Detecting Sinkhole and Selective Forwarding Attack in Wireless Sensor Networks

Umashri Karkikatti¹, Nalini N²

¹PG Scholar, Computer Science Engineering Department, NitteMeenakshi Institute of Technology, Bangalore-64 India
²Professor, Computer Science Engineering Department, Nitte Meenakshi Institute of Technology Bangalore-64, India

Abstract:-Wireless Sensor Networks (WSN’s) are a promising approach that are useful for variety of applications, such as monitoring safety and security of buildings and spaces, military applications, measuring traffic flows, tracking environmental pollutants, etc. Security for WSNs is a very serious and challenging task these days as they have very important personal or national security level information’s in them, mainly following are the challenges faced while designing for a robust secure WSNs, the devices in the sensor networks have severe constraints such as minimal energy, minimal computational and communicational capabilities. And secondly, there is an additional risk of physical attacks such as node capture and tampering, eavesdropping etc. Hence we need a technique which can detect the intrusion of any malicious node in the networks, which can create an alarm for taking appropriate steps to secure the information in the WSN. these techniques should be lightweight because of resource-constrained nature of WSNs[1]. As we are aware of the different kinds of attacks for WSNs. In this paper we propose the lightweight robust technique called Received Signal Strength Indicator (RSSI) for detecting Sinkhole attacks in the WSNs. We have built our own protocol and the RSSI techniques are applied to detect the sinkhole attack. The RSSI technique doesn’t cause communication overhead because it will not load the ordinary nodes since the presence of EM nodes. Also we propose a lightweight scheme called Traffic Monitor Based Selective Forwarding Attack Detection Scheme. Our approach uses EM nodes to eavesdrop and monitor all traffics of the network.RSSI technique was earlier implemented using visual sense. In this paper we have implemented RSSI technique in NS2 simulator. The simulation results show the efficient detection of the Sinkhole attacks in WSNs.

Keywords: WSN, RSSI, detecting sinkhole attacks and selective forwarding attack, intruder detection

1. Introduction

Sensor networks will play an essential role in the upcoming age of pervasive computing, as our personal mobile devices will interact with sensor networks in our environment. Many sensor networks have mission critical tasks, so it is clear that security needs to be taken into account at design time. Sensor networks are always deployed in open and unattended areas, hence they are subject to a diversy, WSNs have limited power supplies, low bandwidth, small memory sizes and limited energy. Above situations require environment to provide secuity. The resource-starved nature of sensor networks poses great challenges for security. Besides the battlefield applications, security is critical in premise security and surveillance, building monitoring, burglar alarms, and in sensors in critical systems such as airports, hospitals[3].

Most of the sensors or network protocols are quite simple, and for this reason are seldom times even more susceptible to attack. A malicious node which presents multiple identities to the network is called Sybil attack. A malicious node which presents multiple identities to the network is called Sybil attack.

1.1 Security Goals

When dealing with security in WSNs, we mainly focus on the problem of achieving so me of all of the following security contributes or services:

- **Confidentiality:** Confidentiality refers to data in transit to be kept secret from eavesdroppers. He re symmetric key ciphers preferred for their low power consumption.
- **Integrity:** Integrity measures that the received data is not altered in transit by an adversary.
- **Authentication:** Authentication enables a node to ensure the identity of the peer with which it is communicating.
- **Availability:** The service should be available all the time.
- **Data Freshness:** It suggests that the data is recent, and it ensures that no old messages have been replayed.
- **Non-repudiation:** It de notes the node can not deny sending a message it has previously sent.
- **Authorization:** It ensures that only authorized nodes can be accessed to network services or resources.

1.2 Attacks on Wireless Sensor Networks

Major attacks on sensor networks are as follows.

- **Jamming:** Jamming interferes with the radio frequencies of the sensor nodes. If t he network then that constitutes complete DoS.
- **Tampering:** A tampering attacker may damage a sensor or node, replace the entire node or part of its hardware to gain access to sensitive information, such as shared cryptographic keys.
- **Spoofed, altered or replayed routing information:** The attacker’s malicious activity can complicate the network and create routing loops, attracting or repelling traffic, generating false error messages, partitioning the network.
- **Sybil Attack:** A malicious node which presents multiple identities to the network is called Sybil attack.
• **Wormholes**: The adversary tunnels messages received in one part of the network over a low latency link, to another part of the network where the messages are then replayed.

