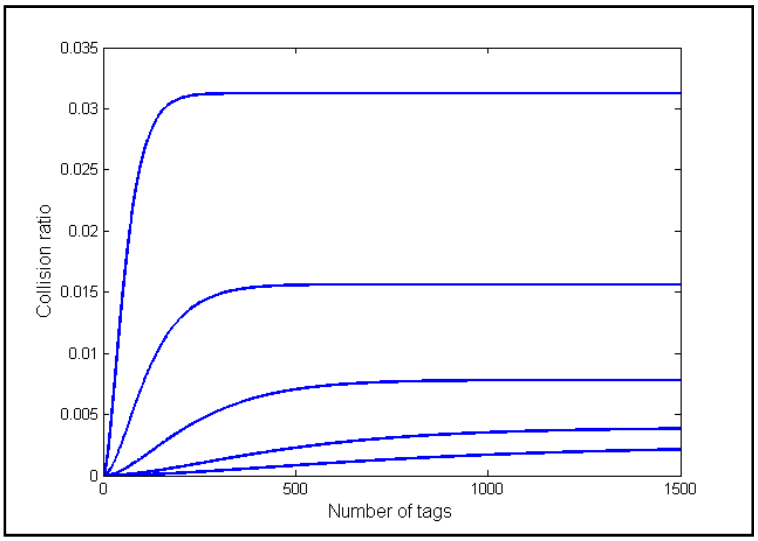


Figure 8.3 Collision ratio for tag identification with different frame size

In DRAP, we propose to use Efficient Dynamic Slotted ALOHA (EDFSA) based communication technique to reduce collisions at the link layer. Generally, in the framed slotted ALOHA anti-collision method, the system efficiency decreases as the number of responding tags becomes larger. However, EDFSA facilitates us to have optimum system efficiency by maintaining dynamic frame size $\mathcal{F}$ in each round. The derivation of $\mathcal{F}$ for each round can be found in [Lee05]. In a WISP network, the number of tag collisions increases with the increase of tags in the system. The relationship between the collision ratio and the number of tags is shown in Figure 8.3, where the $\mathcal{F} \in \{32, 64, 128, 256, 312\}$. We can keep the system in maximum efficiency (35.5%) to decide the next round frame size. This also ensures a reduced collision rate, which allows the DRAP protocol to defend against the DoS attack. So, we lessen the susceptibility to DoS attack by reducing the number of collisions with the use of EDFSA.

8.4. Security Analysis of DRAP

In this section, we analyze DRAP against different types of attacks. For every attack, we first describe how the attack is performed and then how DRAP defends against the attack. R and WT_i are referred to as a legitimate reader and legitimate tag. DRAP is secure against most of the attacks; next we discuss the following two types of attacks and their defenses. Each attack and corresponding defense has three phases:

Phase 1. *Learning phase:* Adversary, Å uses non-destructive oracles such as $\boldsymbol{\mathcal{O}_{Eavesdrop}(R, WT, t)}$, $\boldsymbol{\mathcal{O}_{Impersonate_R}(R, WT, M, t)}$, $\boldsymbol{\mathcal{O}_{Query}(WT, t)}$, $\boldsymbol{\mathcal{O}_{Impersonate_{WT}}(R, WT, M, t)}$, and $\boldsymbol{\mathcal{O}_{Receive}(U, M, t)}$ on a set of target tags and reader. The goal of the adversary is to learn important information related to the tags and reader.

Phase 2. *Attacking phase:* Depending on the security level of the readers, Å may impersonate as a legitimate tag or reader.

Phase 3. *Defend Phase:* DRAP protocol is designed in such a way so that it can defend against the majority of the attacks.

- **Eavesdropping:**

Learning phase: Å executes the oracle $\boldsymbol{\mathcal{O}_{Eavesdrop}(R, WT, t)}$ in the communication between R and WT_i and later uses this information to launch any of the attacks mentioned above.

Attacking phase: Å can learn every piece of information exchanged between R and WT_i such as n_r, n_i, α_i and β_i.

Defend Phase: According to our protocol, Å cannot launch a privacy attack as the protocol does not reveal any sort of private information of the tag or the reader. Even Å fails to track WT_i because each time WT_i is queried, it replies with a new random value. Thus Å cannot figure out any signature to follow WT_i. Even eavesdropping the communication cannot help Å to launch a cloning attack. Å cannot create a fake tag $\widehat{WT_i}$ by executing the oracle

$\mathcal{O}_{Impersonate_{WT}}(R, WT, M, t)$. Even Å cannot act as a legitimate reader to the legitimate tags by executing the oracle $\mathcal{O}_{Impersonate_R}(R, WT, M, t)$.

- **Denial of Service (DoS)**

Learning phase: In this case, Å does not want to derive any information or try to impersonate. The main target of Å is to ensure that a reader cannot access its authorized tags. By executing the oracle $\mathcal{O}_{Eavesdrop}(R, WT, t)$, Å tries to learn information and crate fake tags to install them in the network.

Attacking phase: To launch a DoS attack, Å places many programmed nodes with random sensor data within the network. The task of these malicious nodes is to reply whenever the reader executes an authentication query on the legitimate tags so that the there is a maximum number of collisions in the channel. As a result, the reader/back-end server is not able to authenticate tags easily and with efficient response time.

Defend Phase: As part of our authentication protocol, we propose an EDFSA based communication technique that minimizes the collision rate within a channel. This technique also reduces the collision rate as well as maintains reasonable system efficiency. Moreover, our DRAP protocol is designed in such a way so that it can detect DoS attack and recover from de-synchronization between tags and reader.

In the final dissertation, we plan to include the formal proof mechanism of DRAP against all major attacks, like: tracking, cloning, replay attack, man-in-the-middle attack.

8.5. Performance Evaluation

In our simulation, the authentication server is implemented on a high performance Dell PC. We use Java for the protocol simulation where we use SHA-2 as the hash function (returning 256 bits). The simulated environment consists of 1000 nodes in the network and one legitimate reader. Among the1000 WISP nodes we made 1% ~ 3% nodes to be malicious. The system

efficiency and collision rate is determined in terms of the legitimate nodes. We ran the simulation 300 times and reported the average.

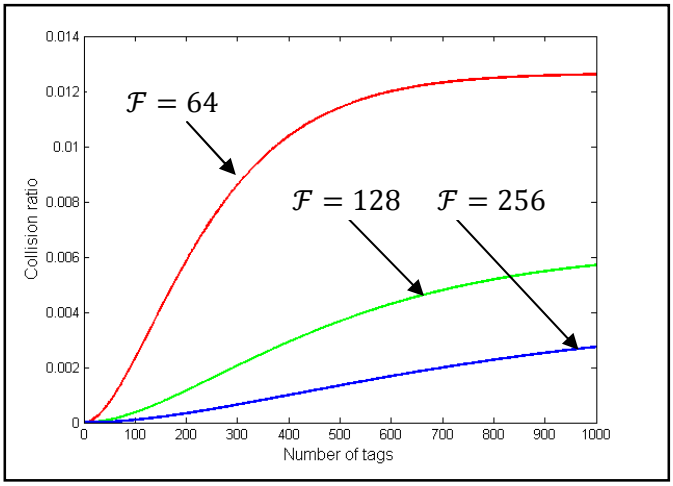


Figure 8.4 Average collision ratio with three different frame sizes

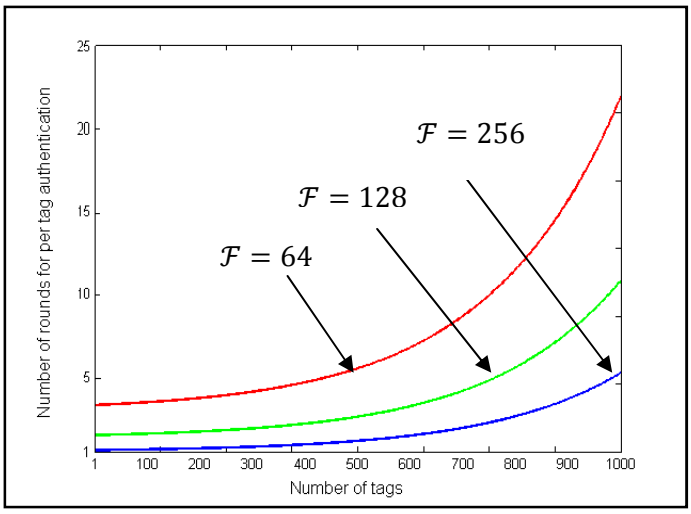


Figure 8.5 Total number of rounds required to authenticate one tag

Our comparison is based on two performance metrics. The first metric is collision rate, which is defined as the ratio of the number of slots with a collision to the frame size. And the second metric is the rounds/iterations required by the reader to authenticate one tag. Now, considering the current state of the network (i.e. number of malicious nodes and number of legitimate nodes are fixed), we executed the DRAP protocol to perform authentication of all valid tags. As the underlying communication mechanism between the tag and the reader, we used our

proposed technique based on EDFSA. Finally, we took the average of 300 collision rates. We also took the average of 300 runs performed to collect rounds required to authenticate one tag.

We performed the above mentioned simulation for three different frame sizes ($\mathcal{F} = 64, 128, 256$). Figure 8.4 shows the collision rate for different numbers of tags in the networks. We can clearly see from the Figure 8.4, that when the number of tags increases the collision rate increases. However, with a larger frame size (ex. 256), the collision rate reduces with the increase of total tags in the system. Figure 8.5 shows the number of iterations required to identify one tag with respect to the number of tags in the system. From this figure, we can see that, with smaller frame size, and with increased number of tags, the collision rate increases. Therefore, more iteration is required to authenticate a single tag. However, when the frame size is increased, even with increased tags in the system, the iterations required to authenticate one tag is ~ 5. Therefore, the system response time is low, since the reader requires less time to authenticate.

8.6. Summary

To address the survivability issue of WISP networks, in this chapter, we propose DRAP (DoS attack Resistant Authentication Protocol). DRAP allows both tag and reader to communicate successfully with each other even if the adversary launches De-synchronization or DoS attack.

8.7. Goals Satisfied by DRAP Protocol

The motivating example of CRFID application for this chapter is sophisticated RFID applications especially designed for enemy move detection in military battlefield. In such applications the main goal of the system is to receive service from the system consistently. Therefore, the system needs to provide service even if the system is under attack. Because of this, ensuring survivability as well as reducing response time are two major goals in these type

applications. DRAP protocol is able to achieve these goals since it is robust and it allows an RFID system to re-synchronize the state of tags and reader if there is de-synchronization of DoS attack.

8.8. Publication

- ***Published:*** Farzana Rahman and Sheikh Iqbal Ahamed, "DRAP: A Robust Authentication Protocol to Ensure Survivability of Computational RFID Networks", In Proc. of ACM Symposium on Applied Computing (SAC 2012). Italy, March, 2012.
- ***Extended Work in Preparation:*** Farzana Rahman and Sheikh Iqbal Ahamed, "Designing Survivable Computational RFID Systems with Robust Authentication Protocol".

8.9. Acknowledgement

This research is awarded by Computational Sciences Summer Research Program (CSSRP) Fellowship for summer 2010 by Marquette University.

