ANALYSIS OF PACKETS ABNORMALITIES IN WIRELESS SENSOR NETWORK

A.H Azni 1, Madiah Mohd Saudi 2, AF Fauzi 3, DNF Awang Iskandar 4
1,2 Faculty of Science and Technology, Universiti Sains Islam Malaysia, Bandar Baru Nilai, 71800 Negeri Sembilan, Malaysia
3,4 Faculti of Computer Science and Information Technology, Universiti Malaysia Sarawak, Kota Samarahan, 94300 Sarawak, Malaysia
email: ahazni@usim.edu.my 1, madihah@usim.edu.my 2, hadinata@fit.unimas.my 3, dnfaiz@fit.unimas.my 4

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 abnormalities 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

1 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.

2 WIRELESS SENSOR NETWORKS

Wireless Sensor Networks (WSN) is composed of a large number of sensor nodes, which is a small, low-cost, 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.

2.1 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]:

- A sensor network should not leak sensor readings to its neighbors. Especially in a military application, the data stored in the sensor node may be highly sensitive.
- In many applications nodes communicate highly sensitive data. Therefore it is extremely important to build a secure channel in a wireless sensor network.
- Public sensor information, such as sensor identities and public keys, should also be encrypted to some extent to protect against traffic analysis attacks.

2.1.2 Data Integrity

With the implementation of confidentiality, an attacker may be unable to steal information [5]. However, this doesn’t mean the data is safe. The attacker can change the data by interrupt or eavesdrops the communication. For example, a malicious node may add some fragments or manipulate the data within a packet. This new data can then be sent to the original receiver. Data loss or damage can even occur without the presence of a malicious due to the harsh communication environment. Thus, data integrity ensures that any received data has not been altered in transit.

2.1.3 Availability

Adjusting the traditional encryption algorithms to fit within the wireless sensor network is not free, and will introduce some extra costs. Some approaches choose to modify the code to reuse as much code as possible or to make use of additional communication to achieve the same goal.

2.2.4 Self-Organization

A wireless sensor network is a typically an ad hoc network, which requires every sensor node be independent and flexible enough to be self-organizing and self-healing according to different situations. There is no fixed infrastructure available for the purpose of network management in a sensor network. This inherent feature brings a great challenge to wireless sensor network security as well. In the same way that distributed sensor networks must self-organize to support multihop routing, they must also self-organize to conduct key management and building trust relation among sensors. If self-organization is lacking in a sensor network, the damage resulting from an attack or even the hazardous environment may be devastating.

2.2 Routing Threats in WSN

WSN pose unique challenges and because of this, traditional security threats that all the other wireless network face cannot assumed for WSN. There are many papers present the significant security problems. Djamel and Lyes in [1] mentioned that two kinds of attacks can be launched against WSN, Passive and Active. In passive attacks the attacker does not disturb the routing protocol. It only eavesdrops upon the routing traffic and end eavours to extract valuable information like node hierarchy and network topology from it. In active attacks, malicious nodes can disturb the correct functioning of a routing protocol by modifying routing information, by fabricating false routing information, and by impersonating other nodes. The simplicity of many routing protocols for WSN makes them an easy target for attacks. The routing attacks in WSN can be classified into the following categories [11]:

2.2.1 Spoofed, altered, or replayed routing information

While sending the data, the information in transit may be altered, spoofed, replayed, or destroyed. Since sensor nodes usually have only
short range transmission, an attacker with high processing power and larger communication range could attack several sensors simultaneously and modify the transmitted information.

2.2.2 Wormholes

Wormhole attack is an attack in which the malicious node tunnels messages from one part of the network over a link, that doesn’t exist normally, to another part of the network. The simplest form of the wormhole attack is to convince two nodes that they are neighbors. This attack would likely be used in combination with selective forwarding or eavesdropping.

2.2.3 HELLO flood attacks.

This attack is based on the use by many protocols of broadcast Hello messages to announce them in the network. So an attacker with greater range of transmission may send many Hello messages to a large number of nodes in a big area of the network. These nodes are then convinced that the attacker is their neighbor. Consequently the network is left in a state of confusion.

2.2 WSN Routing Protocols

Routing protocol is important in WSN. It plays an important role in determining the effectiveness of the application deployed. Routing protocols are created to compromise many aspect of packet transmission effectiveness such as collision prevention, faster time transmission, energy saving and more.

