IMPLEMENTATION AND PERFORMANCE ANALYSIS OF IDENTITY-BASED AUTHENTICATION IN WIRELESS SENSOR NETWORKS

MIR ALI REZAZADEH BAEE

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Master of Computer Science (Information Security)

Faculty of Computing
Universiti Teknologi Malaysia

JANUARY 2014

By the name of Almighty God, the Creator of Heaven and Earth who gave me skill of learning and strength to memorize, I dedicate this thesis to my late father, dear mother, brothers, and sisters for their endless support and encouragement.

ACKNOWLEDGEMENT

I wish to express my gratitude to my supervisor **Dr. Satria Mandala** for his support and encouragement during this project proposal. I really appreciate his time and contributions in guiding me how to do research and craft thesis from findings. I also want to appreciate and acknowledged my other lecturers for their support during the study.

ABSTRACT

The use of Wireless Sensor Networks (WSNs) in different fields of our life has increased for several recent years. It would be used in applications such as military, human-centric, environmental monitoring, and robotics for remote data collection. Compared to traditional networks, WSNs present more challenges and issues due to their limited energy and bandwidth. This major restriction causes WSNs to be vulnerable under serious security threats, such as Denial of Service (DOS), Jamming, and Man-In-The-Middle (MITM). Until last few years, security solutions for WSNs were concentrated based on symmetric encryption algorithms to prepare authentication since, Public Key Infrastructure (PKI) has fallen from grace due to sensor nodes resource constraints. Despite more efficiency of symmetric cryptography than PKI in terms of energy, symmetric cryptosystems have some drawbacks such as key management. In addition, Public Key Cryptography (PKC) with resource hungry algorithm is not suitable for sensor node authentication. Recent researches on implementation of authentication mechanisms in WSNs show that, still sensor nodes suffer due to lack of a safe, fast, and lightweight authentication technique. This project focuses on secure sensor node authentication using Identity-Based Cryptography (IBC) in WSN. The proposed scheme uses Elliptic Curves Digital Signature Algorithm (ECDSA) with 224 bits key length to present a safe and lightweight authentication in compare to other pairing based algorithms. Additionally, the proposed scheme improves the security level of authentication between sensor nodes. Finally, this project implements and evaluates the proposed scheme using several parameters such as security, time, CPU, and memory requirements to measure the effectiveness of proposed scheme.

ABSTRAK

Saban tahun, penggunaan Wireless Sensor Networks (WSNs) dalam pelbagai bidang telah meningkat luas. Ia digunakan di dalam pelbagai aplikasi termasuk dalam bidang ketenteraan, kawalan manusia, pemantauan persekitaran dan robotik. Ia bertujuan untuk mengawal pengumpulan data. WSNs menimbulkan pelbagai cabaran dan isu berbanding rangkaian tradisional. Ini disebabkan oleh batasan tenaga dan jalur lebar. Batasan ini menyebabkan WSNs terdedah kepada ancaman keselamatan yang serius seperti Penafian Perkhidmatan (DOS), Jamming, dan Orang Tengah (MITM). Sehingga beberapa tahun lepas, penyelesaian keselamatan untuk WSNs tertumpu pada enkripsi algoritma simmetri untuk proses pengesahan kerana infrastuktur kunci awam (PKI) tidak berkesan. Ketidakkeberkesanan ini disebabkan oleh batasan sumber nod. System kripto simmetri memnpunyai kelemahan seperti pengurusan kunci. Tambahan pula, kunci awam kriptografi (PKC) dengan kehausan sumber algorithma tidak sesuai untuk pengesahan nod sensor. Kajian terkini dalam pelaksanaan mekanisma pengesahan dalam WSNs menunjukkan bahawa nod sensor masih bermasalah disebabkan kurangnya ciri-ciri keselamatan, kelajuan dan ringan dalam teknik pengesahan. Projek ini fokus kepada keselamatan pengesahan nod sensor dengan menggunakan kriptografi berpaksikan identiti (IBC) dalam WSN. Skema yang dianjurkan menggunakan algoritma lengkungan eliptik tandatangan digital (ECDSA) dengan 224 bits panjang kunci untuk menyajikan pengesahan yang lebih ringan dan selamat berbanding pasangan algorithma yang lain. Skema yang dianjurkan meningkat tahap keselamatan pengesahan antara nod-nod sensor. Konklusinya, projek adalah untuk melaksana dan menguji skema yang dianjurkan dengan menggunakan beberapa parameter seperti keperluan keselamatan, masa, CPU, dan memori untuk mengukur keberkesanan skema yang dianjurkan.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1. Introduction

