© 2016 IJSRSET | Volume 2 | Issue 2 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

VND-NN: Neural Network Based Vampire Node Detection in Wireless Sensor Networks

Rama Chaithanya Tanguturi, C Jayakumar

Department of Computer Science and Engineering, PACE Institute of Technology & Sciences, Ongole, Andhra Pradesh, India

ABSTRACT

Wireless sensor networks are widely used for environment monitoring. The sensor nodes are deployed in the areas of interest to obtain the physical world data. These nodes are resource constrained in power, memory and computation. Boarder security is one of the major applications of WSNs. The sensor nodes are mounted with the environmental sensors (temperature, pressure etc.,) to monitor the environment and forward the sensed data to the base station via mobile sinks. Adversary can easily capture nodes from the network because they are not tamper proof in nature. Once the attacker succeed in capturing a legitimate sensor node, can introduce a variety of attacks. Vampire attack a potential attack in WSNs, which is a resource draining attack. The compromised nodes will misbehave with the legitimate nodes in the network and tries to drain the resources continuously resulting in network collapse. In this paper a neural network based misbehaviour node detection algorithm is proposed. The simulation result shows that the proposed model effectively detects the misbehaviour nodes and conserves the network resources.

Keywords : Neural Network, Wireless Sensor Network, Misbehaviour, Security.

I. INTRODUCTION

Environment monitoring is an important area in the border security. Wireless sensor networks are widely used for military applications. The easy deployment and the low cost sensor nodes made the WSNs more suitable for military purpose[1]. The non- tamper proof nature and the absence of unique identity made the WSNs vulnerable to variety of attacks[2], [3]. Resource draining attacks are dangerous in nature which leads to entire network collapse. Attacker eavesdrops on the network and tries to capture the legitimate nodes in the network. The compromised node modifies the sensed data, which forwards to the mobile sink. Vampire attack a resource draining attack in which the compromised node transmit messages which consume maximum energy in the delivery. Under vampire attack, a single compromised node will influence the resources of the entire wireless sensor network.

In this paper, neural network based vampire node detection was proposed. The WSNs and the neural networks are similar in the architecture. The application of neural network in the context of security of wireless sensor network helps in the detection of vampire attack.

II. METHODS AND MATERIAL

Related Works

A security framework in [4] was proposed to verifies the packets that are in routing state and moving towards destination. It identifies the packets traversed in longer route than the desired shortest path. Intern recognizes the compromised nodes that responsible for the packet route change. This scheme also identifies the routing path alterations by the attacker at the source routing stage. The proposed scheme detects the misbehavior of the packets from source to the destination.

Sensor nodes are operated in two states. Sensing state where the node will monitor the environment and the other sleeping state. The sensor nodes will switch between the two states depending up on the deployment. The sleep mode conserves the battery of the sensor node

whenever possible. In [5] the Attacker does not allow the sensor node entering the sleep state and made the node busy in forwarding the malicious packets misbehaviour detection in [3], is a hypothesis based scheme where the legitimate nodes forward their binary decisions to the information Centre. The compromised nodes transmit the factious data to the information Centre. Expectation maximization algorithm is proposed and the hypothesis testing is carried out to identify the malicious nodes in the wireless sensor network.

A routing tree was generated by the sink [6] and distributed to entire network. Every node participated in the information transmission and forwarding will add tags to the message. The scheme identifies the misbehaved nodes depending on the tags, where the data or the route was modified.

III. RESULTS AND DISCUSSION

3. Proposed Scheme

3.1 Neural Network based Vampire Node Detection (VND-NN):

The network components wireless sensor network are sensor nodes, mobile sink, base station. The multi-layer perceptron (MLP) neural network was implemented in the mobile sinks to predict the future values of the sensor nodes. Therefore, the mobile sink collects the sensor data and uses it for the future predictions.
The algorithm operates as follows:

1. Before receiving the data from a sensor node the implemented neural network in mobile sink will predict the data values based on the previous values at specific time intervals.
2. If the neural network detected values similar to the current sensed values the mobile sink will forward the data to the base station.
3. If the mismatch is predicted or multiple data with same time stamp received by the mobile sink, then alarm will be sent to the network to reduce the resource drain and alert the detection of vampire node.

3.2 Neural Network Design

A two-layered feed forward neural network is designed with one hidden layer and one output layer.

Input parameters:

1) Time
2) Temperature
3) Humidity
4) Wind speed

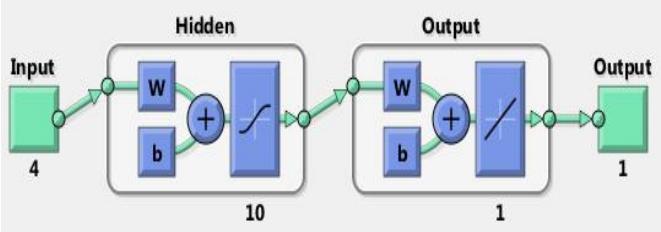

Figure 1. Designed Neural Network for vampire node detection

The designed neural network performed well with 10 hidden layer neurons, one output layer neuron.

