PREVENTION AND DETECTION MECHANISM FOR SECURITY IN PASSIVE RFID SYSTEM

KHOR JING HUEY

UNIVERSITI SAINS MALAYSIA

2013

PREVENTION AND DETECTION MECHANISM FOR SECURITY IN PASSIVE RFID SYSTEM

by

KHOR JING HUEY

Thesis submitted in fulfillment of the requirements
for the degree of
Doctor of Philosophy

October 2013

ACKNOWLEDGEMENTS

First and foremost, my deepest appreciation goes to my dedicated supervisor, Associate Professor Dr. Widad Ismail for her valuable support, patient guidance, and constructive comments throughout the course of my research. A special appreciation goes to my co-supervisor, Dr. Mohammad Ghulam Rahman for his advice, guidance and encouragement. I would like to express my gratitude and appreciation to my field supervisor, Mr. Amir Shauqee Abdul Rahman for his guidance and assistant throughout my research.

I would like to acknowledge all the lecturers, technicians and staff of School of Electrical and Electronic Engineering, USM for the kind cooperation and helping hands. Special thank goes to Mr. Latip and Mdm. Zammira for their assist and guidance throughout my experimental works. I would also like to express my deepest gratitude to USM for providing me with Fellowship and Short Term Grant for funding this research.

I would like to express my deepest gratitude to my parents Mr. Khor Kuan Chong and Mdm. Ooi Kim Hong for their endless love, concern and blessing for me to pursue my Ph.D degree. I would also like to express my sincere gratitude to my siblings, Jing Jiun, Boon Khay, Swee Huat, and Wei Chuan for their care, support and understanding throughout my studies.

I would like to extend my gratitude to my dear friends Edmond Chan, Sew Sun, Tow Leong, Eng and Nick for their motivation and concern throughout my time in

USM. I would also like to thank the research group members; Qayum, Farah, Zalina, Chek Ling, Farhana, and Eejay for their guidance and knowledge sharing throughout my research. To all the people who have helped me directly or indirectly throughout my research, your contributions shall not be forgotten. Thank you.

Khor Jing Huey

October 2013

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ACK	Acknowledgement
AES	Advanced encryption standard
ANOVA	Analysis of variance
ASK	Amplitude-shift keying
AUC	Area under receiving operating characteristic curve
AVISPA	Automated validation of internet security protocols and applications
CAGR	Compound annual growth rate
CBC	Cipher block chaining
CL-AtSe	CL-based attack searcher
DES	Data encryption standard
DoS	Denial of service
DMX	Decoding matrix unit
ECC	Elliptic curve cryptography
EER	Equal error rate
EPC	Electronic product code
FA	False acceptance
FAR	False acceptance rate
FR	False reject
FRR	False rejection rate
GCD	Greatest common divisor
GE	Gate equivalent
Gen 2	EPCglobal Class-1 Generation-2
GUI	Graphical user interface
HB	Hopper and Blum
HF	High frequency
HLPSL	High-level protocol specification language
IF	Intermediate format

JDBC	Java database connectivity
LCG	Linear congruential generator
LF	Low frequency
LFSR	Linear feedback shift register
LPN	Learning parity with noise
MCMC	Malaysian Communications and Multimedia Commission
MD5	Message digest-5
MDC	Modification detection codes
MMS	Miller-modulated subcarrier
NIST	National Institute of Standards and Technology
OFMC	On-the-fly model-checker
PC	Protocol control
PIE	Pulse-interval encoding
P_{NUI}	Non-unequivocal identification probability
PRNG	Pseudo-random number generator
PS	Polynomial selector
ROC	Receiving operating characteristic
RF	Radio frequency
RFID	Radio frequency identification
SATMC	SAT-based Model-Checker
SHA-1	Secure Hash Algorithm-1
SPRA	Scalable pseudo random
T_c	Time cost
TA	True acceptance
TA4SP	Tree automata-based protocol analyzer
TAR	True acceptance rate
Tari	Type A reference interval
TR	True reject
TRA	Tag-then-reader authentication
TRNG	Truly random number generator
UHF	Ultra-high frequency

3DES	Triple data encryption standard

MEKANISMA PENCEGAHAN DAN PENGESANAN DEMI KESELAMATAN DALAM SISTEM RFID PASIF

ABSTRAK

Tag pengenalan frekuensi radio (RFID) kos rendah yang mematuhi piawaian EPCglobal Kelas-1 Generasi-2 adalah sememangnya tidak selamat disebabkan kekangan pengkomputeran. Tesis ini mencadangkan penggunaan mekanisma pencegahan dan pengesanan untuk menyelesaikan isu-isu keselamatan dan privasi. Suatu kriptografi ringan protokol pengesahan bersama yang tahan terhadap penjejakan, penafian perkhidmatan (DoS) dan serangan ulangan adalah dicadangkan sebagai mekanisma pencegahan. Protokol yang dicadang direkakan dengan algoritma kriptografi ringan, termasuk XOR, jarak Hamming, putaran dan penjana linear kongruen (MLCG) yang diubahsuai. Protokol yang dicadang menggunakan 64 bit indeks dibuktikan mempunyai kebarangkalian penafian pengenalan yang terendah. Disamping itu, kerawakan kunci sesi yang dijana daripada MLCG adalah disahkan dengan menggunakan ujian NIST. Selain itu, keselamatan protokol yang dicadang adalah disahkan dengan menggunakan alat analisis formal, AVISPA. Ketepatan protokol yang dicadang ditunjukkan dalam model simulasi yang dibangunkan di Java TCP / soket IP. Seterusnya, protokol yang dicadang dilaksanakan dalam sistem RFID termasuk IAIK UHF Demo tag, TagSense Nano-UHF pembaca dan pangkalan data. GUI diwujudkan dalam bentuk aplikasi Java untuk memaparkan data yang dikesan. Protokol yang dicadang dilaksanakan dalam sistem RFID sebenar melebihi performa daripada protokol lain yang berkaitan kerana masa membaca dan menulis yang digunakan lebih singkat sebanyak 13.46 %. Sistem dibuktikan mampu menghalang penjejakan, DoS, dan serangan ulangan daripada

