International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-7 Issue-4s2, December 2019

Detection of Malicious Nodes in Wireless Sensor Networks based on Features Using Neural Network Computing Approach

B. Rajasekaran, C. Arun

Abstract: ***The detection of malicious or hidden nodes in Wireless Sensor Network (WSN) is important for improving the performance of the WSN. In this paper, distance metric and probabilistic features are extracted from each individual node in WSN with respect to its surrounding nodes. These individual extracted features are given to the input of the classification algorithm. This paper uses feed forward back propagation neural networks for training and testing the individual nodes using the extracted node features. The concert of this hidden node identification in WSN using metric and probabilistic features based classification algorithm analyzed energy consumption, throughput and delay.***

Keywords: ***Malicious, nodes, metric, features, neural networks.***

I. INTRODUCTION

The modern communication system requires high level standards for transferring information between one ends to another end. This is possible only through wireless communication where as digital era is used nowadays for reliable communication. The wireless open channel environment is used as transferring medium between source and destination nodes. This wireless communication is categorized into Wireless Sensor Networks (WSN) and Wireless Body Area Networks (WBAN). The WBAN networks are implemented in humans and it senses the body conditions from various parts of human body and sends these information's to the remote unit. In case of WSN networks, the numbers of sensors are deployed in a random manner and it collects the information from all sensors. This sensed information is sent to remote unit as sink. The number of sensors are grouped under the single node is called as cluster head. The cluster head collects all sensed information from its clustered nodes and each cluster head send these information's to remote sink. In WSN networks, there may be number of cluster heads available with single sink node. Each node in WSN have sensor, analog to digital converter and processor. The sensor senses the surrounding parameters in analog mode and these sensed analog data are converted into digital data by means of analog to digital converter. This converted digital data is processed through processor unit and this processed data is transferred to another node by means of inbuilt wire antenna which is connected to node.

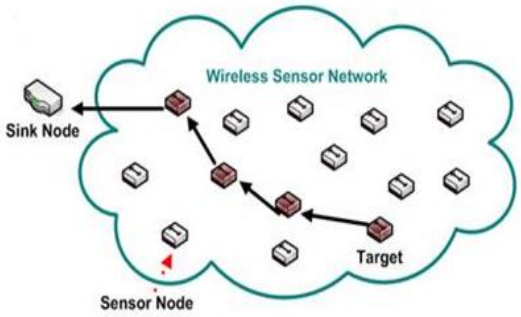

Figure 1: Nodes deployment in WSN network

Fig.1 shows the sensor nodes deployed in WSN environment with sink node connected to the WSN networks. The nodes behavior is changed by external attacker or hacker and these nodes become malicious/ hidden nodes. The performance efficiency of present WSN networks is degraded by number of malicious/hidden nodes. Hence, this paper proposes an efficient technique for identifying theses nodes in WSN in order to improve the performance. This paper is structured as the conventional methodologies in section 2, section 3 proposes an efficient methodology for identifying the hidden/malicious nodes and section 4 shows the simulation results. Section 5 shows the conclusions with future works.

II. LITERATURE SURVEY

Preethi et al. (2018) used adaptive data fusion methodology for identifying the malicious nodes in large WSN networks for improving its performance. The sensed data were fused with identification code and then these data was sent to remote unit in order to prevent the hacking of data by unknown nodes or malicious nodes. The authors achieved 65.1mJ of energy consumption, 56,192 bits/sec as throughput and 5.86 ns as delay for detecting and mitigating the malicious or hidden nodes in WSN environment. Atassi et al. (2013) proposed end to end topology based malicious node identification system for mitigating the malicious nodes in WSN networks. The presence of malicious or hidden nodes consumed high energy and further degrades the performance of the WSN networks.

Manuscript published on 30 December 2019.
*Correspondence Author(s)
B. Rajasekaran, Research Scholar, Dept of ECE, St. Peter's Institute of Higher Education & Research, Chennai. (e-mail: rajasekaranb80@gmail.com)
Dr. C. Arun, Professor, Dept of ECE, R.M.K College of Engineering & Technology, Chennai.

