Detection of malicious node in Industrial Automation for improving the performance of IOT

C.Manikandan[1], V. Alamelumangai[2]

[1,2]Department of Electronics and Instrumentation Engineering, Annamalai University, India.
E-mail: manikandan.aec@gmail.com

Abstract

The performance of the network is severly affected by malicious nodes which send the unwanted and non-related information to the near by nodes. The detection process of maliciou is more complex due to the similar behaviour with respect to non malicious nodes. Hence, this paper proposes an efficient algorithm for the detection of malicious node in industrial automation network environment. The proposed coherent matching algorithm stated in this paper achieved 70.46% of detection rate and also achieved 94.84% of packet delivery ratio as average value from the simulation results.

Keywords: **malicious nodes, industrial automation, detection, network, packet delivery ratio.**

1. Introduction

Today, the usages of internet are high due to the development of technology. The distant devices or units are controlled by a single device through internet. Monitoring and controlling of different numerous devices through internet is called as Internet-of-Things (IoT). This IoT technique can be used in different scenario like home applications, industrial need and military usage. In case of home applications, all the devices used in user home can be continuously monitored and controlled by remote unit through the development of IoT technology between devices. In case of industrial applications, the machines are controlled and monitored by remote unit, through which the accidents in an unmanned area can be avoided. Gartner, Inc estimated the level of growth for the device usage in IoT was 20.8 billion devices in 2020 year. The multimedia data from various service providers are stored in large cloud area. Hence, there must be the high level of data confidentiality in handling these data services between different networks or service providers.

Often, the performance of the network is degraded by dead nodes, selfish nodes and malicious nodes. The dead node is formed in network due to the power degradation in sensor node. Selfish node is the node which does not respond to surrounding nodes and this node is converted into normal node after applying credits to these nodes. The malicious node is a node which can be formed in network due to the lack of power in node. The performance of the network is severly affected by malicious nodes which send the unwanted and non-related information to the near by nodes. The detection process of maliciou is more complex due to the similar behaviour with respect to non malicious nodes. Hence, this paper proposes an efficient algorithm for the detection of malicious node in industrial automation network environment.

2. Literature Survey

Vieira et al. (2003) deviced a novel technique for finding the bahaviour of the node using Byzantine solution. The weight of the node which was presented in cluster was determined using the distance between center node and its surrounding nodes. The threshold based system clssified each node

in cluster area into either malicious or not. Curiac et al. (2007) proposed an algorithm for malicious node identification based on autoregression method. The authors used probability density function for each node in network and based on their lower density value, the node was identified as malicious. The threshold was determined from the set of sensed data and then the regressive value of the node was computed using autoregressive point technique. Atakli et al. (2008) used weight computation methodology in each node of the wireless sensor network to compute the average weight. Then, the authors evaluated the trust value from each node. By comparing the trust value with average weight, the node in sensor network is identified as malicious.

Sung Yul Lim et al. (2013) proposed malicious node classification method using dual threshold values. The authors found the threshold value from the average value of each node in wireless sensor networks. The sensed value from each sensor is compared with threshold to conclude the malicious node behaviour and its impact in performance degradation. Gopalakrishnan et al. (2016) developed malicious node identification scheme which was based on cluster values. The weight of the individual node was estimated from the cluster nodes and based on the cluster node values; the node was concluded as malicious in this paper. The authors analyzed their proposed detection scheme in terms of packet delivery ratio and detection rate.

3. Proposed Methodology

The main objective of this paper is to propose a novel and efficient algorithms to detect malicious nodes in industry network environment. The malicious nodes are detected using pre-testing method in this paper. This proposed technique is explained in the following sections.

3.1 Pre-testing

In this paper, malicious nodes are detected using pretesting approach, in which each node in particular cluster is tested prior to data transmission with other nodes with in their cluster. The proposed method uses coherent matching algorithm to detect the malicious nodes. The node in cluster becomes malicious due to the following two reasons as stated below.

- The battery drainage in node is the main reason for malicious node formation. Each node requires minimum of 90 mJ of energy for data transmission. If the energy drains below 90 mJ, the node annonemously send the irrelavant data to nearby nodes.
- The hackers from outside environment change the characteristics of the normal node into mailicious node.

The malicious nodes are detected using Coherent Matching Algorithm (CMA) which is implemented in cluster head. Cluster head verifies behaviour of each node with in their clustering range. If the particular node within the cluster range identified as malicious node, then this malicious node details are set to other cluster heads in order to prevent the data transmission from this malicious node. The proposed algorithm is explained in the following section.

