Middle-East Journal of Scientific Research 24 (9): 2921-2926, 2016
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2016.24.09.23895

Performance Analysis of Malicious Node Detection System Based on Neuro Fuzzy Classifier Approach

[1]K. Yogitha and [2]V. Alamelumangai

[1]Department of EIE, Annamalai University, India
[2]Department of Electronics and Instrumentation Engineering,
Annamalai University, India

Abstract: Security is the major issue in wireless sensor networks (WSN) and the detection of malicious node is the complex task due to its similarity between malicious node and its surrounding nodes in the network. The main issue in WSN is its security and it must prevent the message leakage during the transmission of the data to other nodes or cluster head in the network. The performance of the WSN will be degraded due to the presence of the malicious nodes and it also consumes more energy. In this paper, direct and indirect trust features are computed for each node in the network. These features are trained and classified using Adaptive Neuro Fuzzy Inference system classifier. The performance of the proposed methodology is analyzed using the performance metrics packet delivery ratio and throughput.

Key words: Security · Throughput · Detection · Trusty nodes · Direct trust values

INTRODUCTION

Sensor networks can be categorized into wired and wireless. Former one requires more components and not supporting the fast communication. The wired sensor networks are not suitable for unattended environments such as earth quake and flooding environment. At these times, the network will be corrupted due to the faults in their transmission lines. The wireless sensor networks (WSN) are preferred in this environment. WSN consists of large number of sensor nodes spread over the entire area of the network and all these sensors are connected to the centre node, called as cluster head and all the cluster heads are connected to the sink in the network. Each sensor node in WSN must have certain individual characteristics and each node has sensor unit, converter unit and transmitter and receiver unit. The sensor unit in sensor node senses the surrounding environment and sends these details to the converter. It converts the measured analog value into digital data and these datas are transmitted through the antennal available in the sensor networks. Fig. 1 shows the architecture of the wireless sensor networks and it contains numbers of cluster and each cluster consists of numbers of sensor nodes. All cluster head in Fig. 1 are connected to base station, which is responsible for controlling the whole network and an authenticator to generate the control messages in the network environment.

The main issue in WSN is its security and it must prevent the message leakage during the transmission of the data to other nodes or cluster head in the network. The node called as malicious node act as a faulty or attacker node which generates the false report to the nearby nodes in network environment. It generates more numbers of control signals and these control signals are sent to the other nodes in the network which make confusion to the other nodes. The performance of the WSN will be degraded due to the presence of the malicious nodes and it also consumes more energy.

The paper is structured as follows. Section 2 discusses various methodologies or techniques for detecting the malicious nodes in wireless sensor networks. Section 3 proposes a novel methodology for the detection of malicious nodes using trust based evaluation algorithm. Section 4 discusses the network simulation setup with its experimental results. Finally, Section 5 concludes the research.

Corresponding Author: K. Yogitha, Department of EIE, Annamalai University, India.

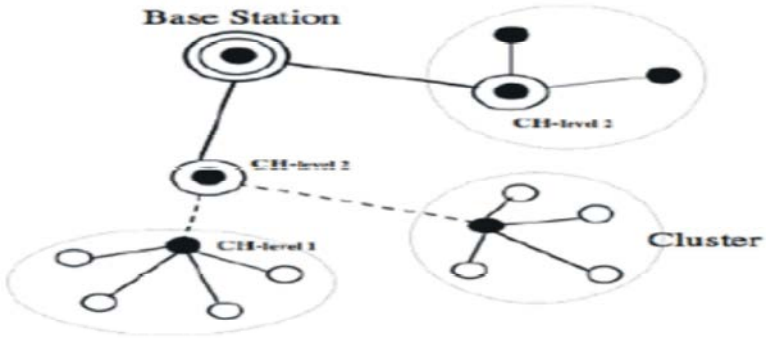

Fig. 1: Wireless Sensor Network

Literature Survey: Hossein Jadidoleslamy [1] used hierarchical technique for detecting the suspicious nodes in wireless area networks and the authors further utilized intrusion detection technique to analyze the behaviour of the network. The authors use clustering approach for identifying the characteristics of the node behaviour in sensor networks. Feng *et al*. [2] developed a trust estimation methodology for analyzing the behaviour of the nodes in wireless sensor environment. The authors applied evidency technique on each node in the network to analyze the characteristics of the node. The trust methodology proposed in this work was based on the characteristics of the individual node in WSN environment. Babu *et al*. [3] predicted the nodes characteristics using recommendation algorithm for trust values estimation on each individual node in WSN environment. The authors extracted the quality of service parameters for individual node analysis to detect the malicious nodes among the set of nodes in wireless network topology.