The authors achieved 62.9 mJ of energy consumption, 52,749 bits/sec as throughput and 6.91 ns as delay for detecting and mitigating the malicious or hidden nodes in WSN environment.

Singh et al. (2012) developed an efficient approach or algorithm for detecting the malicious nodes in WSN networks.

The authors achieved 58.7 mJ of energy consumption, 61,740 bits/sec as throughput and 8.47 ns as delay for detecting and mitigating the malicious or hidden nodes in WSN environment. Padmaja et al. (2007) developed a mechanism for malicious or hidden nodes detection and mitigation using data aggregation algorithm. The authors detected various active and passive attacks in WSN environment for improving the performance of the WSN networks. Pires et al. (2004) designed a methodology for detecting and mitigating the abnormal behavior nodes in WSN networks. The behavior of all nodes in WSN network were monitored continuously by sensing device agent and this information was passed to the central unit for improving the performance of the WSN network by eliminating the malicious nodes. The authors detected suspicious activities of each node in WSN environment for better performance.

III. PROPOSED METHODOLOGIES

The proposed malicious/ hidden node detection methodology consists of feature extraction and classification stages as depicted in Fig.2.

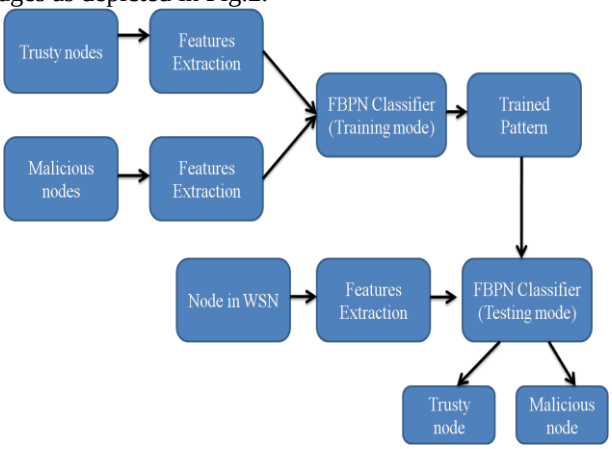

Figure 2: Proposed malicious/hidden node detection method

Distance-Metric Features

The node with normal operations are transferring or receiving the packets from CH or nearby nodes regularly. The node with abnormal operations blocks the data transmission or reception between node and CH or node to other surrounding nodes in WSN environment. This feature will be used in order to classify the nodes behavior for the detection of malicious node in WSN environment. In order to compute or extract this feature from an individual node, the number of packets flow between that corresponding individual node and its nearby node are computed as shown in Fig.3.

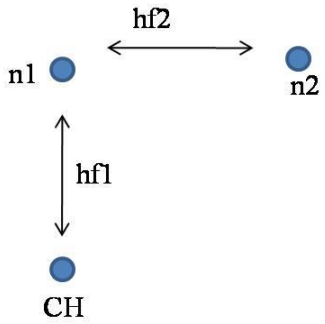

Figure 3: Computation of Distance-metric features

The distance-metric between node n1 and CH is computed using the following equation.

$$Dist_{metric} = \frac{\gamma(n1) + \gamma(CH)}{\sqrt{\gamma^2(n1) + \gamma^2(CH)}}$$

Whereas, γ (node 1) is the coordinates of node 1 and γ (CH) is the coordinates of cluster head.

The distance-metric between node n1 and n2 is computed using the following equation.

$$Dist_{metric} = \frac{\gamma(n1) + \gamma(n2)}{\sqrt{\gamma^2(n1) + \gamma^2(n2)}}$$

Whereas, γ (node 1) is the coordinates of node 1 and γ (CH) is the coordinates of cluster head.

The total distance metric in node 1 by node 2 and cluster head is the average value of distance metrics between node 1 to cluster head and node 1 to node 2.

