



**UNIVERSITI PUTRA MALAYSIA**

**AN INTRUSION TOLERANT SYSTEM ARCHITECTURE FOR  
SECURE AND SELF-HEALING SMART GRID CONTROL  
CENTERS**

**MARYAM TANHA**

**FK 2013 44**



**AN INTRUSION TOLERANT SYSTEM  
ARCHITECTURE FOR SECURE AND  
SELF-HEALING SMART GRID CONTROL CENTERS**

By

**MARYAM TANHA**

Thesis Submitted to the School of Graduate Studies, Universiti Putra  
Malaysia, in Fulfilment of the Requirements for the Degree of Master  
of Science

October 2013

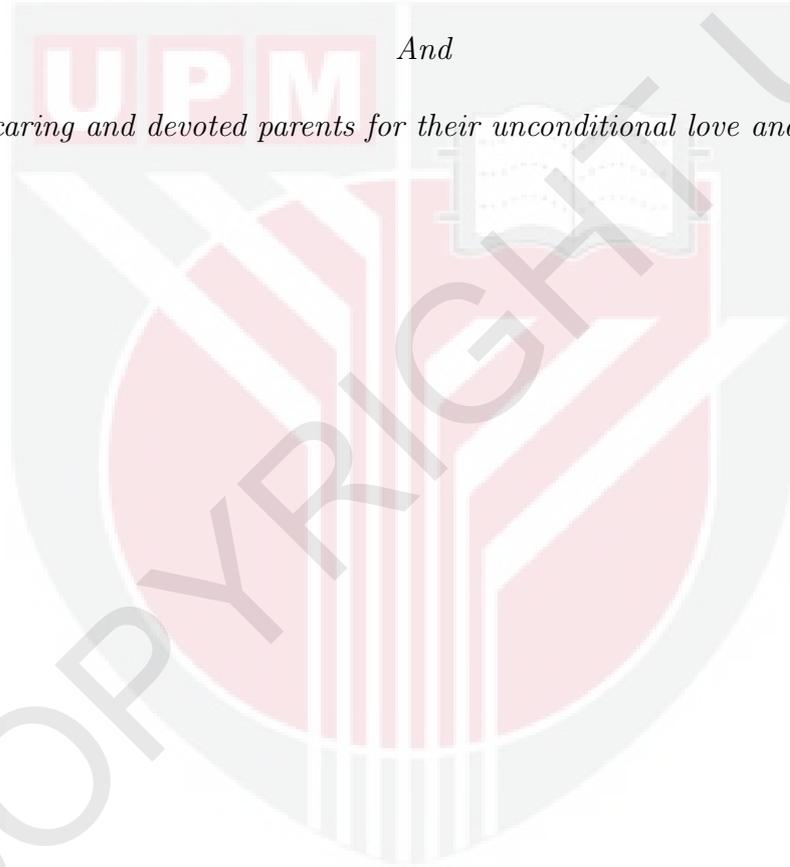
## DEDICATIONS

*This thesis is dedicated to:*

*My dearest husband, Dawood, for his whole-hearted and substantial support*

*And*

*My caring and devoted parents for their unconditional love and support*



© COPYRIGHT UPM

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Master of Science.

