Abstract—This paper presents an innovative wormhole detection scheme using artificial neural network for wireless sensor networks (WSNs). Most detection schemes described in the literature are designed for uniformly distributed sensors in a network, using statistical and topological information and special hardware. However, these schemes may perform poorly in non-uniformly distributed networks. Accordingly, the aim of the proposed research is to detect wormhole attacks for both uniform and non-uniform network environments. Furthermore, the proposed research does not require any special hardware to discover wormhole attacks and causes no significant communication overhead as well. The efficacy of the proposed detection model is measured in terms of detection accuracy, false positive rate, and false negative rate. The results show that the proposed algorithm achieves higher detection and lower false positive rates in comparison with existing statistical wormhole detectors.

Keywords—Artificial neural network; wormhole attack; non-uniform distribution; wireless sensor networks

1. INTRODUCTION

A wireless sensor network is simply a pool of self-directed devices organized into a mutually connected network. Sensors are usually autonomous and spatially distributed within a certain area to monitor targeted physical and environmental conditions, such as temperature, sound, and pressure. In WSNs, free frequency band and open architecture are used for supporting mission critical application in a hostile environment; thus, they are highly prone to various security attacks, such as the wormhole attack.

The wormhole attack is recognized as one of the most detrimental security threats for WSNs [1]. In WSNs, known communication channel is used so that the wormhole attack can be deployed silently without raising any security concerns. Wormhole attackers (node) are connected via virtual tunnel which can be established in many ways (e.g. out of bound hidden channel, packet encapsulation and high powered transmission) [2]. During this attack, a malevolent node, which is controlled by an adversary, records packets from one location in the network, and replays them in another location through a virtual tunnel to another malevolent node. As shown in Fig. 1, the two wormhole nodes E1 and E2, connected by a dedicated link, can capture the packets from one location and replay them to another location.

Fig. 1 Wormhole attack.

Subsequently, this wormhole attack becomes so severe that it might destroy the network or hamper the usual operation of the network by selective dropping of packets; manipulation of traffic; or modifying data packets without revealing their identities.

Therefore, detection of wormhole nodes is an essential task for ensuring the security of wireless sensor networks. Most of the existing countermeasures use distance between nodes, direction, and location abnormality among claimed neighbour nodes as detection features to fight against wormhole attack. To gain a certain level of accuracy, many existing schemes have used complex and highly advanced devices such as directional antenna [3], GPS [4], or ultra sound for distance measurement [5]. In fact, those special devices are very costly for practical deployment. Some statistical wormhole detection schemes based on hop count...
The proposal of the artificial neural network based Detector is detailed in Section 4. The evaluation results are discussed in Section 5. Section 6 includes concluding remarks and future scope of work.

2. RELATED WORK

Numerous counter measures have been proposed to confront the wormhole attacks in WSNs. In [4], the authors have proposed packet leashes to detect wormhole nodes. Two types of packet leashes are used, such as temporal packet leash and geographical packet leash. In temporal leash (TL), a sender adds either sending time or expiration time of packet so that the receiver can verify if the packet has made a journey too far based on maximum transmission speed and time. In the geographical leash (GL), sender includes its own location (using GPS) and sending time. Using GL, the maximum distance between the sender and receiver can be estimated by receiver. This scheme can perform better if strict time synchronization and additional device like GPS are provided.

In [3], a new idea has been introduced to detect wormhole attack. A directional antenna is attached to each sensor node to detect wormhole node. According to the authors, if a sensor sends a packet in a given direction, its receiver will receive it in the opposite direction. Therefore, authenticity of neighbor can be verified by their sending and receiving directions. This scheme appears to require additional hardware (i.e., directional antenna).

The method in [7] detects wormhole node by looking at the connectivity graph for forbidden substructures. Two non-neighbor nodes might have at most $f_k$ common independent $k$-hop neighbors; attack is spotted if the opposite happens. Compared to dense network, forbidden substructures are very hard to find in spare network.

Another category of wormhole detectors has been proposed based on the investigation of the statistical parameters of network, such as number of neighbors and hop count etc. In [8], the statistics of total hop count and neighbor information are monitored by the base station. If the total number of hop counts decrease dramatically or whether the number of neighbors of all nodes increases over a threshold, presence of a wormhole node is declared. However, this scheme causes significant communication and co-ordination overhead.

