DESIGN AND ANALYSIS OF ADHOC ON DEMAND DISTANCE VECTOR ROUTING (AODV) IN WIRELESS SENSOR NETWORK USING NEURAL NETWORK

Atinderpal Singh, Tejinderdeep Singh
M.tech (Scholar) CSE, Global Institute of Management and emerging Technologies, Amritsar
Assistant Professor (CSE) Global Institute of Management and emerging Technologies, Amritsar

Abstract
Recently, Wireless sensor networks became a hot research topic among researchers due to their flexibility and independence of network infrastructures, such as base stations. Due to unique characteristics, such as dynamic network topology, limited bandwidth, and limited battery power, routing in WSN is a particularly challenging task compared to a conventional. And it has experienced serious security problems due to their particular characteristics. Wireless communication can endure interferences or malicious interceptions; whereas, multi-hop communication assumes that each node will perform properly its functions to support network services. Further, self-organization increases the complexity of security management operations as access control, node authentication, secure routing and cryptographic key distribution. Network early work in WSN research has mainly focused on developing an efficient routing mechanism in such a highly dynamic and resource-constrained network. At present, several efficient routing protocols have been proposed for WSN. Most of these protocols have assumed a trusted and cooperative environment. However, in the presence of malicious nodes, the networks are vulnerable to various kinds of attacks. AODV protocol gives high performance gain. In WSN, routing attacks are particularly serious. Aims and objectives of this thesis work is to design and implement NN protocol with SINK hole attack and prevent the system for threat using this hybridisation.

Keywords
WSN, Sink hole attack, AODV routing protocol, Neural Network

INTRODUCTION
A lot of growth has been seen since past in digital electronics and the wireless communication that has lead to the low power and low cost sensor nodes in the small size and it can communicate in short distance [1]. Sensor nodes are considered as the kind of and useful applications in military as well as civilian applications. The main aim of either wired or wireless network is to protect it from any sort of attack like fabrication, eavesdropping, injection and packet drop modifications either completely or selectively [2]. WSN routing is considered as a co-operative process in which the routing information should be share among all nodes from route to destination. There must be strong case in which can be sometime selfish, malicious and misbehaved nodes may exist on the discovered route and cannot fulfil the required rules and regulations imposed. The main objective of data aggregation method is the collection and aggregation of data in some energy efficient manner for enhancing the network lifespan [3].

As the sensor node can discover important redundant data, the same packets from varied nodes may be aggregated for lessening the number of transmissions. The method would be used for achieving efficient energy and optimization of traffic in different routing protocols that are for maintaining and identifying the network routes. The routing algorithm has a significant role in transmission of data from source towards destination. Routing protocols can transfer the packets taking their information towards nodes deployed in sensing region and it helps the nodes for selecting a particular route in the network. Routing algorithms helps for selecting the accurate route from source to destination [4]. Routing information is shared by the routing protocol initially between the immediate neighbours and later in the entire network. The process let the nodes for understanding the network topology. Below figure depicts the routing protocol working.
MATERIALS AND METHODS

This section explains the protocol undertaken for the modelling of simulation work that is AODV (Ad hoc On Demand Distance Vector Routing) with Neural Network classification algorithm for detecting and mitigating sink hole attack.

A Glance of AODV protocol

AODV (Adhoc On Demand Distance Vector) is taken for source being initiated, loop and reactive free routing protocol that develops route among source and destination when required [5]. AODV is different from the counterpart proactive routing protocols as in proactive routing; updates are transmitted periodically that may leads to more overhead. The main aim for the designing of AODV protocol is for reducing the overhead. Each node in AODV routing protocol has the routing table with routing table entry for destination having three significant elements, namely, hop count the next hop and the sequence number [6]. The sequence number is taken as the time stamp and permits the nodes for determining the node route. The node that transfers high sequence number is elected for setting up route with destination like higher sequence number is taken as more accurate route information. The mechanism of AODV is categorized into two modules, namely, Route Discovery and Route Maintenance.

Route discovery utilizes two of the control packets like RREQ (Route Request) and RREP (Route Reply) whereas Route maintenance utilizes RERR (Route Error) packet [7]. The process of route discovery works in the fashion of request response. When the source nodes discover a route with destination node, it transfers RREQ packets towards the reachable neighbours. If the middle node receives RREQ packets and considered as a destination node, the reply would be RREP packet and if it is not the destination node than the broadcasting the RREQ packets towards neighbour nodes [8].

![Fig 2: Propagation of RREQ and Path to RREP to the source](image)

Neural Network

A neural network can be trained to perform a particular function by adjusting the values of the weights between elements [9]. Network function is determined by the connections between elements. There are several activation functions that are used to produce relevant output. Training can be either supervised or unsupervised.