Probabilistic Features

The nodes in WSN environment transmits or forwards the packets from one node to another nearby nodes. The normal node accepts packet transmission request from nearby nodes and ready to transmit the packets. The malicious or hidden nodes do not accept the packet transmission request from nearby nodes. Instead of accepting request from nearby nodes, it transmits dummy packets to nearby nodes. By opting this behaviour as feature, the number of packets transmitted and received over a period is computed between node 1 and node 2, and node 1 and cluster head, as depicted in Fig.4.

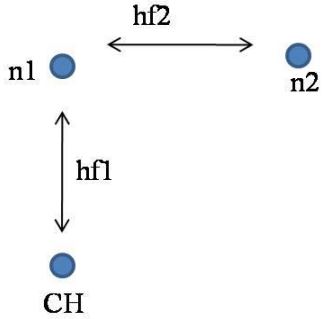

Figure 4: Computation of probabilistic features

The probabilistic feature is computed between nodes in WSN environment based on transmitting and receiving packets between nodes.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

The probabilistic feature between node 1 and cluster head is computed using the following equation,

$$Prob_{feat(n1,c1)} = \frac{\propto(n1) * \beta(n1) + \propto(c1) * \beta(c1)}{\sqrt{\propto(n1) + \propto(c1)}}$$

Whereas, $\propto(n1)$ is the number of forwarding packets through node 1 to cluster head, $\beta(n1)$ is the number of receiving packets through node 1 from cluster head. $\propto(c1)$ is the number of forwarding packets through cluster head to node 1 and $\beta(c1)$ is the number of receiving packets through cluster head from node 1.

The probabilistic feature between node 1 and cluster head is computed using the following equation,

$$Prob_{feat(n1,n2)} = \frac{\propto(n1) * \beta(n1) + \propto(n2) * \beta(n2)}{\sqrt{\propto(n1) + \propto(n2)}}$$

Whereas, $\propto(n1)$ is the number of forwarding packets through node 1 to node 2, $\beta(n1)$ is the number of receiving packets through node 1 from node 2. $\propto(c1)$ is the number of forwarding packets through node 2 to node 1 and $\beta(c1)$ is the number of receiving packets through node 2 from node 1.

The total probabilistic feature of node 1 by node 2 and cluster head is given in the following equation as,

$$Prob_{feat} = Prob_{feat(n1,n2)} + Prob_{feat(n1,c1)}$$

Trust Features

The trust features are computed based on the number of packets correctly received and transmitted on individual node. These features are extracted from individual node by computing its correctly transmitted and received packets. The trust feature of node n1 by node 2 and node 3 is given as,

$$\mathbf{Trust_{feat}} = \frac{\mathbf{TP}}{\mathbf{TP + TN}}$$

Whereas, TP is True Positive which represents correctly transmitted packets from node 1 to either node 2 or node 3. TN is True Negative which represents wrongly transmitted packets from node 1 to either node 2 or node 3. Fig.4 shows the computation of trust features in node 1 by node 2 and node 3.

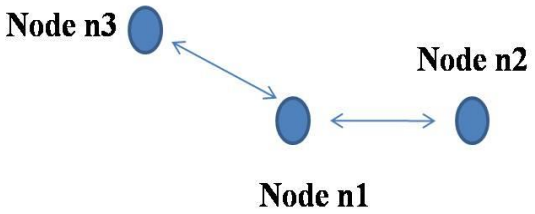

Figure 5: Computation of trust features in node n1

Classifications

It plays an important role in classifying the nodes in WSN environment based on feature set. In this paper, Neural Networks (NN) classification algorithm is used in order to classify the individual nodes in WSN. This classifier has two types as Radial and Feed forward. The radial NN consumes high computational time for the detection of malicious/hidden nodes. Hence, this paper uses Feed Forward Back Propagation Neural Networks (FBPN) for classifying the nodes into either trusty or malicious nodes. This classification algorithm can be operated into training and testing. This FBPN network can have five layers as input, output and hidden layers. In training mode of the classification algorithm, the features are extracted from both trusty and malicious nodes. These features are trained by training mode of this classification algorithm. In testing mode of the classification algorithm, the features from each individual node in WSN are classified based on the trained patterns which are generated during training mode of the classification algorithm.