Humans are constantly inventing new technologies to fulfill their needs. Wireless sensor networks (WSNs) are a still developing technology consisting of multifunction sensor nodes that are small in size and communicate wirelessly over short distances. Sensor nodes incorporate properties for sensing the environment, data processing, and communication with other sensors. The unique properties of WSNs increase flexibility and reduce user involvement in operational tasks such as in battlefields. Wireless sensor networks can perform an important role in many applications, such as patient health monitoring, environmental observation and building intrusion surveillance. In the future WSNs will become an integral part of our lives. However, along with unique and different facilities, WSNs present unique and different challenges compared to traditional networks. In particular, wireless sensor nodes are battery operated, often having limited energy and bandwidth available for communications.

Continuous growth in the use of WSNs in sensitive applications, such as military or hostile environments, and also generally has resulted in a requirement for effective security mechanisms in their system design. Achieving security in resource constrained WSNs is a challenging research task. Some of the security challenges in WSNs include secrecy, data integrity, authentication, key establishment, availability, privacy, secure routing, secure group management, intrusion detection, and secure data aggregation. Moreover, there are many threats and possible attacks on WSNs. Some of these attacks are similar to those that we might find in traditional networks such as routing attacks and DOS attacks. However, some attacks only exist in WSNs. A good example of this is the node capture attack, where an adversary physically captures a sensor node and extracts all of its stored information.

In this project, we introduce wireless sensor networks, their components, applications, and security challenges. Furthermore, we present current WSN node authentication mechanisms and our proposed scheme to obtain a safe and light node authentication in WSNs. In addition, this project implements the proposed scheme and evaluates its performance.

1.2. Problem Background

WSNs are vulnerable to attacks as same as the traditional wireless networks (Modares *et al.*, 2011). Alongside the WSNs vulnerabilities due to the features of wireless communication and ad-hocness, WSNs face more problems. For example, small cheap devices inside the sensor nodes are unlikely to be made intrusion-proof. In addition, sensor nodes often deployed in unprotected area such as battlefield, where makes them more vulnerable to attacks (Perrig *et al.*, 2004). Therefore, it is quite crucial to implement security in WSNs, especially those that are part of mission-critical applications.

Until last few years, security solutions for WSNs was concentrated based on symmetric encryption algorithms (Çamtepe and Yener, 2004; Du *et al.*, 2003; Eschenauer and Gligor, 2002; Haowen *et al.*, 2003; Zhu *et al.*, 2003; Liu and Ning, 2002) to prepare some properties such as authentication and confidentiality since, Public Key Infrastructure (PKI) has fallen from grace due to sensor nodes resource constraints. In addition, Public Key Cryptography with resource hungry algorithms such as Rivest, Shamir, and Adleman Signature Scheme (RSASS) is not suitable for sensor nodes authentication.

Despite more efficiency of symmetric cryptography than PKI in terms of energy (Carman *et al*., 2000), symmetric cryptosystems have some drawbacks. As the first, sensor nodes face the key agreement issue when they must decide on a shared key to make a secure communication. Due to the open and unattended environments, this issue is even worse in WSNs where nodes are commonly distributed. Further, using pairwise keys (Menezes *et al*., 1996) to obtain the ideal level of security in these cryptosystems is necessary. Last recent years studies show that using a safe and fast pairing technique increases the lifetime of sensor node.

Furthermore, the appropriate security strength to be used depends on the sensitivity of the transmitted data being protected, and needs to be determined by the owner of that data. According to the NIST (National Institute of Standards and Technology) recommendation, the transition to the 112-bit security strength shall be accomplished by 2014, except where specifically indicated. It is quite important to implement Elliptic Curves (EC) equal or greater than 224 bits or RSA equal or greater than 2048 bits key size.

1.3. Problem Statement

In order to obtain ideal level of security in WSNs, it is first essential to enable secure authentication of public keys (Kifayat *et al.,* 2010). Otherwise, the communication within the network will be vulnerable to man in the middle attack (Giordano, 2002). Public Key Infrastructure (PKI) requires users to store, exchange, and verify the certificates that issued by itself. These operations have many serious overheads in terms of storage, computation and, and communication (Yang *et al*., 2006) without solving the man in the middle problem. In addition, in last recent years, many researches have been performed for implementation of authentication mechanisms based on ECC and RSA in WSNs. Unfortunately those researches have not supported strong key sizes based on NIST recommendation after 2013. Therefore, still sensor nodes suffer due to lack of a safe, fast, and lightweight authentication technique.