In [9], another statistical approach is proposed, known as SWAN approach, in which each sensor collects the recent number of neighbors. Wormhole attack is identified if the current number of neighbors exhibits unusual increase compared to the previous neighborhood counts taken outside of the wormhole zones. This is a distributed approach so that it doesn’t cause any overhead unlike

[6], node connectivity [7], or neighbourhood count [8][9] do not need any special hardware. Those schemes are usually used with hardware supported scheme as a secondary approach. Furthermore, centralized statistical wormhole detector [8] caused significant network and communication overhead in contrast to distributed approach statistical approach [9]. However, most of the wormhole detection schemes are made to apprehend wormhole nodes where sensor nodes are distributed uniformly, but their performance in case of non-uniformly distributed networks is in question.

In recent years, artificial intelligence technology is combined with network anomaly detection scheme to improve its detection accuracy. It is one of the exemplary intelligent models that is extensively used in a detection system. However, an artificial neural network is a very simplified model of the information processing in the human brain. This network consists of interconnected processing units, works in a parallel fashion to find non-linear solution to a particular problem. Its adaptive and self-learning criteria helps to increase the competence of an anomaly detection model [10].

In this paper, we propose a novel detection scheme based on an artificial neural network using neighborhood count. The proposed detection model is able to detect wormhole attacks in non-uniform sensor distributions and does not need any special hardware. Here, we have introduced a mobile node, called as detector node (DN) that visits a random location within the network area and collects neighborhood counts. When DN moves into a wormhole attack zone, the collected number of neighbors by DN are increased abruptly (uniform network scenario) or slightly (non-uniform network scenario) compared to non-affected zone. This abnormality is captured by DN as evidence of the presence of wormhole attack and gathered in a dataset. DN collects the number of neighbors both in the presence and absence of wormhole nodes. Dataset is used for training and testing of neural network. After training phase, test dataset is fed into a neural network and based on the output of the network, we decide the existence of wormhole attack in the network.

We studied detection accuracy, false positive rate and false negative rate through simulation in detail. Our simulation results have confirmed that an artificial neural network based wormhole detector can detect wormhole attack with high precision and negligible false positive and false negative rates compared to statistical based wormhole detector.

The remainder of this paper is organized as follows: Section 2 presents the literature survey of detecting wormhole attack and its counter measure for WSNs. We discuss the artificial neural network in Section 3. The
centralized approach. However, both schemes perform better in uniformly distributed network, but their performance is in question where sensors are distributed non-uniformly.

3. ARTIFICIAL NEURAL NETWORK

Artificial neural network (ANN) is a computational scheme that is modeled after the human brain. ANN consists of interconnected complex information processing unit, called neuron; they work together to find non-linear solution of certain problems [11]. Neural networks learn or adopt with input examples that flows through it. However, they consist of three general layers: input layer, hidden layer and output layer. Perhaps, the Multilayer layer perception (MLP) is the most widely used scheme of neural network. Fig. 2 shows a standard multilayer feed forward network.

![Multi-layer neural network](image)

Fig. 2 Multi-layer neural network.

Operation of neural networks can be described in two phases: Training and Testing. There are several methods, but simplest and the most popular training method is generalized delta rule, which also known as backpropagation [12].

Input features from the input layer are shared with adjacent hidden layer through unidirectional branches [13]. Those input values are multiplied by some weights and then summed. Similarly, all output of hidden layer propagates to the output layer (This is called forward propagation). The value of the output layer is compared with desired output. This error between actual output and desired output are measured and propagated backward to adjust the branch weights. On other words, we minimize the cost or energy of the error function, $J(\theta)$, by using back pass of back propagation algorithm defined as:

$$J(\theta) = \frac{1}{2m} \sum_{a=1}^{m} (h_a(\theta) - y_a)^2 \tag{1}$$

The $y_a$ defines the desired output of the $a^{th}$ input training example, $h_a(\theta)$ represents actual output of neural network and $m$ represents total number of training examples. During the back pass of back propagation, each branch weights is updated using (2):

$$\theta_{ij} = \theta_{ij} - \alpha \frac{df(\theta)}{d\theta_{ij}} \tag{2}$$

The $\theta_{ij}$ is the weight between $i^{th}$ and $j^{th}$ neuron and $\alpha$ is the learning rate. The weight adjustment procedure is performed recursively up to maximum epoch.