• **Hello flood attacks**: If in any routing protocols, nodes broadcast hello messages to announce their presence to their neighbors. A node receiving such messages can assume that at the node when a hello message is sent and other messages are in its range. An attacker with a high-powered antenna can convince every node in the network that it is the correct neighbor.

• **Sinkhole Attack**: In a sinkhole attack, the adversary’s goal is to attract traffic from a part of the network to a compromised node. Traffic is thus redirected to a node that may not be able to handle the traffic or may refuse to forward it.

• **Selective Forwarding Attack**: In a selective forwarding attack, the attacker selectively drops packets based on some predefined criterion, which makes it even harder to detect. Even though there can be many different versions of these attacks, in our implementation, we focus on an address-based selective forwarding attack. As shown in Fig. 2, the attacker selectively drops packets based on the source address. In this example, the attacker forwards all packets except those from orange nodes.

### 2. Related Work

The first theory for the detection of sinkhole attacks was proposed by Ngai [4]. This approach involved base station in the detection process, wherein it sends the request for all the nodes in the network for their IDs. In return, the nodes reply with their IDs to the BS. The ID consists of the node position, next hop position, and the node context. The information received is then used to build a network flow graph for identifying the sinkhole.

Krontiris used a distributed rule-based detection system to detect sinkholes [5]. Two rules were implemented to detect intrusion detection system. An alarm is sent by the intrusion detection system when either one of the rules is violated by the node IDs of the nodes. If this is not the case, produce an alert and broadcast it to your neighbors.”

Rule 2: “For each overhead route update packet, check the sender field, which must be the node ID of one of your neighbors. If this is not the case, produce an alert and broadcast it to your neighbors.” A collaborative approach can then be used to identify and exclude the sinkhole.

In later work, Krontiris, and Dimiropoulos proposed a similar rule-based approach [6]. Their two rules were: “For each overhead route update packet, check the sender field, which must belong to one of your neighbors” and “For each [parent, child] pair of your neighbors, compare the link quality estimate against the current routing table. If the difference cannot exceed 50.” While this approach will not by itself identify a node as a sinkhole, extension to a collaborative approach should be used.

Yu [14] proposed a lightweight security scheme for detecting selective forwarding attacks. The detection scheme uses a multi-hop acknowledgment technique to launch alarms by obtaining responses from intermediate nodes.

### 3. Assumptions and Network Model

WSNs has many sensor nodes and a BS. Sensor nodes are characterized by low power, low bandwidth, low communication and computational capabilities, whereas the BS has a high bandwidth, high power and hence multiple nodes can send data to the BS for processing. In the case of one communication model, which is at a very high risk of sinkhole attack. The untrusted node may be able to detect the data or perform selective forwarding attack. Most of the current routing protocols in the sensor network work in a way that is susceptible to the sinkhole attack.

The physical displacement attack is very harmful for the WSNs because it can lead to start of other severe attacks. We assume that at the beginning a static network, next
we assume that attackers can physically displace or remove some of the sensor nodes. Finally we assume that the BS and EM node are physically protected or has temper robust hardware [8], hence it acts as central trusted authority in our algorithm design.

4. RSSI Based Technique to Detect Sinkhole Attack

4.1 Calculating the RSSI value

Tumrongwittayapak and Varakulsiripunth proposed a system that uses the RSSI (Received Signal Strength Indicator) value with the help of extra monitor (EM) nodes to detect sinkhole attacks [9 10]. The RSSI [7] technique measures the power of the signal at the receiver. The RSSI has been used mainly for RF signal, and the estimate unit is dBm or mW. We assume bi-directional radio links between two neighboring sensors. Referring to the path loss based model, we calculate the distance between the transmitter and receiver with the effective propagation loss like multi-path propagation and shadow fading. Most widely used signal propagation model [11] is the lognormal shadowing model shown as below,

\[
R(d) = P_t - PL(d_0) - 10\eta \log_{10}(d/d_0) + X
\]

