Using Zone-Sampling Based Trace Back Algorithm and Modified Echo State Networks to Detect and Prevent Denial-of-Service Attacks in MANETs

Tuka Kareem Jebur

College of Management and Economic, Al-Mustansiriyah University, Iraq

ABSTRACT

Denial-of-Service Attack effect of MANETs by consume resources that prevent the rightful users to access to their services, this paper use (ZSBT) algorithm it will be trace the malicious node, when each a node in network by using this algorithm will give packet zone ID with a probability and then this packets forward. After these packets will be receiving, then using modified echo state neural (ESN) to prevent malicious node from sending data to destination by determine node that consumer more resource, packets lose or the victim could reset the path between the attacker and itself. the simulation applying by using matlab2016 and the result showed in proposed method with 200 node, 10 second average time (0.132273) compare with other method PSO algorithm (20.569) and multilayer neural network (MLP) (1.137473), drop packed in proposed method (0.0), PSO algorithm (1.776604) and MLP (9.390808), accuracy in proposed method with (10) malicious node (96.96) compare with another method.so the suggestion method reduce packed drop and jitter, delay and choosing optimal path from source node to destination node.

Keywords: MANET, DOS attack, Echo stat neural network (ESN), Zone-Sampling based trace back algorithm (ZSBT), Particle swarm optimization (PSO), Multi-layer perceptron.

* Corresponding: tukakareem@uomustansiriyah.edu.iq
**Introduction**

MANETs can be defined as a group of wireless nodes with no centralized management or fixed equipment, for example, base stations or access points. The network is made unpredictable by high dynamic topology over time. Send packets and receive packets can be doing by node at the same time. Additional MANET features such as: limited bandwidth, packed loses, low power, restricted range of transmission, and security of major problems. [1] Many security issues face MANET DoS or Denial-of-Service attack one type of them, is used to disable legitimate users' access to a target network or web resource. This is usually accomplished by overloading the target (often a web server) by sending malicious requests that cause the target resource to malfunction or disable it altogether.[2] Huge malicious node injects by DOS attack to the MANETs that can be caused a denial of the services. ZSBT method and Modified ESN modeling uses a simulated MANET environment for detecting and prevents nodes under DOS attack.

The following sections are organized as follows: Section 2 describe some of related work, a background MANET security and define DOS, ZSTB is given in Section 3. Describe suggest method to hoe detect and prevent attack. Experimental simulation results are given in Section conclusions discussed in section 5.

**Related Work**

Many researchers' efforts to detect or prevent attacks through the use of artificial neurons or ZSBT are described below: Mohamed Idhammad and et al in 2017 [3] they suggest use ANN technology to detect a DoS attack. Multi-layer perception improve accuracy and detection time, Different studies have been carried out of evaluate the efficiency of the suggested technique by using two general data sets, UNSW-NB15 and NSL-KDD. These method only detection DOS not prevent.

Masoomeh Sharifzadeh et al in 2015 [4] in this article suggested to use ANN by uses a distinct parameter to detect an attack by DOS. But the issue is that the weight of the repetitive association and limit changes by the sensitivity of the network and threshold.

Akilandeswari, V.; Shalinie, S.M.in 2012, [5], they suggest applying method where marked packet on every router involved in communication with a view to track the source of the packet. However, its provide pore result because ANN using old data set long and take time to detection DDOS.

Nikita et al. in 2015 [6], The proposed BPNN is easy to implement. the DOS attack detection will be resolved in this method, The Productivity rate of the network output will be enhanced and delay will be reduced. The method does not require any More hardware and is software based. D. Divya I 2013 [7], the proposed ANN and ZSBT applying in MANET environment to detect DOS attacks. This method reducing time that need to detect dos attack but cannot prevent attack according the power consume or packet lose in the node.

**Security in Manets**

With high-speed network technologies, a lot of data is transmitted via the Internet and other public channel which is deemed confidential. MANET's nature dynamic topology make it simple to attack, in the other side which is many mechanisms suggest solving security issues like ANN its help to make machines and networks more secure. [8] There are two categories in MANET attacks: passive attacks that include eavesdropping of data, Active attacks include actions such as modification, replication and DoS attacks [9].

**Denial of Service (DOS) Attack**

Kind of attack on a MANET network where the perpetrator does not access to a computer or network resource by disrupting the services of the Internet-related host when the target device or resource is overcharged with excessive requests in an effort to overload the system and prevent the execution. Certain or All apps that is legal [10].