penyerang dengan keperluan pengiraan yang sederhana berbanding dengan protokol lain yang berkaitan. Disamping itu, kaedah pemadanan cap jari elektronik dicadangkan untuk digunakan sebagai mekanisma pengesanan untuk mengesan tag palsu. Kuasa tag yang diterima dan pembalikkan kuasa tag digunakan sebagai cap jari elektronik dalam kaedah padanan cap jari yang unik. Dua ujian statistik iaitu ujian-t dan ujian ANOVA, digunakan dalam kaedah padanan cap jari. Lima kaedah pemadanan cap jari dibentangkan dan dikategorikan berdasarkan tindak balas kuasa tag dan ujian statistik yang digunakan. Kaedah V yang menggunakan ujian ANOVA bertiga arah untuk menganalisis pembalikkan kuasa tag mempunyai keputusan yang paling tepat. Ini adalah kerana kaedah V yang mempunyai 3 faktor (jenis tag, frekuensi, dan kedudukan) mempunyai kawasan bawah lengkung (AUC) tertinggi (0.999) dan nilai kadar kesalahan yang sama (EER) terendah (0.01). Selain itu, kadar penerimaan palsu (FAR) dan kadar penyingkiran palsu (FRR) yang diperolehi adalah 0.1 % dan 1.3 % setiap satu. Oleh itu, gabungan mekanisma pencegahan dan pengesanan boleh meningkatkan perlindungan sistem RFID untuk mencegah penjejakan, DoS, dan serangan ulangan, serta mampu mengesan tag palsu dengan cekap.

PREVENTION AND DETECTION MECHANISM FOR SECURITY IN PASSIVE RFID SYSTEM

ABSTRACT

Low-cost radio frequency identification (RFID) tags conforming to the EPCglobal Class-1 Generation-2 standard are inherently insecure due to computational constraints. This thesis proposed the use of both prevention and detection mechanisms to solve the security and privacy issues. A lightweight cryptographic mutual authentication protocol which is resistant to tracking, denial of service (DoS) and replay attacks is proposed as a prevention mechanism. The proposed protocol is designed with lightweight cryptographic algorithm, including XOR, Hamming distance, rotation and a modified linear congruential generator (MLCG). The proposed protocol using 64 bits index is proved having the lowest non-unequivocally identification probability. In addition, the randomness of the session key generated from the MLCG is verified using NIST test suite. Besides that, the security of the proposed protocol is validated using the formal analysis tool, AVISPA. The correctness of the proposed protocol is demonstrated in a simulation model developed in JAVA TCP/IP socket. Next, the proposed protocol is implemented in RFID system including IAIK UHF Demo tag, TagSense Nano-UHF reader and back-end database. A GUI is created in a form of JAVA application to display data detected from tag. The proposed protocol implemented in real RFID system outperforms other related protocols because of 13.46 % shorter read time and write time consumed. The system is proved to be able to prevent tracking, DoS, and replay attacks from adversaries with moderate computation requirement compared to other related protocols. In addition, electronic fingerprint matching method is proposed to be used as

detection mechanism to detect counterfeit tags. The received and backscatter powers of tag are proposed to be used as unique electronic fingerprint in the fingerprint matching method. Two statistical tests, namely, t-test and ANOVA test, are used in the fingerprint matching method. Five fingerprint matching methods are presented and are categorized based on the power response of tag and the statistical test used. Method V which uses three way ANOVA test to analyze backscatter power of tag has the most accurate results. This is because Method V which has 3 factors (tag type, frequency, and position), has the highest area under curve (AUC) (0.999) and lowest equal error rate (EER) (0.01) values. Besides that, the false acceptance rate (FAR) and false rejection rate (FRR) obtained are 0.1 % and 1.3 %, respectively. Therefore, the combination of prevention and detection mechanisms can enhance the protection of the RFID system in preventing tracking, DoS, and replay attacks as well as able to detect counterfeit tags efficiently.

CHAPTER 1

INTRODUCTION

1.0 Background

Radio frequency identification (RFID) has been pervasively adopted in many areas, such as supply chain, library, healthcare management, and waste management. An RFID system offers contactless identification, automatic retrieval of data, and wireless data storage (Hagl and Aslanidis, 2009). RFID tags do not require line-of-sight communications. Hence, this technology provides a significant improvement in identification, tracking, monitoring, and stocking of objects compared to barcode technology (Ngai *et al.*, 2008). Data reading using RFID also enhances performance and productivity by increasing the accuracy and speed of information communication. A RFID system can be operated using three basic components, namely, tag, reader, and back-end server. A passive tag stores the object's information in a microchip and data stored can be read remotely using reader (Kim *et al.*, 2006). The reader communicates with the tag in a bidirectional way through the antenna. The tag and the reader must work at the same specified frequency and comply with same regulations and protocols to guarantee the compatibility of the communication system (Ngai *et al.*, 2007). The back-end server uses middleware to filter and store all the information in the tag. A middleware platform filters input data and emits them to the application.