Where, \( R(d) \) is the RSSI value recorded at distance \( d \), \( P_t \) is the transmit power, \( PL(d_0) \) is the path loss for a reference distance \( d_0 \), \( \eta \) is the path loss exponent, and \( X \) is a Gaussian random variable with zero mean and \( \sigma^2 \) variance, that models the random variation of the RSSI value. RSSI-based localization scheme is introduced in [12]. It argues that if at least four sensors monitor radio signals, then a user cannot hide its location. Suppose node \( Em_i \) receives radio signal from node \( A \), then the RSSI is

\[
R_{Em_i} = (P_A.K)/(d_{Em_i})^\alpha
\]

Where \( P_A \) represents transmitter power at node \( A \), \( R_{Em_i} \) is RSSI value, \( K \) is constant, \( d_{Em_i} \) is Euclidean distance between node \( EM_i \) and node \( A \), and \( \alpha \) is distance-power gradient. Suppose node \( j \) receive radio wave from node \( A \) at the same time, then the \( R_{Em_i} \) is similar to equation.

The RSSI ratio of node \( EM_i \) to \( EM_j \) is

\[
R_{Em_i}/R_{Em_j} = ((P_A.K)/(d_{Em_j})^\alpha)/((P_A.K)/(d_{Em_i})^\alpha)
\]

(3)

And the user’s location \( (x, y) \) can be computed by solving following equation through four receivers \( EM_i, EM_j, EM_k \) and \( EM_l \):

\[
\begin{align*}
(x-x_{Em_i})^2 + (y-y_{Em_i})^2 &= (R_{Em_i}/R_{Em_j})^{1/\alpha}((x-x_{Em_j})^2 + (y-y_{Em_j})^2) \\
(x-x_{Em_j})^2 + (y-y_{Em_j})^2 &= (R_{Em_j}/R_{Em_k})^{1/\alpha}((x-x_{Em_k})^2 + (y-y_{Em_k})^2) \\
(x-x_{Em_k})^2 + (y-y_{Em_k})^2 &= (R_{Em_k}/R_{Em_l})^{1/\alpha}((x-x_{Em_l})^2 + (y-y_{Em_l})^2) \\
(x-x_{Em_l})^2 + (y-y_{Em_l})^2 &= (R_{Em_l}/R_{Em_i})^{1/\alpha}((x-x_{Em_i})^2 + (y-y_{Em_i})^2)
\end{align*}
\]

Where \( x_{Em_i} \) and \( y_{Em_i} \) is the location of node \( EM_i \), and other notation is similar.

4.2 Visual Geographic Map Creation

When the network initializes, an assumption is made that an intruder will not attack for at least the first \( T \) periods, termed as Safe period, so that the system can learn about the normal behavior of the network such as routing information, position of all sensor nodes. Then we calculate a Visual Geographic Map (VGM) of the network by using RSSI value from the EM nodes. The visual geographic map is the graphical representation of the network model and simulates the traffic flow from the nodes to the BS.
VGM depending on the data from the four EM nodes as shown in figure 5.

4.3 RSSI based sinkhole attacks detection scheme

A brief explanation of our scheme is as shown in the figure below. Whenever any sensor node sends its message to the network, all the four EM nodes will receive the message and RSSI value. Next if the destination of the received message is BS, then all of the EM nodes will send RSSI value to RBSD to determine the position of the sensor nodes, then the VGM is updated. If the normal flow of the message is not seen in the VGM, then the Sinkhole attack is detected as shown in the figure 6 and 7.

5. Traffic Monitor Based Selective Forwarding Attacks Detection Scheme

The Selective forwarding attack is a byproduct of sinkhole attack; it is much more dangerous than Sinkhole attack. We propose a lightweight scheme called as Traffic Monitor Based Selective Forwarding Attacks Detection scheme. Our protocol uses EM nodes to monitor all traffic of the network as shown in the figure below.

As we see in the above algorithm EM node eavesdrops all the traffic in the network. And if the destination is BS then EM node generates the data (Node ID, Source ID, NextHop ID) to TM BSFD (Traffic Monitor Based Selective Forwarding Attacks Detector). TMBSFD then creates the trace table for the comparison of the data and hence for detecting if the selective forwarding detection. TM BSFD checks first if or if Source ID = Source IDTT , if this condition is NO then it resets the timer and the process again starts or else if Source ID = Source IDTT then the next condition is Node IDEM = Node IDTT if this condition is YES then it updates the
TT and reset the timer. Later it checks if Trace node = BS then it deletes the entire row in the TT else it checks for the timer threshold value, if it is more than the threshold value then it detects as Selective forwarding attack happening.

