
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  
†Centre for Pre-University Studies, Universiti Malaysia Sarawak, 94300 Sarawak, Malaysia

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
Attacks on WSNs can be classified from two different levels of views; attack against security mechanism or against basic mechanisms (like routing mechanisms) and some of the major attacks are as follows [7], [8]:

- Denial of Service (DoS) attack: It occur at different layers such as jamming and tampering (physical layer); collision, exhaustion, unfairness (link layer); neglect and greed, homing, misdirection, black holes (network layer); malicious flooding and desynchronization (transport layer).
- Worm hole attack: When the neighboring nodes think the message was sent from the sender node (which is usually out of range), so they attempt to send the message to the originating node, but it never arrives since it is too far away.
- Sinkhole attack: The adversary’s aim is to lure nearly all the traffic from a particular area through a compromised node, creating a metaphorical sinkhole with the adversary at the center.
- Sybil attack: A single malicious node will appear to be a set of nodes and will send incorrect information to a node in the network.
- Selective Forwarding attack: When certain nodes do not forward many of the messages they receive, the network.
- Passive information gathering: Interception of the messages containing the physical locations of sensor nodes allows an attacker to locate the nodes and destroy them.
- Node capturing: A particular sensor might be captured, and information stored on it might be obtained by an adversary.
- False or Malicious Node: The insertion of false information by the compromised nodes within the network.
- Hello flood attack: The Hello flood attacks can be caused by a node which broadcasts a Hello packet with very high power, so that a large number of nodes even far away in the network choose it as the parent and all messages now need to be routed multi-hop to this parent, which increases delay.

III. SECURITY MECHANISM IN TINYSEC FOR WSNs

TinySec is a lightweight secure link layer security solution for tiny sensor devices of WSNs that consume low energy and memory usage [3]. There are four main aims of TinySec [3]:

- Access control: Only authorized nodes which possess the shared group key should be able to participate in the network.
- Integrity: A message should only be accepted if it was not altered in transit to prevent man-in-the-middle attacks where an adversary overhears, alters, and re-broadcasts messages.
- Confidentiality: Unauthorized parties should not be able to infer the content of messages.
- Ease of use: TinySec should not be difficult to use for a new or existing users.

The core of TinySec is an efficient block cipher and keying mechanism that is tightly coupled with the Berkeley TinyOS [9] radio stack. TinySec currently utilizes a single, symmetric key that is shared among a collection of sensor network nodes. Before transmitting a packet, each node first encrypts the data and applies a Message Authentication Code (MAC), a cryptographically strong unforgeable hash to protect data integrity. The receiver verifies that the packet was not modified in transit using the MAC and then deciphers the message.

TinySec also supports two different security mechanism which are Authentication-only (TinySec-Auth) and Authentication Encryption (TinySec-AE) [3] for security solution in WSNs. In authentication only mode, TinySec authenticates the entire packet with a MAC, but the data payload is not encrypted. With authenticated encryption, TinySec encrypts the data payload and authenticates the packet with a MAC. The MAC is computed over the encrypted data and the packet header. However, it compromises the level of security with these authentication and encryption measures. Therefore, in this paper we studied how far the impact of these security implementation on the performance of network.

TinySec’s packet format is based on the current packet format in TinyOS. The common fields are destination address, active message (AM) type, and length. Active message types are similar to port numbers in TCP/IP. The AM type specifies the appropriate handler function to extract and interpret the message on the receiver. These fields are unencrypted because the benefits of sending them in the clear generally outweigh any extra protection from keeping them secret. Figure 1 and Figure 2 show the different packet format of TinySec-Auth and TinySec-AE.

IV. SIMULATION TOOL, SETTINGS AND METRICS

Here we give the emphasis for the evaluation of TinySec-Auth and TinySec-AE security mechanism in order to identify their effects on the performance of the network. The simulations are performed using AVrora network simulator latest version Beta 1.7.115 that is an open source discrete event simulation tool, which means it simulates events such as sending, receiving, forwarding and dropping packets.
A. Simulation Tool

AVRora[10] is a suite of simulation tools for WSN by UCLA Compilers Group. It is originally created to simulate Atmel AVR microcontroller-based sensor nodes with clock-cycle accurate execution of microcontroller programs, allowing real program to be run with precise timing. It takes an object dump of in tinyos programs over AVR platforms such as mica2/micaz and is capable of single node emulation for verification of the program as well as multiple node simulation. AVRora is implemented in Java and runs code in an instruction-by-instruction fashion. AVRora also provides many useful features to support the research on WSN, like control flow graph generation, energy analysis, and mobility extension model.