Computation of Energy Consumption

The energy consumption of transmitting nodes in WSN is computed as,

$$Trans_{node} = \frac{E_d \times v \times d_{in}^{v-1}}{d}$$

Whereas, d_{in} is the number of bits to be transmitted, d is the distance between node 1 and node 2, E_d is the energy availability in node 1 and v is the Gamma factor which ranges from 1 to 10 and it is determined using the following condition.

$$v = \begin{cases} \geq 5, & if\ d \geq 1m \\ < 5, & if\ d < 1m \end{cases}$$

The energy consumption of receiving node in WSN is computed as,

$$R_{node} = Trans_{node} \times v \times E_r$$

Whereas, Er is the energy in node 1 and it is computed using the following equation.

$$E_r = \frac{V_{node1} \times I_{node1}}{bitrate_{node1}}$$

The bit rate of node 1 is determined using the number of bits received and the distance between node 1 and node 2 and it is given as,

$$bitrate_{node1} = \left(\frac{d_{out}}{d}\right)^{v}$$

IV. RESULTS AND DISCUSSION

The proposed malicious or hidden node detection methodology stated in this paper is applied on WSN environment with Additive White Gaussian Noise (AWGN) channel state between sender and receiver nodes. Each node in WSN network is having 1000 Joules of energy as initial criteria and 100 nodes are spread over 1000 m* 1000 m as width and height of the simulation environment. Each node in WSN environment consumes 30 mJ of energy for transmitting, receiving and processing the data from one node to another node for each transaction. For each cycle period, each node transmits maximum of 300 packets. The 25 nodes are converted into malicious nodes among the set of 100 nodes in WSN environment. The function of the malicious nodes is to transmit dummy packets to nearby nodes in order to destroy the energy level of the nearby nodes. The proposed methodology is evaluated with respect to energy consumption, throughput and delay metrics.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Energy Consumption

Every node in WSN environment consumes certain amount of energy for each transaction of packets from one node to another node. The increased number of malicious or hidden nodes in WSN environment may linearly increases the energy consumption level. The energy consumption is measured in milli joules and it is analyzed with respect to number of malicious nodes. Table 1 shows the performance analysis of proposed method in terms of energy consumption with respect to number of malicious nodes in WSN system environment. From Table 1, the proposed malicious or hidden node detection methodology consumes 11.1 mJ of energy for the injection of 5 number of malicious nodes and consumes 63.9 mJ of energy for the injection of 25 malicious nodes in WSN environment. The proposed methodology consumes 37.6 mJ of energy as an average for the injection of 'N' number of malicious nodes. It is very clear from Table 1, the energy level gradually decreases with respect to increasing the malicious node counts. Fig.6 shows the performance analysis graph for energy consumption.

Table 1: Performance analysis of proposed method in terms of energy consumption

Number of malicious nodes	Energy consumption (mJ)
5	11.1
10	23.8
15	38.1
20	51.1
25	63.9
Average	**37.6**

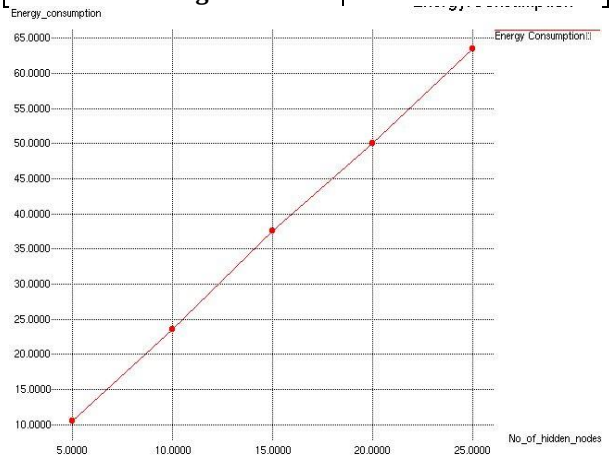

Figure 6: Analysis of energy consumption

Throughput

The transmission and reception capability of packets through nodes in WSN environment is defined by throughput and it is measured in bits per second. The increased number of malicious or hidden nodes in WSN environment may linearly decreases the value of throughput.

