Detection of gray hole attack in Wireless Sensor Networks using Support Vector Machine

Manish Kumar
Research Scholar, JIJT University, Rajasthan, India
manishnit4u@gmail.com

Abstract — The research demonstrates simulation of gray hole attack in wireless sensor networks in NS2. A node is suspected to be malicious if there is a large drop of packets observed at the node resulting very few or none of the packets are observed to reach the destination. First a modified AODV protocol is implemented for simulation of gray hole attack in wireless sensor network in the simulating environment. Thereafter detecting the same by making use of contingency table generated by the classification model based on support vector machine using trace file created during simulation.

Keywords — gray hole hole; wireless sensor network; AODV, malicious; SVM; Contingency, confusion

I. INTRODUCTION

The advances in the fields of semiconductor technology and development of more efficient broadband wireless technology have brought about the deployment of greater efficient WSNs in phrases of value, speed and space. Thus bridging the space among WSNs and the out of doors world. These WSNs are made of many dispersed however self sustaining gadgets which cooperate collectively to monitor real global conditions. Some to say situations involved are temperature, sound, vibration, pressure. These find a wide software inside the regions of transportation monitoring, and sensing of nuclear, organic and chemical sellers.

A wireless sensor community (WSN) is a mesh community which include a set of compact and automated gadgets. These devices are called sensing nodes having its own sources and computational functionality. These nodes are dispersed across a properly-described location representing an advert hoc network and are capable of talk amongst themselves. In a wi-fi sensor network there may be a class of certain unique nodes with the capability to method and keep the data gathered over the network. These nodes are higher referred to as sink nodes. The communiqué between nodes is over a couple of hops if they may be now not inside every other's transmitting and receiving variety [1].

Wireless sensor community are used to accumulate critical statistics from the installed surroundings where they may be embedded. The data amassed is processed with the aid of the sensor nodes and then forwarded over non-at ease channels to sink node for further processing. The sensor networks have huge application within the regions of surroundings, infrastructure, public protection, medical, safety and transportation.

These programs areas are open and possibly to be attacked. These assaults are performed through malicious node. Malicious node are considered to be a silent killer of WSN. As those nodes are hooked up explicitly by way of the attacker into the relaxed environment so that it will perform malicious assaults. In this thesis the malicious node are taken into consideration which will carry out grayhole and black hole attack.

Many specific varieties of attacks recognized to exist in a WSN along with spoofing the various fields of a message packet even as it is in transit. It is carried out in this sort of way that the recipient receives is an altered copy as opposed to unique message being sent through the supply [2].

The grayhole is well-known denial of service attack, in which a malicious node absorbs all packets by false claiming a new route to the destination. It absorbs all the packets instead of forwarding them to the destination.

A famous denial of service attack in which a malicious node draws all packets by using false claiming a new path to the vacation spot. It absorbs all the packets with out forwarding them to the destination.

A grayhole hole node is clearly the only that always respond to each RREQ message with a RREP message. Even when it does no longer have an real direction to the destination node. When the records packet reaches the grayhole hole node. It drops all of the packets as opposed to forwarding them to next in route hop. As a result none of the packets are capable of reach the vacation spot.

The packet dropping attack as defined as grayhole hollow node assault is proven within the research. In which a malicious node absorbs all the records packet and is just like the blackhole hollow inside the universe that absorbs the whole lot that involves it. It uses all of the liabilities toward the path discovery packets of the on demand protocol higher called AODV [3].

In reality the grayhole attack in WSN makes to compromise course establishment in a community. A malicious node that pronounces a routing message with a further everyday high power is capable of misinform a massive wide variety of nodes. These nodes try to use the malicious node as their next hop in their path to the sink. But the nodes those are at a much-away distance might in reality be sending their messages within the state of unawareness. A comparable situation, grayhole assault appearing as a malicious node is capable of convince all neighboring nodes those are commonly a couple of hops from the sink node that they are simply one hop away from the vacation spot node. These nodes in response try and send their packets without delay to the sink node, that’s unable to hear them [4].

Hu, Perrig, and Johnson have offered a singular approach to countermeasure these malicious attacks in advert hoc networks. It includes additional data to be encapsulated to the usual packets to be able to restrict its maximum allowed tour distance. The cited method is referred to as packet leash. The packet leash technique has its own dangers together
with the increase inside the processing time of the packets and in its length [5].