**Multi-Layer Perceptron**

It is feed-forward network comprises have three layer: input, hidden, output layers, computer units, often referred to as synapses, which are connected through the weighted arcs. Consider an MLP with non-linear function Zi activation of the ith unit. The MLP calculates its input information using the following models in each concealed

\[
\text{unit}_i = f(\text{ai}) \quad \text{-----------------(1)}
\]

\[
\text{ai} = \sum_j \text{wij}_j + \text{bi} \quad \text{-----------------(2)}
\]
Tuka Kareem Jebur

Where $a_i$ is given by a weighted linear sum of the outputs of other units, $w_{ij}$ is the synaptic weight from unit $i$ to unit $j$, and $b_i$ is a bias associated with unit $i$. [3]

**Echo State Networks**

It is recurrent neural network (RNN) reservoir and a readout module. Have three layers, a high hidden layer, the output in the hidden layer the weights are fixed and randomly assigned to the output. The weights modified during training, error function is quadratic in ESNs make up a successful reservoir computing framework with applications in several engineering and nonlinear modeling tasks. [11]

**Zone-Sampling Based Trace Back Algorithm (ZSBT)**

Partition algorithm that divided network into zone (cluster). outcome of the time series clustering. Fig. 2 depicts the pseudo code of the modified DTW. three processes in this algorithm first: initialization the second: zone sampling process and the third: path reconstruction process, when partition area of network to the zone. each zone continue node that determine zone ID to packet with the IP address and then forward packet when packet receives to destination the attacker node can be identified easily and the network is protected from such attacks according the ID zone. [7]

**Particle Swarm Optimization (PSO)**

Optimization algorithm, inspired by swarm behavior such as birds the total number of birds is called population size. this algorithm has object to opt the optimal solution among different available solutions after the attempt and consider solutions until the object function no longer improves then this solution obtained by the whole swarm. [12]

**Material and Method**

Many efforts are made by researcher that has been conducted to detect or prevent DOS attack by using ANN. the proposed system have two stage: In first stage applying (ZSBT) algorithm divided network to the zone give each node id and IP address in order determine the victim node (by using attacker), the second stage applying modified ESN neural network to prevent malicious node (node the consumer more power than other node that determined by ZSBT algorithm) then choosing optimal path according the following parameter: minimum packed lose, jitter, minimum delay, minimum power consumer and maximum packed delivery ratio.

**Algorithm 1: Zone- Sampling Based Trace back algorithm.**

1. **Input:**
2. number of n node, node path, zone path, network size, packed size
3. **Output:** determine the optimal number of node victim

4. **Steps:**
5. **Step 1.** Initialization process: every node constructs a chain and lets the victim be the head.
6. The method chain is used to reconstruct the attack path by sorting the zone ID information in the packets and have the following constrain:
7. 1- a node receives a packet
8. 2- if the node is the victim, then ZSBT algorithm goes to Step 3
9. 3- the path reconstruction process is executed.
10. 4- else the ZSBT algorithm goes to Step 2, the zone sampling process is executed.
11. **Step 2.** Zone sampling process. It has the following steps:
12. 1- the node writes its zone ID into the node with a probability $p$ and then forwards the packet. Two static fields, zone ID and distance in each packet are reserved.
13. 2- zone ID is used to record the zone ID of the node on the path.
14. 3- Distance represents the distance from current node to the victim and its initial value is set as zero. The concrete actions each node takes are as the following.
15. (a) Get its zone ID from the zone map. The method to divide zones and to get zone ID has been discussed above.
16. (b) Encoder a random number $v$ from $[0, 1]$ and compare it with the
Algorithm 2: Modified ESN neural network.

**Input:**
- number of random node \( N \), number of data point \( D \), number of weights of the teacher

**Output:** the optimal number of true node in network, optimal path

**Steps:**

**Step 1.** Provide a random RNN.

1. Create a random dynamical reservoir RNN, using PSO algorithm
2. Initialize the PSO population. Set the parameters such as population size, maximum iteration number, and initialize the velocity of each particle to 0,
3. Attach input units to the reservoir by creating random all-to-all connections
4. Create output units. (Substitute the particle position into the objective function and calculate the target vector)
   - If the task requires output feedback
   - Then install randomly generated output-to-reservoir connections (all-to-all connection).
   - Else If the task does not require output feedback, do not create any connections to/from the output units in this step.

**Step 2:** Harvest reservoir states.

Drive the dynamical reservoir with the training data \( D \) for times \( n=1,...,n_{\text{max}} \). In the demo example, where there are output-to-reservoir feedback connections, this means to write both the input \( u(n) \) into the input unit and the teacher output \( y(n) \) into the output unit ("teacher forcing").