4. PROPOSED ALGORITHM

The proposed algorithm is a network based approach in which the number of neighbors is used as detection feature to confront wormhole attack.

![Impact of wormhole attack](image)

Fig. 3 Impact of wormhole attack.

However, a mobile sensor node, known as detector node ($D_N$) is deployed in an area where sensor nodes could be uniformly or non-uniformly distributed. $D_N$ moves around this sensor field and collects the neighborhood count. When it reaches into the communication range of the wormhole node, counted number of neighbors would increase sharply or a little based on sensor distribution. This change is captured and gathered in a dataset, $D_{set}$ along with other collected number of neighbors. For instance, as shown in Fig. 3, the detector node $D_N$ moves from the one location $A_1$ to another location $A_2$. Then $D_N$ will receive the new neighbor beacon message from sensor nodes within its communication range, $A_{com}$. At the same time, sensors, around the $E_2$, also send beacons via $E_1$ as they are connected through a virtual tunnel.

As we know, the performance of a neural network highly depends on how the neural network is trained and training dataset containing potential features. $D_N$ involves in gathering $D_{set}$ with adequate data samples. However, it is
assumed that a wormhole attack does not exist in the network in the first half of the detection process. In this first half, the detector node gathers $KxN$ data samples which are called negative training examples. Similarly, the same amount of neighborhood counts are collected in the presence of wormhole nodes, known as positive training examples. After that, these two types of data samples are mixed up so that training can be performed appropriately. Then $MxN$ data samples are drawn and stored in a training dataset, $D_{train}$. At the same time, $PxN$ data samples from the main dataset are stored in $D_{test}$ for testing the trained neural network.

**Proposed Algorithm:**

1. Collect $KxN$ negative Data samples
2. Collect $KxN$ positive Data samples
3. Mix up the positive and negative data samples
4. Select $MxN$ data samples from $D_{set}$ and store in $D_{train}$
5. Select $PxN$ data samples from $D_{set}$ and store in $D_{test}$
6. Train the neural network with appropriate parameters
7. Test the neural network
8. If $output \geq 0.8$ then wormhole attack exist
9. If $output < 0.8$ then wormhole attack does not exist
10. Update $D_{train}$ by $D_{test}$ for further training
11. Reset $D_{test}$ and update with new data samples gathered by $D_N$

Furthermore, data samples of $D_{train}$ are fed into the input layer of the neural network. Training procedure is performed repeatedly until it reaches the maximum epoch. Testing procedure involves the checking of the neural network whether it is able to classify the wormhole attack or not. If only the output of the trained network is greater than 0.8, then the presence of wormhole attack is declared.

After testing, data samples of $D_{test}$ updates $D_{train}$ for further training by removing its old elements. This will minimize the error level that was achieved in the training phase. $D_{test}$ entries are cleared up and updated with new data examples collected by $D_N$ in real time.

**5. SIMULATION AND RESULTS**

In this section, we have demonstrated the simulation and the results after applying our proposed model of detecting wormhole attacks. First phase of the experiment has been conducted to see if the proposed scheme is able to classify the wormhole attack in the network or not. In the second phase, we have evaluated the percentage of detection accuracy, false positives and false negatives of the proposed detection scheme. We have also investigated the performance of the proposed algorithm by deploying different sensor distributions.

In the simulation setup, 500 sensor nodes are distributed in the square field of 1000 meters by 1000 meters. Each sensor node including $D_N$ has 50 meters radio range. A pair of wormholes is placed on a location of 300 meter by 300 meter and 700 meters by 700 meter. Random waypoint model is used as the mobility model for the simulation[9].

A multi-layer, feed-forward network with backpropagation algorithm has been used for the experiments. Both input and hidden layer contain 100 neural nodes. On the other hand, the output layer has only one (01) neural node. Conversely, we have used a sub data set, $D_{train}$ comprising of 9000 randomly selected data points from $D_{set}$ for training, in which each data point consists of 100 neighborhood counts collected by $D_N$. During the training period, minimum error tolerance level was set to $1e-05$. The Table 1 shows the parameters which are used during the training phase.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>No of feature</td>
<td>1</td>
</tr>
<tr>
<td>No of Data points (training)</td>
<td>9000x100</td>
</tr>
<tr>
<td>No of Data points (testing)</td>
<td>1000x100</td>
</tr>
<tr>
<td>Architecture</td>
<td>[100,100,1]</td>
</tr>
<tr>
<td>Performance</td>
<td>1.00E-05</td>
</tr>
<tr>
<td>Learning rate, $\alpha$</td>
<td>1.00E-02</td>
</tr>
<tr>
<td>Epoch</td>
<td>9000</td>
</tr>
<tr>
<td>CPU time</td>
<td>15 mins</td>
</tr>
</tbody>
</table>