**AN INTRUSION TOLERANT SYSTEM ARCHITECTURE FOR  
SECURE AND SELF-HEALING SMART GRID CONTROL  
CENTERS**

BY

**MARYAM TANHA**

**October 2013**

**Chair: Fazirulhisyam Hashim, PhD**  
**Faculty: Engineering**

The ever-increasing, novel and sophisticated cyber threats underscore the need for more robust and resilient security approaches. The situation would be further aggravated due to the dependence of many critical infrastructures on information and communication technology. Critical infrastructures require automatic response and self-healing capabilities to handle multifarious malicious attacks while remaining survivable and secure. The cyber security is of great importance for critical infrastructures due to far-reaching societal and economic impacts caused by failure or malfunction of their key components (in particular, control centers) resulting from malicious attacks on the communication infrastructure. Unfortunately, conventional security mechanisms, namely prevention and detection systems have limitations to suffice for the crucial operation of critical infrastructures such as smart grid. For this reason, a new security paradigm referred to as intrusion tolerance needs to be incorporated into critical infrastructures. The intrusion tolerance is envisaged to complement the existing security solutions, as well as to provide availability (as the top security priority) and self-healing capabilities for control centers of critical infrastructures. However, intrusion tolerance techniques are associated with substantial cost. This dissertation proposes an intrusion tolerant system architecture which incorporates distinctive features, namely hybrid and hierarchical rejuvenation mechanism as well as dynamic redundancy level. The aforementioned characteristics are formulated in such a way to decrease the incurred intrusion tolerance cost while improving security. The security of the proposed architecture is analytically evaluated, and the acquired results show improvements compared to two established intrusion tolerant system architectures. The incurred cost in terms of overhead is also analyzed, and the outcomes demonstrate the cost-effectiveness of the proposed architecture.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia  
sebagai memenuhi keperluan untuk ijazah Master Sains

**SATU SENI BINA PENCEROBOHAN TOLERAN SISTEM  
UNTUK KE SELAMAT DAN PEMULIHAN DIRI PINTAR PUSAT  
KAWALAN GRID**

OLEH

**MARYYAM TANHA**

Oktober 2013

**Pengerusi: Fazirulhisyam Hashim, PhD**  
**Fakulti: Kejuruteraan**

Ancaman siber yang semakin meningkat, baru dan canggih menekankan keperluan bagi kaedah keselamatan yang lebih kukuh dan berdaya tahan. Keadaan ini akan menjadi lebih teruk akibat kebergantungan banyak infrastruktur kritikal kepada teknologi maklumat dan komunikasi. Infrastruktur kritikal memerlukan tindak balas automatik dan keupayaan pemulihan diri untuk menangani pelbagai serangan berniat jahat manakala mengekalkan keupayaan hidup dan selamat. Keselamatan siber adalah amat penting untuk infrastruktur kritikal kerana kesan sosial dan ekonomi yang meluas disebabkan oleh kegagalan atau kerosakan komponen utama mereka (khususnya, pusat kawalan) akibat daripada serangan berniat jahat ke atas infrastruktur komunikasi. Malangnya, mekanisme keselamatan konvensional, iaitu sistem pencegahan dan pengesanan mempunyai had untuk mencukupi dalam operasi penting infrastruktur kritikal seperti grid pintar. Berdasarkan sebab ini, satu paradigma keselamatan baru yang merujuk kepada toleransi pencerobohan perlu dimasukkan ke dalam infrastruktur kritikal. Toleransi pencerobohan dijangka akan melengkapkan penyelesaian keselamatan yang sedia ada, serta menyediakan ketersediaan (sebagai keutamaan keselamatan tertinggi) dan keupayaan pemulihan diri untuk pusat kawalan infrastruktur kritikal. Walaubagaimanapun, teknik toleransi pencerobohan dikaitkan dengan kos yang besar. Disertasi ini mencadangkan satu seni bina sistem toleran pencerobohan yang menggabungkan pelbagai ciri yang tersendiri, iaitu mekanisme rejuvenasi hibrid dan hierarki serta tahap lebih dinamik. Ciri yang disebutkan di atas dirumuskan dengan cara sedemikian untuk mengurangkan kos pencerobohan toleransi bertanggung disamping meningkatkan keselamatan. Keselamatan bagi seni bina yang dicadangkan dinilai secara analitikal, dan keputusan yang diperolehi menunjukkan peningkatan apabila dibandingkan dengan dua seni bina sistem toleran pencerobohan yang sedia ada. Kos yang ditanggung dari segi overhead juga

dianalisis, dan hasil menunjukkan keberkesanan seni bina yang dicadangkan.



## ACKNOWLEDGEMENTS

I would like to express my deep gratitude to my supervisor, Dr. Fazirulhisyam Hashim for his generous support and great encouragement to conduct this research as well as his valuable comments to enhance the quality of the dissertation.

