FORMAL VERIFICATION OF RFID SYSTEM USING MODEL VERIFICATION AGENT

MUHAMMAD TARMIZI BIN LOCKMAN

UNIVERSITI TEKNOLOGI MALAYSIA

FORMAL VERIFICATION OF RFID SYSTEM USING MODEL VERIFICATION AGENT

MUHAMMAD TARMIZI B. LOCKMAN

A thesis submitted in fulfillment of the
requirements for the award of the degree of
Master of Science (Computer Science)

Faculty of Computer Science and Information Systems
Universiti Teknologi Malaysia

JANUARY 2012

Dedicated to my dear parents, Mr Lockman Shariff and Mrs Rusni Salleh, my supportive colleagues and my friends. Thank you very much for you motivation, support and understanding.

ACKNOWLEDGEMENT

I wish to extend my appreciation to those who have contributed directly and indirectly to the preparation of this research. I would like to thank and express my gratitude especially to my supervisor, Assoc. Prof. Dr. Ali Selamat, for his commitment in terms of time and advice. Throughout my research, he has encouraged me to develop independent thinking and research skills. He stimulated my analytical thinking and greatly assisted me with the scientific writing. His support and passion towards this research has encouraged me to complete this thesis.

Special thanks to Assoc. Prof Dr Wan Mohd Nasir and Assoc. Prof Dr Siti Zaiton who were the examiners for the first assessment of my masters. They had provided valuable comments and suggestions for my research directions. A special word of thanks also goes to the Ministry of Science, Technology & Innovation (MOSTI), Malaysia and Research Management Center, Universiti Teknologi Malaysia (UTM), in providing financial support under the Vot 79200 for this research.

Last but not least, I would like to express my gratitude and appreciation to my family and friends for all their encouragement, inspiration and patience they had given at every step during the whole research progress.

ABSTRACT

Radio Frequency Identification (RFID) technology has brought about revolutionary changes to software system development that supports major applications in advanced business and asset management. Over the years, many RFID applications have been implemented and integrated into the existing system especially in asset management. When the number of RFID devices and system connected to the existing system increases, the network traffic will be overloaded and congested. This would cause problems in reading the RFID tags and could reduce the effectiveness of the existing system in operation. Although many researches have been done on the RFID system, research on formal verification of RFID system has not yet been fully explored. In this thesis, the architecture of a Model Verification Agent (MVA) is presented to verify the processes involved in the RFID utilizations based on the properties of format, syntax and slot of time. In comparison to conventional techniques such as testing and simulation of tracking errors, this thesis proposes a MVA approach to formalize the RFID processes in RFID system. The architecture of MVA is applied on the case study of RFID applications using the MVA to support the verification process. The formal specification language of MVA is designed using Linear Temporal Logic (LTL) and this is supported by the Communication Sequence Processes (CSP) in Concurrency Workbench of New Century (CWB-NC) tool. Two case studies have been used to validate the proposed model; RFID embedded smart card and RFID shopping system. Specifications in the MVA have proven to improve the efficiency of the RFID process based on the properties of the specified RFID system. Finally, the use of MVA has demonstrated that the approach is able to identify errors in the specifications of the RFID system design. This research will assist developers to find errors and improve the implementation of RFID based system developments for various applications.