In the testing phase, the testing dataset is fed into the input layer. Then we look into the output of the neural network to see whether it identifies the existence of wormhole attack in the given network. Fig. 4 shows that the proposed detection scheme can classify the “wormhole attack” and “no wormhole attack” successfully.
In the second phase, we wanted to evaluate the performance of the proposed scheme by using different sensor distributions in a given area. The total number of sensors and radio range of each sensor including $D_1$ remain same as the first phase. In this experiment, sensors are distributed according to several distributions such as uniform, Gaussian, Poisson, exponential, beta and gamma distribution. For each sensor distribution, we have calculated the percentage of the detection accuracy, false positives and false negatives.

Fig. 5 Percentage of detection accuracy.

Fig. 5 shows the percentage of detection accuracy of ANN based detection scheme with different sensor distributions. In this graph, the highest detection accuracy is recorded as 99.981% when sensors are distributed according to Uniform distribution, whereas the lowest detection accuracy is measured 97.015% for exponential sensor distribution. Furthermore, detection accuracy for Gaussian distribution is almost same as the uniform distribution. Accordingly, 97.662%, 98.01%, and 97.873% detection rates are measured for Poisson, beta and gamma sensor distribution. Thus, the average detection accuracy calculated for the detection system is 98.32%.

Fig. 6 Percentage of false positive.

Fig. 6 compares false positive rates of this scheme with the Variation of deployed sensor distributions. The lowest false positive rate is achieved for the uniform sensor distribution, and the highest false positive rate is recorded for the exponential sensor distribution, which are 0.019% and 2.885%, respectively. For the Gaussian sensor distribution, false positive rate is relatively low as uniform sensor distribution. The false positive rate for the beta sensor distribution is 2.115%. At the same time, false positive rates are approximately same for Poisson and Gamma sensor distribution, but not as high as Exponential sensor distribution.

Fig. 7 Percentage of false negative rate.

Fig. 7 illustrates the changes in false negative rates over different sensor distributions. In this graph, lowest false negative 0% is obtained for uniform sensor distribution among all sensor distributions. However, false negative rate is relatively high for the exponential sensor distribution compare to other sensor distributions. Here, Gaussian and Poisson sensor distributions show almost equal false negative rates. Similarly, almost similar false negative rate is achieved when the sensors are distributed according to beta and gamma distribution.

An analysis of Fig. 5, Fig. 6 and Fig. 7 shows that the proposed detection scheme can perform better for the Uniform sensor distribution in contrast to the other non-uniform sensor distributions; though its performance is quiet improved compared to other existing wormhole detectors. In uniform sensor distribution, number of neighbors is increased abruptly when detector node is in the communication range of wormhole node. In contrast, the number of neighbors increases slightly or very small in magnitude when sensors are distributed non-uniformly. Therefore, detector node collects the number of neighbors as the evidence of wormhole attack more precisely in uniform sensor distribution compared to non-uniform sensor distributions.

In Fig. 8, we compare the performance of proposed detection scheme with other existing statistical wormhole detector. Proposed scheme is outperformed in all performance categories except false negative rate. Proposed detection scheme has higher detection accuracy with lower false positive rate, which are accordingly 98.25% and 1.71%. Though proposed scheme exhibits 0.02% false
negative rates unlike other two statistical wormhole detectors, this false negative rate is apparently negligible considering its high detection accuracy and lower false positive rate.

Fig. 8 Comparison of different statistical wormhole detectors.

6. CONCLUSIONS

This paper presents a novel detection model based on neighborhood count using ANN for wireless sensor networks. The goal of this proposed detection scheme is to detect wormhole attacks in any sensor distribution with high detection accuracy and low false positive rate, especially in non-uniform network environment. The proposed scheme shows promising performances through simulation. The detection accuracy is increased and false positive is decreased significantly compared to other statistical wormhole detectors. Future work is needed to enhance the detection scheme to locate wormhole nodes and to eradicate them from any sensor network.

REFERENCES