Also, I am very grateful to the members of my supervisory committee, Associate Professor Dr. Shamala K. Subramaniam and Dr. Khairulmizam b.Samsudin for their help and support to achieve my research dissertation.



I certify that a Thesis Examination Committee has met on 4 October 2013 to conduct the final examination of Maryam Tanha on her thesis entitled “AN INTRUSION-TOLERANT SYSTEM ARCHITECTURE FOR SECURE AND SELF-HEALING SMART GRID CONTROL CENTERS” in accordance with the Universities and University Colleges Act 1971 and the Constitution of the Universiti Putra Malaysia [P.U.(A) 106] 15 March 1998. The Committee recommends that the student be awarded the Master of Science.

Members of the Thesis Examination Committee were as follows:

**Alyani binti Ismail, PhD**

Associate Professor  
Faculty of Engineering  
Universiti Putra Malaysia  
(Chairman)

**Abd. Rahman bin Ramli, PhD**

Associate Professor  
Faculty of Engineering  
Universiti Putra Malaysia  
(Internal Examiner)

**Mohd Zainal Abidin bin Ab. Kadir, PhD**

Professor  
Faculty of Engineering  
Universiti Putra Malaysia  
(Internal Examiner)

**Tiong Sieh Kiong, PhD**

Associate Professor Ir.  
Universiti Tenaga Nasional Malaysia  
(External Examiner)

---

**NORITAH OMAR, PhD**

Associate Professor and Deputy Dean  
School of Graduate Studies  
Universiti Putra Malaysia

Date: 19 December 2013

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of Master of Science. The members of the Supervisory Committee were as follows:

**Fazirulhisyam Hashim, PhD**

Senior Lecturer  
Faculty of Engineering  
Universiti Putra Malaysia  
(Chairperson)

**Shamala K. Subramaniam, PhD**

Associate Professor  
Faculty of Computer Science and Information Technology  
Universiti Putra Malaysia  
(Member)

**Khairulmizam b.Samsudin, PhD**

Lecturer  
Faculty of Engineering  
Universiti Putra Malaysia  
(Member)

---

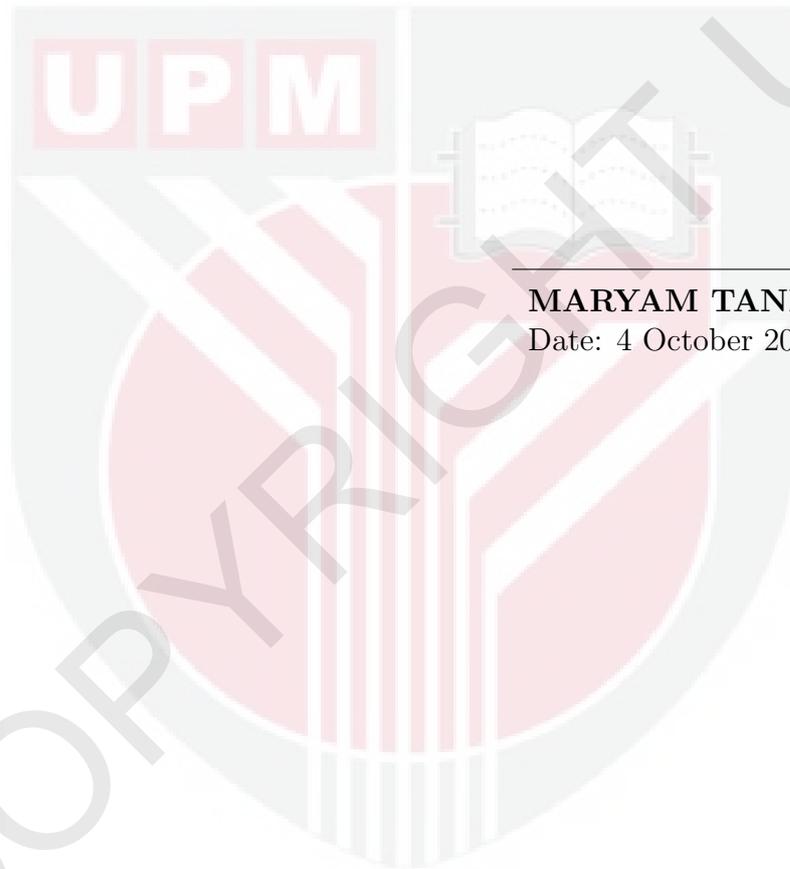
**BUJANG BIN KIM HUAT, PhD**

Professor and Dean  
School of Graduate Studies  
Universiti Putra Malaysia

Date:

## DECLARATION

I declare that the thesis is my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously, and is not concurrently, submitted for any other degree at Universiti Putra Malaysia or at any other institution.



---

**MARYAM TANHA**

Date: 4 October 2013

## TABLE OF CONTENTS

	Page
<b>ABSTRACT</b>	ii
<b>ABSTRAK</b>	iii
<b>ACKNOWLEDGEMENTS</b>	v
<b>APPROVAL</b>	vi
<b>DECLARATION</b>	viii
<b>LIST OF TABLES</b>	xi
<b>LIST OF FIGURES</b>	xii
<b>LIST OF ABBREVIATIONS</b>	xv
<b>CHAPTER</b>	
<b>1 INTRODUCTION</b>	1
1.1 Introduction	1
1.2 Problem Statement and Motivation	2
1.3 Aims and Objectives	3
1.4 Thesis Scope	3
1.5 Study Module	4
1.6 Thesis Organization	4
<b>2 LITERATURE REVIEW</b>	7
2.1 Overview	7
2.2 Cohesive Intrusion Tolerance for Critical Infrastructures	8
2.2.1 A general misconception about intrusion tolerance	8
2.2.2 Intrusion tolerance versus classical security mechanisms	9
2.2.3 Paradigms of intrusion tolerance	15
2.2.4 Adopting intrusion tolerance techniques in critical infrastructures	21
2.2.5 Intrusion tolerant system architectures	22
2.2.6 Intrusion tolerance research challenges and issues	25
2.3 Cyber Security in Smart Grid as a Critical Infrastructure	27
2.3.1 Smart Grid and Communication Networks	27
2.3.2 Smart Grid Cyber Security	28
2.4 Summary	33
<b>3 METHODOLOGY</b>	34
3.1 Overview	34
3.2 Proposed ITS Architecture for Control Centers of Critical Infrastructures	34
3.2.1 Replication & diversity module	36
3.2.2 Compromised/faulty replica detector	37
3.2.3 Reconfiguration module	37

3.2.4	Auditing module	39
3.2.5	Proxy module	39
3.2.6	Cooperative operation of replication and reconfiguration modules	39
3.2.7	A case study: Trojan horse attack on smart grid control centers	44
3.3	Analytical Model and Security Performance Analysis	45
3.3.1	System model	46
3.3.2	Availability formulation	48
3.3.3	MTTSF formulation	52
3.3.4	SLA as another security performance measure	54
3.4	Cost Analysis	55
3.4.1	Simulation setup	56
3.5	Summary	57
<b>4</b>	<b>RESULTS AND DISCUSSION</b>	<b>58</b>
4.1	Overview	58
4.2	Analytical Results	58
4.2.1	Availability	58
4.2.2	MTTSF	61
4.2.3	Acquired analytical results and the security of control centers of critical infrastructures	63
4.3	Cost Analysis Results	64
4.3.1	Rejuvenation cost	65
4.3.2	Redundancy cost	69
4.3.3	Summary	75
<b>5</b>	<b>CONCLUSION AND FUTURE WORKS</b>	<b>76</b>
5.1	Conclusion	76
5.2	Thesis Contributions	76
5.3	Recommendations for Future Works	77
	<b>REFERENCES/BIBLIOGRAPHY</b>	<b>79</b>
	<b>BIODATA OF STUDENT</b>	<b>85</b>
	<b>LIST OF PUBLICATIONS</b>	<b>87</b>