**UNIVERSITI TEKNOLOGI MARA**

# CHAINED IDENTITY ATTESTATION (CIA) METHOD IN PREVENTING NODE IMPERSONATION ATTACK IN WIRELESS SENSOR NETWORK

**NORHAFLYZA BINTI MARBUKHARI**

Thesis submitted in fulfillment
of the requirements for the degree of
**Master of Science**
**(Computer Engineering)**

**Faculty of Electrical Engineering**

**November 2018**

# ABSTRACT

A Wireless Sensor Network (WSN) system incorporates a gateway that provides wireless connectivity back to the wired environment and distributed nodes. The nature of the sensor nodes that are located remotely and unattended has exposed itself to node impersonation attack. This kind of attack can be further classified into physical and active attack where the nodes identity are being copied or stolen and in worst case scenario, it can be removed from their locations and duplicated in the lab. Several node identity authentication methods have been developed and proposed by few researchers to overcome or mitigate their problem. However, with the nature of Wireless Sensor Network (WSN) nodes that are left unattended, the problem still exits. This work presents new method in mitigating node impersonation attack. This method is called Chained Identity Attestation (CIA). The main objective of this project is to mitigate node impersonation attack in WSN environment, in term of identity cloning. A test bed consisting of two sensor nodes and a base station is set up to verify and analyse its feasibility in a real environment using mathematical analysis, the developed protocol is proven to overcome node cloning or node impersonation attack. Successful authentication between sensor nodes and base station are reported to confirm the functionality of the proposed new method. Feasibility of the proposed method in term of processing time and energy consumption is presented and compared with the original DHKE method. The results prove the security and feasibility of the developed protocol.

# ACKNOWLEDGEMENT

Firstly, I wish to thank God for giving me the opportunity to embark on my MSc and for completing this long and challenging journey successfully. My gratitude and thanks go to my supervisor Ir Dr Yusnani Mohd Yussoff and co-supervisor Dr. Murizah Kassim.

My appreciation goes to all my colleagues and friends for helping me with this project.

Finally, this thesis is dedicated to my husband, my mother and the loving memory of my very dear late father for the vision and determination to educate me. This piece of victory is dedicated to all of you. Alhamdulillah.

# TABLE OF CONTENTS

# CHAPTER ONE
# INTRODUCTION

## 1.1 Research Background

Wireless Sensor Network (WSN) system incorporates a gateway that provides wireless connectivity back to the wired world and distributed nodes. With the advancement of sensor development in recent years, WSN has become a key technology for the Internet of Things (IoT) infrastructure. This technology also attracts worldwide attention due to its mobility and low-cost, as well as many other significant factors, such as self-organizing, self-healing and having dynamic network topology to cope with node malfunctioning or failures. Moreover, the system should have the ability to withstand bad environmental conditions, heterogeneity of nodes, scalability during and after deployment, as well as ease of use.

In the meantime, since the nature of WSN is left unattended for a certain amount of time, this has caused security flaws that can mortify the execution of a system. During the WSNs' deployment in any system, an attacker will always try to attack the nodes and ruin their identities by injecting false information or installing malicious codes. Such unethical activity will finally enable the hacker to extract sensitive information from the communicating nodes or disable the functions of the WSNs. Therefore, it is critical to enhance and apply security measures by verifying the sensor node identity to protect the whole system.

One of the most crucial attacks that can affect the entire communication process in WSN is known as node impersonation attack. The problem generally occurs during data transmission of sensitive information thus it is important to make sure that all the equipment in WSN is secured to prevent from this kind of threat. In this attack, the attacker tries to impersonate the identity of a legitimate node in the network, thus receiving messages directed to the node it fakes. For example, during transmission of a patient's private information from sensor node to the medical instrument, the attacker can clone itself, act as the communicating user and then send incorrect information or replace it with a false data to the medical officer. This will eventually cause internal problems and may result in wrong analysis of patient's information.