Counterfeiting is prevalent throughout the world, especially in the pharmaceutical and information technology sectors (Staake *et al.*, 2005). Global counterfeit industries generate an estimated $670 billion annually

(MarketsandMarkets, 2010). Therefore, manufacturers started to utilize RFID technology to fight counterfeiting issues (Piramuthu, 2008, Tuyls and Batina, 2006, King and Zhang, 2009, Li and Lim, 2009). RFID that offers contactless identification and automatic data management enables real-time monitoring of authentic products (Hagl and Aslanidis, 2009). Global RFID market is expected to grow at a compound annual growth rate (CAGR) of roughly 17 % to a value of approximately $9.7 billion in the period 2011 to 2013 (Rncos, 2010). Rapid growth in RFID market is triggered by emerging usage of RFID technology in various applications.

Based on market lifecycle analysis of 2009, Asia Pacific has the potential to overtake Europe by year 2020 in level of activeness of national RFID programs implemented. Malaysia has a mature RFID market compared to other Asia Pacific countries. Based on market observation, the Malaysian RFID market in 2009 reached approximately $9.5 million. The RFID market is anticipated to further grow to roughly $33.8 million by the end of 2016 with a CAGR of 19.8 % (Sebastian, 2010). During the period 2011 to 2015, several core sectors in Malaysia including government service sector, manufacturing sector, agriculture sector, transport and communication sector and wholesales sector will be granted with a total amount of $1,105 million to develop with RFID technology. Return of investment (ROI) analysis for the five sectors are expected to reach $5,525.6 million (Mcmc, 2010). In addition, with the usage of RFID technology, total factor productivity (TFP) contribution is expected to have an increase of 0.55 % and for labor productivity rate is an increase of $0.247 per nominal gross domestic product (GDP) hour in 5 years duration (Sebastian, 2009).

Malaysian Communications and Multimedia Commission (MCMC) governs Malaysia's RFID frequency allocation. The frequency band for RFID in Malaysia is from 919 MHz to 923 MHz, with a total bandwidth of 4 MHz. RFID equipments manufactured in Malaysia shall be certified under the Communications and Multimedia (Technical Standards) regulations (Minan, 2007). In 1997, the first RFID technology was introduced in Malaysia in which is the Malaysian electronic toll payment system, also known as Touch'n Go system. The first RFID passport (E-passport) in the world is issued by Malaysia in 1998 (Juels *et al.*, 2005). The E-passport contains the information of the holder's travel history including time, date and place of entries and exits from the country. In 2006, the Malaysian Road Transport Department had implemented RFID license plates (Mah, 2008) that contain car owner and vehicle information to enable police officer to detect the location of the stolen car. In addition, the world's smallest RFID microchip (MM chip) with the size of 0.4 mm x 0.4 mm is released under the Malaysia Microchip Project in 2007 (Might, 2007). Hence, Malaysia is in a leading position in Asia in terms of the growth of implementation RFID technology due to several leading edge applications have been implemented and new RFID microchip is delivered.

EPCglobal is the industry-driven reference for RFID standardization that develops standards to describe all the components and architecture of RFID tags, readers, and information systems (Martínez-Sala, 2009). EPCglobal Class 1 Generation 2 (Gen 2) standard is the second generation RFID air interface protocol. This protocol is ratified as ISO 18000-6C by International Organization for Standardization (Razaq *et al.*, 2008). RFID tags that conform to Gen 2 standard are known to be inexpensive and are broadly used in many identification and tracking

methods. Gen 2 tag memory consists of four distinct banks, including bank00 (reserved memory), bank01 (EPC memory), bank10 (TID memory) and bank11 (user memory). An electronic product code (EPC) tag has two security features including kill command to permanently silence a tag and the access command to control the access of a tag memory (Bailey and Juels, 2006). A kill command with a valid 32-bit kill password is used to permanently deactivate a fraud tag. An access command with a valid 32-bit access password is used to trigger a tag into secure state. Tag's information is protected as read or write process could be conducted only when the tag is in the secure state. EPC tags offer higher reliability, greater read range and enhanced security and privacy protection. Hence, the high performance of the EPC tags is the key contributor to the deployment of RFID technology in various applications.

1.1 Problem Statements

RFID protocols that proposed by researchers can be divided into four categories, namely, full-fledged, simple, lightweight, and ultralightweight protocols (Chien, 2007). A full-fledged protocol uses complex cryptographic functions that require intensive computation resource (Feldhofer and Wolkerstorfer, 2007). A protocol is considered as simple protocol if random number generator and hash function are used (Wong *et al.*, 2006). A lightweight protocol uses random number generator and cyclic redundancy code (CRC) function instead of hash function (Chien and Chen, 2007). An ultralightweight protocol requires simple mathematic functions, including bitwise XOR, OR, and AND (Karthikeyan and Nesterenko, 2005, Peris-Lopez *et al.*, 2006c, Peris-Lopez *et al.*, 2009c). However, a Gen 2 tag does not support the expensive asymmetric and the hash function (Juels, 2005). A

complex cryptographic encryption cannot be deployed in a Gen 2 tag for security purpose (Sun and Ting, 2009). Hence, Gen 2 tag is capable to support lightweight and ultralightweight protocols only. The security levels of ultralightweight protocols are weaker than lightweight protocols due to the former protocols are more vulnerable to passive attacks (Hernandez-Castro *et al.*, 2009, Peris-Lopez *et al.*, 2009a).