ABSTRAK

Teknologi Pengenalan Frekuensi Radio (RFID) telah membawa revolusi kepada pembangunan sistem perisian untuk menyokong aplikasi utama dalam perniagaan dan pengurusan aset. Beberapa tahun kebelakangan ini, aplikasi RFID telah banyak dilaksanakan dan diintegrasikan dengan sistem yang ada terutama dalam pengurusan aset. Apabila bilangan perkakasan dan sistem RFID yang bersambungan pada sistem sedia ada meningkat, trafik pada sistem rangkaian akan mengalami limpahan dan sesak. Hal ini akan menyebabkan masalah untuk membaca tag RFID dan seterusnya mengurangkan keberkesanan operasi pada sistem sedia ada. Walaupun banyak kajian telah dilakukan pada sistem RFID, kajian ke atas pengesahan formal RFID masih belum dieksplorasi secara meluas. Dalam tesis ini, seni bina Ejen Pengesahan Model (MVA) dipersembahkan untuk menentusahkan proses yang terlibat dalam penggunaan RFID berdasarkan ciri-ciri format, sintaks dan sela masa. Sebagai perbandingan, teknik konvensional seperti ujian dan simulasi pengesanan kesilapan, tesis ini mencadangkan MVA digunakan untuk memformalkan proses di dalam sistem RFID. Seni bina MVA diterapkan di dalam kajian kes sistem RFID yang mana MVA digunakan untuk menyokong proses pengesahan. Bahasa spesifikasi formal MVA direka dengan menggunakan Logik Linear Waktu (LTL) dan ini disokong oleh Proses Urutan Komunikasi (CSP) di dalam alat Keserentakan Meja Kerja di Abad Baru (CWB-NC). Dua kajian kes telah digunakan untuk mengesahkan model yang dicadangkan; iaitu sistem RFID kad pintar dan sistem RFID membeli-belah. Spesifikasi MVA telah membuktikan peningkatan kecekapan RFID berdasarkan sifat-sifat sistem RFID yang dinyatakan. Akhir sekali MVA telah menunjukkan bahawa pendekatan ini mampu mengenal pasti kesilapan pada spesifikasi reka bentuk sistem RFID. Kajian ini akan membantu pereka bentuk sistem untuk menentukan ralat dan memperbaiki pelaksanaan pembangunan sistem berasaskan RFID dalam pelbagai aplikasi.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

BDD	-	Binary Decision Diagram
CTL	-	Computational Tree logic
CWB-NC	-	Concurrency Workbench of New Century
CSP	-	Communication Sequence Process
FDR	-	Failure Divergence Refinement
HDL	-	Hardware Description Language
KQML	-	Knowledge Query and Manipulation Language
LCC	-	Lightweight Coordination Calculus
LTL	-	Linear Temporal Logic
MAP	-	Multi Agent Protocol
MAS	-	Multi Agent System
MVA	-	Model Verification Agent
PLA	-	Physical Layer Agent
PMS	-	Progress Monitoring System
PTL	-	Propositional Temporal Logic
QoS	-	Quality of Services
RFID	-	Radio Frequency Identification
RP	-	Symbol for "Read" for reading process in RFID System
SDLC	-	System Development Life Cycle
SMV	-	Symbolic Model Verifier
TCTL	-	Time Computational Tree Logic
TLA	-	Top Layer Agent
VIS	-	Verification Interacting with Synthesis

LIST OF SYMBOLS

□	-	LTL symbol for "now" and "forever"
→	-	LTL symbol for "now" or "sometime" in the future
∀	-	LTL symbol for "for all" or "always" true
¬	-	LTL symbol for "negation"
◊	-	LTL symbol for "eventually" or "not" never true
|=	-	LTL symbol for "satisfy"
Λ	-	LTL symbol for "and"
V	-	LTL symbol for "or"
Iff	-	LTL symbol for "if and only if"
< >	-	Spin symbol for "eventually"
φ	-	Properties
AP	-	Symbol for atomic proposition
v	-	Symbol for "valid"
i	-	Symbol for "invalid"
f	-	Symbol for "fuzzy"
δ	-	Symbol for total transition relation
	-	Symbol for labeling function in Kripke Structure
C	-	The Kripke Structure symbol for "subset"

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Introduction

RFID is referred to as radio frequency identification. This technology is suitable for identification and detection of object within a certain radius of area. RFID works with automatic recognition and identification, by retrieving the information using the RFID tags. This tag can be installed into an item or person for recognition and tracking the asset (Harold and Eric, 2007). In accordance with the evolution of the RFID, it is one of the important services in the supply chain management and asset management that offer a better performance in the industry and business activity. Most of the business operations used a conventional system to manage their assets that can affect the performance and quality of services (QoS) (Asif and Mandviwalla, 2005; Strassner and Fleisch, 2005). With the rapid growth of business operation and management, RFID is used to introduce several fast and cost-saving tools for asset management and problem-solving for identification.

Thus, it will reduce the processing time and human involvement by implementing detection and product management using the RFID in the conventional system (Michael and McCathie, 2005).