Chang *et al*. [4] proposed malicious node detection system using cooperative bait technique which efficiently detects the abnormal nodes in larger network area. The authors solved the limitations in dynamic source routing protocol of the present malicious node detection system. The authors achieved 97% average packet delivery ratio in their proposed methodology for malicious node detection. Patel *et al*. [5] proposed the methodology for detecting the malicious nodes in smart wireless sensor networks. The authors used passive eavesdropping reduction algorithm to prevent the message leakage in network environment. Michel Toulouse *et al*. [6] developed an intrusion detection and elimination systematic network architecture which was based on anomaly-based fully distributed methodology. The author's detected denial of service attacks and black hole attacks in larger network environment.

The following points are drawn from the conventional malicious node detection system as stated below.

- There was low network performance when the malicious nodes were higher in network environment.
- Most of the conventional methods were based on the recommendation technique.
- Conventional methods needed the robust characteristics of the nodes behaviour during the detection process, which lead to the time consuming process.

Proposed Methodology: Clustering the nodes in WSN simplify the malicious node detection process. In this paper, we cluster the network into numbers of clusters and each cluster has one cluster head. Here, the clustering of the nodes is done by evaluating the weight of each node in the network. For example, the weight of the node (nc_1) is computed using its surrounding eight neighbouring nodes as shown in Fig. 3 and it can be given as,

$$W_{nc1} = \sum_{n=1}^{8} 2^{n-1}.\phi(n_i - n_{c1}) \quad (1)$$

where, n_i is the no. of neighboring nodes and n_{c1} is the center node which the weight should be calculated.

The weight function of the node (nc_1) is computed using the following equation as,

$$\phi(n_i - n_{c1}) = \begin{cases} 1, & n_{c1} \geq n_i \\ 0, & n_{c1} < n_i \end{cases} \quad (2)$$

The weight of the node (n_2) is computed using its surrounding eight neighbouring nodes as shown in Fig. 3 and it can be given as,

$$W_{n2} = \sum_{n=1}^{8} 2^{n-1}.\phi(n_i - n_2) \quad (3)$$

The weight function of the node (n_2) is computed using the following equation as,

$$\phi(n_i - n_2) = \begin{cases} 1, & n_2 \geq n_i \\ 0, & n_2 < n_i \end{cases} \quad (4)$$

The cluster head (CH) of the nodes is computed based on the weight functions as depicted in Eqn. (5).

$$Cluster\ Head\ (CH) = \begin{cases} n_{c1}, & if\ \ w_{nc1} > w_{n2} \\ n_2, & if\ \ w_{n2} > w_{nc1} \end{cases} \quad (5)$$

The cluster head must have the highest weight than the other nodes in wireless sensor networks.

Consider node n_3 to be checked for its classifications as either malicious or normal node. The nodes behaviour is verified by both direct and indirect methods as shown in Fig. 3. Let total no. of packets sent to n_3 by n_1 is S_{n1} and total no. of acknowledges received from n_3 in n_1 is R_{n1}. The trust estimation of node n_3 by n_1 is computed using the following formula as,

$$IR_{n1-n2} = \frac{S_{n1} + R_{n1}}{1 - (S_{n1} + R_{n1})} \quad (6)$$

Let total no. of packets sent to n_3 by nc_1 is S_{nc1} and total no. of acknowledges received from n_3 in nc_1 is R_{nc3}. The trust estimation of node n_3 by nc_1 is computed using the following formula as,

$$IR_{n_{c1}-n_{c3}} = \frac{S_{nc1} + R_{nc3}}{1 - (S_{nc1} + R_{nc3})} \quad (7)$$