Routing protocols in WSN might differ depending on the application and network architecture. In general, routing in WSN can be divided into flat base routing, hierarchical based routing and location based routing depending on the network structure. Furthermore, these protocols can be classified into multi-path-based, query-based, negotiation based, Qos-based and coherent-based depending on the protocol operation [12].

In flat-based routing, all nodes are typically assigned equal roles or functionality. In hierarchical based routing, nodes play different role in the network. In location based routing, sensor node’s positions are exploited to route data in the network. A routing protocol is considered adaptive if certain system parameters can be controlled in order to adapt to the current network conditions and available energy levels.

2.2.1 Ad hoc On Demand Distance Vector (AODV)

The Ad hoc On Demand Distance Vector (AODV) protocol is a routing protocol designed for ad hoc mobile networks. It is an on demand algorithm, meaning that it builds routes between nodes only as desired by source nodes. It maintains these routes as long as they are needed by the sources.

AODV is a hop-by-hop routing protocol [1]. When a node needs to send a data packet to a destination to which it has no route, it has to broadcast a route request (RREQ) to all its neighbors, and then each neighbor does so until reaching the destination (or a node with a valid route to the destination). This node sends a route reply (RREP) packet that travels the inverse path until reaching the source. Upon the reception of this reply each intermediary updates its routing table. In this way a route between the source and the destination is built. Since it relies on the distance vector principle, AODV assigns monotonically increasing sequence numbers to routes, which define route freshness, as well as hop count, which defines route optimality.

3 METHODOLOGY

To achieve the objectives of the project, we investigated and address a specific security protocol related to WSN. There are so many protocols involved in WSN. In general, each layer has their own protocols in order to ensure the security threats in WSN. However, we decided to use routing protocol in network layer for the analysis.

In addition, there are a few protocols contributed in routing protocol to ensure the network security in WSN such as GPSR, DSR, TinyOS and others. Hence, we decided to use only one of the protocols for the analysis. Then, we studied and analyzed the existing protocols to identify the suitable protocol for this project.

AODV protocol has been selected as the appropriate protocol in this study. To define as much possible information of the protocol, we reviewed the existing paper related to AODV protocol to get more information. Then, we simulate the protocol and analyze the simulation result to measure the performance and efficiency of the protocol by differentiates the throughput of the simulation without the malicious node and within the malicious node.

In this project, a particular network designing tool or simulator, called Network Simulator 2 (NS2) version 2.29 is being used to
model the network, create the scenarios and simulate the scenarios that have been created and obtaining the result for the analysis.

The network scenario may be deployed based on a wide range of parameters such as network size which consist the number of nodes, communication distance, speed of packet transmitting and others. The network can be used to simulate the detection of vectors traveling across the sensor network field.

NS2 was created based on Unix environment. It works very well with Linux. It’s also possible to install and run NS2 from in Windows machine. However, we need Cygwin to run the simulation. The simulation also supported by the Tcl script and C++ programming language. Then, the simulation results were analyzed in Microsoft Excel.

4 ROUTING PROTOCOL ANALYSIS

Figure 1 shows that a green node will transmit the data into the server. In the transmission, the node will sent the signal to its neighbors randomly before reach the sink signal. Unfortunately, one of its neighbors which is a red node is a malicious node that wants to attack the transmission data for the hijack. Then, it will eavesdrop and intercept the data before forward it. Therefore, the data transmission of this communication is vulnerable to attack and not secure.

There are several type of routing protocol contribute in WSN to ensure the security such as directed diffusion, LEACH, GPSR, TinyOS, DSR, AODV and other. Although, from all type of these protocols, only AODV protocols will be analyze details in the project.

The AODV routing protocol is a reactive routing protocol [15]; therefore, routes are determined only when needed. Figure 2 shows the message exchanges of the AODV protocol.

![Figure 2: AODV protocol messaging](image)

The major vulnerabilities present in the AODV protocol are:
- Deceptive incrementing of Sequence Numbers: Destination Sequence numbers determine the freshness of a route. The destination sequence numbers maintained by different nodes are only updated when a newer control packet is received with a higher sequence number. Normally the destination sequence numbers received via control packets cannot be greater than the previous value held by the node plus one. However, malicious nodes may increase this number to advertise fresher routes towards a particular destination.
- Deceptive decrementing of Hop Count: AODV prefers route freshness over route length. In that, a node prefers a control packet with a larger destination sequence and hops count over a control packet with a smaller destination sequence and hop count. However, if the destination sequence numbers are the same then the route with the least hop count is given preference. Malicious nodes frequently exploit this mechanism in order to generate fallacious routes that portray minimal hop counts.