Chapter 9: Ensuring Reliability in Computational RFID based Critical Systems

Recently, WISP tags, one example of CRFID tags, have been used in indoor activity recognition, vital signs identification, sleep quality, and other health status monitoring systems [Buettner08a]. In [Chaudhri08], WISPs are used for sensing and monitoring exercises involving free weights. Hoque et al. [Hoque10b] proposed a sleep monitoring system based on the WISP tags. Recently WISP has been used for low power wireless security research [Chae07, Czeskis08, and Salajegheh09]. By using the 3D accelerometer of WISP, Saxena et al. developed a motion detection system that also works as a means to ensure security [Saxena10]. These systems are considered as critical RFID applications where the decision accuracy or reliability of the system is very important. These types of systems can be very popular in the healthcare and wellness application domain if the protocols designed for such systems can provide necessary security features and can assure reliability of system's decision. With the appropriate protocols in place, these technologies can be applied to home healthcare [Haigh06], elderly care [Haigh06], smart hospitals [Bardram07], medication adherence [Lundell07], smart kindergartens, smart homes [Srivastava01], etc.

Within the above mentioned CRFID based critical applications, one area of research is the problem of monitoring a large set of WISP tags and then identifying the missing ones. The missing WISP tag data may introduce errors in the resolved decision of the system which reduces the reliability of the system's decision. Therefore, in order to maintain system reliability a monitoring protocol needs to be executed frequently to find the missing tags of the environment and so it should be made efficient in terms of execution time.

Aside from home healthcare systems, detecting missing tags is an important problem in other settings too, such as warehouses, hospitals, pharmacy, and prisons. In a warehouse, it is sometimes necessary to know if a product is missing due to theft, administrative error or vendor fraud. Similar situations may exist in a large hospital where tens of thousands of pieces of

equipment and other objects need to be tracked. Highly related to this is a recent paper by Tan, Sheng and Li [Tan08], who designed novel protocols to detect missing tags within a certain probability. However, the protocols cannot detect missing tags with certainty (i.e. 100%) and more importantly, they cannot tell which tags are missing. Identification of missing tags has also been investigated by Li et al. in [Li10]. They proposed a series of missing tag detection protocols but they are not suitable for WISP tags since they do not have any mechanisms for handling sensor data of the WISP tags. To address the problems mentioned above, we propose a missing tag detection protocol that follows the following two guidelines to achieve efficiency and ensure low response time -

1) Reduce collision rate and

2) Let the tags report their presence by transmitting sensor data so that another round of data collection is not needed.

The aim of this protocol is to ensure that the resolved decision of the system based on the tag data of the environment is reliable

9.1. Our Major Contributions

- We consider the problem of how to accurately and efficiently monitor a set of WISP tags for identifying the missing tags.
- We propose two tag monitoring protocols, *MTD* (*M*issing *T*ag *D*etection) that does not require the reader to collect *ID*s from each WISP tag, but is still able to accurately detect missing ones.
- Our first monitoring protocol, *Simple MTD*, eliminates the transmission contention among tags but it is not defensive against two attacks.
- Our second protocol, *Reliable MTD*, increases reliability and is secure against major attacks. To ensure low response time, this protocol reduces information volume that needs to be transmitted from the tag.

- Reliable MTD is efficient as it allows the WISP tags to send their sensor data in the same round of messaging in which the tag identification data is received.

Organization of the chapter: The rest of the chapter is organized as follows. Section 9.2 describes our major motivation to address the problem of missing WISP tag detection. In this section we also characterize reliability from our protocol's perspective. In section 9.3, we present the system model of a WISP based home healthcare system. Section 9.4 describes the MTD protocols. This section is followed by section 9.5, presenting the security analysis of reliable MTD protocol. Section 9.6 describes the performance comparison of the two protocols.

9.2. Motivation

As a motivating example of CRFID based critical system, let's consider a scenario where CRFID tags are used to determine the physiological status in a home healthcare system. This system depends on collecting raw sensor data from the environment and inferring important health status. In these types of systems, even subtle changes in the behavior of the patient can give important signs of the onset and progression of certain diseases. Typically, this type of system is composed of three subsystems (Figure 9.1) - the body area network (BAN), the home network, and the central processing node, which also acts as a gateway to the Internet. Usually the implementation of BAN depends on deploying different sensors for collecting different environmental and human behavioral parameters (for example: room temperature, humidity, heart rate, pulse, etc.). Moreover, the physical condition of the patient has to be sensed in an unobtrusive manner by using as few sensors as possible. Recently WISP tags have been used in the implementation of BAN in such systems. Since WISP tags alone have the capability to sense various parameters, they allow the inference of important health status and activities by intelligent analysis. Since these systems depend on every tag data for collective information analysis, the absence of any tag data may eventually introduce error in the resolved health status.

For example, Table 9.1 shows a computational RFID tag based health status monitoring environment consisting of three WISP tags that are used to monitor the health status of a person who recently had a heart attack. At time t_1, the pulse rate and body temperature measuring tags show high readings. Since the heart rate measuring tag shows normal reading, the system can make an accurate decision that the person has a fever. But, at time t_2, the heart rate monitoring tag is missing and due to high pulse rate and high temperature, the system makes an incorrect decision. The system decides that the person has a fever. But in reality the person has high blood pressure which is very dangerous for a patient who recently had a heart attack.

Therefore, in such systems, before making a decision based on the collective information analysis, it is very important to detect the tags that are missing in the system. Otherwise, the absence of any tag data may result in reduced reliability of the system's decision. In this chapter, by "*missing tag*", we refer to an event when the sensor data is not reported back to the reader. This event may occur due to the physical absence of the tag, some programming error in the tag, some hardware error inside the tag or maybe the tag needs to be replaced in order to function properly. In all these cases, the missing tag event needs to be fixed either by replacing a new tag or by re-programming the tag accurately. But in order to fix the "*missing tag event*", the system needs to detect it first.

Table 9.1 Example of system error due to missing WISP Tags

Time	WT_1 (Heart rate)	WT_2 (pulse)	WT_3 (Body Temp)	Real Health status	Inferred Health status	System Accuracy
t_1	Normal	High	High	Fever	Fever	Correct
t_2	Missing	High	High	High Blood pressure	Fever	Incorrect

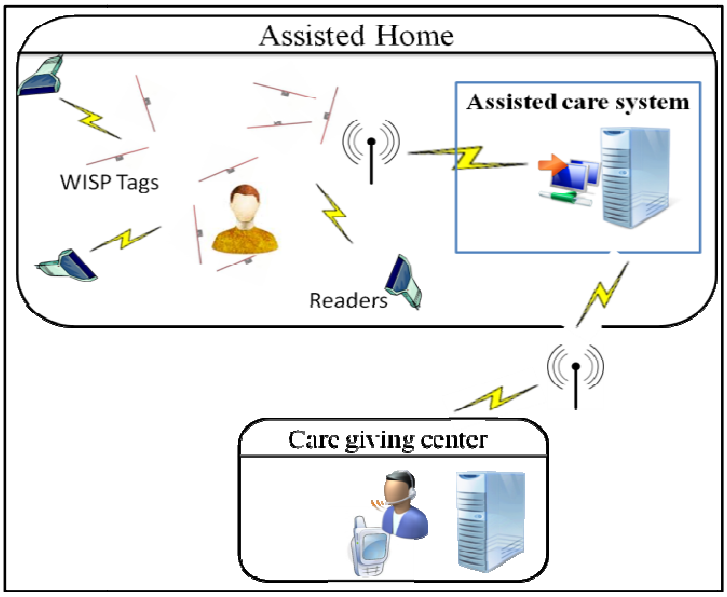


Figure 9.1 Architecture of WISP based home healthcare system

To address the above mentioned problem, we propose a protocol in this chapter to identify the missing tags and collect sensor information from the existing tags only. Since any missing raw data from the tags may incorporate errors in the system's decision making process, it is important to ensure that all tags are present in the environment to maintain the reliability of the system's decision

Reliability Characterization. In literature several different notions of reliability have been proposed so far. In general, the definition of reliability is– *the probability that a system will perform its intended function for a given interval of time under specified operating conditions*. In our system, we consider our protocol to be successful if it can identify the tags that are missing in the system. For example, let's assume that r tags' data is missing out of N tags in the system at time t. We say that our protocol is reliable if the probability of detecting r missing tags is close to 1. We define reliability as follows:

Definition 1. Reliability, R(ts), is the probability of a system performing successfully during the time period [0, ts].

$$R(ts) = P(X = r) \approx 1$$

$here, X = Number\ of\ missing\ tags'\ data\ within\ a\ set\ of\ N\ tags$

Identifying missing tags is a very important problem that has practical significance and existing tag collection protocols can be adapted to solve this problem. In a typical tag collection protocol, the reader collects the IDs from every RFID tag in the set, and returns all the IDs back to the server. The server uses the collected data to determine whether there are any missing tags. Since a collision yields no useful information to a reader, this protocol uses a slotted ALOHA-like scheme to minimize collisions. Tree based protocols [Myung06] can also be used for this purpose. However, slotted ALOHA [Lee05, Zhen05] based algorithms reduce the probability of collisions as tags are scheduled to transmit at separate times. So, here we propose slotted ALOHA based protocol to solve the problem.

9.3. System Model

9.3.1. Problem definition

In our system, we assume that the server has a group of objects, and a WISP tag with a unique *ID* is attached to each object. We refer to this group of objects as a set of tags. We consider this set of tags to be *"intact"* if all the tags in the set are physically present together at the same time. The problem is to design time efficient reliable protocols for the reader to exchange information with the tags in order to identify the missing ones.

9.3.2. Protocol goal

The goal of the protocol is to accurately determine whether a set of WISP tags is intact and collect the sensor data from the existing tags only.

9.3.3. Architecture of the system

The architecture of a WISP based system is shown in Figure 9.2. There are four main components in the system:

Issuer: The issuer initializes each tag during the deployment by writing the tag's information into its memory. The issuer also authorizes the reader to the tags. We can think of the issuer as a certificate authority (CA).

WISP Tag: Each WISP tag in the system is denoted as WT. The issuer assigns a unique identification ID_i to the ith WISP tag WT_i of the system.

Reader: The reader is connected to the backend server. In our system, the WISP tag is the prover and the reader is the verifier. The reader receives all the secret information by the issuer during the deployment.

Server: The server contains the database of all tags. We assume that the communication channel between the reader and the backend server is secure.

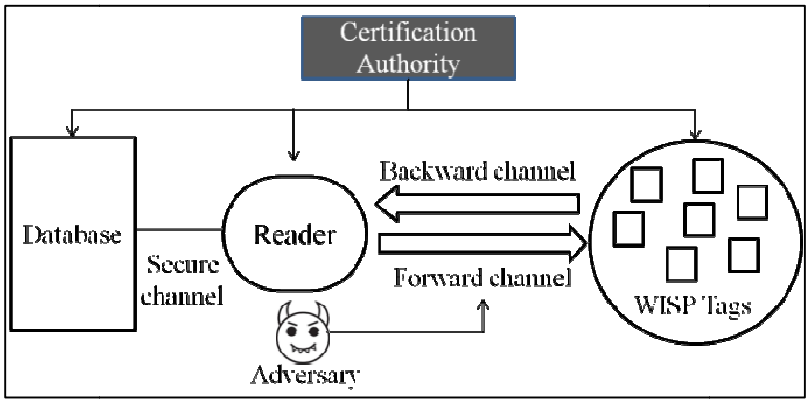


Figure 9.2 System architecture of WISP based network

We assume that the reader and all the tags in the system has the knowledge of XOR operation and $h(.)$, an irreversible one way hash function, to protect the integrity of the message. The outputs of $h(.)$ cannot be linked back to its input so that an adversary cannot link back the tag ids. There are many efficient hash functions in the literature. In this work, we use SHA-1 hash function that outputs 160 bits. Communication between the reader and the tags is time-

slotted. Reader uses a "*synch*" command to synchronize the clocks of the tags and reader. The reader uses a '*slot start*' command to start a slot.