In supervised training, system learns by predicting outcomes for known examples. System compares its predictions with the known results and learns from the mistakes.

In unsupervised training, system with no output or result is shown as part of training process [10]. With the delta rule, as with other types of back propagation, learning is a supervised process that occurs with each cycle or 'epoch' (i.e. each time the network is presented with a new input pattern) through a forward activation flow of output, and the backward error propagation of weight adjustments. Simply, when a neural network is initially presented with a pattern, it makes a random 'guess' as to what it may be. Neural networks are typically organized in layers. Layers are made up of number of interconnected 'nodes' which contain an 'activation function' [11]. Patterns are presented to the network via the 'input layer', which communicates to one or more 'hidden layers' where the actual processing is done via a system of weighted 'connections'. The hidden layers then link to an 'output layer' where the answer is output [12].
Sink hole attack

Sink hole attack is a kind of attack that allure the data by pressurizing the neighbours via distributing false routing data by intimating them the path towards the exact nodes [13]. By this process, the sink hole node tries to draw the network traffic to itself. Later, it changes the data packet or can drop the packets. It enhances the network overhead and lessens the network lifetime by increasing energy consumption and ultimately demolishes the network. It estimates the sequence number of source node cautiously and produces the bogus RREQ by the chosen source and destination with enhanced sequence number as compare to proposed source sequence number. It integrates alone towards the source route with transferring of the bogus RREQ [14].

As shown in figure 1, the node 2 develops the bogus RREQ that looks because it is implemented by node 0. As depicted, 999 is the sequence number of bogus packet that is higher than the unique sources.
Fig 5: Bogus RREP generation [20]

The middle node under the route finds that node 2 is lying on the hop distance towards node 0 and for transferring the packet towards node 0, the data packet might move via node 2. Sink hole 2 may effectively repeat the process and locate most of the local network traffic towards itself. Later, the node 2 may considers the malicious acts as modifying and traffic dropping [15].

SIMULATION MODEL

Sink Hole Attack is one of the dominant attacks. In this attack, a node presents itself as it has the shortest path to convey the message to the desired node and thus, the source node starts sending the packets to the destination node via that node. But, as it was the malicious node, instead of sending the packets further in the network, it starts dropping them and thus, compromi

ses the security. Much of the work has been done before by other writers over Sink Hole attack in WSN using various different procedures. Some made use of digital signature; some introduced a new node in the network. In this research work, the mitigation of sink hole attack is done by using neural network using AODV routing protocol.

Below are the steps being used for simulating the whole process:

Step 1: Initialize.
Step 2: Prepare network nodes n and set length and width.
Step 3: Set the route from source to destination with AODV Protocol.
Step 4: Acquire parameter graph.
Step 5: Randomly pick one of any node as sink hole node.
Step 6: Acquire parameter graph again.
Step 7: Call neural network and eliminate node from network
Step 8: Optimize parameters.
Step 9: Stop.
Start

Prepare the network with n nodes, length and width

Set the Route from source to destination via AODV Protocol.

Acquire parameter graph

Randomly pick one of the node as sink hole node

Acquire parameter graph again

Call neural network and eliminate that node from the network

Optimize parameters

Stop

Fig 6: Simulation Flowchart
SIMULATION RESULTS

In this work, AODV routing protocol is used for generating the path from source to destination. Neural network is used for analyzing and mitigating sink hole attack. This section explains the results obtained after the simulation of the whole work.

Fig 7: Neural network performance

Above figure demonstrates the Neural Network model for training employed as through in MATLAB 2010 with the support of Neural Network Toolbox. In neural network, 3 iterations have been chosen. Gradient value chosen for neural network is 1 and validation checks are 6.

Fig 8: Mean Square Error Vs Epochs

Above figure is for mean square error Vs epochs and shows that out of 20 repetitions, the neural network is stationery at 3rd Repetition and after developing back, it novelies the 2nd repetition results best for the assessment. Blue line is for training, green line is for validation, red line is for testing.
Above figure 9 symbolizes the graphical clarification of the neural network and it’s just a mirror of the figure which has been demonstrated for MSE.

\[
MSE = \frac{\sum_{m,n}[I_1(m,n) - I_2(m,n)]^2}{M \times N}
\]

In the above Figure 10, due to Sink Hole attack, the PDR value is low but when NN (Neural Network) is applied on the system then the PDR value increased from 88% to 95%.