In the software System Development Life Cycle (SDLC) there are several important factors that need to be taken seriously which are during the phase of requirement analysis and design. The reason of the requirement analysis is to determine the user expectations that will be satisfied by the condition of the system. Moreover it can reduce the errors caused from ambiguous requirements of the various users. The important goal of design phase is to satisfy the software requirements specification and describe the structure of the system by decomposing the system into its logical components. The design then will translate the requirements into a representation of the software that can satisfy the user requirement before the development phase begins. The requirements analysis can be obtained through the specification and the models of the systems. Most developers write the specifications in natural languages. However they cannot confirm the correctness of the system when specifying the behavior of an integrated and complex system. Formal method is a solution that can overcome this issue in which it is preferred to be used in system development phase (Beckert *et al.,* 2006). This is because the systems properties can usually be specified clearly and detailed in a formal language as it is represented by the mathematical approach.

Currently, the RFID system has been improved by system developers in many problem such as building security and inventory management. The capabilities of the RFID system is the variation of it usages compared to the main RFID system tasks of tracking and identification. Although the results are impressive, problems can still occur in the system when many components are unable to communicate with each other (Michael and McCathie, 2005). There are issues in several cases of the RFID systems that were identified previously when the unpredictable risk in operations occurred in the computing processes. For example an error in identified group of item that need to send in the export container can affect and reduce the efficiency in processing and can be more problematic when dealing with the trust and

satisfaction of user. To avoid and trace this problem, the specification of the backend of the system is needed to specify by ensured that the system is built right. Thus, a formal verification using model checking can be implemented to handle the risk of the RFID system. Researchers have successfully employed the model checking technique in the formal verification of the distributed systems, including hardware components, communication protocols and security protocols. Probabilities for each of the errors of the system can be identified by the unique counter example process to identify the unseen errors and bugs for the concurrent states. At the same time, model checking can perform automatically with an exhaustive search to determine whether the specification is true or not (Edmund *et al*., 1999).

Nowadays, most of researchers in the formal method community has shown an interested in model checking approach with the performance of an excellent result. (Bonnie *et al.*, 2005) denoted that the model checking is able to aid the design. (Xiao and Li, 2006) has proved that the analysis and verification using model checking is competent to support the security protocols. (Wimmer *et al*., 2008) has investigated the probabilistic of model checking tools and the results seemed to be reliable. (Roberson *et al*., 2008) has proved that model checking is an efficient approach for a convenient method of the type system. Previously, all these efforts have significant contributions in their own rights and interests in which some of the area is incredible but the verification on the RFID system is still lacking in the research.

Therefore, in this thesis a formal verification agent based on the RFID systems has been modeled with model checking in a formal method approach is proposed. The proposed model verification can be verified by the specification and model of the RFID system in order to meet the system specification and requirement. The following sections state the problem background of this work, problem statement, hypothesis, aim, objectives, scopes, significance of the research and thesis organization.

1.2 Problem Background

RFID technologies have been used in various areas, especially in the area of supply change management and asset tracking. Reliable data transfer between the layers of the RFID system from bottom layer to the upper layer need to be managed properly when readers read the raw data from the tag. This is because the reader needs to extract the raw data and classify the original data to the backend of the RFID system and the RFID middleware is the way to achieve that. However, the risk faced by the uncertainties of data is higher on the high traffic when reader read a tag because the system lacks of concern towards the reliability and the security of the system (Bonnie *et al.*, 2005). There are previous researchers, for example (Feng and Ying, 2007) have proposed the multi agent technology to integrate with the RFID system. They proposed a system that can monitor the in-transit of item status and the information produced several solutions by using a multi agent technology. Using a multi agent technology the data received from the reader can be processed locally before can be transferred to the backend of the RFID system. This can optimize the system by reducing the size and cost of data transfer. Multi-agent technology not only functions as an integration of functions but can also verify the RFID system operation to enhanced the reliability of data, load balancing to handle large quantity of RFID data and organized data for sorting and efficient query respond (Jian and Heung, 2007).