9.3.4. Preliminaries and Assumptions

A home healthcare infrastructure may have multiple synchronized readers covering the entire home but we logically treat them as one. We assume that the reader has access to a database that stores the ids of all tags. This assumption is necessary for any missing-tag detection protocol. If we do not have the ids of the tags, even after the reader collects the ids directly from all the tags, we still do not know if any of the tags are missing. If the database is lost due to a database failure, we can recover the information by reading the ids from the tags one at a time. In this case, we will not be able to detect the tags that have already been lost because we have no way to know of their existence in the first place. However, after collecting the ids of the existing tags, we may use our proposed protocol to monitor the intactness of this set of tags.

Communication between the reader and the tags is time-slotted. Our protocols are request-response based protocol, in which the reader issues a request in a time slot and then zero. One or more tags respond in the subsequent time slots. We assume that an RFID reader is able to distinguish the slots with no reply, single reply, or multiple replies. We define these slots as empty slot (E), single-reply slot (S), or collision slot (C) respectively. In each types of slot, there can be three possible responses − 1) A bit string of 0 - meaning that no tags have replied, 2) A bit string of sensor values- meaning that one tag has replied sensor data in that slot, and 3) Collision - meaning multiple tags have replied in that slot.

If a slot is supposed to be single and it has a bit string of sensor values, it means that the tag is present and the event corresponding to that slot is correct (OK). If a slot is supposed to be empty but it has a bit string of sensor values, it might be an indication of an attack (A). On the other hand, if a slot is supposed to be single-reply slot but it has a bit string of 0, it is indication that the tag is missing (M). Based on the three types of slots and three different outcomes in each

slot, there can be nine situations in our system (see Figure 9.3). The focus of this work is limited to the six situations corresponding to the lower triangular (along with the diagonal) part of the table shown in Figure 9.3. Therefore, we assume that the attacker is benign who will not introduce any error in the system by replying in any slot or by launching replay attack. However, the attacker is able to eavesdrop and track. The capabilities of the attacker and the security analysis of MTD are discussed in a later section. Slots can also be characterized as *multi-bit response slots* and *single-bit response slots*. The length of a multi-bit response slot is denoted as t_l, which allows the transmission of a long response carrying multi-bits (ex. l bit) information. The length of a single-bit response slot is denoted as t_s, which allows the transmission of a short response carrying only single bit information.

slot type / outcome	**E**	**S**	**C**
E	*OK*	A	A
S	M	*OK*	A
C	M	M	*OK*

Figure 9.3 Table of possible situations in the system

9.4. Monitor and Collect (MTD) Protocols

In this section we describe our protocols. We consider an RFID reader, R and a set of N WISP tags, $WT*$. We denote the frame size as f and the random number generated by reader/tag as r. The server contains a table of tag entries. Each entry of the table contains the corresponding tag *id.* Table 9.2 summarizes the notations.

All of our protocols have two phases− *Learning Phase* and *Execution Phase*. The learning phase is similar for the two protocols and it is executed only once; at the beginning of a protocol when the tag monitoring system is launched for the first time. After that point, only the execution phase will be executed by the MTD protocol to detect missing tags and to collect existing sensor information. The execution phase is different for each protocol and this phase has two steps− *Monitor Step* and *Collect Step*. The goal of the monitor step is to detect missing tags

and the goal of the collect step is to collect sensor data from the tags. We will discuss these two steps for each of the protocols later.

Table 9.2 Notations for MTD protocol

Symbol	Meaning
$WT*$	Set of RFID tags
R	RFID Reader
r	Random number
f	Frame size
$h(.)$	One way hash function
SP	Slot position within frame
BR	Bit Record generated by the reader with the replies of tags
BR_{server}	Bit Record generated by the server ahead of time
e_dat	Encrypted sensor data
r_dat	Raw sensor data

Learning Phase: Since the reader is connected to the database using a secure connection, it can collect ids of all the tags directly from the database. The reader can then use these ids to authenticate one tag at a time. Reader can use any standard authentication protocol [Hoque09a]. If the reader can successfully authenticate all the tags, the set of tags is intact. Otherwise, tags that cannot be authenticated are considered as not existing. Using this process, the reader can learn about the tags that currently exist within the system. From then on, the reader can perform the Execution phase of the MTD protocol to detect missing tags within this set of tags. Instead of authentication, the reader can also broadcast the ids of the tags one at a time and wait for a fixed time period for receiving the response from the tag. However, this process of tag presence learning is not secure since an adversary may learn tag ids by eavesdropping. If the time required for reader's authentication query and a tag's response is denoted as t_l (as query and response are

supposed to be multi-bit), then the estimated time for learning phase is $N * (2 * t_l)$, for a system with N tags.

9.4.1. Simple MTD Protocol

Monitor Step: In monitor step of simple MTD protocol, the reader will issue a request such that only an authenticated tag can understand, and the tag will reply only if the query is intended for itself. All other tags will keep silent. Since we assume that each tag has a unique id, only one tag will reply resulting in no collisions. At the end of the list, the reader will inform the server if there are any missing tags. The Simple MTD protocol works as follows:

R : $\boldsymbol{compute}$ $req_i = h(id_i \oplus r_i)$

$R_i \rightarrow WT*$: $\boldsymbol{broadcast}$ $req_i \parallel r_i$

$WT*$: $\boldsymbol{compute}$ $t\_req_i = h(id_i \oplus r_i)$

$\boldsymbol{if}$ $(t\_req_i == req_i)$

$reply$

$\boldsymbol{else}$ $remain\ silent$

R : $\boldsymbol{if}$ $receive\ reply$

$tag\ found$

$\boldsymbol{else}$ $tag\ missing$

The verification of each tag's existence takes $(t_l + t_s)$ time and the total execution time is $N * (t_l + t_s)$. Where, t_l = reader's query time (multi-bit data) and t_s = tag's response (single-bit reply, can be 0 or 1).

Collect Step: In this step, the reader signals each of the tags to reply with their sensor values one at a time. To maintain security, the sensor data has to be encrypted using some standard encryption technique. If the time required to transmit encrypted sensor data is t_{data}, the collection step will take $N_p(t_{data} + t_s)$. Where,

$N_p = number\ of\ tags\ present\ in\ the\ system$

therefore, $N_p = N - N_m$

$N_m = number\ of\ missing\ tags\ in\ the\ system$

$t_s = reader's\ signaling\ time\ for\ each\ tags$

Total time for the entire simple MTD protocol is:

$T = N(t_l + t_s) + N_p(t_s + t_{data})$

9.4.2. Reliable MTD Protocol

The simple MTD protocol is not completely secure and time efficient. In this protocol, an adversary can observe all the transactions. Since the adversary does not know the content of the query, observing the existence of an answer may not be very useful, but it will allow the adversary to track the tag. This protocol is also vulnerable to an eavesdropping attack. To overcome the shortcomings of simple MTD, we propose Reliable and Secure MTD protocol in which the reader is assumed to be honest.

Given a set of N WISP tags, Reliable MTD returns a Bit Record (BR) to the server to check if the set of tags is intact and lets the server collect the sensor values. We will discuss the data structure of a Bit Record soon.

In this protocol, we assume that WISP tags resolve collisions using a slotted ALOHA [Lee05, Zhen05] like scheme. The reader first broadcasts a frame size and a random number, (f, r), to all the tags. Here, r is a random number and f is the frame size. The frame consists of f short-response time slots right after the request. Each tag uses the random number r and its id to hash to a Slot Position, SP, between $[1, f]$ where $SP = h(id \oplus r) \bmod f$. Each tag creates an encrypted version of the sensor data, $\_dat$, using the following method:

$$e\_dat = h(id) \oplus r\_dat$$

Finally the tag sends the encrypted data, e_dat, to the slot position SP. Tags that successfully transmit their data are instructed to keep silent in the following rounds. Tags that

pick the same slot for replying will face a collision and they will be given chance to retransmit in subsequent rounds. For each round, the reader forms a Bit Record (BR) by maintaining an array of slot positions. Whenever the reader receives any sensor data, it is stored in that slot position. Upon receiving 0 or collision, respective values are stored in corresponding slot positions.

We modify the slot picking behavior used in typical tag collection protocol so that instead of having a tag pick a slot and return its id, we let the tags reply with the encrypted sensor data value e_dat, signifying that the tag has chosen the slot. In other words, instead of the reader receiving

$$\{\cdots \mid id1 \mid 0 \mid id6 \mid collision \mid \ collision \ \mid \cdots\},$$

where, 0 indicates no tag has picked that slot to reply, and collision denotes multiple tags trying to reply in the same slot, the reader will receive −

$$\{\cdots \mid e\_dat \mid 0 \mid e\_dat \mid collision \mid \ collision \mid \cdots\}.$$

After receiving the replies, the reader can insert a random number, r, in the collision slot. The final BR created by the reader from existing tag's reply has the following structure:

$$BR = \{\cdots \mid e\_dat \mid 0 \mid e\_dat \mid r \mid r \mid \cdots\}.$$

This is more secure since the tag is not returning its id, and the sensor data is sent in encrypted form which seems purely random to the adversary. Our protocol exploits the fact that tags pick reply slots in a deterministic fashion. Thus, given a particular random number r and frame size f, a tag will always pick the same slot to reply. Because the server knows the ids of all tags, it knows in which slot each tag is supposed to respond with their sensor data. The server knows that it is supposed to get random numbers in the collision slots and it will discard those random numbers. The server knows the locations of the empty, singleton and collision slots. In fact the server can create its own bit record (BR_{server}) ahead of time, with 0 for the empty slots, 1 for the singleton slots, and random bits for the collision slot. The server can use this bit record BR_{server} to compare with the BR transmitted by the reader to identify the missing tags.

Algorithm 1: *Interaction between server and reader(R)*

1. Server sends (f, r) to the reader R
2. R executes Algorithm 4
3. All nearby tags executes Algorithm 3
4. Pre-compute BR_{server} for all tags $WT*$
5. Receive BR from R
6. **for** $i = 1 : f$ **do**
7. **if** $(BR_{server}(i) == 1)$)
8. **if** $(BR(i)$ ***not empty***)
9. $i\ th\ tag\ is\ present$
10. **else** $i\ th\ tag\ is\ not\ present$
11. **end**

Figure 9.4 Algorithm for interaction between server and reader

Algorithm 2:*Interaction between WISP tags and reader* (R)

1. Reader broadcasts (f, r) to all tags $WT*$
2. Each tag WT_i executes Alg. 3
3. Reader executes Alg. 4
4. Reader returns BR to the server

Figure 9.5 Algorithm for interaction between tags and reader

Algorithm 3: *Algorithm executed by WISP tags*

1. Receive (f, r) from R
2. **for** Each tag WT_i (where i = 1 to N)
3. **compute** $SP_i = h(id_i \oplus r) \bmod f$
4. **compute** $e\_dat_i = h(id_i) \oplus r\_dat_i$
5. **end**
6. **while** R broadcasts Slot Position (SP) **do**
7. **if** $(SP == SP_i)$ **then**
8. **return** e_dat_i to R
9. **end**

Figure 9.6 Algorithm executed by WISP tags in MTD protocol

Algorithm 4: *Algorithm executed by reader R*

1. **Define** BR of length f
2. **Initialize** all entries of BR to 0
3. **for** Slot Position $SP = 1\ to\ f$ **do**
4. Broadcast SP and listen for reply
5. **if** $(reply\_string != collision)$
6. $BR[SP] = reply$
7. **else**
8. $BR[SP] = r$
9. **end**
10. **return** BR to the server

Figure 9.7 Algorithm executed by the reader in MTD protocol

If a slot is supposed to be singleton but the server finds it to be empty, then the tag that is mapped to that slot must be missing. This process can verify the existence of all tags that are mapped to the singleton slots. But it cannot verify existence of the tags that are mapped to the collision slots.