**Table 1. PDR with and without optimization w.r.t number of rounds**

<table>
<thead>
<tr>
<th>No. of rounds</th>
<th>Without optimization</th>
<th>With optimization</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>91.6</td>
<td>92.8</td>
</tr>
<tr>
<td>2</td>
<td>90.8</td>
<td>93</td>
</tr>
<tr>
<td>3</td>
<td>91.8</td>
<td>94.4</td>
</tr>
<tr>
<td>4</td>
<td>91.1</td>
<td>93.9</td>
</tr>
<tr>
<td>5</td>
<td>93.2</td>
<td>96</td>
</tr>
</tbody>
</table>
Delay is a major limitation for estimating a protocol which must be low for good presentation. It is the delay in the broadcast of data from source to destination. From figure 11, it is concluded that delay has been condensed from 5 to 1.8 using NN.

Table 2. Delay with and without optimization w.r.t number of rounds

<table>
<thead>
<tr>
<th>No. of rounds</th>
<th>Without optimization</th>
<th>With optimization</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>5</td>
<td>1.8</td>
</tr>
<tr>
<td>2</td>
<td>11.2</td>
<td>5.6</td>
</tr>
<tr>
<td>3</td>
<td>8</td>
<td>6</td>
</tr>
<tr>
<td>4</td>
<td>11.9</td>
<td>5.9</td>
</tr>
<tr>
<td>5</td>
<td>11.8</td>
<td>5.7</td>
</tr>
</tbody>
</table>

Throughput is the quantity of nodes sent over the network in given time without any delay in the network. The above figure 12 shows the throughput value after using NN and without using NN. It has been seen that value of throughput is being enhanced in the figure. The value of Throughput w.r.t nodes varies from 400 to 700 using NN.
Table 3. Throughput with and without optimization w.r.t number of rounds

<table>
<thead>
<tr>
<th>Without optimization</th>
<th>400</th>
<th>450</th>
<th>250</th>
<th>300</th>
<th>475</th>
</tr>
</thead>
<tbody>
<tr>
<td>with optimization</td>
<td>700</td>
<td>750</td>
<td>550</td>
<td>600</td>
<td>775</td>
</tr>
<tr>
<td>No. of rounds</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

Table 4. Energy Consumption with and without optimization w.r.t number of rounds

<table>
<thead>
<tr>
<th>Without optimization</th>
<th>53</th>
<th>50</th>
<th>50</th>
<th>52</th>
<th>61</th>
</tr>
</thead>
<tbody>
<tr>
<td>with optimization</td>
<td>44</td>
<td>40</td>
<td>40</td>
<td>42</td>
<td>50</td>
</tr>
<tr>
<td>No. of rounds</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

**Fig 13: Energy Consumption Vs Total number of rounds**

Energy Consumption is the range of the energy expended by every node for transmission of data packets. To consume nodes proficiently and wisely is one of the vital features of sensor networks. As wireless sensor nodes are organized with non-chargable batteries with insufficient energy supply, a sensor network cannot works well after a fraction of nodes run out of energy. From graph 13, it has been seen that energy consumption has been reduced from 53 to 44NN respectively.

Table 4. Energy Consumption with and without optimization w.r.t number of rounds

**CONCLUSION**

Wireless sensor network is a group of dedicated transducer having a communication infrastructure for the monitoring and recording of different positions. Typically, parameter monitored is the temperature, humidity, pressure, speed and wind direction, light intensity, the intensity of the vibration, the intensity of the main voltage, the chemical concentration levels of pollutants and feature of living body. In this, we have suggested a scheme to detect SINK hole attack in WSNs and the path is generated from source to destination using AODV.

WSN is an autonomous multi-hop wireless network. Mobile nodes do not have pre-built infrastructure, each of them. The nodes can be moved and acted in any directed router. To facilitate communication in the Ad-hoc network, the routing protocol is critical and its primary goal is to establish accurate and effective routes between nodes, since, so many routing protocols have been proposed in WSN.

In this proposal, we have analysed the effect of sink hole attack. The path is generated initially from source to destination using AODV protocol and by picking one of the node and considered it as a Sink Hole Node with Neural Network (NN), that catch the node to lump and eliminate the problematic in the performance of NN. The simulation has been done using the MATLAB. The simulation results shows that when the sink hole node exists in the network, it affects and decreases the performance of network and it can be optimised by using NN optimization algorithm.

A hypothetical network was constructed for the simulation purpose and then monitored for a number of parameters. We have simulated our model for various nodes. Initial position for the node is specified in a movement scenario file created for the simulation using a MATLAB. The nodes move randomly among the simulation area.

In the future work, the combination routing protocols with the optimization technique and with the classifier may be possible to minimize the error rate and to prevent the route from the attackers.
REFERENCES


[17] https://www.researchgate.net/figure/257877942_fig3_Figure-2-AODV-route-discovery-process-5-a-Propagation-of-the-RREQ-b-Path-of-the


[19] https://www.researchgate.net/figure/277132972_fig3_Fig-3-Bogus-RREQ-Circulation

[20] https://www.researchgate.net/figure/277132972_fig4_Fig-4-Bogus-RREP-Circulation