Many studies have been conducted over the years to find the best solution in improving the security level of Gen 2 ultra-high frequency (UHF) passive RFID tag. The security protection of an EPC tag against eavesdropping, impersonation, and cloning threats is difficult because it has no explicit authentication and security functionalities (Juels, 2005). EPC tags, which are known to be inexpensive, are broadly used in many identification and tracking methods. However, the use of EPC tags is inherently insecure. The most challenging security threats in an RFID EPC tags are privacy threats in terms of eavesdropping and impersonation, as well as threats on tag cloning (Kim *et al.*, 2006, Lehtonen *et al.*, 2009). Hence, an RFID system is vulnerable to suffer from variable attacks including denial of service (DoS) attack, attacking and modifying tag threat, traffic analysis threat and spoofing attack (Yanjun, 2010). The potential invasion of privacy and security due to lack of encrypted message between an RFID reader and a tag has raised various concerns from the public (Chein and Chen, 2009). Privacy threat when a tag number combines with personal information becomes serious where users are exposed to location threat, constellation threat, transaction threat, preference threat, and breadcrumb threat (Kim *et al.*, 2007). The privacy of the public must be protected by ensuring the meaning of

private information transmitted between the RFID reader and the tag is secure from attackers.

EPC tags offer minimal resistance against eavesdropping, which is one of the most serious threats in RFID communication (Rieback *et al.*, 2006). Communication between a legitimate tag and a reader is often unprotected and can be easily intercepted by adversaries. In addition, an EPC tag is vulnerable to impersonation threat because of its characteristic of releasing data information to any compatible reader (Berbain *et al.*, 2009). Impersonation occurs when an entity attempts to gain access to resources and information by pretending and adopting the identity of an authorized user (Mitrokotsa *et al.*, 2008). EPC tags are vulnerable to cloning threats because they do not have explicit anti-cloning features (Choi *et al.*, 2009). These tags have low functionality and cannot perform cryptographic algorithm to prevent tag cloning. EPC tags are exposed to skimming attacks, in which tags disclose vital data and information to any query reader (Razaq *et al.*, 2008). This indicates that EPC tags lack authentication and encryption, which can enable readers to collect information of the tags they scan. Hence, any adversary can gather required information and can manipulate the collected information to clone counterfeit tags (Wong *et al.*, 2006). This information may be used to create counterfeit tags that bear the same information as that of a legitimate tag. Counterfeit tags can be attached to bogus products and disguise these as authentic products in the market (Mirowski *et al.*, 2009, Lehtonen *et al.*, 2007). The counterfeit tag issue is very serious because it is capable of causing a menace ranging from public privacy and safety issues to loss of industry revenues.

1.2 Research Objectives

The aim of this research is mainly to enhance security and privacy for low-cost RFID tags. The main objectives of this research can be summarized as follow:

i. To investigate prevention and detection mechanisms to improve security in low-cost RFID communication system.

ii. To design, analyze, and test a lightweight cryptographic algorithm that conforms to the Gen 2 standard in the aspects of secure from tracking, DoS, and replay attacks for prevention mechanism in real RFID communication system.

iii. To design and evaluate a unique fingerprint matching method to detect counterfeit and legitimate tags efficiently based on tag power response for improved detection mechanism.

iv. To characterize and suggest the proposed prevention and detection mechanisms for low-cost RFID communication system.

1.3 Scope of Work

Both prevention and detection mechanisms are deployed in order to protect RFID system from privacy threats in term of tracking, DoS, replay, and tag cloning attacks. A lightweight cryptographic mutual authentication protocol that using simple mathematical functions, including bitwise XOR, rotation, Hamming distance, and pseudo-random number generator (PRNG) function are designed to protect the data

secrecy. The robustness of designed protocol is analyzed and proved secured by using AVISPA formal analysis tool. A back-end database and graphical user interface (GUI) are developed to create a complete RFID communication system. The proposed protocol is loaded into IAIK UHF demo tag. The proposed protocol is conforming to the Gen 2 standard and is suitable for deployment in a low-cost RFID tag. The specifications of the Gen 2 standard that are applied in the proposed protocol are listed below:

i. RFID system operating in the 919 MHz - 923 MHz frequency range.

ii. Tag modulates a backscatter signal only after receiving the requisite command from a reader.

iii. Tag shall support FM0 modulation with a data rate of 40kb/s for tag to reader communication.

iv. Tag shall support Type A Reference Interval (Tari) value of 25 μs (26.67 kb/s) for reader to tag communication.

v. Tag memory shall be logically separated into four distinct banks, namely, reserved memory, EPC memory, TID memory, and user memory.

In addition, counterfeit tags can be detected by employing electronic fingerprint matching method. Power response of tag, namely, received and

backscatter powers of tag, is used as unique fingerprint information and is stored in database to distinguish between legitimate and counterfeit tags. The efficiency of using the power responses of tag to detect counterfeit tags is proved.

1.4 Design Methodology

A comprehensive study on low-cost passive UHF RFID system, RFID communication air interface standards, RFID tag unique fingerprint, and statistical algorithm for tag unique fingerprint matching method was done. The research was carried out in three phases, namely:

i. Design and analysis of lightweight protocol,

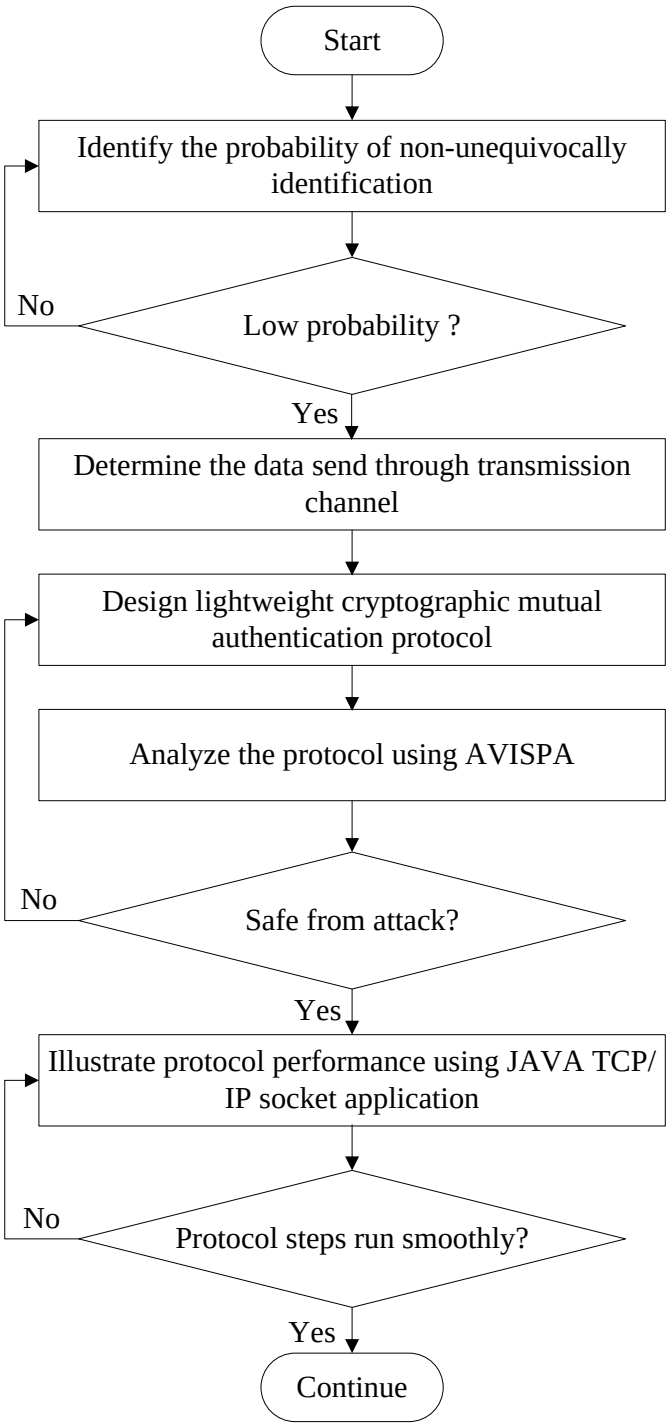
ii. Experimental on reliability of protocol designed,

iii. Identify and match tag unique fingerprint.

In the initial phase, a lightweight cryptographic mutual authentication protocol is designed to increase the security and privacy level of a low-cost RFID communication system. Gen 2 is selected as a benchmarking RFID air interface standards for the communication between RFID reader and tag. The performance and functionality of the proposed protocol is illustrated using a JAVA TCP/IP socket application. TCP Spy is used to capture the data sent and received between the socket communication channels to verify the possibility of man-in-the-middle attacks. AVISPA security protocols validation tool is used to analyse the security level and robustness of protocol designed.

In the second phase, a complete RFID communication system is developed. A GUI is developed by using JAVA and the back-end database is created by using MySQL. The proposed protocol is loaded into the IAIK UHF Demo tag to test the robustness of RFID communication. Experimental measurement is conducted to collect experimental results. The data collected is analyzed and evaluated to prove the reliability of the proposed protocol. Figure 1.1 shows the flowchart of the overall research activities.

In final phase, power response of EPC tags, namely, received and backscatter powers of tag, are deployed as unique fingerprint to detect counterfeit tags. The power response of each tag is measured and stored in the database for further reference. T-test and ANOVA test are used to distinguish between legitimate and counterfeit tag efficiently. The reliability of the statistical tests is tested to match tag unique fingerprint efficiently.


Start
Identify the probability of non-unequivocally identification
No
Low probability ?
Yes
Determine the data send through transmission channel
Design lightweight cryptographic mutual authentication protocol
Analyze the protocol using AVISPA
No
Safe from attack?
Yes
Illustrate protocol performance using JAVA TCP/ IP socket application
No
Protocol steps run smoothly?
Yes
Continue