The throughput is analyzed with respect to number of malicious nodes. Table 2 shows the performance analysis of proposed method in terms of throughput with respect to number of malicious nodes in WSN system environment. From Table 2, the proposed malicious or hidden node detection methodology achieves 88,700 bits/sec of throughput for the injection of 5 numbers of malicious nodes and achieves 74,150 bits/sec of throughput for the injection of 25 malicious nodes in WSN environment.

The proposed methodology achieves 81.910 bits/sec as an average throughput for the injection of 'N' number of malicious nodes.

It is very clear from Table 2; the value of throughput gradually decreases with respect to increasing the malicious node counts. Fig.5 shows the performance analysis graph for throughput.

Table 2: Performance analysis of proposed method in terms of throughput

Number of malicious nodes	Throughput (bits/sec)
5	88,700
10	86,100
15	82,500
20	78,100
25	74,150
Average	**81,910**

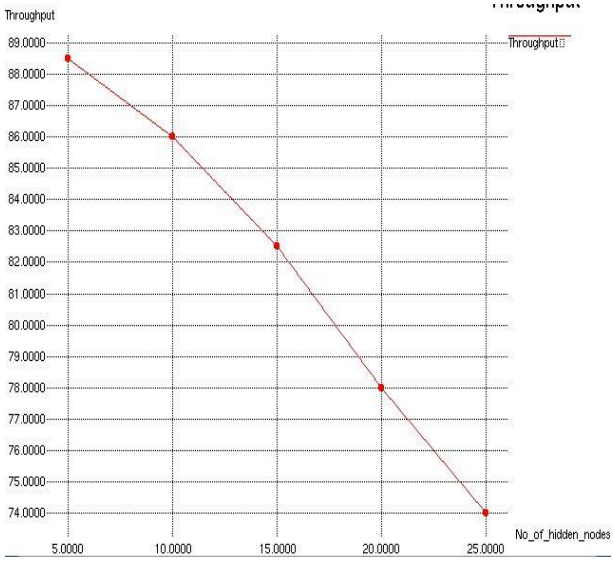

Figure 7: Analysis of throughput

Delay

Each node in WSN environment takes certain period of time for transmission and reception of packets from one node to another node. It is generally measured in ns and it is gradually increased by number of malicious nodes or hidden nodes in WSN environment. The delay is analyzed with respect to number of malicious nodes. Table 3 shows the performance analysis of proposed method in terms of delay with respect to number of malicious nodes in WSN system environment. From Table 3, the proposed malicious or hidden node detection methodology achieves 0.6 ns of delay for the injection of 5 numbers of malicious nodes and achieves 4.5 ns of delay for the injection of 25 malicious nodes in WSN environment. The proposed methodology achieves 2.53ns as an average delay for the injection of 'N' number of malicious nodes. It is very clear from Table 3; the value of delay gradually increases with respect to increasing the malicious node counts. Fig.6 shows the performance analysis graph for delay.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Table 3: Performance analysis of proposed method in terms of delay

Number of malicious nodes	Delay (ns)
5	0.6
10	1.55
15	2.5
20	3.3
25	4.7
Average	**2.53**

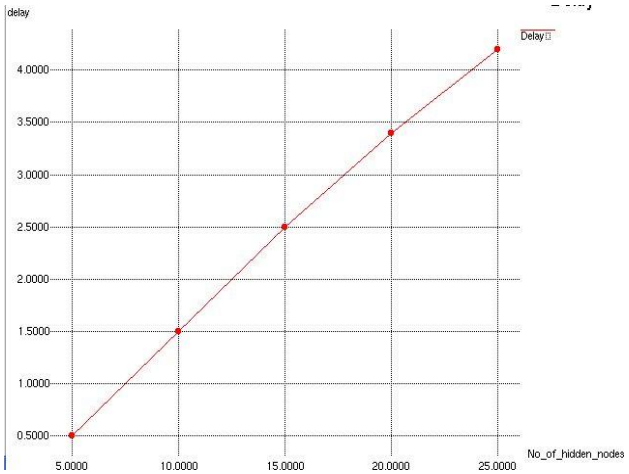

Figure 6: Analysis of delay

Table 4: Performance analysis of proposed method in terms of delay

Methodologies	Energy consumption (mJ)	Throughput (bits/sec)	Delay (ns)
Proposed work (in this paper)	**37.6**	**81,910**	**2.53**
Preethi et al. (2018)	65.1	56,192	5.86
Atassi et al. (2013)	62.9	52,749	6.91
Singh et al. (2012)	58.7	61,740	8.47