In order to verify the existence of the tags that faced collisions during the first round, the reader executes the simple MTD protocol to learn of their presence. In the first round of reliable MTD, the reader detects missing tags and collects sensor values in the same time slot. But in following rounds, each existing tag's detection and sensor data collection takes at most $(t_l + t_l)$ time. For tags that are mapped to a collision slot as well as missing, the reader only needs t_l time to detect its absence since there is no response time for them. Therefore, the execution time of complete reliable MTD is.

$$T = f * t_l + t_l * N_{mc} + 2 * t_l * N_c$$

where N_c is the number of tags mapped to the collision slots and present. N_{mc} is the number of tags mapped to collision slots but missing. Alg. 1 (see Figure 9.4) shows the overall interaction between the reader and the server. Each tag in the set executes Alg. 3 (see Figure 9.6) independently.

The reader executes Alg. 4 (see Figure 9.7) to generate the BR and return it to the server. Notice MTD algorithm only requires a single round for missing tag detection and data collection. Furthermore, in Alg. 4, the tag does not need to return the tag id to the reader. Rather the tag sends the encrypted sensor value (that seems random to the attacker) to inform the reader of its presence. This reduces the communication cost since a second round of messages is not required to send the sensor data to the reader.

9.4.3. Protocol description

Monitor Step: In this step, the reader first broadcasts a frame size and a random number, (f, r), to all the tags. Each WISP tag WT_i uses its own tag id_i and r to generate $SP_i = h(id_i \oplus r) \bmod f$. At the same time, each tag calculates its own sensor data, $e\_dat = h(id) \oplus r\_dat$. When the slot position broadcasted by the reader matches with SP_i, tag WT_i replies e_dat in that slot position to the reader. Upon receiving replies from different tags, the reader forms the Bit Record (BR) of length f (frame size) to transmit to the server. Initially the reader assigns 0 to all the slot positions. However, the reader stores $reply\_string$ in those slot positions where it receives a reply. The reader stores a random number in the slot position where it receives a collision. This technique of bit assignment allows our search protocol to be secure against some major attacks which we will discuss in next section. The BR is then transmitted to the server. The server calculates Bit Record, BR_{server}, for all the tags ahead of time. We assume that the frame size (f) is large enough to accommodate enough tags in the first round without collision.

Next, the server compares between received BR and BR_{server}. If any slot position of BR_{server} contain 1 and that slot position of BR does not contain any data, the server become aware of that the tag data is missing. For the tags that faced collision in the first round, the reader broadcasts those ids one after another. If the reader does not receive sensor data for any particular tag, it is detected as missing.

Collect Step: The collect step is executed by the server after the monitor phase is over. In this phase, the server computes the raw sensor data from the $reply\_string$ corresponding to each tag. The $reply\_string$ is an encrypted form of the raw sensor data. However, only the server can determine the correct sensor value since ids for different tags are only known by the server. The server can compute the hash of the id, i.e. $h(id)$. The server can XOR the hash, $h(id)$, with e_data to determine r_data using following steps:

for Each tag WT_i (where i = 1 to N)

compute $r\_dat_i = h(id_i) \oplus e\_dat_i$

end

9.5. Protocol Analysis

In this section, we analyze our second protocol, Reliable MTD protocol, against different types of attacks.

9.5.1. Attack Model

The goal of an adversary in a WISP based home healthcare system is to counterfeit a real tag with its real data such that it can only be distinguished from the real one with small probability. Evidently, this fake tag can let a fake object be identified as an authentic one. In this system, an adversary is denoted as $\hat{A}$. We assume $\hat{A}$ is an active adversary who can listen to all the communications between the tag and the reader. The adversary can, for example, impersonate a tag and communicate with the valid reader. The adversary can even query a valid tag and learn the tag's response. Each reader and tag controlled by the adversary are denoted as $\hat{R}$ and $\widehat{WT}$, respectively. $\hat{R}$ is unauthorized to have access to any real tags since $\hat{R}$ has no secret information (i.e. id) like the real reader R. However, the adversarial reader $\hat{R}$ can communicate with a valid tag. Even the fake tag $\widehat{WT}$ can communicate with a legitimate reader. In both cases, the ultimate goal of the adversary is to perform various attacks in the system.

We assume that the adversary, the adversarial reader, and the adversarial tag have polynomially bounded resources. In addition, the adversary can launch physical attacks. However, the hardware based defenses against physical attacks are beyond the scope of this work. Our assumptions also include that the reader cannot be compromised. In our system, we consider following oracle construction:

$\boldsymbol{\mathcal{O}_{Eavesdrop}(R, WT, t)}$: The adversary eavesdrops within a channel to listen to the communication at time t between reader R and one of its communicating tag WT.

$\boldsymbol{\mathcal{O}_{Impersonate_R}(R, WT, M, t)}$: The adversary impersonates a reader R in a protocol session at time t and sends a message M to the tag WT.

$\boldsymbol{\mathcal{O}_{Impersonate_{WT}}(R, WT, M, t)}$: The adversary impersonates a tag WT in a protocol session at time t and sends a message M to the reader R.

$\boldsymbol{\mathcal{O}_{Query}(WT, t)}$: The adversary queries a tag $\boldsymbol{WT}$, to learn information during protocol session at time t.

$\boldsymbol{\mathcal{O}_{Receive}(U, M, t)}$: The adversary receives a message M from an entity U (e.g., either WT or R) during the execution of protocol session at time t.

9.5.2. Security Analysis

For every attack, we first describe how the attack is performed by an adversary. Then how our protocol protects against the attack is explained. R and WT_i are referred to as a legitimate reader and legitimate tag. Each attack and defense, as a whole, has three phases:

Phase 1. Learning phase: This phase represents pre-attack preparations. Adversary, $\hat{A}$ uses non-destructive oracles such as $\boldsymbol{\mathcal{O}_{Eavesdrop}(R, WT, t)}$, $\boldsymbol{\mathcal{O}_{Impersonate_R}(R, WT, M, t)}$, $\boldsymbol{\mathcal{O}_{Query}(WT, t)}$, $\boldsymbol{\mathcal{O}_{Impersonate_{WT}}(R, WT, M, t)}$, and $\boldsymbol{\mathcal{O}_{Receive}(U, M, t)}$ on a set of target tags and reader. The goal of the adversary is to learn information related to tags and reader.

Phase 2. Attacking phase: $\hat{A}$ starts to attack. $\hat{A}$ may impersonate as a legitimate tag or reader.

Phase 3. Defend Phase: Reliable MTD protocol is designed in such a way so that it can defend against the majority of the attacks performed by the adversary $\hat{A}$. Due to space limitation, here we only discuss three attacks.

- **Privacy Preservation**

Learning Phase: Here, $\hat{A}$ repeatedly queries WT_i with different (f, r) using $\boldsymbol{\mathcal{O}_{Impersonate_R}(R, WT_i, M, t)}$ to collect replies from the tags.

Attacking phase: $\hat{A}$ executes $\boldsymbol{\mathcal{O}_{Receive}(U, M, t)}$ oracle to learn replies from the tags and create a bit record. The goal of the attacker is to learn the ids of different tags and also the raw sensor values so that it can infer human activity or environmental situation. This is known as privacy violation.

Defend Phase: Our protocol can preserve the privacy of individual WISP tags since none of the tags reply their id. Therefore, the adversary cannot infer the ids from the replies of the tags. $\hat{A}$ cannot even find out the original sensor data. Each tag replies with an encrypted sensor data, $h(id) \oplus r\_dat$ which can be decrypted only by the server. Since the server only knows the id of different tags, only it can compute the hash value. So, none but the server can decrypt the encrypted sensor data to collect the raw data.

- **Tracking**

Learning Phase: Here, $\hat{A}$ tries to track WT_i over time. $\hat{A}$ succeeds if it can distinguish WT_i from other tags.

Attacking phase: Under this attack, $\hat{A}$ repeatedly queries WT_i with different (f, r) using oracle $\boldsymbol{\mathcal{O}_{Query}(WT_i, t)}$ to learn about the slot picking behavior of the tags. Then the adversary executes oracle $\boldsymbol{\mathcal{O}_{Receive}(U, M, t)}$ to receive replies from the tags. The goal of the attacker is to get a consistent reply that may become a signature of WT_i.

Defend Phase: MTD is resistant against tracking. Let an adversary $\hat{A}$ eavesdrop on the transaction between a reader R and the existing tags. So $\hat{A}$ knows the queries and replies but $\hat{A}$ cannot reverse compute the replies. The adversary can certainly be sure that monitoring has taken place. However, it will not be able to figure out which tag replied in which slot since it does not have the ids of the tags. Moreover, the slot picking behavior of the tags changes with the change of f and r. As a result, the outputs of all the tags seems to be purely random to the adversary $\hat{A}$.

- **Eavesdropping**

Learning Phase: $\hat{A}$ executes the oracle $\boldsymbol{O_{Eavesdrop}(R, WT_i, t)}$ and later uses this information to launch different attacks (ex. replay attack)

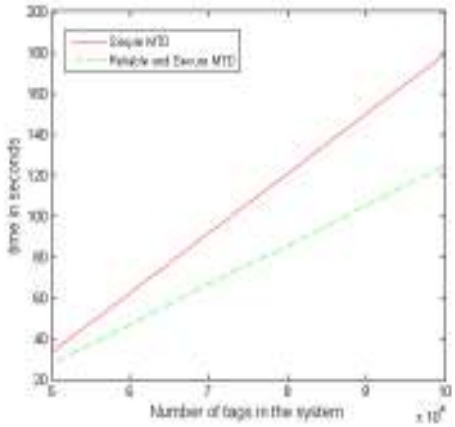
Attacking phase: $\hat{A}$ can learn every piece of information exchanged between R and WT_i. The goal of $\hat{A}$ is to use the data to impersonate a fake reader or a fake tag.

Defend Phase: Our protocol is powerful against this attack. In our protocol $\hat{A}$ will not be able to find out the expected reply of the tags. $\hat{A}$ will not be able to find out any relation between the slot positions and tag replies. In each monitoring pass, all tags will pick a different slot based on the random number sent by the reader. $\hat{A}$ can only observe the data sent by the reader and the tags. But $\hat{A}$ will not be able to link the outputs of two parties and it will not be able to decrypt sensor data. It cannot even replay the messages since it cannot compute the correct slot position (given f and r) without the knowledge of id. Therefore, $\hat{A}$ cannot impersonate R or $WT_i$and it cannot launch replay attack by using previous values.