In tasks without output feedback, the reservoir is driven by the input \( u(n) \) only. This results in \( \epsilon \)
Result and Desiccation

Table 2: Parameter setting.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shape of Region</td>
<td>Random</td>
</tr>
<tr>
<td>Traffic type</td>
<td>UDP</td>
</tr>
<tr>
<td>Number of Nodes</td>
<td>10-200</td>
</tr>
<tr>
<td>Packet Size</td>
<td>20-64kb (random and fixed)</td>
</tr>
<tr>
<td>Routing Protocols</td>
<td>ZSBT and modified ESN.</td>
</tr>
<tr>
<td>Simulation time</td>
<td>1000 s</td>
</tr>
<tr>
<td>Malicious node</td>
<td>0, 1, 2 and 10</td>
</tr>
</tbody>
</table>

Table 4: Comparative between different method to send and receive packet.

<table>
<thead>
<tr>
<th>Number of packet</th>
<th>PSO sending packet</th>
<th>MLP sending packet</th>
<th>Proposed method sending packet</th>
<th>PSO received packet</th>
<th>MLP received packet</th>
<th>Proposed method received packet</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>152458</td>
<td>200129</td>
<td>304543</td>
<td>33279</td>
<td>55230</td>
<td>273014</td>
</tr>
<tr>
<td>40000</td>
<td>162459</td>
<td>200130</td>
<td>315554</td>
<td>38280</td>
<td>60231</td>
<td>314015</td>
</tr>
<tr>
<td>20000</td>
<td>172460</td>
<td>200131</td>
<td>326565</td>
<td>43281</td>
<td>65232</td>
<td>419016</td>
</tr>
<tr>
<td>140000</td>
<td>182461</td>
<td>200132</td>
<td>337576</td>
<td>48282</td>
<td>70233</td>
<td>535017</td>
</tr>
<tr>
<td>220000</td>
<td>192462</td>
<td>200133</td>
<td>348587</td>
<td>53283</td>
<td>75234</td>
<td>675018</td>
</tr>
<tr>
<td>270000</td>
<td>202463</td>
<td>200134</td>
<td>359598</td>
<td>58284</td>
<td>80235</td>
<td>725019</td>
</tr>
<tr>
<td>310000</td>
<td>212464</td>
<td>200135</td>
<td>370609</td>
<td>63285</td>
<td>85236</td>
<td>835020</td>
</tr>
<tr>
<td>360000</td>
<td>222465</td>
<td>200136</td>
<td>381620</td>
<td>68286</td>
<td>90237</td>
<td>985021</td>
</tr>
<tr>
<td>400000</td>
<td>232466</td>
<td>200137</td>
<td>392631</td>
<td>73287</td>
<td>95238</td>
<td>1044032</td>
</tr>
</tbody>
</table>
Table 2: Comparative between different methods to determine parameter (average time, packet drop).

<table>
<thead>
<tr>
<th>Number of network node</th>
<th>Average time using proposed method (s)</th>
<th>Average time using PSO algorithm (s)</th>
<th>Average time using MLP (s)</th>
<th>Packet drop using proposed method</th>
<th>Packet drop using PSO algorithm</th>
<th>Packet drop using MLP</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>0.124871</td>
<td>0.416</td>
<td>1.137473</td>
<td>0.0</td>
<td>1.2848809</td>
<td>1.722914</td>
</tr>
<tr>
<td>5</td>
<td>0.125553</td>
<td>0.514</td>
<td>4.372224</td>
<td>0.0</td>
<td>1.839863</td>
<td>1.990808</td>
</tr>
<tr>
<td>10</td>
<td>0.124235</td>
<td>0.62</td>
<td>5.372224</td>
<td>0.0</td>
<td>1.30268444</td>
<td>1.990808</td>
</tr>
<tr>
<td>20</td>
<td>0.134917</td>
<td>1.502</td>
<td>6.372224</td>
<td>0.0</td>
<td>4.0151</td>
<td>2.390808</td>
</tr>
<tr>
<td>30</td>
<td>0.134599</td>
<td>1.846</td>
<td>7.372224</td>
<td>0.0</td>
<td>1.9565</td>
<td>3.390808</td>
</tr>
<tr>
<td>40</td>
<td>0.134281</td>
<td>2.944</td>
<td>8.372224</td>
<td>0.0</td>
<td>1.46182</td>
<td>4.390808</td>
</tr>
<tr>
<td>50</td>
<td>0.133863</td>
<td>4.619</td>
<td>9.372224</td>
<td>0.0</td>
<td>1.46182</td>
<td>5.390808</td>
</tr>
<tr>
<td>80</td>
<td>0.133745</td>
<td>10.053</td>
<td>10.372224</td>
<td>0.0</td>
<td>2.19553</td>
<td>6.390808</td>
</tr>
<tr>
<td>100</td>
<td>0.133427</td>
<td>9.356</td>
<td>11.372224</td>
<td>0.0</td>
<td>1.984906</td>
<td>7.390808</td>
</tr>
<tr>
<td>150</td>
<td>0.133009</td>
<td>18.336</td>
<td>12.372224</td>
<td>0.0</td>
<td>1.0403386</td>
<td>8.390808</td>
</tr>
<tr>
<td>170</td>
<td>0.132391</td>
<td>20.336</td>
<td>13.372224</td>
<td>0.0</td>
<td>1.776604</td>
<td>8.390808</td>
</tr>
<tr>
<td>200</td>
<td>0.132273</td>
<td>20.569</td>
<td>1.137473</td>
<td>0.0</td>
<td>1.776604</td>
<td>9.390808</td>
</tr>
</tbody>
</table>