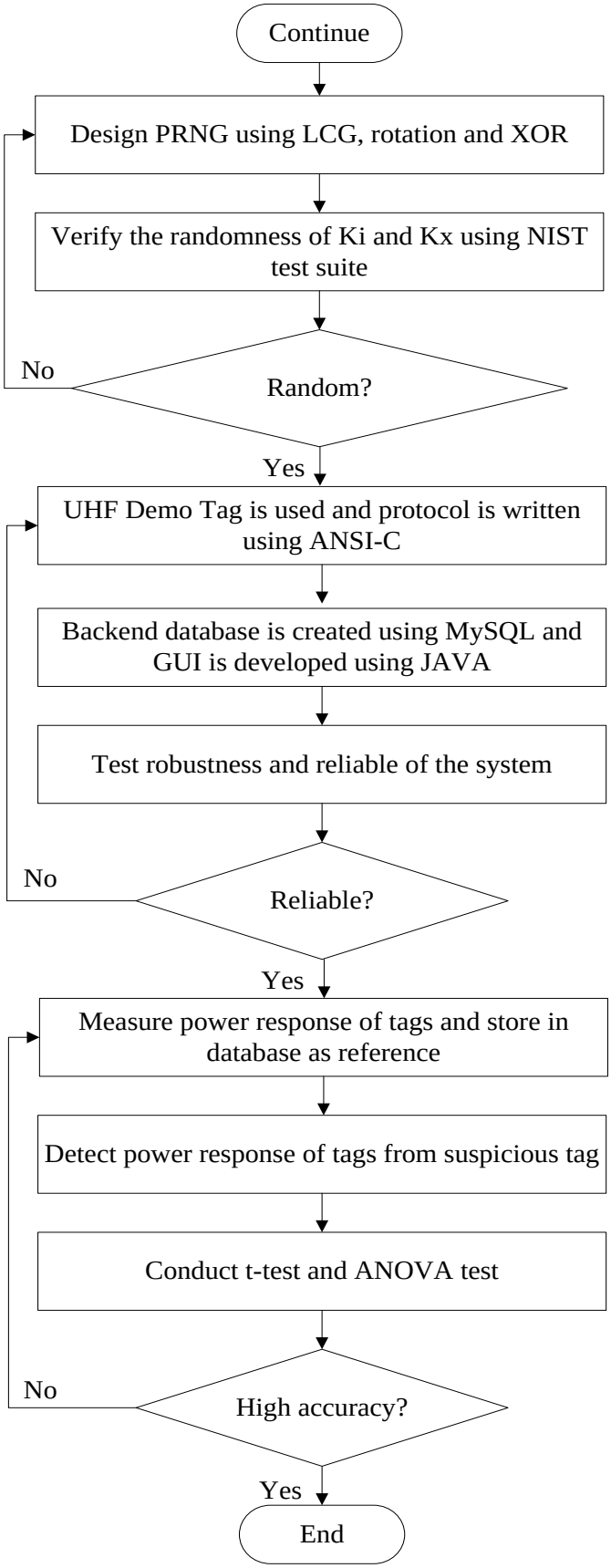


Figure 1.1: Flowchart of research activities

1.5 Thesis Outline

The thesis consists of five chapters. Chapter 1 (Introduction) introduces a brief background on RFID communication system and development history of RFID in Malaysia. The global and local RFID market analysis and an overview of Gen 2 standard is presented in this chapter. The problem statements are described to verify the direction of the research. The research objectives are stated together with the scopes of the project. A brief description of design methodology is elaborated and the overall thesis outline is summarized in the last section of the chapter.

Chapter 2 describes the functionality of basic components in an RFID system. The detailed Gen 2 standard is elaborated in this chapter. This is followed by the description of various type of security threats that facing by the RFID communication system. The most recent lightweight and ultralightweight cryptographic protocols as well as unique fingerprint of tag that proposed by researchers are also presented.

Chapter 3 covers the methodology in designing lightweight cryptographic protocol and electronic fingerprint matching method. The basic mathematical functions which used in designing the cryptographic protocol are described. In addition, AVISPA formal analysis tool used to verify the security of protocol designed is elaborated. The subsequent section is the elaboration of complete RFID system that consists of UHF Demo tag, TagSense reader, GUI, and database of back-end server. The functionality of each component is described in this chapter. Next, the unique electronic fingerprint method is presented.

Chapter 4 shows the implementations, results, and discussion on the analysis of the matching indexes used in the protocol. The design of proposed protocol is presented and the analysis of the designed PRNG is conducted. The security analysis of proposed protocol is verified from the simulation result of AVISPA formal analysis. The possibility to implement proposed protocol is proved by using JAVA TCP/IP socket application. The simulation result of TCP Spy is used to identify the messages that captured in transmission channels. The performance of implementation of proposed protocol in the real RFID communication system is analyzed.

Chapter 5 describes the implementation, results, and discussion on the reliability of fingerprint matching methods. The detailed experimental procedures in conducting measurement of received and backscatter powers of tag are shown. The overview of statistical tests including t-test and analysis of variance (ANOVA) test are presented. Besides that, the efficiency tests, namely, false acceptance rate (FAR), false rejection rate (FRR), receiver operating characteristic (ROC), area under ROC curve (AUC) and error equal rate (EER) are elaborated in this section. The efficiency of the t-test and the ANOVA test in distinguish legitimate from counterfeit tags are verified.

Chapter 6 concludes the overall research findings that reflect the accomplishment of the listed objectives. In addition, some recommendations for future research are suggested to improve the performance of the present research. The recommendations for future research are provided based on the conclusions obtained.

CHAPTER 2

LITERATURE REVIEW

2.0 Introduction

RFID technology was first used in military application, called 'Identify Friend or Foe' during World War II. In recent decade, RFID technology has replaced the barcode system because of its higher reliability, read rate, and read range. The high performance of RFID is a key contributor to the deployment of RFID technology in various applications. Researchers have focused on several research topics related to the RFID communication system. The research topics includes reliable communication in different environments, securing the communication between tags and readers, efficient communication protocols, optimization of characteristics, and ensuring location privacy (Henrici, 2008).

Cryptographic protocols are important in providing a secure communication in RFID system. A RFID protocol has different characteristics, including security, complexity, and performance. The characteristics mentioned depend on several layers in designing the protocol. A RFID protocol can be designed using one or a number of cryptographic primitives. An algorithm in a certain configuration is chosen for each of these primitives. The algorithm is then can be implemented in software to develop various kind of application. Low-cost RFID tags have low complexity because of the computational constraint. The resource scarce environment causes the RFID tags susceptible to various security problems. Hence, the RFID protocol should be designed with the lowest impact of vulnerabilities. The protocol should be designed to reach several goals to enhance the security and

privacy of an RFID system. The goals include maintaining data security; preventing counterfeiting, illegitimate access, unwanted recognition and tracking, as well as coping with DoS attack (Henrici, 2008).

2.1 Basic RFID System

RFID is a technology that allows RFID reader to remotely send command to read and store information on RFID tag. An RFID system comprises of three major components, namely, RFID reader, tag, and back-end system. RFID middleware application uses multiple scripting languages, including JavaScript, extension markup language, and hypertext preprocessor (PHP) (Mitrokotsa *et al.*, 2008).