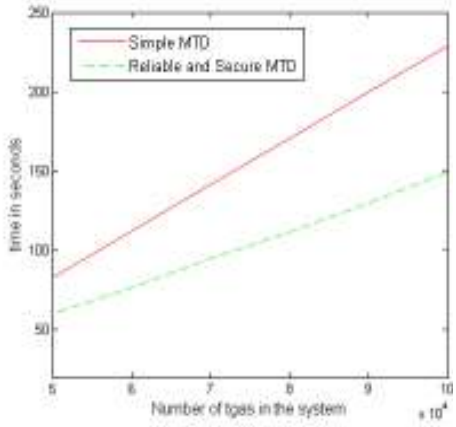
9.6. Evaluation Results

In this section, we evaluate the efficiency of our two protocols by simulation. We use two metrics to compare the performance of the protocols − 1) protocol execution time and 2) time to determine the first missing tag. The protocol execution time metric tells us how long it takes for a protocol to identify exactly how many tags are missing and which tags are missing. The second

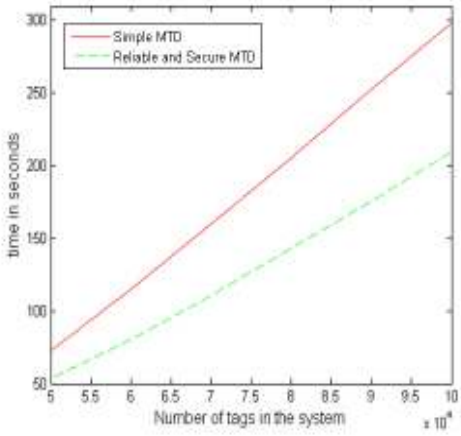
metric tells us how long it takes a protocol to identify the missing-tag event, i.e. at least one tag is missing.



(a) Number of missing tags follows an exponential distribution with mean 20000

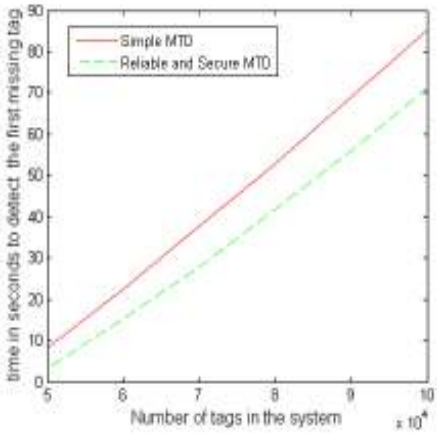


(b) Number of missing tags follows an exponential distribution with mean 35000

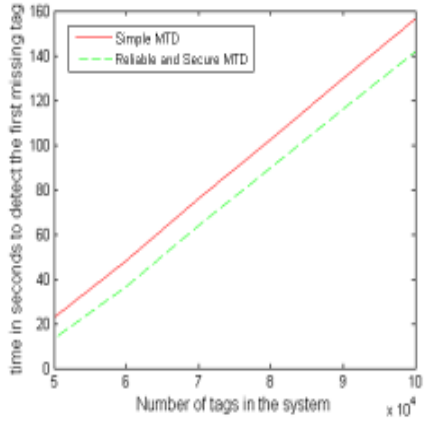


(c) Number of missing tags follows an exponential distribution with mean 45000

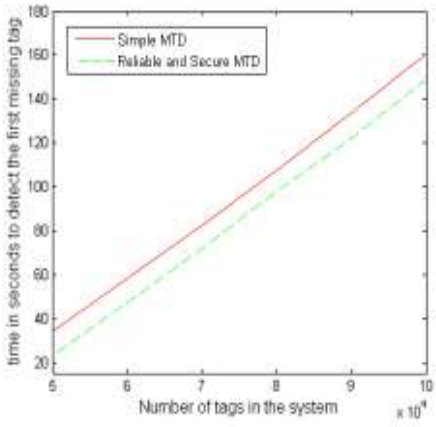
Figure 9.8 Comparison of Simple and Reliable MTD protocol based on protocol execution time



(a) Number of missing tags follows an exponential distribution with mean 20000



(b) Number of missing tags follows an exponential distribution with mean 35000



(c) Number of missing tags follows an exponential distribution with mean 45000

Figure 9.9 Comparison of Simple and Reliable MTD protocol based on the time to detect the first missing tag

According to the technical specification of Philips I-Code system [Buettner08], a reader needs $0.4ms$ to detect an empty slot, $0.8ms$ to detect a collision or a singleton slot, and $2.4ms$ to transmit a 96-bit piece of data. In our simple MTD protocol, we need to consider only the time to transmit short responses ($t_s = 0.4\ ms$), long responses ($t_l = 0.8\ ms$) and time to transmit sensor

data ($t_{data} = 2.4\ ms$). However, in the Reliable MTD protocol, we only need to identify single reply slots and collision slots. The efficiency of reliable MTD is also dependent on frame size f. A smaller f has fewer slots, which results in faster performance. We assume the duration of each slot is equally long.

In our simulated WISP environment, we considered $N = 50{,}000$ to $100{,}000$ WISP tags and one legitimate reader. Figure 5.8 shows the execution time of our two protocols. We assume that the number of missing tags in the system follows an exponential distribution with mean = 10000 in Figure 9.8(a), mean = 35000 in Figure 9.8(b) and mean = 45000 in Figure 9.8(c). We ran each simulation 100 times with different random seeds and took the average of these values to produce a point on the graph. The first set of simulation results (Figure 9.8 (a) (b) (c)) shows that the reliable MTD protocol performs increasingly better than the simple MTD protocol, especially when there is a large number of missing tags in the system. For example, when N = 100000, the time of the reliable MTD is 65.3% of the time taken by simple MTD.

The second set of simulations studies the relation between the number of missing tags and the time to detect the first missing tag. From the experimental results shown in figure (Figure 9.9 (a) (b) (c)) it is evident that it takes less time to find out whether some tags are missing than to actually identify all of them. This is also an important feature for systems that require a quick check on the tags on whether the set of tags is intact. All the results of Figure 9.9 also illustrate that the simple MTD takes more time to detect missing tag than the Reliable MTD protocol.

9.7. Discussion

The overall goal of this research work was to investigate the solution of missing WISP tag detection that can be very significant in any WISP based monitoring systems. Since the decision making of such a system depends on each individual WISP tag, the absence of any tag data may raise questions about reliability of the system's decision. If the missing tag event goes undetected and any wrong decision is taken by the system, it can be even more critical from the

point of view of the system's user. Therefore, from the point of view of system's functionality accuracy, missing WISP tag detection is an important problem.

In this chapter, we propose a simple and reliable missing tag detection protocol that can be useful in the above mentioned application areas where reliability and security is the primary focus. However, our protocol has a minor limitation. In secure and reliable MTD, there can be situations where existing tags in the systems are compromised by an adversary and are instructed to keep silent during the execution of the protocol. We call this type of attack a "concealing attack". It is very hard to defend against a concealing attack and it is out of the scope of this work. However, investigation of defense mechanism for concealing attack can be a good future work.

9.8. Goals Satisfied by MTD Protocol

The motivating example of CRFID application for this chapter is critical CRFID applications where the reliability of the system's decision is really very important. In such applications the main goal of the system is ensure that the decision taken by the system is reliable or accurate enough since the overall collective decision of the system may have an impact on human lives. Therefore, ensuring decision making reliability (by indentifying missing data in the system) as well as reducing response time are two major goals in these types of applications. MTD protocol is able to achieve these goals since it allows identifying the missing tags as well as ensures system security and decision reliability.

9.9. Summary

In this chapter, we considered the problem of identifying the missing tags in CRFID based critical systems. To address this problem, we propose a secure protocol to monitor for missing tags, identified the missing ones without sacrificing the performance of the system.

9.10. Publication

- ***Published:*** *Farzana Rahman* and Sheikh Iqbal Ahamed, "MonAC: Detecting Missing Tags for Improved Accuracy in Computational RFID based Assisted Environments", *In Proc. of the ACM Symposium on Research in Applied Computation (ACM RACS 2012)*, USA, October, 2012.
- ***Under Review:*** *Farzana Rahman* and Sheikh Iqbal Ahamed, "Towards Improving Security and Reliability of Computational RFID based Assisted Environments", In a journal.

Chapter 10: Conclusions and Future Work

In this chapter, we summarize the contributions of the dissertation and present some future research directions.

10.1. Research Achievements

RFID technology is increasingly being deployed in diverse applications ranging from inventory management to counterfeiting prevention. With the emergence and deployment of computational RFID tags, the application of this technology will become even more extensive. Nonetheless, RFID tags have yet to replace the ubiquitous barcode found on almost every grocery product. This slow adoption is partly due to the security and privacy concerns over the pervasive deployment of RFID tags. With commodities as varied as bank notes, airport luggage, and clothing items, the security and privacy aspects of each system need to be individually addressed. Usually general RFID authentication protocols are used for ensuring security and preserving privacy in all applications. However, each RFID application has its own specific requirements. For example, RFID systems for healthcare, supply chain and military battlefield have different security, privacy and performance requirements. Therefore, our focus in this dissertation is to ensure that RFID system specific goals are met without sacrificing performance.

To address the above mentioned goals, the methodologies that we have presented in this dissertation represent a complete solution to the security and privacy issues of couple of major real life RFID applications. We can use encryption and digital signatures in our scheme despite the use of passive read/write tags, which are resource constrained. This scheme can be deployed without any changes to the existing EPC Class 1 architecture. Further, it can be integrated with the EPC Network.

The main achievements of the research presented in this dissertation can be summarized as follows:

- **Detecting Counterfeits in Large Scale RFID Systems Using Batch Authentication Protocol:** In Chapter 6, we propose to detect counterfeit tags in large scale system using efficient batch authentication. In large scale RFID applications (such as supply chain, retail industry, and pharmaceutical industry) tag authentication is used to detect counterfeit products. However, RFID authentication protocols are mainly per-tag based where a reader needs to authenticate tags sequentially. This increases the overall protocol execution time. To address this, we propose Frames Slotted ALOHA (FSA) based protocol, *FTest*, to meet the requirements of prompt and reliable batch authentication in large-scale RFID applications. FTest can determine the validity of a batch of tags with minimal execution time which is a major goal of large-scale RFID systems. FTest can reduce protocol execution time by ensuring that the percentage of potential counterfeit products is less than a user-defined threshold. Our experimental result demonstrates that FTest performs significantly better than the existing counterfeit detection approaches, e.g. authentication techniques.
- **Preserving Privacy in RFID based Healthcare Systems:** In Chapter 7 we address the tradeoff between privacy and reliability in RFID based healthcare systems. RFID has received considerable attention within the healthcare community since early 2000. However, the prospect of wide spread use of RFID in the healthcare area has also triggered discussions regarding privacy. There are basically two types of privacy preservation issues in RFID based healthcare: 1) A privacy preserving authentication protocol is required while sensing RFID tag for different identification and monitoring purposes; 2) A privacy preserving access control framework is required to maintain user preferred privacy while accessing various healthcare services based on RFID identification data. To address the above mentioned research issues, we propose two component based framework (PriSens-HSAC). The PriSens component proposes a group based anonymous authentication protocol to solve the tradeoff between the scalability and privacy problems of RFID sensing in healthcare. The HSAC component proposes a privacy preserving healthcare service access mechanism to maintain the users' privacy while accessing various

healthcare services. To the best of our knowledge, it is the first framework to provide increased privacy in RFID based healthcare using authentication along with access control technique.

- **Ensuring Survivability of RFID Systems using a Robust Authentication Protocol:** In Chapter 8 we introduce computational RFID tags and their possible application areas. WISP tags are an example of Computational RFID (CRFID) which is used in many sophisticated applications like: enemy move detection in military battlefields, and activity inference in elderly care systems. In these types of systems, an adversary may create more collisions to initiate a de-synchronization attack. This, in turn, may result in Denial of Service (DoS) attack, increase the system response time, and jeopardize the survivability of the system. In an effort to address the survivability issues in CRFID based sophisticated applications, we propose DRAP protocol. This protocol can return desynchronized tags and readers to their synchronous state. Therefore, it provides robustness and ensures survivability. Our simulation results show that DRAP reduces the collision rate significantly to increase the system performance.

