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.