Trace table contains 3 columns mainly Trace node, Source ID and Timer. TMBSFD inserts the data in the row for each SourceIDEM = SourceIDTT and updates the same if NodeIDEM = Node IDTT, the third column timer is the time taken for every transaction between the source node and the BS. A threshold value is set and checking is done for the time for every transaction.

Figure 10: Example of EM Message and Trace Table

6. Simulation Setup and Results

We simulate a WSN with 100m X 100m field in which 25 nodes are placed with uniform random distribution. The sensors have radio range of 40m. A BS is placed at the centre of the network to collect data from the sensors. After that a sinkhole is added to the network at random coordinates of x,y for emulating a sinkhole attack.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simulation Area</td>
<td>100mX100m</td>
</tr>
<tr>
<td>No of Sensor nodes</td>
<td>25</td>
</tr>
<tr>
<td>Transmission Range</td>
<td>40m</td>
</tr>
<tr>
<td>Routing Protocol</td>
<td>AODV</td>
</tr>
<tr>
<td>Data Rate</td>
<td>20 per 0.005 sec</td>
</tr>
<tr>
<td>Packet Size</td>
<td>64 bytes</td>
</tr>
<tr>
<td>Simulation Time</td>
<td>12 sec</td>
</tr>
</tbody>
</table>

We evaluate the performance of our sinkhole detection algorithm through simulations. We have used NS-2 [15] for the simulation which lessens the network load. Sensor network packages [16] are configured on the top of NS-2, which involves the configuration of phenomenon channel, data channel, phenomenon nodes with the phenomenon routing protocol to capture real-time events. A threshold value is set and checking is done for the time for every transaction.

The success rate represents the percentage that our algorithm can correctly identify the sinkhole, the false positive rate represents the percentage that our algorithm identifies sinkhole falsely and the false negative rate represents the percentage that our algorithm is not able to identify any sinkhole but it exists. The graph below shows the success rates for dropping rates of 0, 0.2, 0.4, 0.6 and 0.8 respectively. 0% dropping rates, we see that the success rates are 100%. From 20-80% dropping rates the success rates are almost near to 100%.

Figure 12: Percentage of detecting Sinkhole Attacks

Figure 13 and Figure 14 show the false-positive rate and the false negative rate in detecting sinkhole attack. The simulation results indicate that the error rates are quite low. There is no false-positive and false-negative errors when dropping rate is between 0% to 40%. The error rates increase slightly with increasing of the dropping rate and the number of malicious nodes. When the number of malicious nodes increases, there is more incorrect network flow information provided to the BS. If many correct messages are dropped, the remaining wrong information can mislead the BS. The BS may incorrectly detect the malicious node and lead to a false-positive error. Similarly, the BS may receive inadequate number of messages to identify the intruder and bring a false-negative error.
The below Figure 15 shows the percentage of detecting Selective Forwarding Attacks which Trace Table size equal 128 bytes and Threshold value > 70 milliseconds. The results as seen are accurate and hence showcase effective efficient Selective Forwarding Attack Detection. Figure 16 shows the result of False Negative Rate and Figure 17 shows the result of False Positive Rate.

7. Conclusion and Future Scope

In this paper, we presented an effective method for identifying sinkhole attacks in a wireless sensor network. We introduced RSSI-based lightweight solution for detecting the Sinkhole attack in WSN. The functionality of the detection scheme is tested and the performance is analyzed in terms of detection accuracy. Also we proposed a lightweight scheme called Traffic Monitor Based Selective Forwarding Attack Detection Scheme. We have implemented RSSI technique in NS2 simulator. The simulation results show the efficient detection of the Sinkhole attacks and Selective Forwarding Attacks in WSNs. We achieve detection with 100% completeness and less percentage of false positive rates. In future work we will try to answer how we can extend our protocol to cope with other attacks in the WSNs.

References


Author Profile

Dr. Nalini N is currently working as Professor in computer science engineering in Nitte Meenakshi Institute of Technology Bangalore-64

Umashri Karkikatti is currently pursuing masters degree program in computer science engineering in Nitte Meenakshi Institute of Technology Bangalore-64 India.