- **Detecting Missing WISP Tags for Improved Decision Reliability of CRFID based Systems:** In Chapter 9, we present missing tags detection protocols for CRFID based critical systems. Recently, WISP tags, one type of CRFID tags, have been used to monitor indoor activity, vital signs, sleep quality, and health status remotely. However, these critical CRFID based systems are very sensitive in terms of decision reliability. Any missing tag data in these systems may introduce error in the final decision of the system and this may reduce system's decision reliability. To address this problem and to maintain system's decision reliability, we propose two tag monitoring protocols for CRFID based critical systems based on probabilistic methods. We also report the performance comparison of our protocols. The goal of these protocols is to improve the security and decision reliability of CRFID based critical systems.

10.2. Future Research Directions

There are many possible research topics for further study within the area of RFID security and privacy. We mention some possible research directions related to the work described in this dissertation:

- In FTest Protocol, we assumed that all tags (both legitimate and counterfeit) will be honest, i.e., all tags will reply when queried by a reader. In our attack model, we did not consider counterfeit tags that may not reply to hide their identity during the query phase. However, in an active adversarial environment the counterfeit tags may not reply at all to hide their identity and we name this attack as "concealing attack". It is very hard to defend against concealing attack and it is out of the scope of this dissertation. Therefore, one future research direction would be to investigate defense mechanisms against concealing attack in FTest Protocol.
- One other future research direction in case of FTest protocol is to investigate the protocol performance for different batch sizes and for varying Δ values. In this regards, one could also investigate the design of a lightweight batch authentication protocol based on key transportation and authentication using threshold secret sharing scheme which provides strong security on low-cost RFID tags.
- In PriSens-HSAC framework, one research investigation could be to investigate the performance and accuracy of the entire framework by utilizing it in various real scenarios for different user roles like: Physician, Emergency care provider, and Pharmacist. To better investigate the privacy preservation issue one could also test the accuracy of the framework by simulating the system scenario under various attacks.
- One other research direction in case of PriSens-HSAC framework can be to investigate the privacy levels achieved for different types of service requests and different attacks.
- Another future research direction in the context of privacy preservation in RFID systems could be to study the privacy threats in RFID data publishing phase and show that traditional

anonymization techniques are not applicable for RFID data due to its challenging properties: high-dimensional, sparse, and sequential. Future research can also be focused to adopt a newer privacy model like LKC-privacy that can overcome these challenges in the data publishing phase.

- In DRAP Protocol, we use EDFSA based communication technique while the tag and reader communicates with each other to reduce the collision rate so that optimum system efficiency can be achieved. However, one future research could be to investigate how the protocol performs when the underlying communication technique is varied. The underlying communication technique can be varied by varying the frame sizes for the following protocols: pure slotted ALOHA, framed slotted ALOHA, dynamic framed slotted ALOHA.
- One major future research work could be to develop an emulator for secure RFID protocol testing so that the real performance of all the protocols proposed in this dissertation can be tested. The aim of this future work could be to better understand the nature of various attacks launched in different RFID system and how our protocols can address them. This work can be further extended by investigating the performance of our protocol under collaborative attack.
- This dissertation only considers RFID protocols using symmetric cryptography, primarily those using hash functions. There are a number of other general RFID protocols that needs further study, including RFID protocols using asymmetric cryptography. There could also be many attacks on RFID systems that we have not identified. Thus, further study of such protocols and possible attacks would be really significant.
- In this dissertation, we have also assumed that the channel between the back-end server and the reader is secure. Therefore, we have not dealt with security threats arising on that channel. However, in some applications, this communication channel may be unsecure, for example, the channel me be an unsecure wireless channel. Thus, development of secure authentication protocols over this channel should be studied further.

Chapter 11: Bibliography

[Ahamed08a] Ahamed, S. I., Rahman, F., Hoque, E., Kawsar, F., and Nakajima, T. (2008). Secure and Efficient Tag Searching in RFID Systems using Serverless Search Protocol. In Journal of Security and Its Applications, Vol.2, No.4. 2008. 57-66.

[Ahmed08b] Ahamed, S. I., Rahman, F., Hoque, E. (2008). ERAP: ECC based RFID Authentication Protocol. In Proc. of IEEE International Workshop on Future Trends of Distributed Computing Systems (FTDCS 2008), Kunming, China, October 21-23, 2008, pp.219-225.

[Ahmed08c] Ahamed, S. I., Rahman, F., Hoque, E., Kawsar, F., and Nakajima, T. (2008). YA-SRAP: Yet Another Serverless RFID Authentication Protocol. In Proc. of International Conference on Intelligent Environment (IE08), Seattle, USA, July, 2008, pp. 640--.

[Ahmed08d] Ahamed, S. I., Rahman, F., Hoque, E., Kawsar, F., and Nakajima, T. (2008). S^3PR: Secure Serverless Search Protocols for RFID. In Proc. of IEEE International Conference on Information Security and Assurance (ISA 2008), Korea, April, 2008, pp.187-192.

[Ahmed08d] Ahamed, S. I., Rahman, F., Hoque, E., Kawsar, (2008). Secured Tag Identification Using EDSA (Enhanced Distributed Scalable Architecture), In Proc. of ACM Symposium on Applied Computing (ACM SAC 2008), Brazil, March, 2008. pp. 1902-1907.

[Age] Intel Corporation. Age-in-place. www.intel. com/research/prohealth/cs-aging_in_place.htm.

[Avoine12] Avoine, G. “Bibliography on security and privacy in RFID systems”. Available Online (http://lasecwww.epfl.ch/˜gavoine/rfid/), 2012.

[Avoine05] Avoine, G., and Oechslin, P. “A scalable and provably secure hash based RFID protocol”. In Proc. of PerCom Workshop-PerSec 05, 2005. pp. 110- 114.

[Avoine07] Avoine, G., Buttyan, L., Holczer, T., and Vajda, I. "Group-based private authentication". In Proc. of WoWMoM 07. 2007. pp. 1-6.

[Avoine08] Avoine, G. Security and Privacy in RFID Systems. Technical Report. http://www.avoine.net/rfid/, 2008.

[Awarehome] Georgia Institute of Technology. Awarehome.www.cc.gatech.edu/fce/ahri/.

[Bardram07] Bardram, J. E. and Christensen, H. B. Pervasive computing support for hospitals: An overview of the activity-based computing project. IEEE Pervasive Computing, 6(1):44–51, 2007.

[Becker04] Becker, P. S. M.Y. Cassandra: flexible trust management, applied to electronic health records. In Proc. of Computer Security Foundations Workshop. 2004, pp. 139–154.

[Beaudin07] Beaudin, J., Intille, S. S., Tapia, E. M., Rockinson, R. and Morris, M. E. Context-sensitive microlearning of foreign language vocabulary on a mobile device. In Ambient Intelligence, Vol. 4794. Lecture Notes in CS Springer, 2007. pp.55–72.

[Bhatti06] Bhatti, A. G. R., Moidu, K. Policy-based security management for federated healthcare databases (or rhios). In Proc. of the Workshop on Healthcare Information and Knowledge Management. 2006. pp. 41–48.

[Blackert03] Blackert, W.J., Gregg, D.M., Castner, A.K., Kyle, E.M., Hom, R.L., and Jokerst, R.M. Analyzing interaction between distributed denial of service attacks and mitigation technologies. In Proceedings of DARPA Info. Survivability Conf. and Expo.Vol. 1. 2003. 26- 36.

[BlueBean] BlueBean. "The Benefits of RFID in the Healthcare Organization, RFID Solutions for the Healthcare Industry". 2007. Last accessed - March 2012 at http://www.rfidhealthcare.com/

[Bringer06] Bringer. J., Chabanne, H., and Emmanuelle, D., et al. (2006). HB++: a lightweight authentication protocol secure against some attacks. In International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing (SecPerU 06), IEEE, IEEE Computer Society Press. pp. 28-33.

[Buettner10] Buettner, M., Prasad, R., Philipose, M., and Wetherall, D. Recognizing daily activities with RFID-based sensors. In Proceedings of Ubiquitous computing. 2009. 51-60.

[Buettner08a] Buettner, M., Greenstein, B. , Sample, A., Smith. J. R. and Wetherall, D. "Revisiting smart dust with RFID sensor networks". In Proc. 7th ACM Workshop on Hot Topics in Networks. 2008.

[Buettner08b] Buettner, M., Greenstein, B., Prasad, R., Sample, A., Smith, J. R., Yeager, D. and Wetherall, D. "Demonstration: Rfid sensor networks with the intel wisp," in 6th ACM Conference on Embedded Networked Sensor Systems. 2008.

[Buettner09] Buettner, M., Prasad, R., Philipose, M., and Wetherall, D. "Recognizing daily activities with rfid-based sensors". In Proc. Ubicomp. 2009.

[Byun05] Byun, N. L. J.W, Bertino, E. Purpose based access control of complex data for privacy protection. In Proc. of SACMAT. 2005, pp. 102–110.

[Cha05] Cha, J. R. and Kim, J. H. Novel Anti-collision Algorithms for Fast Object Identification in RFID System. In Proceedings of Parallel and Distributed Systems. 2005. 63-67.

[Chae07] Chae, H.J., Yeager, D.J., Smith, J.R., and Fu, K. Maximalist Cryptography and Computation on the WISP UHF RFID Tag. In Proceedings of RFID Security. 2007.

[Chaudhri08] Chaudhri, R., Lester, J., and Borriello, G. "An RFID based system for monitoring free weight exercises". In Proc. SenSys. 2008.

[Chatmon06] Chatmon, C., Le, T. V., and Burmester, M. “Secure anonymous RFID authentication protocols”. Technical report, Florida State University, Department of Computer Science, Tallahassee, Florida. USA. 2006. http://www.cs.fsu.edu/~burmeste/TR-060112.pdf

[Chen10] M., Chen, S., Gonzalez, Q., Zhang, M., Li, V., Leung. A 2g-rfid based e-healthcare system. In Proc. Wirel CommunMag 17(1). 2010. pp. 37–43

[Chien07] Chien, H.Y., and Chen, C. H., et al. (2007). Mutual authentication protocol for RFID conforming to epc class 1 generation 2 standards. In Computer Standards Interfaces, Vol. 29, Ed. 2. pp. 254-259.

[Czeskis08] Czeskis, A., Koscher, K., Smith, J.R., Kohno, and T. RFIDs and Secret Handshakes: Defending Against Ghost-and-Leech Attacks and Unauthorized Reads with Context-Aware Communications. In Proceedings of Computer and Comm. Security. 2008. 479-490.

[Dafa-Alla05] A.F., Dafa-Alla, Kim, E. H., Ryu, K. H., Heo, Y. J. PRBAC: an extended role based access control for privacy preserving data mining. In Proc. of ACIS International Conference on Computer and Information Science. 2005. pp. 68- 73.

[Diaz02] Diaz, C., Seys, S., Claessens, J., and Preneel, B. “Towards measuring anonymity”. In Privacy Enhancing Technologies Workshop (PET 2002). USA. 2002. pp. 54-68.

[Dimitriou06] Dimitriou, T. “A secure and efficient rfid protocol that could make big brother (partially) obsolete”. In Proc. of PerCom 06. pp. 269-275.

[eShepherd] Exavera Technologies, “eShepherd overview,” http://www.exavera.com/healthcare/eshepherd.php.

[EPCGLOBAL]“EPCglobal Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz-960MHz”.

