UNIVERSITI TEKNOLOGI MARA

Performance Evaluation of Identity-Based Encryption (IBE) Remote Attestation Protocol in Wireless Sensor Networks

ROSZAINIZA ROSLI

Thesis submitted in fulfillment
of the requirements for the degree of
Master of Science

Faculty of Electrical Engineering

February 2014

AUTHOR'S DECLARATION

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

Student I.D. No. : 2010405002

Programme : Master in Electrical Engineering (EE780)

Faculty : Electrical Engineering

Thesis Title : Performance Evaluation of Identity-Based Encryption (IBE) Remote Attestation Protocol in Wireless Sensor Networks

Signature of Student :

Date : February 2014

ABSTRACT

Remote attestation is a trusted computing activity which aims at establishing integrity of systems in a network. Therefore, remote attestation is important to be applied in Wireless Sensor Networks (WSNs) due to exposed nature of WSNs. However, to apply attestation on WSN will lead to high computation costs. Hence, efficient energy management is crucial since sensor nodes are resource constrained devices. This research was conducted with the main objective of evaluating the performance of Identity-Based Encryption (IBE) remote attestation protocol. The study involves two major parts i.e., the theoretical calculation and test-bed implementation of an IBE-Trust attestation. A comprehensive performance analysis of IBE-Trust attestation had been shown in this thesis by validating it with existing protocol and by comparing it between theoretical performance and real world implementation. Theoretical calculation was done based on XBee payload specification on diffirent input of data size regarding on the protocol. The real world implementation was carried out in the Wireless Laboratory at Faculty Electrical Engineering where a test bed consists of a sensor node and a base station connecting wirelessly through Xbee 802.15.4. As a result, on real world implementation, IBE-Trust shows a comparable performance between existing protocol and theoretical calculation. The work done in this thesis can be a benchmark for future performance comparison in different size of network, communication or others.

ACKNOWLEDGEMENTS

In the name of Allah, I would like to take this opportunity to express my deep gratitude and sincere appreciation to my supervisor Assoc. Prof. Dr. Habibah Hashim for the understanding, support and brilliant ideas that she have shared with me throughout the project implementation and thesis writing.

I would also like to take this opportunity to show my appreciation to all my friends especially to Mrs. Yusnani Yusoff, Mr. Lukman Hakim and Mr. Anuar Mat Isa for their encouragement, advice and cooperation during my postgraduate study in the faculty.

Finally, it is my greatest pleasure to dedicate this work to my husband, my daughter, my parents and family for their never ending moral support and understanding.

TABLE OF CONTENTS

CHAPTER ONE: INTRODUCTION

CHAPTER TWO: LITERATURE REVIEW

CHAPTER THREE: METHODOLOGY