1.4. Purpose of Study

Security is critical in many WSN applications where sensitive data is exchanged (Butty *et al*., 2003). The values measured by the sensors can be very significant with respect to the implicit or explicit information that they carry. For example, WSNs can be deployed in a hostile environment that prevents any physical communication with the base station, such as battlefields (Alemdar and Ibnkahla, 2007). On the other hand, attackers can capture nodes and use them to gain access to confidential messages exchanged in the WSN. The attacker may also try to eavesdrop the data transmitted in the WSN (Haowen and Perrig, 2003). Service availability and data confidentiality are major requirements for any WSN but they have to be achieved with minimal processing and energy requirements (Yick *et al*., 2008). Being energy efficient as compared to other public key schemes, IBC (Shamir, 1985) based on elliptic curves (Chatterjee and Sarkar, 2011; Silverman, 2010) will be the main contribution in this project. This project highlights the topic of Implementation and Performance Analysis of Identity-Based Authentication in Wireless Sensor Networks, since it defines the robustness of the whole WSN against attacks that try to obtain the private keys of the sensor nodes. Usually, a single trusted base station is assumed to exist and to act as the central private key generator (C-PKG). This imposes a single point of failure in WSNs which are highly exposed to adversaries. In addition, the C-PKG can publish the secret keys of any node without being detected. It can even impersonate the identity of any node with the help of a network master key by exploiting its private key to sign or decrypt its messages as there is no way to distinguish between the honest sensor node and the malicious C-PKG (Lopez *et al*., 2009).

1.5. Objectives of Study

- To propose new scheme for secure authentication among sensor nodes in WSN.
- To improve security level of authentication between sensor nodes in WSN.
- To implement the proposed scheme in WSN.
- To evaluate the proposed scheme in WSN.

1.6. Research Questions

- How to develop lightweight authentication in WSN?
- How to make a trustable authentication between sensor nodes in WSN?
- How to implement a secure authentication within WSN?
- How to evaluate the proposed scheme in WSN?

1.7. Significant of Study

This study presents a secure sensor node authentication in wireless sensor network and proposes a new scheme for improving current node authentication issues. Furthermore, the proposed scheme decreases battery consumption in sensor nodes. The scheme, does not restrict the network in size, it is easily expandable.

Regarding to the last announcement by NIST, it is noticed that RSA with 1024 bit length of key and ECC with 160 bit length of key will be expired until the end of 2013. Therefore, the results of this project are very significant for both industry and researchers which intend to implement new security mechanisms in sensor node.

1.8. Scope of Study

This project presents a new sensor node ID-Based authentication scheme using Elliptic Curve Digital Signature Algorithm (ECDSA) in WSNs. This project only focuses on sensor node-to-node authentication in WSNs.

1.9. Project Goal

This project focuses on secure sensor node ID-Based authentication scheme using Elliptic Curve Digital Signature Algorithm (ECDSA) in WSNs. The proposed scheme uses Elliptic Curves Cryptography (ECC) to present a lightweight authentication mechanism through sensor nodes in WSN. Additionally, the proposed scheme improves the security level of authentication through sensor nodes compare to PKI, symmetric cryptosystems, or other implementation of ID-Based Signature in WSN. Finally, this project implements the proposed scheme in WSN and evaluates it using several parameters such as time, power, and memory to measure the effectiveness of proposed scheme.

1.10. Organization of Paper

This section presents how this paper is organized. This proposal has six chapters, which are Introduction, Literatures Review, Research Methodology, Implementation, Results, and Conclusion.

- Chapter 1: Introduction. This chapter outlines the whole project and outcome.
- Chapter 2: Literature Review. This chapter provides the readers a critical look at the technologies used in this project and the analysis of existing system.

- Chapter 3: Research Methodology. This chapter identifies the research methodologies available and used inside the project. It identifies the operational outline, approach and techniques used throughout the project.
- Chapter 4: Implementation. This chapter initially focuses on implementation of proposed scheme using OMNET++.
- Chapter 5: Results. This chapter presents the results of proposed scheme.
- Chapter 6: Conclusion. This chapter concludes project findings.

1.11. Summary

This chapter has provided the overview of the project and discussed its problem background. It also has described the aim and objectives of the project besides of the project scope. In addition, this chapter has outlined the significance of the project and the benefited parties.