The studies involves a mechanism based totally on analyzing the behaviour characteristics of every node gift in the wi-fi sensor network during transmission. The simulation become achieved against two cases, one inside the presence of malicious node which acts as a grayhole or a grey hollow and the second, whilst the stated node behaved as non-malicious or in other words inside the absence of grayhole or grey hollow assault. The separate hint files are generated with the aid of tracking the network behavior during transmission. The evaluation of generated hint documents in said instances is completed using support vector system based totally version leading to the prediction of a suspected node as a grayhole or grey hollow.

The capabilities together with total packets ship, obtained, forwarded and brought to each hop have been monitored, recorded and supplied as an input to the class version.

There are many technically exciting research demanding situations regarding WSNs. Some to say are the improvement of fashions and equipment for the layout of better WSNs structure additionally elaboration of popular protocols in WSN tailored to work robustly on positive situations. One of the maximum vital issues that stays unchallenged is protection. The research will focuses on safety in WSNs. More exactly, the work focuses on investigating models to discover internal attacks on WSNs.

II. SIMULATION MODEL

This section provides the information regarding simulating environment and results generated. The NS2 is used to simulate the wireless sensor network environment in order to evaluate the data and carry out necessary analysis. The network is created with the properties as mentioned in the table (1) where the channel or the medium for transmission is wireless, the propagation is set to be Two ray ground making an assumption that a signal sent from one node to another does not travel in a straight line or a unique path but eventually also through a reflection in the ground. topology used is wireless physical. The address associated with each node is of type MAC following IEEE standard 802.11. The Improvement of performance at the destination node by applying different types of queues at the routers observed. The drop tail queue with priority is implemented where drop of packets can only take place at the rare end of the queue. The congestion and the packet drops can be reduced at the link node by appropriate selection of queue type at the link node [7].

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Attributes</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Channel</td>
<td>Wireless Channel</td>
</tr>
<tr>
<td>2</td>
<td>Propagation</td>
<td>Two Ray Ground</td>
</tr>
<tr>
<td>3</td>
<td>Phy</td>
<td>Wireless Phy</td>
</tr>
<tr>
<td>4</td>
<td>Mac</td>
<td>802_11</td>
</tr>
<tr>
<td>5</td>
<td>Queue</td>
<td>DropTail/PriQueue</td>
</tr>
<tr>
<td>6</td>
<td>Link Layer type</td>
<td>LL</td>
</tr>
<tr>
<td>7</td>
<td>Antenna</td>
<td>OmniAntenna</td>
</tr>
<tr>
<td>8</td>
<td>ifqlen</td>
<td>50</td>
</tr>
<tr>
<td>9</td>
<td>Nodes</td>
<td>7</td>
</tr>
<tr>
<td>10</td>
<td>Routing protocol</td>
<td>AODV</td>
</tr>
</tbody>
</table>

All the nodes are located on a grid of 900 X 900 field with well-defined specific x and y coordinates. The nodes are located in such a way that no two nodes share the same coordinates on the grid as shown in fig.(1).

Fig (1). Showing the deployment of seven nodes in the wireless sensor network

The N number of nodes were used in the simulation. Where N = \{n0, n1, n2, n3, n4, n5, n6\}. The node n0 is defined as source node, the node n5 as malicious gray hole attack node and node n3 is defined as destination node also known as sink node. The traffic is sent by the source node n0 to the sink node n3 over multiple hops in the network.

2.1. Mathematical Model Used For Detection.

Given X = \{x1, x2, ...., xn\}, where X represents the set of nodes in the wireless sensor network; where n is the total number of nodes.

Given Y = \{y1, y2, ...., ym\} where Y represents the set of distinct features associated with each node. These include send (s), receive (r), drop (d) and forward (f).