[Engberg04] Engberg, S., Harning, M., and Jensen, C. D. Zero-knowledge device authentication: Privacy & security enhanced RFID preserving business value and consumer convenience. In Conference on Privacy, Security and Trust – PST, New Brunswick, Canada, October 2004.

[Feldhofer03] Feldhofer, M. A proposal for authentication protocol in a security layer for RFID smart tags, 2003.

[Ferraiolo92] Ferraiolo, D. and Kuhn, D. R. Role based access control. In Proc. of Conference on National Computer Security, National Institute of Standards and Technology, MD. 1992. pp. 554–563.

[Fujitsu] Fujitsu develops world's first 64KByte high-capacity FRAM RFID tag for aviation applications, 2008. Last accessed June 2010. http://www.fujitsu.com/global/news/pr/archives/month/2008/20080109-01.html

[Gilbert05] Gilbert, H., Robshaw, M., and Sibert, H., et al. (2005). An active attack against HB+ – a provably secure lightweight authentication protocol. Manuscript, 2005.

[Godik03] Godik, T. M. S. Extensible access control markup language (xacml). Technical Report v1.1, 2003.

[Haigh06] Haigh, K. Z., Kiff, L. M. and Ho, G. The Independent LifeStyle AssistantTM (I.L.S.A.): Lessons Learned. Assistive Technology, 2006.

[Harrop08] Harrop, P. and Harvey, T. C. “RFID for Healthcare and Pharmaceuticals”. In IDTechEx, 2008.

[He05] He, C. G., Cao, C. Z., Bao, S. D. An Enhanced Role-Based Access Control Mechanism for Hospital Information Systems. In Proc. of Conf.on Computational Intelligence and Security. 2011. pp. 1001-1005.

[Henrici04] Henrici, D., and MÄuller, P., et al. (2004). Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers. In Proceedings of the International Workshop on Pervasive Computing and Communication Security (PerSec 04), IEEE, IEEE Computer Society Press. NY, USA. pp. 149-153.

[Henrici08] D. Henrici, P Müller. "Providing Security and Privacy in RFID Systems Using Triggered Hash Chains". In Proceedings of IEEE PerCom, 2008. pp. 50-59.

[Hinske07] Hinske, S. "Determining the Position and Orientation of Multi-Tagged Objects Using RFID Technology". In Proc. of Pervasive Computing and Communications Workshops (PerCom Workshops 2007). 2007. pp.377-38.

[Holleman08] Holleman, J., Yeager, D., Prasad, R., Smith, J., and Otis, B. NeuralWISP: An Energy Harvesting Wireless Neural Interface with 1-m Range. In Proceedings of Biomedical Circuits and Systems Conference. 2008. 37-40.

[Hooyman02] Hooyman, N. and Kiyak, H. "Social Gerontology: A Multidisciplinary Perspective," 6th ed., Allyn and Bacon, 2002.

[Hopper00] Hopper, N., and Blum, M., et al. (2000). A secure human-computer authentication scheme. Tech. Rep. CMU-CS-00-139, Carnegie Mellon University, 2000.

[Hopper01] Hopper, N. J., and Blum, M., et al. (2001). Secure human identification protocols. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 01), Springer-Verlag. pp. 52–66.

[Hoque09a] Hoque, M. E., Rahman, F., Ahamed, S. I., and Park, J. H. Enhancing Privacy and Security of RFID System with Serverless Authentication and Search Protocols in Pervasive Environments. In Springer Wireless Personal Communication, Vol. 55, No. 1. 2009. 65-79.

[Hoque09b] Hoque, M. E., Rahman, F., and Ahamed, S. Supporting Recovery, Privacy and Security in RFID Systems Using a Robust Authentication Protocol. In Proceedings of ACM Symposium on Applied Computing. 2009, 1062-1066.

[Hoque10a] Hoque, M. E., Rahman, F., and Ahamed, S. I. S-Search: Finding RFID Tags Using Scalable and Secure Search Protocol. In Proceedings of Symposium on Applied Computing. 2010. 439-443.

[Hoque10b] Hoque, E. Dickerson, R., and Stankovic, J. A. Monitoring Body Positions and Movements during Sleep using WISPs. In Proceedings of ACM Wireless Health. ACM, NY, USA. 2010. 44-53.

[Hoque11] Hoque, M. E., Rahman, F., and Ahamed, S. I., "AnonPri: An efficient anonymous private authentication protocol", In Proc. of PerCom 11, 2011. pp. 102-110.

[Ilic05] Ilic, C. Using tags to make teeth, RFID Journal, http://www.rfidjournal.com/article/articleview/1206/1/1/, d--ownloaded 22 January 2005.

[IND-CPA] http://en.wikipedia.org/wiki/Ciphertext_indistinguishability

[Intel] Intel Research Seattle, http://seattle.intel-research.net/wisp/#pub (last accessed: 27th Feb. 2010)

[Jiang05] Jiang, B., Smith, J., Philipose, M., Roy, S., Rajan, S. K., and Mamishev, A. (2005). Energy scavenging for inductively coupled passive RFID systems. In IEEE Trans. on Instrumentation and Measurement. 2005. 984-989.

[Jin09] Jin, H. H. J., Ahn, G.J. Patient-centric authorization framework for sharing electronic health records. In Proc. SACMAT. 2009. pp. 125-134.

[Juban04] Juban, R. L., and Wyld, D. C. Would you like chips with that?: Consumer perspectives of RFID. Management Research News, 27(11/12), 29-44. 2004.

[Juels05a] Juels, A., (2005). RFID security and privacy: A research survey. RSA Laboratories.

[Juels05b] Juels, A., Molnar, D. and Wagner, D., et al. (2005). Security and Privacy Issues in Epassports. In Proceedings of the Conference on Security and Privacy for Emerging Areas in Communications Networks (SecureComm 05), IEEE, IEEE Computer Society Press. NY, USA. pp. 74-88.

[Juels06] Juels, A., and Weis, S. Defining strong privacy for RFID. In. Proceedings of the Cryptology ePrint Archive, Report 2006/137, IACR. 2006.

[Kodialam06] Kodialam, M., and Nandagopal, T. "Fast and reliable estimation schemes in RFID systems". In Proc. of MOBICOM 06. 2006. pp. 322-333.

[Laurie07] Laurie, A., (2007). Practical attacks against RFID. In Network Security. pp. 4-7.

[Lee05] Lee, S., Joo, S. D., and Lee, C. W. An Enhanced Dynamic Framed Slotted ALOHA Algorithm for RFID Tag Identification. In Proceedings of MobiQuitous. 2005. 166- 172.

[Lee08] Lee, D. W., Bang, O. K., Im, S. Y. and Lee. H. J. "Dual bias Q-algorithm and optimum weights for EPC Class1 Generation 2 protocol". In 2008 European Wireless. 2008. pp. 1-5.

[Li07] Li, Y., and Ding, X., et al. (2007). Protecting RFID communications in supply chains. In Proceedings of the Symposium on Information, Computer and Communications Security, (ASIACCS 07). ACM Press, NY, USA. pp. 234-241.

[Li10] Li, T., Chen, S. and Ling, Y. "Identifying the Missing Tags in a Large RFID System," Proc. of ACM Mobihoc, 2010.

[Lu07] Lu, L., J. Han, L. Hu, Y. Liu, and L. M. Ni. "Dynamic key updating privacy-preserving authentication for RFID systems". In Proc. of PerCom 07. 2007. pp. 13-22.

[Lu09] Lu, L., Han, J., Xiao, R. and Liu, Y. "ACTION: breaking the privacy barrier for RFID systems". In Proc.of INFOCOM 09. pp.1953-1961.

[Lundell07] Lundell, J., Hayes, T., Vurgun, S., Ozertem, U., Kimel, J., Kaye, J., Guilak, F. and Pavel, M. Continuous activity monitoring and intelligent contextual prompting to improve medication adherence. In EMBS, pages 6286–6289, Aug. 2007.

[Ma10] D. Ma and G. Tsudik. "Security and privacy in emerging wireless networks ". In Wireless Comm., vol.17, no.5, pp.12-21. 2010.

[Mayes09] Mayes, K., Markantonakis, K., and Hancke, G. et al. (2009). Transport ticketing security and fraud controls. In Elsevier Information Security Technical Report, Vol. 14, Ed. 2. pp. 87-95.

[Mitchell03] Mitchell, C. J. Cryptography for mobile security. In C. J. Mitchell, editor, Security for Mobility, IET Telecommunications, chapter 1, pages 3{10. The Institution of Engineering and Technology, December 2003.

[Menezes96] Menezes, A. J., Oorschot, P. C., and Vanstone, S. A. Handbook of Applied Cryptography, volume 6 of Discrete Mathematics and Its Applications. CRC Press, 1996.

[Michahelles07] Michahelles, I., F., Fleisch, E. “Dual ownership: access management for shared item information in RFID-enabled supply chains”. In Proc. of Pervasive Computing and Communications Workshops (PerCom Workshops 2007). 2007. pp.337-341. doi: 10.1109/PERCOMW.2007.40

[Molnar04] Molnar, D. and Wagner, D. “Privacy and security in library RFID: Issues, practices, and architectures”. In Proc. of CCS 04. 2004. pp. 210-219.

[Molnar05] Molnar, D., Soppera, A., and Wagner, D. “A Scalable, Delegatable Pseudonym Protocol Enabling Owner-ship Transfer of RFID Tags”. In Proceedings of SAC, 2005. pp. 276-290.

[Myung06] Myung, J. and Lee, W. Adaptive Binary Splitting: A RFID Tag Collision Arbitration Protocol for Tag Identification. In Proceedings of the Conference on Broadband Networks. 2006. 347- 355.

[Munishwar09] Munishwar, V.P., Singh, S., Mitchell, C., Xiaoshuang, W., Gopalan, K., Abu-Ghazaleh, N.B "RFID based localization for a miniaturized robotic platform for wireless protocols evaluation". In Proc. of Pervasive Computing and Communications, (PerCom 2009). 2009. pp.1-3.

[Neill08] Neill, M. O. "Low cost SHA-1 hash function architecture for RFID tags". In Proc. of RFIDSec 08, 2008.

[NFC] Limitations of NFC [Last accessed: 21 Sept 2012] http://www.smartcard.co.uk/articles/R2R%20Technology%201_0.pdf

[Nohara07] Y. Nohara, S. Inoue, H. Yasuura. "Unlinkability and real world constraints in RFID systems". In Proc. of Pervasive Computing and Communications Workshop (PerCom Workshops 2007). 2007. pp.371-376.

[Nohl06] Nohl, K., and Evans, D. "Quantifying information leakage in tree-based hash protocols". In Proc. of ICICS 06. 2006. pp. 228-237.

[Ohkubo03] Ohkubo, M. , Suzuki, K. and Kinoshita, S. "Cryptographic approach to privacy friendly tags". In Proc. of RFID Privacy Workshop, MIT, MA, USA, 2003.

[Pervasive1] Pervasive Computing definition, URL: http://www.parliament.vic.gov.au/sarc/EDemocracy/Final_Report/Glossary.htm

[Pervasive2] Pervasive Computing framework, URL: http://framework.v2.nl/archive/archive/node/text/default.xslt/nodenr-156647

[Piramuthu06] Piramuthu, S., (2006). HB and related lightweight authentication protocols for secure RFID tag/reader authentication. In CollECTeR 2006.

[Pollinger08] Pollinger, Z. A. "Counterfeit goods and their potential financing of international terrorism." In Michigan Journal of Business Vol. 1, No. 1. 2008. pp. 85–102.