Table 4 compares the proposed malicious node detection methodology with conventional methodologies as Preethi et al. (2018), Atassi et al. (2013) and Singh et al. (2012). The proposed methodology stated in this paper consumes 37.6 mJ of energy, 81,910 bits/sec as throughput and 2.53 ns of delay. Preethi et al. (2018) consumed 65.1 mJ of energy, 56,192 bits/sec of throughput and 5.86 ns of delay. Atassi et al. (2013) consumed 62.9 mJ of energy, 52,749 bits/sec of throughput and 6.91 ns of delay. Singh et al. (2012) consumed 58.7 mJ of energy, 61,740 bits/sec of throughput and 8.47 ns of delay.

V. CONCLUSIONS

This paper proposes a classification approach based malicious or hidden nodes in WSN networks. The nodes behavior in WSN are extracted as features as probabilistic features, distance metric features and trust features. These features are classified using feed forward back propagation neural networks. The proposed methodology consumes 37.6 mJ of energy as an average for the injection of 'N' number of malicious nodes. The proposed methodology achieves 81.910 bits/sec as an average throughput for the injection of 'N' number of malicious nodes. The proposed methodology achieves 2.53ns as an average delay for the injection of 'N' number of malicious nodes.

REFERENCES

1. Preethi M , Rashmi Purad, Kavya D S, Chandrakala H ," A Technique for Malicious Node Detection for Adaptive Data Fusion in Wireless Sensor Networks", International Journal of Scientific and Research Publications, Volume 8, Issue 6, June 2018.
2. M. Singh, G. Mehta, C. Vaid and P. Oberoi, "Detection of Malicious Node in Wireless Sensor Network Based on Data Mining," 2012 International Conference on Computing Sciences, Phagwara, 2012, pp. 291-294.
3. Atassi, N. Sayegh, I. Elhajj, A. Chehab and A. Kayssi, "Malicious Node Detection in Wireless Sensor Networks," 2013 27th International Conference on Advanced Information Networking and Applications Workshops, Barcelona, 2013, pp. 456-461.
4. P. Padmaja and G. V. Marutheswar, "Detection of Malicious Node in Wireless Sensor Network," 2017 IEEE 7th International Advance Computing Conference (IACC), Hyderabad, 2017, pp. 193-198.
5. W. R. Pires, T. H. de Paula Figueiredo, H. C. Wong and A. A. F. Loureiro, "Malicious node detection in wireless sensor networks," 18th International Parallel and Distributed Processing Symposium, 2004. Proceedings., Santa Fe, NM, USA, 2004, pp. 24-27.
6. Roy Sandip et al., "Secure data aggregation in wireless sensor networks: Filtering out the attacker's impact", IEEE Transactions on Information Forensics and Security, vol. 9, no. 4, pp. 681-694, 2014.
7. K Pradeepa, WR Anne, S Duraisamy, "Design and implementation issues of clustering in Wireless Sensor Networks", International Journal of Computer Applications, vol. 47, no. 11, pp. 23, 2012.
8. R Azarderskhsh, A Reyhani, "Secure clustering and symmetric key establishment in heterogeneous wireless sensor networks", Eurasip Journal on Wireless Communications and Networking Article ID: 893592, pp. 1-12, 2011.
9. K. Kalpakis, K. Dasgupta, P. Namjoshi, "Efficient algorithms for maximum lifetime data gathering and aggregation in wireless sensor networks", Computer Networks, vol. 42, no. 6, pp. 697-716, August 2003.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)