Given total number of distinct features (m) = 5

\[ D = \sum_{j=1}^{m} \sum_{i=1}^{n} x_{ij} \]

\[ X \in (x_1, x_2, \ldots, x_n); \ Y \in (y_1, y_2, \ldots, y_m) \quad (1.1) \]

Detection(D)=\{x_{1y1} + x_{2y1} + x_{3y1} + \ldots + x_{ny1} \} \quad (1.2)

\[ Y \in \{0, 1\} \]

0 = absence of feature

1 = presence of feature

Assuming the single feature with the maximum drop at the attack nodes and there is only one malicious node then the above equations (1.2) will become

\[ (D) = \{x_{1y1}, x_{2y1}, x_{3y1}, \ldots \ldots \} \]

\[ \Rightarrow \{x_{1y1}, x_{2y1}, x_{3y1}, \ldots \ldots, x_{ny1} \} \quad (1.3) \]

The equation (1.1) will be reduced to

\[ D = \sum_{i=1}^{n} x_{iy1} \quad (1.4) \]

Therefore,

\[ D = (x_{1y1} + x_{2y1} + x_{3y1} + x_{4y1} + x_{5y1} + x_{6y1} + x_{7y1}) \quad (1.5) \]

Substituting the values of y1 in the above equation whereby \( E \in \{0, 1\} \). Assuming ‘drop d’ is present only at node ‘x5’.

\[ D = \{x_1 * 0 + x_2 * 0 + x_3 * 0 + x_4 * 0 + x_5 * 1 + x_6 * 0 + x_7 * 0 \} \]

\[ = \{x_5 \} \]

Assuming there drop is found at more than one nodes. Let it be at x2 and x3, n=7 and m=1;

\[ D = \max (\sum_{i=1}^{n} x_{iy1}) \text{ where } y \in \{0, 1\} \]

\[ = \max (\{x_{1y1} * 0 + x_{2y1} * 0 + x_{3y1} * 1 + x_{4y1} * 0 + x_{5y1} * 1 + x_{6y1} * 0 + x_{7y1} * 0 \}) \]
III. RESULTS

The simulation was run for 100 ms with packet size = 1000, traffic type = CBR (Constant bit rate), traffic rate = 0.1Mbs. The AODV (Ad hoc on demand) routing protocol after making necessary modification is used to perform the desired routing of packets from source to sink node and following observations were made.

![Density Plot of Nodes](Image)

Fig 2: Showing the density plot of nodes in presence of grayhole attack.

The predicted contingency table was generated without grayhole hole attack by the SVM model as shown in table (3). It is observed that the total number of packets sent by the source node (n0) = 1238, the number of packets received by the sink node (n3) = 0 as there is drop of 1238 packets at the grayhole hole node (n5).

![Density Plot of Packet Types](Image)

Fig 3: Showing the density plot of nodes in absence of grayhole hole attack.

It can be clearly observed the low density peak in fig(2) at destination node indication of no packets reaching the destination (n3) as there is grayhole hole present in network. While in the fig(3), a high peak can be observed at destination node (n3) which is an indication that the packets are arriving at the destination node and further the absence of any grayhole attack.

The increase in the drop of packets was observed in the presence of grayhole hole attack while the simulation was run over period of 100ms. The number of packets dropped were found to be equal to the number of packets being sent by the source node as shown in table (2).

IV. CONCLUSION

(a). The drop in the density curve can clearly be observed with respect to time while the packets travel from source (n0) to sink node (n3) as shown in fig (2). This drop in the density curve is a clear indication of the presence of some malicious activity during the transmission. The low peaks in the density curve for node (n3), (n4), (n5) and (n6) proves that there was no drop of packets observed in the absence of grayhole hole attack while the simulation was again run over period of 100ms. The number of packets sent from the source were found to be equal to the number of packets received at the destination as shown in table (3).

The predicted contingency table in the presence of grayhole hole attack by the SVM model is shown in table (4). It is observed that the total number of packets sent by the source node (n0) = 1238, the number of packets received by the sink node (n3) = 0 as there is drop of 1238 packets at the grayhole hole node (n5).

![Table](Image)

Table 3: Showing total packets send, received, forwarded, dropped and packet density ratio during different intervals in the absence of grayhole hole attack.