4.1 Design Requirement

In having a complete simulation model, the flow must begin with create derived models of nodes and links. This is important part to illustrate the implementation and illustration of routing protocol that want to be tested. Then, second step starting with customizing the network environment. These processes are a programming task using Tcl script and C++ programming language. After that, run the simulation in NS2. Lastly, get the simulation result and analyzes it.

4.2 Simulation Testing and Result

The packets abnormalities were analyzed on AODV protocol under a malicious node. In this
simulation, we configured a malicious node’s behaviors by modifying the node forwarding mechanism. It is a selfish behavior of a node to increase its network performance. There were three sessions produced for the simulation in order to analyze the packets abnormalities by using NS2 supported by NAM simulator. Each session differentiated by used different number of nodes in the scenario with following parameters:

Table 1: Simulation parameters (session 1)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simulation time</td>
<td>60 ms</td>
</tr>
<tr>
<td>Number of mobile nodes</td>
<td>3</td>
</tr>
<tr>
<td>Routing protocol</td>
<td>AODV</td>
</tr>
<tr>
<td>Propagation Delay</td>
<td>100 ms</td>
</tr>
<tr>
<td>Traffic</td>
<td>Constant bit rate</td>
</tr>
</tbody>
</table>

Table 2: Simulation parameters (session 2)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simulation time</td>
<td>60 ms</td>
</tr>
<tr>
<td>Number of Mobile Nodes</td>
<td>6</td>
</tr>
<tr>
<td>Routing Protocol</td>
<td>AODV</td>
</tr>
<tr>
<td>Propagation Delay</td>
<td>100 ms</td>
</tr>
<tr>
<td>Traffic</td>
<td>Constant bit rate</td>
</tr>
</tbody>
</table>

Table 3: Simulation parameters (session 3)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simulation time</td>
<td>60 ms</td>
</tr>
<tr>
<td>Number of mobile nodes</td>
<td>9</td>
</tr>
<tr>
<td>Routing Protocol</td>
<td>AODV</td>
</tr>
<tr>
<td>Propagation Delay</td>
<td>100 ms</td>
</tr>
<tr>
<td>Traffic</td>
<td>Constant bit rate</td>
</tr>
</tbody>
</table>

For the evaluation we use the following metrics:

1. Packet Delivery Ratio: The packet delivery ratio of a receiver is defined as the ratio of the number of data packets actually received over the number of data packets transmitted by the sender.
2. End-to-end Delay: It is defined by calculate the delay of each transmitted packet during the simulation. Average delay is calculated by dividing the total delay by the number of packets arrived at destination.
3. Packets Redundancy: The packets redundancy defined as the percentage of the duplicated packets over the received packets. Its evaluation was analyzed only on flooding.

The simulation result show in the figure 4 below:

Figure 3: Average packet delivery ratio

Figure 4: Comparison end-to-end delay within malicious node and without malicious node

Figure 5 Overall packet delivery ratios under flooding

Figure 6: Overall packet redundancy under flooding

According to the result of analysis, packets delivery ratio decrease within the attendance of the malicious nodes. Figure 3 show that the packets delivery ratios of the simulation without the malicious nodes are higher than the packets delivery ratios of the simulation within the malicious nodes. Since a modification of the forwarding methods will dropping the forward able packets with specified
rates, the malicious nodes will be able to reduce the number of packets received. Besides that, delay of the packets transmission will also increase when the malicious node interrupt the network as shown in figure 4. Figure 5 show the overall packets delivery ratios under flooding. The packets delivery ratio will decrease when flooding occurs. Then, figure 6 illustrated the packets redundancy under flooding. Packets redundancy will be consistent when it achieves the maximum redundancy values. Figure 6 shows the maximum redundancy values under flooding is 50 percent.

5 CONCLUSION

Security threats in WSN will affect the performance of data transmissions. It is shown by the results of the simulation that the malicious node has high effect on packets behaviors. Based on the results, the delivery packet ratio will decrease within the malicious node attendance. Then, the time a packet takes to travel from the source to destination node also will increase.

Therefore, people should be emphasizing on security threats in WSN. Besides that, a new protocol also should be introduced to improve the security of packets transmissions and its effectiveness. This aim is important to ensure the performance and security of future networks.

REFERENCES