Another issued that has been discussed is by Shengguang *et al.* (2008) have proposed a system that integrates the RFID technology with web based geographic information system and Short Message System (SMS) for intelligent managements of the assets. Here, the system has a problem in the time and speed of processing when sending a message and information about the assets to the backend of the system. Abdel-Naby and Giorgini (2006) has proposed a possible integration between the multi agent framework and RFID system at the backend of system. The progress of the work with the RFID tags can be better detected through the area that contains the RFID reader. Hyun-Seok *et al.* (2006) have described this in their previous works on the security protocol of the RFID. They have specified the

problem by using a Compiler of Security Protocol Analyzer (CASPER), communication sequence process (CSP) and FDR model checking tool. Then, they have analyzed and solved data security with the RFID security protocol in which their authentication method guarantees data privacy between the RFID tags and RFID reader. For some of the methods however, there are still needs to enhance the verification issues to control the errors of data on the RFID tags.

Previous researchers have done many works that focused on the backend of the system to verify and validate the RFID data. Therefore, in this research a different approach is taken to focus on the RFID layer issues in the RFID system. Here, the model verification agent is proposed to minimize the consequences and uncertainty of issues that occurred in the RFID Management System. The model verification agent will check and verify a communication protocol in the RFID system which involves data transfer and security by detecting RFID tags in a specific time frame. This research is enhancing the verification focus on the RFID communication layer as RFID system have difficulty and limited issues to verify data errors, hardware failures, deadlocked and data transfer problem. The proposed model verification agent will then be designed towards the current issues and verified with an alternative model checker to ensure that the system deployed is functional, accurate, reliable, robust and secure.

The software agents are technology that provides autonomous, flexible and dynamic computational entities in solving problems (Timothy and Scott, 2000; Yan, Kian and Jian, 2004). This is because according to Gerhard (2000), agents are working in a goal oriented environment which have the ability to sense, communicate and achieve the given task in a specific time or timeframe. Thus, the behaviors of this agent have made them capable to help users in order to solve their problems. Therefore, by applying agents in the RFID system architecture, the verification agent will manage to enhance the verification of the RFID data. In the formal verification, model checking used the mathematical approach to specify specification and verification of the distributed systems. This technique is suitable for verifying the complex system (Bonnie *et al*, 2005). In this research agents and

model checking in formal method are applied to verify the design of the RFID system at the communication layer. The proposed of model verification agent in the test of case study has been concerned that it has a potential in handling a verification process. In this research, the aim is to investigate the capabilities of model verification agent in order to verify the RFID data for management and data transfer issue.

1.3 Problem Statements

In this study, the intention is to come up with a method to provide insights into solving the verification issue. Therefore in order to solve this issue, the following questions need to be addressed.

(i) How the modeling and specification of agent can play a role in verifying the process of verification in the RFID system?

(ii) What is the suitable design and model is in formalize model verification agents to do the verification in the RFID architecture and system?

(iii) What is the step in modeling the informal specification of the system to be formalize using a formal language with the agent?

(iv) How is this formalization of model verification agent will be able to show the process of errors in the RFID system?

(v) There are many tools for model checking in formal method approach; what is the recommended model checker that can be the representative for the RFID system.

1.4 Hypothesis

In this research, the proposed model verification agent on the RFID system is intended to improve the performance of verification that can increase the reliability of data transfer and verify the RFID data for the RFID system. Therefore, several assumptions have been specified in this research regarding the statement and properties of the RFID system:

(i) Model Verification Agent (MVA) that resides in the RFID layer will increase in its' effectiveness of communication between the RFID layers and formal method model checker is one of the impact factors on the result of verification. Therefore, an appropriate model checker will enhance the verification results.

(ii) The first property that needs to be concerned is in terms of the format and syntax. Model verification agent (MVA) is responsible to check and verify a format and syntax of the RFID system. For example, the RFID tag that have been read in input form (UID,Trn_Code,No_Block,S_Key) satisfies a given specification of the desired RFID system before input information can be continue to the next stage. The system will generate error reports to the system that automatically terminate the reading process. This process is important to prevent RFID tags that are not trusted from accessing the RFID System.

