

UNIVERSITI TEKNOLOGI MARA

**FRAMEWORK OF TRUSTED
WIRELESS SENSOR NODE
PLATFORM FOR WIRELESS SENSOR
NETWORK**

YUSNANI MOHD YUSSOFF

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

Faculty of Electrical Engineering

September 2013

AUTHOR'S DECLARATION

I declare that the work in the thesis was carried out in accordance with the regulations of Universiti Teknologi MARA. It is original and is the result of my own work, unless otherwise indicated or acknowledged as referenced work. This thesis has not been submitted to any other academic institution or non-academic institution for any degree of qualification.

I, hereby, acknowledge that I have been supplied with the Academic Rules and Regulations for Post Graduate, Universiti Teknologi MARA, regulating the conduct of my study and research.

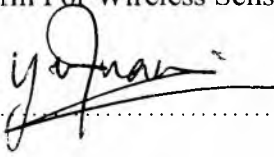
Name of Student : Yusnani Mohd Yussoff

Student I.D. No. : 2009608912

Programme : Degree of Philosophy

Faculty : Faculty of Electrical Engineering

Thesis Title : Framework of Trusted Wireless Sensor Node
Platform For Wireless Sensor Network

Signature of Student : 

Date : September 2013

ABSTRACT

Wireless Sensor Networks (WSNs) have shown great promise as the emerging technology for data gathering from unattended or hostile environment. The advancement in micro-electro-mechanical sensor technology, wireless communication technology and the recent scavenging energy have gradually expanding the acceptance of WSN related applications. The design of sensors that are small, low cost, low power and combined with its unattended nature has made it more viable and indirectly promotes its popularity for future solutions in various real-life challenges. One of the most challenging yet important security issues in Wireless Sensor Network is in establishing trusted and secured communication between sensor node and base station. While the term trusted has been widely used referring to valid nodes in the group, this thesis refer the term trusted based on Trusted Computing Group (TCG) specifications. With limitations in the present solutions such as late discovery of invalid nodes such in Trust Management System and high energy consumption with external security chip due to the used of Trusted Platform Module chip; a Framework of a Trusted Wireless Sensor Node is presented. The framework incorporates ideas from TCG and Identity-based cryptosystem by Boneh Franklin to ensure trusted and secured communications between sender and receiver which might be between sensor node and base station or between sensor nodes in the network. The research aim to come out with a credential based trusted sensor network to verify the authenticity of sensor nodes in the network. Finally the proposed trusted framework is evaluated for the potential application in resource constraint devices by quantifying their power consumption on selected major processes. The result proved the proposed scheme can establish trust in WSN with less computation and communication and most importantly eliminating the need for neighbouring evaluation such in Trust Management System or relying on external security chip. Finally, proposed works benefit in eliminating clone or duplicated nodes in the WSN thus reduced the number of false and unwanted messages in the Wireless Sensor Network.

TABLE OF CONTENTS

AUTHOR’S DECLARATION	ii
ABSTRACT	iii
ACKNOWLEDGMENTS	iv
TABLE OF CONTENTS	v
LIST OF TABLES	ix
LIST OF FIGURES	x
LIST OF ABBREVIATIONS	xii
CHAPTER ONE: INTRODUCTION	1
1.1 INTRODUCTION	1
1.2 MOTIVATIONS	1
1.3 OBJECTIVES	3
1.4 SCOPES AND LIMITATIONS OF THE STUDY	3
1.5 METHODOLOGY	4
1.6 SIGNIFICANT CONTRIBUTIONS	5
1.7 THESIS OUTLINES	6
CHAPTER TWO: LITERATURE REVIEW	8
2.1 INTRODUCTION	8
2.2 WSNS APPLICATION	8
2.1.1 WSNs Constraint	9
2.1.2 Nature of WSNs Nodes	11
2.1.3 Security Challenges in WSNs	12
2.3 THREATS, VULNERABILITIES AND ATTACKS IN WSN	13
2.2.1 Threats	13
2.2.2 Vulnerabilities	13
2.2.3 Attacks	14
2.4 TRUST AND SECURITY REQUIREMENT IN WSNS	16
2.3.1 Trust in WSNs	17

2.3.2	Security Chips	19
2.3.3	Security Requirements	22
2.5	FORMAL ANALYSIS AND MODEL CHECKING	23
2.6	RELATED WORK	25
2.5.1	Security Solutions in WSNs	25
2.5.2	Hardware Based Security and Trust Establishment in Embedded Devices	28
2.5.3	Identity-based Secure Communication Protocol	32
2.7	CHAPTER SUMMARY	36
 CHAPTER THREE : TRUSTED COMPUTING		 37
3.1	INTRODUCTION	37
3.2	TRUST ACCORDING TO TCG	37
3.3	TRUSTED PLATFORM	38
3.2.1	Property	39
3.2.2	Integrity Measurement and Storing	39
3.2.3	Attestation	41
3.4	CHAPTER SUMMARY	42
 CHAPTER FOUR: METHODOLOGY		 43
4.1	INTRODUCTION	43
4.2	DEVELOPMENT OF TRUSTED NODE	43
4.3	INTEGRATING TCG SPECIFICATIONS INTO ARM11 PLATFORM	45
4.2.1	ARM11 Security Features	45
4.2.2	Implementation of Trusted Sensor Node	46
4.4	ANALYSIS METHOD	59
4.3.1	Energy Analysis	59
4.3.2	Memory Analysis	60
4.3.3	Protocol Efficiency	61
4.3.4	Formal Analysis	61
4.5	CHAPTER SUMMARY	64