B. Simulation Settings

In this work, we consider a network of nine nodes placing initially in a grid topology as shown in Figure 3. The performance of TinySec-Auth and TinySec-AE are evaluated in terms of packet transmission time, average number of packet received and energy consumption. Table 1 shows the simulation parameters used in this evaluation.

C. Simulation Metrics

In order to evaluate the capability of TinySec-Auth and TinySec-AE on how they perform in WSNs, we focused on two metrics as follows:

- Packet transmission time: This metric can be defined as the time taken to sent data by the source to the base station (sink).
- Average number of packet received: This metric can be defined as the average number of packet received by the sink throughout the simulation time.
- Energy consumption: Energy consumption is defined as the amount of energy consumed by nodes in the network through radio communication and processing. So, the total network energy consumed, given as $P_E$, can be calculated by adding all energy consumed by each nodes for transmission (TX), received (RX) and processing throughout the simulation time. The equation for total energy consumption is written as below where this equation totals up the energy consumed in all nodes when they send and receive the association and data packets.

$$P_E = \sum_{i=1}^{n} (E_{TX}^i + E_{RX}^i)$$

V. Experimental Results

There are several experiments have been conducted in order to show the impact of TinySec security measures on the network performance of WSNs. Three important evaluation metrics have been analyzed which are packet transmission time, average number of packet received and energy consumption.

A. Effects on Packet Transmission Time

Figure 4 shows the different time required to send packet using TinySec-Auth and TinySec-AE. From the simulation results, TinySec-AE took more time to send data to sink in comparing to TinySec-Auth which is 0.9 percent in different. This is due to extra computation time taken for the cryptography to be performed in TinySec-AE. In addition, TinySec-AE has increased its packet size by 5 bytes from the original TinyOS packet size that effects its performance in the network.

B. Effects on Average Number of Packet Received

From the simulation results in Figure 5, the average number of packet received by sink node using TinySec-AE is much higher when comparing to TinySec-Auth implementation. This might be due to extra packet size in the authentication process. As a bigger size of packet will require longer time to transmit which effect the performance of TinySec-AE in WSNs. The extra computation incurred by implementing TinySec-AE also contributed to the low average number of packet received by using TinySec-AE.
C. Effects on Energy Consumption

Figure 6 shows the different total energy consumed by all nodes when sending and receiving packets in using TinySec-Auth and TinySec-AE mechanisms. From the simulation results, TinySec-AE has consumed more than 5 percent of energy in comparing to TinySec-Auth. The reason for the higher energy consumption by using TinySec-AE is because of extra packet overhead incurred in the implementation of this security mechanism.

VI. RELATED WORK

This section reviews the recent related work which directly or indirectly aims at evaluating the existing security mechanisms in WSNs. There are several previous research works which attempt to evaluate different security mechanisms of WSNs as in [8], [11]. The authors of [8] evaluated different security mechanism in terms of packet delivery ratio, latency and energy consumption. In [11], the authors evaluated the performances of two different cryptosystems in terms of their response time, memory usage and packet length. In this paper, we evaluated both authentication and encryption measures in TinySec [3] in terms of packet transmission time, average number of packet received and energy consumption as in [8]. We studied TinySec [3] because this security protocol is fully-implemented link-layer security protocol that has been implemented on TinyOS [9] which is the most dominant choice as operating system for WSNs.

VII. CONCLUSION AND FUTURE WORK

In this paper we have presented the evaluation of TinySec security mechanisms in WSNs on different evaluation metrics which are packet transmission time, average number of packet received and energy consumption. We have demonstrated through extensive simulation that there is significant differences between the performance of TinySec-AE with TinySec-Auth due to different packet size, computation time and security measure implemented. From the simulation results, we can conclude that TinySec-AE cannot perform better than TinySec-Auth in WSNs for trade off between the more secured mechanism used and network performance wise. In this case, we believe that there is certainly a need for an improvement of TinySec security mechanism to balance between both performance and secured networks to successfully implement TinySec in WSNs.

There are several avenues for further studies:

• To design a secure and lightweight TinySec that can perform better in WSNs.
• To evaluate the proposed TinySec in mobile and static WSNs environment.

ACKNOWLEDGMENT

This research work is supported by the Ministry of Education through the Fundamental Research Grant Scheme (FRGS/ICT03(01)/993/2013(34)). The authors would like to thank Universiti Malaysia Sarawak (UNIMAS) and Faculty of Computer Science and Information Technology (FCSIT) for the research opportunity and support in providing space and tools in conducting this research work.
REFERENCES


