2009 Fifth International Conference on MEMS NANO, and Smart Systems

Analysis of Packets Abnormalities in Wireless Sensor Network

A.H Azni, Azreen Azman, Madihah Mohd Saudi, AH Fauzi, DNF Awang Iskandar
Universiti Sains Islam Malaysia Bandar Baru Nilai, 71800 Negeri Sembilan, MALAYSIA
Universiti Malaysia Sarawak, Kota Samarahan, 94300 MALAYSIA
e-mail: ahazni@usim.edu.my, azreen@usim.edu.my, madihah@usim.edu.my, hadinata@fit.unimas.my, dnfaiz@fit.unimas.my

***Abstract*—Wireless Sensor Networks (WSNs) use tiny, inexpensive sensor nodes with several distinguishing characteristics: they have very low processing power and radio ranges, permit very low energy consumption and perform limited and specific monitoring and sensing functions. However, its security becomes an issue because in WSNs, there is virtual communication by passing the data through sensor via internet. Caused of its limited capability, an intruder can attack the communication easier. Furthermore, routing in wireless sensor networks has, to some extent, been reasonably well studied. However, most current research has focused primarily on providing the most energy efficient routing. There is a great need for both secure and energy efficient routing protocols in WSN. Therefore, this project studies about the packets in WSN. To achieve the objectives, this project used AODV routing protocol to analyze the packets abnormalities in WSNs by using simulation technique. To show the differentiations of packets behaviors, the simulations have been conducted on AODV routing protocol under malicious node and without malicious node. It also conducts an analysis of packets behavior on flooding attack.**

Keywords-WSN, Packet Abnormalities, Security Threats, AODV

I. INTRODUCTION

Wireless sensor network (WSN) consists of thousands, even millions of tiny devices equipped with signal processing circuits, microcontrollers, and wireless transmitters or receivers, in addition to embedded sensors. Nodes are randomly and densely deployed over the sensing field, leading therefore to a need for auto organization capability. Due to sensor networks improvised nature, it frequently established in insecure environments, which make them susceptible to attacks. These attacks are launched by participating malicious nodes against different network services. Then, these malicious nodes will interrupt the network communication during transmitting data in WSN. It will change the packets behaviors to abnormal. Hence, these malicious nodes may conquer the network by eliminating other nodes that connecting to the network.

Therefore, this project aims to do an analysis of packets abnormalities in WSN by using Network Simulator 2 (NS2). Since the routing protocols, which act as the binding force in these networks are a common target of these nodes, this project will simulate the protocol in order to analyze the packets abnormalities in WSN. The simulation will be conducted by simulating the routing protocol within the malicious nodes and without the malicious nodes. After that, the results of the both simulations will be analyzing and differentiating to compare the packets behaviors in order to find out the packet's abnormalities.

II. WIRELESS SENSOR NETWORKS (WSN)

Wireless Sensor Networks (WSN) is composed of a large number of sensor nodes, which is a small, lowcost, low-power device that communicate on short distances, sense environmental data and perform limited data processing. It forms a particular class of ad hoc networks that operate with little or no infrastructure. Djamel and Lyes in [1] mentioned that several such wireless sensors are in a region of self-organize.

Typical functions in a WSN include sensing and collecting data, processing and transmitting sensed data, possibly storing data for some time, and providing processed data as information e.g. to called sink node [2]. The basic idea of this functions is to disperse tiny sensing devices; which are capable of sensing some changes of incidents, parameters and communicating with other devices, over a specific geographic area for some specific purposes like target tracking, surveillance, environmental monitoring etc. Information based on sensed data can be used in agriculture and livestock, assisted driving or even in providing security at home or in public places.

Today's sensors can monitor temperature, pressure, humidity, soil makeup, vehicular movement, noise levels, lighting conditions, the presence or absence of certain kinds of objects or substances, mechanical stress levels on attached objects, and other properties. Therefore, the WSN is an important mechanism to be used in the in military, medical, monitoring and other applications.

A. Security Requirement in WSN

A sensor network is a special type of network. It shares some commonalities with a typical computer network, but also poses unique requirements of its own. Below are the important requirements that should be considered:

2.1.1 Data Confidentiality.

In sensor networks, the confidentiality relates to the following [3][4] :

978-0-7695-3938-6/09 $25.00 © 2009 IEEE
DOI 10.1109/ICMENS.2009.64