(iii) The last property that needs to be concerned is the time consumed by the operation. Congestion can occur during the heavy reading processes of the RFID tags and when this happened, it will affect reading processes at once for the RFID system. For example, the lack of the middleware in RFID system to serve many requests at one time during busy traffic will impact the system performance. The proposed model can provide an authentication proved in a specific slot of time to process the exact RFID tag in the time frame. The system will ignore the RFID tag if the RFID tag is not authenticated.

1.5 Aim

The research aims to develop the verification approach of the RFID system using a model verification agent. This model is capable to verify RFID data in communication protocol of the RFID system which can manage the system in terms of the reliable data transfer and system effectiveness.

1.6 Objectives

Below are the objectives for this research:

(i) To study and analyze the available agent technology and formal method implementation in RFID systems with regard to the verification issues in RFID systems.

(ii) To propose a model for verification methods used in RFID system implementation for verification of RFID layers in various applications.

(iii) To test the proposed model using a model checker in together with a formal method technique.

1.7 Scopes

(i) This study will focus on the development of verification agent for RFID system. This research will apply the technology of agent and formal method technique to verify the processing of data in the RFID system.

(ii) Verification agent that has been developed will support the RFID system to ensure the process data from reader is verified before the system can be developed. The processing of RFID data will be transformed into model and language to be used as the model checker.

(iii) This research only focuses on verification of the specification and modeling of the RFID system with formal method approach and does not include validation.

(iv) The proposed MVA specification is developed using the formal method technique and how the MVA works with the properties is presented in the state diagram.

(v) The effectiveness and accuracy of the proposed model verification agent will be tested with CWB-NC model checker. The attributes that this study will measure is focusing on the format in RFID data transaction which includes the unique identity number or user identity (UID) on data and the synchronization of data by a distinguished data type.

(vi) This research does not develop a system but only a part of the system has been testified. Several RFID systems will be tested to enhance the correctness of the RFID system based on two properties: checking format and syntax and slot of time.

1.8 Significant of the Research

(i) To improves and enhances the verification model of conventional RFID system in the area of formal verification to verify multi agent system in the distributed and complex system.

(ii) To demonstrates the importance of the formal verification in determining and specifying the complex properties by modeling the system specification.

(iii) It reveals the capability of formal method technique in giving advantages in the software development process.

1.9 Contribution of the work

(i) To improves performance of system by reduction of heavy reading processes of the RFID tag. The design of the model and algorithm for each state process should be generally understandable and capable to be implemented in the system for process verification. With this, the workload for management and identification can be reduced and perhaps will also increase the quality of services of the system.

(ii) To detects error by satisfying the specification during the system implementation. This can save time in system development process. MVA aims to solve the problem of uncertainties and unprecedented data transfer between the RFID layers.

(iii) To prevent the difficulties to RFID system in their filtration and management of information through the RFID middleware by determining RFID layer for verification using an agent based system. This research focuses on designing an MVA that is able to interact with each other to conduct verification processes based on the mentioned RFID layer.

1.10 Thesis organization

In this chapter, the motivation and background of the problems are presented as well as the outline for the purposes and objectives of this research. Moreover, the contribution and the importance of this research are also highlighted. The thesis is organized as follows:

(i) Chapter 1 provides a motivational background of the research introduction. This chapter describes the background, problem statement, hypothesis, aim, objectives, scope, significances of research, contribution of work and ends with an overview of the thesis organization.

(ii) Chapter 2 presents the summarization of the related previous work on the RFID technology, agent technology and formal method: model checking.

(iii) Chapter 3 elaborated the methodologies and steps adopted to perform the purposed Model verification agent (MVA) in this research.

(iv) Chapter 4 presents the Model Verification Agent with the steps of MVA performs is demonstrated in more detail in this chapter.

(v) Chapter 5 presents the testing and analysis result of MVA approach with model checker based on two case studies: Embedded smart card system and RFID shopping system.

(vi) Chapter 6 respectively presents the summary of the conclusion of this research with the finding of this research and suggestion for future research.

1.11 Summary

The introduction of formal verification in RFID system has been justified and discussed including the problem background, objectives, scope, significance of research and contribution of research. In order to enhance and increase the correctness of the RFID system, the following section describes the review of previous works related to formal verification using the agent and formal method. Following this, a research methodology has been proposed for improving the RFID system based on the objectives that have been defined in this chapter.