Let total no. of packets sent to n_3 by n_2 is S_{n2} and total no. of acknowledges received from n_3 in n_2 is R_{n3}. The trust estimation of node n_3 by n_2 is computed using the following formula as,

$$IR_{n2-n3} = \frac{S_{n2} + R_{n3}}{1 - (S_{n2} + R_{n3})} \quad (8)$$

Let total no. of packets sent to n_3 by n_4 is S_{n4} and total no. of acknowledges received from n_3 in n_4 is R_{n4}. The trust estimation of node n_3 by n_4 is computed using the following formula as,

$$IR_{n4-n3} = \frac{S_{n4} + R_{n3}}{1 - (S_{n4} + R_{n3})} \quad (9)$$

The beta function of the node n_3 is determined using the following Equation (10) as,

$$\beta = \frac{IR_{n_{c1}-n_{c3}}}{IR_{n1-n3} + IR_{n2-n3} + IR_{n4-n3}} \quad (10)$$

The cumulative distribution function of the node n_3 is determined using beta function and it is given as,

$$CDF = 1 - e^{-x/\beta} \quad (11)$$

where, x = node weight of n_3 and β is the beta function of node n_3.

Total trust features of node n_3 are the addition of direct trust features and indirect trust features. The indirect trust features are computed based on the surrounding nodes n_1, n_2, n_4 and nc_1. The indirect trust features are the derived cumulative distribution function of node n_3.

The direct trust value of node n_3 can be measured by nc_1 is given as,

$$DT(n_{c1}, n_3) = \frac{\alpha(n_{c1}, n_3)}{\alpha(n_{c1}, n_3) + \beta(n_{c1}, n_3)} \quad (12)$$

The alpha function (α) between node n_3 and node nc_1 is estimated using the following Eqn. (13) as,

$$\alpha(n_{c1}, n_3) = w_{nc1} \times CDF + W_{n3} \times (1 - CDF) \quad (13)$$

where, w_{nc1} is the weight of the node nc_1 and w_{n3} is the weight of the node n_3.

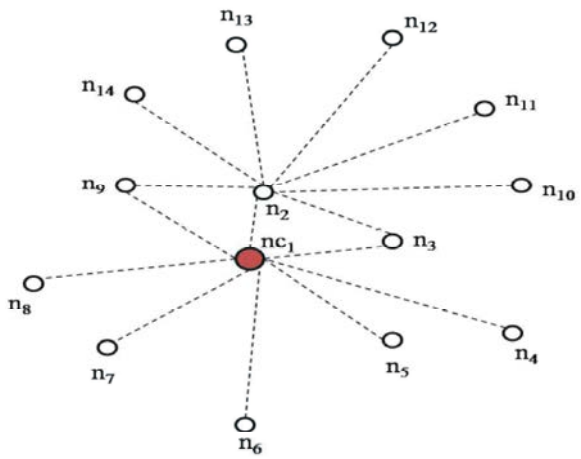

Fig. 2: Clustering using weight of the nodes

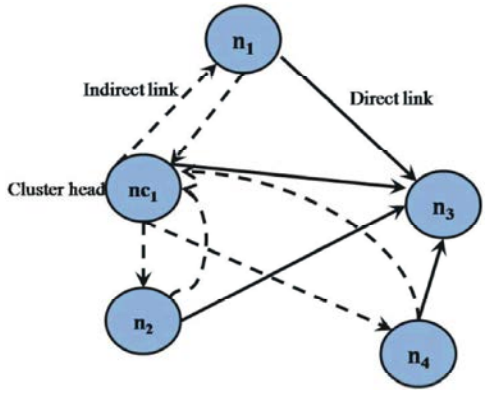

Fig. 3: Trust estimation

The beta function between node nc_1 and w_{n3} is computed as,

$$\beta(n_{c1}, n_3) = \frac{S_{nc1} + R_{n3}}{1 - (S_{nc1} + R_{n3})} \quad (14)$$

The computed features (direct and indirect) are given to the classifier to classify the node's behaviour into either normal or malicious. In this paper, Adaptive Neuro Fuzzy Inference (ANFIS) classifier is used to classify the node's behaviour based on the trust features. This classifier is operated in training and testing modes for the classification of node's behaviour. This classifier produces high value when the test node is malicious and produces low value when the test node is normal node.