[Qian08] Qian, C., Ngan, H., and Liu, Y. et al. (2008). Cardinality Estimation for Large-scale RFID Systems. In Proceedings of IEEE PerCom (Percom 08). pp 30-39.

[Rahman 11] Rahman, F., Hoque, M. E. and Ahamed, S. I., (2011). REBIVE: A Reliable Private Data Aggregation Scheme for Wireless Sensor Networks. In Proc. of ACM Symposium on Applied Computing (ACM SAC 2011), Taiwan, March 2011. pp. 439-444.

[Rahman12a] Rahman, F. and Ahamed, S. I. "Looking for needles in a haystack: Detecting Counterfeits in Large Scale RFID Systems using Batch Authentication Protocol", In Proc. of IEEE PerCom Workshop on Pervasive Wireless Networking (PWN12). Switzerland. 2012. pp. 811 - 816.

[Rahman12b] Rahman, F. and Ahamed, S. I. "I am not a goldfish in a bowl: A Privacy Preserving Framework for RFID based Healthcare Systems", In Proc. of IEEE 14th International Conference on e-Health Networking, Applications and Services (Healthcom 2012). China. 2012.

[Rahman12c] Rahman, F. and Ahamed, S. I. "Efficient Detection of Counterfeit Products in Large Scale RFID Systems with Batch Authentication Protocols", Accepted to be published in Journal of Personal and Ubiquitous Computing, Springer-Verlag. 2012.

[Rahman12d] Rahman, F. and Ahamed, S. I. "DRAP: A Robust Authentication Protocol to Ensure Survivability of Computational RFID Networks", In Proc. of ACM Symposium on Applied Computing (SAC 2012). Italy. 2012.

[Rahman12e] Rahman, F. and Ahamed, S. I. "MonAC: Detecting Missing Tags for Improved Accuracy in Computational RFID based Assisted Environments", In Proc. of the ACM Symposium on Research in Applied Computation (ACM RACS 2012). USA. 2012.

[Reader] http://www.thebarcodewarehouse.co.uk/Assets/Images/Products/16006.jpg

[Rieback06] Rieback, M., Crispo, B., and Tanenbaum, A. The evolution of RFID security. In Proceedings of Pervasive Computing, Vol. 5, No. 1. 2006. 62-69.

[RFID_Journal] http://www.rfidjournal.com/article/print/4613

[Rivera08] Rivera, N., Mountain, R., Assumpcao, L., Williams, A. A., Cooper, A.B., Lewis, D. L., Benson, R. C., Miragliotta, J. A., Marohn, M., and Taylor, R. H. ASSIST - Automated System for Surgical Instrument and Sponge Tracking. In Proceedings of the IEEE International Conference on RFID. Las Vegas, Nevada, USA 2008.

[Rieback07] Rieback, M., Crispo, B., and Tanenbaum, A., et al. (2006). The evolution of RFID security. In the Journal of IEEE Pervasive Computing. Vol 5, Num. 1. pp. 62-69.

[Roussos08] Roussos, G. and Kostakos, V. "RFID in pervasive computing: state-of-the-art and outlook". In Elsevier journal of Pervasive and Mobile Computing, Vol 5, No 1. 2008. pp. 110 - 131.

[Sample07] Sample, A. P., Yeager, D. J., Powledge, P. S., and Smith, J. R. Design of a passively-powered, programmable platform for UHF RFID systems. In Proceedings of Conf. on RFID. 2007. 149-156.

[Salajegheh09] Salajegheh, M., Clark, S., Ransford, B., Fu, K., and Juels, A. CCCP: Secure remote storage for computational RFIDs. In Proceedings of USENIX security symposium. 2009. 215-230.

[Saxena07] Saxena, S. Ganguly, S. Bhatnagar, R. Izmailov. "RFInD: an RFID-based system to manage virtual spaces". In Proc. of Pervasive Computing and Communications Workshops (PerCom Workshops 2007). 2007. pp.382-387.

[Saxena10] Saxena, N. and Voris, J. Still and Silent: Motion Detection for Enhanced RFID Security and Privacy without Changing the Usage Model. In Proceedings of the Workshop on RFID Security. 2010.

[Segawa09] Segawa, N. Behavior Evaluation of Sika Deer (Cervus Nippon) by RFID System. In WISP Summit. 2009.

[Seo06a] Seo, Y., and Kim, K., et al. (2006). Scalable and untraceable authentication protocol for RFID. In Proceedings of the International Workshop on Security in Ubiquitous Computing Systems (Secubiq 06), Lecture Notes in Computer Science, Seoul, Korea.

[Seo06b] Seo, Y., Lee, H., and Kim, K., et al. (2006). A lightweight authentication protocol based on universal re-encryption of RFID Tags. Available at: caislab.icu.ac.kr/Paper/paper_files/2006/CISC_1115_Youngjoon.pdf

[Shannon48] Shannon, C. "A mathematical theory of communication". In Bell System Technical Journal, Vol. 27, 1948. pp. 379-423 and 623-656.

[Sheng09] Sheng, B., Li, Q., and Mao, W. "Efficient Continuous Scanning in RFID Systems". In Proceedings of IEEE INFOCOM. 2009. pp. 1- 9.

[Song09] Song, B., (2009). RFID authentication protocols using symmetric cryptography. Thesis.

[Srivastava01] Srivastava, M. B., Muntz, R. R. and Potkonjak, M. Smart kindergarten: sensor-based wireless networks for smart developmental problem-solving enviroments. In MOBICOM, pages 132–138, 2001.

[Stallings99] Stallings, W. Cryptography and Netwrok Security: Principles and Practice. Prentice Hall, Upper Saddle River, New Jersey, second edition, 1999.

[Tan08] Tan, C. C., Sheng, B. and Li., Q. “How to monitor for missing RFID tags”. In Proc. of ICDCS 08. 2008. pp. 295-302.

[Tsudik06] Tsudik, G., (2006). YA-TRAP: yet another trivial RFID authentication protocol. In Proceedings of the International Conference on Pervasive Computing and Communications (PerCom 06), IEEE, IEEE Computer Society. New York, USA. pp.-643.

[Turcu09] Turcu, C. E., Turcu, C. and Popa, V. An RFID-Based System for Emergency Health Care Services. In Proc.of WAINA ‘09. USA, pp. 624-629.

[UIUC] http://www.cs.uiuc.edu/homes/zaher/cyberphysical/sensors.html (last accessed: 27th Feb. 2010)

[Vogt02] Vogt, H. “Efficient Object Identification with Passive RFID Tags,” Proc. of IEEE PERCOM, 2002.

[Wang04] Wang, B.T., and Schulzrinne, H. An IP traceback mechanism for reflective DoS attacks. In Proceedings of Canadian Conference on Electrical and Computer Engineering, Vol. 2, 2004. 901 - 904.

[Wang06] Wang, Y., Attebury, G., and Ramamurthy, B. A survey of security issues in wireless sensor networks. In IEEE Communication. Surveys Tutorials, vol. 8. 2006. 2–23.

[Weis03] Weis, S. “Security and privacy in radio-frequency identification devices”. Master thesis, Massachusetts Institute of Technology (MIT), Massachusetts, USA, 2003.

[Weis04] Weis, S., Sarma, S., Rivest , R., and Engels , D. “Security and privacy aspects of low-cost radio frequency identification systems”. Lecture notes in Computer Science, 2004.

[Weiser91] Weiser, M. The computer for the twenty-first century. Scientific American, 265(3):95–104, September 1991.

[WikiTag] Source: http://en.wikipedia.org/wiki/File:Tags.jpg

[Weiser93] Weiser, M., (1993). Some computer science problems in ubiquitous computing. In Communications of the ACM, Vol. 36, No. 7. pp. 75-84.

[Wessel05] Wessel, R. "RFID bands at the Jacobi Medical Center". 2005. Last accessed - March 2012 at http://www.rfidgazette.org/2005/12/rfid_bands_at_t.html].

[Wood03] Wood, A. D., Stankovic, J. A., and Son, S. H. JAM: A Jammed-Area Mapping Service for Sensor Networks. In Proceedings of Real-Time Systems Symposium. 2003. 286-297.

[Yang07] Yang, N. Z. N., Barringer, H. A purpose-based access control model. In Proc. of IAS. 2007, pp. 143–148.

[Yao09] Yao, Q., Qi, Y., Han, J., Zhao, J., Li, X. and Liu, Y. et al. (2009). Randomizing RFID private authentication. In Proc. of Pervasive Computing and Communications Workshop (PerCom Workshops 09). pp.1-10.

[Yao10] Yao,W., Chu, C., and Li, Z. The Use of RFID in Healthcare: Benefits and Barriers. In Proceedings of the IEEE International Conference on RFID-Technology and Applications. 2010.

[Yeager08] Yeager, D.J., Powledge, P.S., Prasad, R., Wetherall, D., Smith, J.R. Wirelessly-Charged UHF Tags for Sensor Data Collection. In Proceedings of the Conference on RFID. 2008. 320-327.

[Yang10] Yang, L., Han, J., Qi, Y. and Liu, Y. "Identification free batch authentication for RFID tags". In Proc. of ICNP. 2010. pp.154-163.

[Yunhao03] Ni, L.M., Yunhao, L., Yiu, C. L., Patil, A.P. “LANDMARC: indoor location sensing using active RFID”. In Proc. of Pervasive Computing and Communications (PerCom 2003). 2003. pp. 407- 415.

[Zecca09] Zecca, G., Couderc, P., Banatre, M., Beraldi. R. “Swarm robot synchronization using RFID tags”. In Proc. of Pervasive Computing and Communications (PerCom 2009). 2009. pp.1-4.

[Zhen05] Zhen, B., Kobayashi, M., and Shimizui, M. Framed aloha for multiple RFID objects identification. In IEICE Transactions on Communications, vol. E80-B, no. 3. 2005. 991–999.

Chapter 12: Appendix

Glossary of Terms

Term	Definition
Anonymity	Anonymity is the state of not being identifiable within a set
Authentication	Authentication means the act of confirming someone (or something) as authentic.
Backend server/ central server/ backend database	A backend server is a trusted server that contains all the information of all tags in RFID system and it can access these information from its database by using the tag's response as a key
Eavesdropping	Eavesdropping is the act of secretly listening to the private conversation between two parties
Gen 2	The second generation air interface for communication between an RFID reader and tag, administered by EPC global Inc. It deals with the modulation scheme, packet structure, command language and methods for dealing with collision.
Lightweight Cryptography	Cryptographic operations that require low computational and processing power to be performed
Nonce	A random number that never repeats its value
Pervasive computing	Pervasive computing provides an environment where information and services can be accessed remotely from the environment specially through wireless technologies
Privacy	The notion of controlling where, when, to whom and what amount of information is provided to the external entities

Public key cryptography	A class of algorithms for cryptography that use a pair cryptographic key: public key (known to public) and private key (known only to the owner).
RFID systems	RFID is an abbreviation of Radio Frequency IDentification. It is a data collection technology that uses electronic tags for storing data.
RFID tags	A microchip attached to an antenna that is packaged in a way that it can be applied to an object. The tag picks up signals from and sends signals to a reader. The tag contains a unique serial number.
Reader	A device used to communicate with RFID tags. The reader has one or more antennas, which emit radio waves and receive signals back from the tag.
Security	Process of creating a computing platform that ensures only allowed actions are performed.
Symmetric key cryptography	A class of algorithms for cryptography that use shared secret cryptographic keys
WISP	WISP stands for Wireless Identification and Sensing Platform. WISPs have the capabilities of RFID tags, but also support sensing and computing.