<table>
<thead>
<tr>
<th>S.no</th>
<th>Run time</th>
<th>Send</th>
<th>Received</th>
<th>Forwarded</th>
<th>Dropped</th>
<th>Packet density ratio</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0-10</td>
<td>113</td>
<td>113</td>
<td>228</td>
<td>0</td>
<td>901.769</td>
</tr>
<tr>
<td>2</td>
<td>10-20</td>
<td>238</td>
<td>238</td>
<td>478</td>
<td>0</td>
<td>428.151</td>
</tr>
<tr>
<td>3</td>
<td>20-30</td>
<td>363</td>
<td>363</td>
<td>728</td>
<td>0</td>
<td>280.716</td>
</tr>
<tr>
<td>4</td>
<td>30-40</td>
<td>488</td>
<td>488</td>
<td>978</td>
<td>0</td>
<td>208.811</td>
</tr>
<tr>
<td>5</td>
<td>40-50</td>
<td>613</td>
<td>613</td>
<td>1228</td>
<td>0</td>
<td>166.231</td>
</tr>
<tr>
<td>6</td>
<td>50-60</td>
<td>738</td>
<td>738</td>
<td>1478</td>
<td>0</td>
<td>138.075</td>
</tr>
<tr>
<td>7</td>
<td>60-70</td>
<td>863</td>
<td>863</td>
<td>1728</td>
<td>0</td>
<td>118.076</td>
</tr>
<tr>
<td>8</td>
<td>70-80</td>
<td>988</td>
<td>988</td>
<td>1978</td>
<td>0</td>
<td>103.137</td>
</tr>
<tr>
<td>9</td>
<td>80-90</td>
<td>1113</td>
<td>1113</td>
<td>2228</td>
<td>0</td>
<td>91.554</td>
</tr>
<tr>
<td>10</td>
<td>90-100</td>
<td>1238</td>
<td>1238</td>
<td>2478</td>
<td>0</td>
<td>82.310</td>
</tr>
</tbody>
</table>

The increase in the drop of packets was observed in the presence of grayhole hole attack while the simulation was run over period of 100ms. The number of packets dropped were found to be equal to the number of packets being sent by the source node as shown in table (2).

![Table](Image)

Table 5: Contingency table showing the packets dropped, forwarded, received, send as per the contingency table in presence of grayhole hole attack.

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Nodes</th>
<th>F</th>
<th>R</th>
<th>S</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>n0</td>
<td>2</td>
<td>1258</td>
<td>1238</td>
</tr>
<tr>
<td>2</td>
<td>n1</td>
<td>1238</td>
<td>1238</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>n2</td>
<td>1238</td>
<td>1238</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>n3</td>
<td>0</td>
<td>1238</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>n4</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>n5</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>n6</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

- S. No.: Source node number.
- Nodes: Node number.
- F: Forwarded packets.
- R: Received packets.
- S: Sent packets.
- S. No.: Sink node number.

The increase in the drop of packets was observed in the presence of grayhole hole attack while the simulation was run over period of 100ms. The number of packets dropped were found to be equal to the number of packets being sent by the source node as shown in table (2).
these nodes are either malicious or not present in the route to
the destination.

(b). There is a no drop in the density curve with respect to
time once the packets travel from source (n0) to sink node
(n3) as shown in fig (3). This no drop condition in the
density curve clearly depicts the absence of any malicious
activity during the transmission.

(c). The plots shown in the fig(2) support the fact that
there is a malicious node present in the network as indicated
by the drop field presence and fig(3) clearly indicate the
absence of drop field in the data in the absence of malicious
node.

(d). The SVM model was able to predict the malicious
node (n5) from the suspected nodes n3, n4, n6 with great
accuracy using the trace file data.

REFERENCES

challenges: Mobile networking for “smart dust”. In International
Conference on Mobile Computing and Networking (MOBICOM),
Hole-and-Cooperative-grayhole-Hole-Attacks-in-Wireless-Ad-
hoc-Networks” (ICSI) International journal of Computer
Mobile networking for “smart dust”. Journal of Communications
defense against wormhole attacks in wireless ad hoc networks.
Proceedings of the 22nd Annual Joint Conference of the IEEE
Computer and Communications Societies (INFOCOM 2003),
April 2003.
Manhattan Street Network in NS2," Communication Systems,
Networks and Applications (ICCSNA), 2010 Second
International Conference on, Hong Kong, 2010, pp. 441-443.