RESULTS AND DISCUSSION

In this paper, network simulator version 2 is used to simulate the wireless sensor networks. The sensor network is initially constructed with 100 numbers of nodes and each node has the inbuilt omni directional antenna to transmit and receive the data and control messages from other nodes in the network. The energy level of the inbuilt battery of each node is kept as 1000 Joule at an initial stage. Each node consumes certain amount of energy during the data transmission and reception and the energy consumption is entirely based on the distance between two nodes and the amount of data to be transmitted or received over the wireless medium. Dynamic source routing protocol is assigned in each node for finding the shortest path between nodes in network.

The performance of the proposed malicious node detection system is analyzed in terms of packet delivery ratio and throughput.

Table 1 shows the PDR comparisons with conventional methodologies as Chang *et al*. [4], Babu *et al*. [3] and Feng *et al*. [2]. The proposed methodology stated in this paper achieves 98.28% PDR while the other conventional methods Chang *et al*. [4] achieved 95.37%, Babu *et al*. [3] achieved 93.47% and Feng *et al*. [2] achieved 94.26%.

Table 2 shows the PDR comparisons of the proposed method and other conventional methods with respect to numbers of malicious nodes. The proposed methodology for malicious node detection system achieves 98.28% PDR when there is 10 numbers of malicious nodes, 96.37% PDR when there is 15 numbers of malicious nodes, 95.37% PDR when there is 20 numbers of malicious nodes, 93.49% PDR when there is 25 numbers of malicious nodes and 91.35% PDR when there is 30 numbers of malicious nodes.

Table 1: PDR comparisons with conventional methodologies

Methodology	Year	PDR (%)
Proposed work	2016	98.28
Chang *et al*. [4]	2015	95.37
Babu *et al*. [3]	2014	93.47
Feng *et al*. [2]	2011	94.26

Table 2: PDR comparisons with respect to numbers of malicious nodes

# of malicious nodes	Proposed method	Chang *et al*. [4]	Babu *et al*. [3]	Feng *et al*. [2]
10	98.28	95.37	93.47	94.26
15	96.37	96.01	92.28	96.98
20	95.37	92.46	95.76	93.29
25	93.49	91.36	91.37	91.03
30	91.35	84.48	89.85	92.89

Table 3: Throughput comparisons with conventional methodologies

Methodology	Year	Throughput (bits/sec)
Proposed work	2016	12, 378
Chang *et al*. [4]	2015	11, 395
Babu *et al*. [3]	2014	10, 383
Feng *et al*. [2]	2011	11, 674

Table 4: Throughput comparisons with respect to numbers of malicious nodes

# of malicious nodes	Proposed method	Chang *et al*. [4]	Babu *et al*. [3]	Feng *et al*. [2]
10	12, 378	11, 395	10, 383	11, 674
15	11, 393	10, 986	10, 120	11, 438
20	10, 753	10, 891	9865	11, 276
25	9864	9654	9753	9720
30	9764	9654	8740	9276

The proposed methodology stated in this paper achieves 12, 378 b/s throughputs while the other conventional methods Chang *et al*. [4] achieved 11, 395 b/s, Babu *et al*. [3] achieved 10, 383 b/s and Feng *et al*. [2] achieved 11, 674 b/s, as shown in Table 3 and the same is plotted in Fig. 4.

Table 4 shows the PDR comparisons of the proposed method and other conventional methods with respect to numbers of malicious nodes. The proposed methodology for malicious node detection system achieves 12, 378 bits/sec throughputs when there is 10 numbers of malicious nodes, 11, 393 bits/sec throughputs when there is 15 numbers of malicious nodes, 10, 753 bits/sec throughputs when there is 20 numbers of malicious nodes, 9864 bits/sec throughputs when there is 25 numbers of malicious nodes and 9764 bits/sec throughputs when there is 30 numbers of malicious nodes and the same is plotted in Fig. 5 [7-9].