2.1.1 RFID Reader

An RFID reader consists of an antenna, a microprocessor, and an interface device for forwarding data to the back-end system (Henrici, 2008). RFID reader communicates with tag and back-end system by receiving and sending data in the transmission channel. In addition, RFID reader is able to write data into tag memory, authenticates tag as well as powers up passive RFID tag via electromagnetic field. RFID readers can be categorized into two categories, namely, stationary reader and mobile reader (Kamoun, 2009). Stationary readers have a fixed location and network connection. In contrast, mobile or handheld readers can be moved around that offer more flexible applications.

2.1.2 RFID Tag

An RFID tag consists of antenna, microchip and encapsulation. RFID tag can be classified based on its functionality, power supply, and operating frequency.

i. Functionality

RFID tags have memory size from a single bit up to several kilobytes. Tag memory technologies are categorized into non-volatile and volatile storages. The non-volatile storage includes read only, write once, read many (WORM), and read/write. The volatile storage is used for performing calculation after tag power up. Tag can be classified into five broad classes based on the tag computation capability (Bailey and Juels, 2006).

Class 1: Passive read-only tags offer only basic functionality, including a fixed EPC identifier, a tag identifier, kill function, and optional password-protected access control.

Class 2: Passive tags offer same functionality as Class 1 but with read-write memory as well as extended tag identifier, user memory and authenticated access control.

Class 3:Semi-passive tags offer all Class 2 functionality as well as possess sensor and on-tag power source.

Class 4: Active tags offer all Class 3 functionality as well as tag-to-tag communications and ad-hoc networking.

Class 5: Active tags can communicate with all classes of tags.

ii. Power supply

Passive tag obtains power from the electromagnetic field of reader. The tag does not have an internal source of power. Semi passive tag has own power supply for the microchip but communicate by obtaining energy from the electromagnetic field of reader. Active tag

uses own source of power (i.e. battery) to support all activities. Hence, active tag has more functionality and able to communicate over a longer distance compared to passive tag. However, passive tag outperformed active tag in terms of cost, size, and lifetime. This is because passive tag offers low-cost, small size and economic lifetime due to no internal source of power.

iii. Operating frequency

The operating frequency of a tag is categorized into four categories to enable communication between tag and reader. The electromagnetic spectrum consists of low frequency (LF) (125-134 kHz), high frequency (HF) (13.56 MHz), UHF (860- 960 MHz), and microwave (2.54-5.8 GHz) (Hagl and Aslanidis, 2009). Different frequencies have different physical properties. HF tags are designed to carry more data and longer read range. LF tags offer better signal penetration of objects and have little absorption through liquid (Zuo, 2010).

2.1.3 Back-end System

A back-end system is required to process data obtained from tags. A back-end system consists of two parts, namely, middleware and applications. Middleware plays an important role in back-end system to perform all data grouping and filtering tasks (Ghayal *et al.*, 2008). Middleware is used to provide unified interface and semantics towards various applications. The middleware should be designed with full-features and be able to support different hardware (Lin *et al.*, 2009). The middleware acts as a server to connect hardware at one end and support a number of

applications at another end. Applications are the software components that act as an end user interface of a complete RFID system. Applications are used to interpret the data obtained from reader and configure the middleware.

An RFID middleware consists of four layers, namely, reader interface, data processor and storage, application interface, and middleware management.

i. Reader interface

Reader interface is the lowest layer of middleware that used to handle interaction with the hardware.

ii. Data processor and storage

This layer processes all the raw data obtained from the reader by storing, filtering, and grouping the obtained data.

iii. Application interface

This layer configures the RFID middleware by providing an API for the applications. The layer manages the application with the interface of middleware.

iv. Middleware management

This layer manages the configuration of middleware by providing information to the processes running in the middleware.

2.1.4 Advantages of RFID Technology

RFID technology is able to replace the barcode system because RFID technology offers better performance and functionality. RFID technology outperforms barcode system with the following properties.

i. No line of sight requirement
ii. Read and write capability of the tag memory
iii. Higher data capacity
iv. Higher data rate
v. Longer reading range
vi. Multiple tag read capability
vii. Reusability of the tag
viii. Resistance to environmental influence
ix. Durability and reliability

Migration from HF RFID system to UHF RFID system promises a more reliable, effective, real time, and scalable data management system. UHF RFID readers are able to detect multiple tags simultaneously. UHF technology is less prone to distortion error caused by tags overlay each other compared to HF technology. In addition, UHF RFID system offers longer read range and faster read rate than barcode and HF RFID systems. The higher UHF RFID reader detection rate characteristic guarantees an easier scanning process for tracking activities. Ubiquitous UHF RFID data management system enables real-time data sharing and tracking for heterogeneous applications.

2.1.5 RFID Technology in Data Management

Malaysian libraries implemented barcode system in managing materials in the past decade. However, the barcode system has slow read rate and requires line of sight detection. On the contrary, RFID technology offers better and efficient managing system. In year 2007, Multimedia University (MMU) has implemented HF RFID technology to facilitate library search and enable multiple books tracking in real time (Rahman, 2007). Smart Shelf is a device that used to pinpoint the exact location of books in library. The device communicates in 13.56 MHz and exploits the short-range RFID technology. It can automatically identify books within a distance of 30 cm relative to the shelf and can detect whether a book is being misplaced, missing or rented. The device is deployed to facilitate library search and enable multiple books tracking in real time. In year 2009, Penang Public Library has become Malaysia's first library to implement an RFID system compliant to the Gen 2 standard. The library deploys an automated RFID self-check-in and self-check-out station that enables patrons to manage their own transactions, review their account status, and renew materials in real time. The system uses RFID tags which has fast reading rate and the data is recorded using an RFID inventory management system. Hence, accurate and fast inventory on its vast quantity of library assets is guaranteed. In addition, the system is equipped with anti-theft UHF reader with a detection range of 7 meters that triggers an alarm when it detects tagged books that have not been coded as borrowed exiting the library.