4. Data Base

In this paper, the data used to train and validate the neural network is provided by the National Atmospheric Research Laboratory (Department of Space, Government of India), Gadanki, Andhra Pradesh, India

5. Neural network evaluation

5.1 Mean Square Error evaluation

The data base is divided in to three categories as training, validation and testing. The data is shared between the three categories as 70% for training, 15% for validation and 15 % for testing. Mean square error is a performance metric used for designed vampire node detection algorithm for evaluation. Fig.2 shows the errors in every phase of training, validation and testing for the designed neural network. The mean square error is 0.31864 which is small. The best validation occurred at 34 iterations.

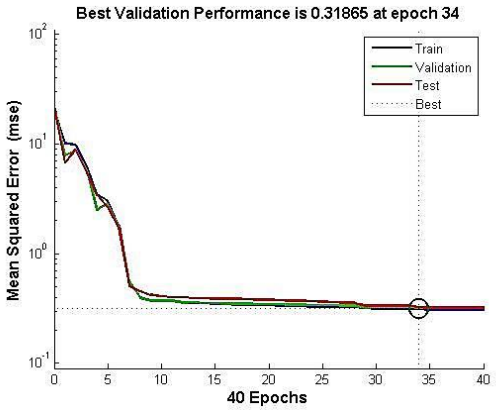

Figure 2. Neural network performance curve for Training, Validation and Test

5.2 Regression Evaluation

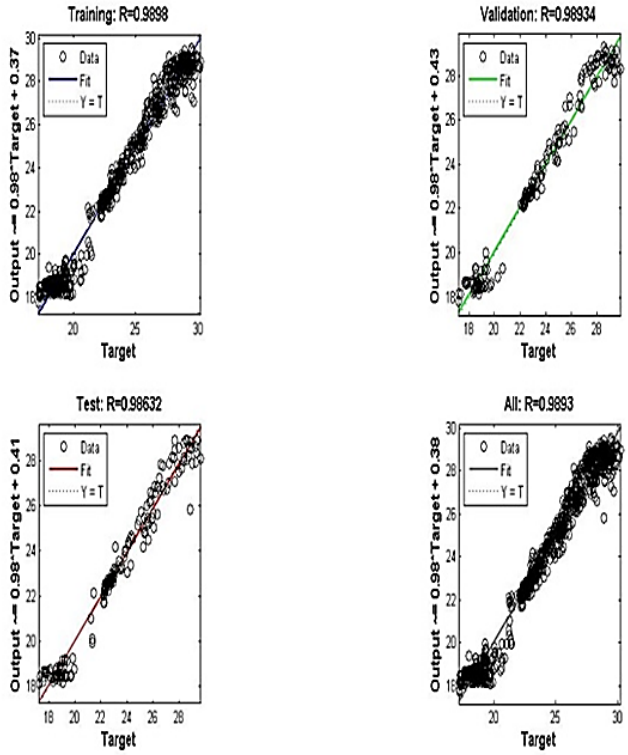

Figure 3. Performance curve based on the regression

Regression evaluation is a key metric in the evaluation of the neural network. The regression value for the training, validation and testing phase is shown in fig.3. The closeness of regression (R) value to towards '1' indicates the efficiency of the designed neural network. The designed neural network fits well with the proposed algorithm as the regression value is 0.989 and is near to'1' as shown in fig.3.

IV. CONCLUSION

In this paper we proposed a neural network based security scheme for wireless sensor networks to detect the resource draining attacks (vampire attack). The proposed neural networks suits well with the vampire node detection algorithm. The performance of the neural network is evaluated using the metrics mean square error and the regression. The simulation results show that the designed network has low errors and high detection rate.

V. REFERENCES

[1] I. F. Akyildiz, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," IEEE Commun. Mag., vol. 40, no. 8, pp. 102–114, Aug. 2002.

[2] D. R. Raymond, S. F. Midkiff, A. Wood, and J. Stankovic, "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses," pp. 74–81, 2008.

[3] E. Soltanmohammadi, M. Orooji, and M. Naraghi-Pour, "Decentralized hypothesis testing in wireless sensor networks in the presence of misbehaving nodes," IEEE Trans. Inf. Forensics Secur., vol. 8, no. 1, pp. 205–215, 2013.

[4] E. Y. Vasserman and N. Hopper, "Vampire attacks: Draining life from wireless ad Hoc sensor networks," IEEE Trans. Mob. Comput., vol. 12, no. 2, pp. 318–332, 2013.

[5] F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues for Ad-Hoc Wireless Networks," in Proc. Seventh Int'l Workshop Security Protocols, 1999.

[6] C. Wang, T. Feng, J. Kim, G. Wang, and W. Zhang, "Catching packet droppers and modifiers in wireless sensor networks," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 5, pp. 835–843, 2012.