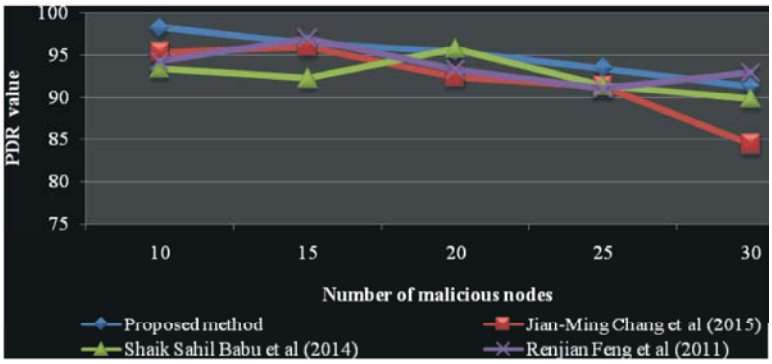

Fig. 4: PDR comparisons

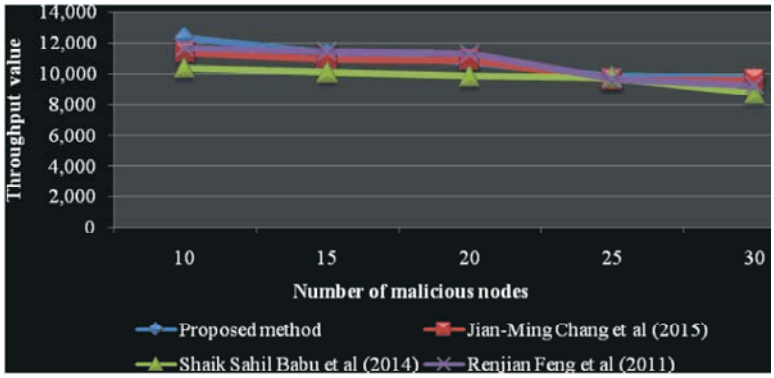

Fig. 5: Throughput comparisons

CONCLUSION

In this paper, the behaviour of the nodes in wireless sensor networks are analyzed based on the feature set which are computed using both direct and indirect methods. These computed trust features are trained and classified using ANFIS classifier to classify the test node into either normal or malicious node. The proposed system is analyzed with respect to number of malicious nodes in network. The performance of the system is affected by increasing numbers of malicious nodes. The proposed system achieves 98.28% PDR and 12, 378 bits/sec throughput.

REFERENCES

1. Hossein Jadidoleslamy, 2011. Hierarchical intrusion detection architecture for wireless sensor networks, International Journal of Network Security & Its Applications (IJNSA), 3(5).
2. Feng, R., X. Xu, X. Zhou and J. Wan, 2011. A Trust Evaluation Algorithm for Wireless Sensor Networks Based on Node Behaviors and D-S Evidence Theory, Sensors, 11: 1345-1360.
3. Babu, S.S., A. Raha and M.K. Naskar, 2014. Trust Evaluation Based on Node's Characteristics and Neighbouring Nodes, Recommendations for WSN, Wireless Sensor Network, 6: 157-172.
4. Chang, J.M., P.C. Tsou, I. Woungang, H.C. Chao and C.F. Lai, 2015. Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach, IEEE Systems Journal, 9(1).
5. Patel, K.S. and J.S. Shah, 2015. Detection and avoidance of malicious node in MANET, International Conference on Computer, Communication and Control (IC4), pp: 1-4.
6. Toulouse Michel, Bui Quang Minh and Philip Curtis, 2015. A Consensus Based Network Intrusion Detection System, Proceeding of the 5th International Conference on IT Convergence and Security (ICITCS), pp: 1-6.
7. Marti, S., T.J. Giuli, K. Lai and M. Baker, 2000. Mitigating routing misbehavior in mobile ad hoc networks. Proceeding of the 6th Annu. Intl. Conf. MobiCom, pp: 255-265.

8. Rubin, I., A. Behzad, R. Zhang, H. Luo and E. Caballero, 2002. TBONE: A mobile-backbone protocol for ad hoc wireless networks, proceeding of the IEEE Aerospace Conference, pp: 2727-2740.

9. Zahariadis, T., H .C. Leigou, P. Trakadas and S. Voliotis, 2010. Mobile Networks: Trust Management in Wireless Sensor Networks, European Transactions on Telecommunications, 21: 386-395.