Table 3: Comparative between deferent methods to determine the Jitter in network with attack.

<table>
<thead>
<tr>
<th>Number of malicious node</th>
<th>Jitter Proposed method with attacks (ms)</th>
<th>Jitter in MLY with attacks (ms)</th>
<th>Jitter in PSO with attacks (ms)</th>
<th>Accuracy% in proposed method</th>
<th>Accuracy% in PSO algorithm</th>
<th>Accuracy% in MLY</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>0.79</td>
<td>7.86</td>
<td>11.21</td>
<td>92.82</td>
<td>0.17</td>
<td>5.13</td>
</tr>
<tr>
<td>4</td>
<td>0.88</td>
<td>7.89</td>
<td>11.27</td>
<td>93.54</td>
<td>0.22</td>
<td>5.22</td>
</tr>
<tr>
<td>6</td>
<td>0.97</td>
<td>7.92</td>
<td>11.33</td>
<td>94.2</td>
<td>0.27</td>
<td>5.31</td>
</tr>
<tr>
<td>7</td>
<td>1.06</td>
<td>7.95</td>
<td>11.39</td>
<td>94.89</td>
<td>0.32</td>
<td>5.4</td>
</tr>
<tr>
<td>8</td>
<td>1.15</td>
<td>7.98</td>
<td>11.45</td>
<td>95.58</td>
<td>0.37</td>
<td>5.49</td>
</tr>
<tr>
<td>9</td>
<td>1.24</td>
<td>8.01</td>
<td>11.51</td>
<td>96.27</td>
<td>0.42</td>
<td>5.58</td>
</tr>
<tr>
<td>10</td>
<td>1.33</td>
<td>8.04</td>
<td>11.57</td>
<td>96.96</td>
<td>0.47</td>
<td>5.67</td>
</tr>
</tbody>
</table>

Fig.1 Packet Drop Rate with 1-10 Malicious Node.

Fig.2 Average time vs. number of node.

Fig.3 Accuracy vs. number of nodes.

Fig.4 Jitter vs. number of nodes.
In table (2) with using (200) node the average time and Packet drop in proposed method (0.132273), (0.0) is smaller when compare with PSO (20.569), (1.776604), MLY(1.137473) (9.390808).

In table (3) with (3-10) malicious node the simulation result showed in suggest method is fewer compare with PSO and MLP with 100m that take (1.33) and accuracy (96.96) because this method take the optimal path with low cost and minimum packed lose.

In table (6) sending and received data packed in suggests method its optimal number of data because it avoiding losing data packed compare with the other methods.

In Fig. 1, 2 Comparison of average time and the drop packet with 200 nodes and malicious node (1-10) the proposed method take lower time compare with PSO and MLP.

In Fig. 3, 4 the percentage of accuracy (96.96) and jitter (1.33) of data sent in proposed algorithm with (10) malicious node and simulation time 100 second.

In Fig. 5,6 The result shows packets that received in suggest method is huge compare with other method like PSO, MLP.

Conclusion

This article paper suggest method to detection and prevent DOS attack based on ZSBT algorithm and modified echo state Neural Networks, ZSBT use to detect malicious node the neural was optimized to enhance the accuracy, reduce time prevent attack and find optimal path with reduce packet drop, jitter, average time will reduce. The suggest method was compared with an MLP and PSO algorithm and the results in suggest method showed taken minimum time, low power consume to detect and prevent attack than MLP and PSO. For future works intend to use genetic neural network to detect accurately other network attacks.

Acknowledgements

This research has not received any material support from any donor.

References

Tuka Kareem Jebur


