2013 First International Conference on Artificial Intelligence, Modelling & Simulation

Evaluation of Security Mechanisms for Information Dissemination in Wireless Sensor Networks

Mohamad Nazim Jambli*, Sinarwati Mohamad Suhaili†, Nurul Sahida Mansor*, Johari Abdullah*, Halikul Lenando*
*Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak, 94300 Sarawak, Malaysia
{jmnazim, nurulsahida, ajohari, cool}@fit.unimas.my
† Centre for Pre-University Studies, Universiti Malaysia Sarawak, 94300 Sarawak, Malaysia
mssinarwati@preuni.unimas.my

***Abstract*—In recent years, extensive research has been conducted on Wireless Sensor Networks (WSNs) due to their wide range of potential applications ranging from commercial to critical military and health care applications. For most of these applications, security is an important requirement. However, security mechanisms in WSNs differ from traditional ad-hoc networks due to their energy and resource constraints. Due to these constraints, the sensor nodes are vulnerable to security threats because the traditional security measures are not enough to protect these nodes during information dissemination in WSNs. Thus, in this paper we have studied TinySec security measures; Authentication-only (TinySec-Auth) and Authentication Encryption (TinySec-AE) in order to evaluate the suitability of these security measures for WSN applications. We have evaluated these TinySec mechanisms in terms of packet transmission time, average number of packet received and energy consumption. The simulation results show that TinySec-AE consumed more energy and required more time to transmit packet in comparing to TinySec-Auth due to higher computational time and longer packet size for extra encryption mechanism.**

Keywords*—*Wireless Sensor Networks; Information Dissemination; Security

I. Introduction

Recently, many research has been conducted on Wireless Sensor Networks (WSNs) due to their wide range of potential applications. The enormous potential of this technology can be seen ranging from commercial to critical military and health care applications [1]. In these networks a large number of small sensor nodes are deployed, each capable of collecting, storing, processing observations and communicating over short-range wireless interfaces and multiple hops to central locations called sinks. These networks also collect and disseminate information or data from the hostile environment and left unattended for several weeks or months for environmental monitoring. However, the nodes in WSNs have severe resource constraints due to their lack of processing power, limited memory, bandwidth and energy [2]. Since these networks are usually deployed in remote places and left unattended, they are vulnerable to security threats because the traditional security measures are not sufficient to protect these networks during information dissemination process.

The researchers in WSNs have proposed various security mechanisms which are optimized for these networks with resource constraints. A number of security mechanisms has been proposed by several researchers in WSNs including TinySec [3], MiniSec [4], LLSP [5] and LEDS [6]. Both TinySec and LLSP are the link layer security mechanisms, while MiniSec and LEDS provide network layer end-to-end security. Most of these mechanisms adding some critical security measures in terms of computational power, energy consumed and memory usage that poses significant challenges in designing a suitable security mechanism for WSNs.

In this paper, through extensive simulation we only evaluated the capability of TinySec security measures; Authentication-only (TinySec-Auth) and Authentication Encryption (TinySec-AE) in order to identify the suitability of these two security measures for WSN applications and their effect on the performance of the network. The evaluation is conducted through simulation in terms of packet transmission time, average number of packet received and energy consumption.

The rest of the paper is organized as follows. In Section II, we summarized the vulnerabilities and known attacks in WSNs. Next, we briefly described security mechanisms in TinySec which includes Authentication-only (TinySec-Auth) and Authentication Encryption (TinySec-AE) in Section III. Then, the simulation tool used, setup parameters and evaluation metrics are outlined in details in section IV. The simulation results are presented in section V. In Section VI, we includes the recent related work on the existing security mechanisms in WSNs. Lastly, section VII concludes the paper and outlines the future work.

II. Security Vulnerabilities and attacks in WSNs

Although there are tremendous number of potential WSN applications can be deployed such as environment monitoring, military and surveillance applications, the nature of the sensors itself poses a number of security threats when deployed in these applications. These threats are due to the wireless nature and resource constraints of the sensor networks and resources on the wireless sensor nodes. This means that security architectures used for traditional wireless networks is not possible to be used on these networks. Furthermore, WSNs have an additional vulnerability because nodes are often placed in a hostile and unattended environment with no

978-1-4799-3251-1/13 $31.00 © 2013 IEEE
DOI 10.1109/AIMS.2013.76