Malaysian government has allocated $1,105 million for development of core sectors using RFID technology under the Tenth Malaysia Plan (RMK-10) for the period of 2011 to 2015. From the allocation, a sum of $232.11 million is provided for infrastructure development (Minan, 2007). Hence, strategies for a national RFID

roadmap are planned for the next five years. One of the plans is the development of Malaysian RFID port that offers less queue time at the gate. This is because clearance process would be more efficient due to the container data can be verified by officers instantly using hand-held reader. In addition, RFID postal in managing mails for government agencies within Putrajaya is deployed. All the mails and street posting box are attached with passive RFID tags. The implementation of RFID technology can ensure that all the mail items are delivered to correct government agencies on time. The location, date and time of delivery can be guaranteed to prevent any loss or incorrect delivery of mail items (Mcmc, 2010).

RFID technology has evolved to transform data management system into more efficient and reliable system. Many studies are conducted to implement RFID system in data managing system, including attendance, libraries, and healthcare system. Derakhshan *et al.* discussed the research problems associated with different layers of the suggested system architecture for RFID data management (Derakhshan *et al.*, 2007). Three architecture layers were examined to determine the related research problems, including layers for data capture, business process, and enterprise application. Behera and Kushwaha showed the adoption of RFID technology for attendance monitoring (Behera and Kushwaha, 2009). The system was developed to detect the presence of tags, acknowledge the presence of the user, and push the data to the back-end system. UHF antenna was utilized to make people management system completely ubiquitous. The application programming interface (API) was designed to become the same core that could be used as a common interface in any middleware application. Najera *et al.* presented the integration of RFID technology in two specific healthcare scenarios (Najera *et al.*, 2011). A medical equipment

tracking system based on passive UHF RFID for healthcare facilities was analyzed to enable both real-time location and theft prevention. A solution for the care and control of patients based on passive HF RFID was also illustrated in their paper. A backup data source from the wristband of the patient was used to provide an offline working mode, aiming to increase application reliability in case of network failure. Ching and Tai formulated a set of criteria to evaluate UHF RFID against HF RFID as a possible library service transformation tool (Ching and Tai, 2009). Two pilot tests were conducted by them to evaluate the two technologies. The results showed that UHF RFID outperformed HF RFID in terms of tag reading rate, multiple item detection rate, orientation of tag detection, read range, and sensitivity of detection gates.

2.2 Gen 2 Standard

Gen 2 standard is the second generation RFID air interface protocol developed by EPCglobal. This standard defines specifications for a complete communication link between RFID reader and tag, including the physical layer, collision arbitration algorithm, command and response structure, and data-coding methodology (EPCglobal, 2005). The RFID system is operated in the frequency range between 860 MHz and 960 MHz. MCMC allocates frequency band between 919 MHz and 923 MHz for the RFID operating frequency in Malaysia. The standard offers faster read and write speed, lower misread tag probability, enhanced security and privacy, and anti-collision capability (AlienTechnology, 2005). Gen 2 standard is designed to meet a balance between functionality and cost. Hence, the low production costs of EPC tags are striking worldwide deployment of UHF RFID technology.

2.2.1 Physical Layer

The communication link between reader and tags is half-duplex. A reader receives information from tags by transmitting an unmodulated radio frequency (RF) carrier and listening for a backscattered reply. A reader modulates an RF carrier using double-sideband amplitude shift keying, single-sideband amplitude shift keying, or phase-reversal amplitude shift keying. All the modulations use a pulse-interval encoding (PIE) format as shown in Figure 2.1. Based on the PIE symbols, Tari is the reference time interval for reader to tag signalling. Tari is also the duration of a data-0. The high value indicates carrier wave and the low value indicates attenuated carrier wave. Tari values in the range of 6.25 µs and 25 µs shall be used for the duration of an inventory round. PIE encoding is used in reader to tag communications because it is able to provide ample radio frequency energy to power up tags.

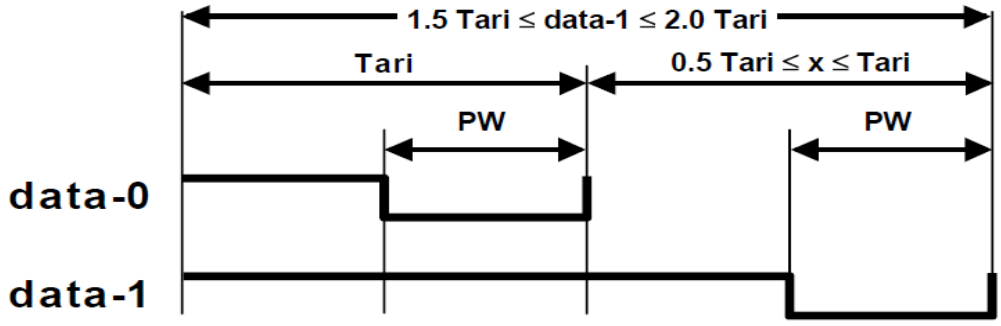


Figure 2.1: PIE symbols (EPCglobal, 2005)

The tags receive the operating energy from the same modulated RF carrier. The tags communicate information by backscatter modulating the amplitude or phase of the RF carrier. The tags shall encode the backscattered data as either FM0 or Miller-modulated subcarrier (MMS) in response to reader commands.