Step 1: Determine the Energy Metric (EM) of the particular node in cluster with respect to the following equation.

$$E_1 = \sum_{i=1}^{N} w_i \times (1 - din_i) \quad (1)$$

Where, w_i is the weight of the particular node and din_i is the number of data bits in an individual packet i.

The EM is based on the weight of the individual node. The weight of the individual node in cluster is computed based on the number of packets correctly and wrongly received from its corresponding cluster head and it is stated as,

$$w_i = \frac{(\alpha+1)*(\beta-1)}{\sqrt{R^2-1}} \quad (2)$$

Where, α is the number of packets received at an individual node from cluster head and β is the number of packets sent from individual node to cluster head. 'R' is the distance between individual node and cluster head.

The distance between individual node and cluster head is given as,

$$R = \sqrt{(Ox - Cx)^2 + (Oy - Cy)^2} \quad (3)$$

Where,

(Ox, Oy): Coordinates of the individual node.

(Cx, Cy): Coordinates of the cluster head.

Step 2: Determine the Coherent Factor (CF) of the individual node in cluster as,

$$CF = \frac{\sum_{i=1}^{N} E_i \times (SA)_{packet\ i} + (DA)_{packet\ i}}{N} \quad (4)$$

The CF determines the originality of the source and destination address. In this paper, the length or size of the source and destination address is 10 bits long and the data length is 16 bits long. The performance of the proposed malicious node detection system is high when the value of CF is high and the performance of the proposed firewall system is low when the value of CF is low.

Step 3: Determine the connectivity factor(C_i) of the individual node in cluster using the following equation as,

$$C_i = \frac{E_i}{CF_i} \times \sqrt{\frac{(E_i-1)\times(CF_i-1)}{N}} \quad ; \quad i = 1\ to\ N \quad (5)$$

The connectivity factor of the node in its corresponding cluster decides the behaviour of the incoming packets from its surrounding nodes. The value of connectivity factor must lie between 0.6and 1. If the computed connectivity factor is not in the range, then the proposed system performance is low and there may be number of malicious packets.The number of nodes in particular cluster is N.

Step 4: Find the Coherent Matching Index (CMI) of the individual node as stated in below equation as,

$$CMI_i = \frac{E_i}{(C_i-1)\times N} \quad (6)$$

The node can be concluded as malicious and non-malicious as per the following conditions.

Node= { Non-malicious; CMI ≤ 0.5;
Malicious; CMI > 0.5;

4. Results and Discussion

In this paper, the proposed pretesting approach is tested using coherent matching algorithm on the nodes which are present in industrial automation network. The proposed system is simulated using Network Simulator 2 version with 50 number of sensor nodes. The performance of the proposed coherent

matching algorithm is analyzed in terms of packet delivery ratio and detection rate. The malicious nodes affect the performance of data transmission and reception in industrial automation network. Its performance is evaluated by determining the number of correctly received packets in each node in network environment. Table 1 shows the performance analysis of proposed method interms of packet delivery. The malicious node is injected into network environment from the count 5 to 25 over 50 number of sensor nodes.

The proposed coherent matching algorithm stated in this paper achieved 94.84% of packet delivery ratio as average value from simulation results as depicted in Table 1.

Table 1 Performance analysis of proposed method interms of packet delivery ratio

No.of malicious nodes	Packet delivery ratio (%)
5	98.3
10	96.1
15	94.9
20	93.1
25	91.8

Table 2 shows the performance analysis of proposed method interms of detection rate. It is defined as the ability to detect the number of malicious nodes in network environment. The detection process becomes more complex when there are many numbers of malicious nodes. The proposed coherent matching algorithm stated in this paper achieved 70.46% of detection rate as average value from simulation results as depicted in Table 2.

Table 2 Performance analysis of proposed method interms of detection rate

No.of malicious nodes	No.of detected nodes	Detection rate (%)
5	4	80
10	7	70
15	11	73.3
20	13	65
25	16	64

Table 3 shows the performance comparisons of proposed method with state of arts interms of packet delivery ratio and detection rate.

Table 3 Performance comparisons of proposed method with state of arts

Methodology	Packet delivery ratio (%)	Detection rate (%)
Pproposed (in this paper)	94.84	70.46
Gopalakrishnan et al. (2016)	86.71	61.9
Atakli et al. (2008)	82.46	59.7

5. Conclusions

This paper proposes an efficient algorithm for the detection of malicious node in industrial automation network environment. The malicious nodes are detected using Coherent Matching Algorithm (CMA) which is implemented in cluster head. Cluster head verifies behaviour of each node with in their clustering range. If the particular node within the cluster range identified as malicious node, then this malicious node details are set to other cluster heads in order to prevent the data transmission from this malicious node. The proposed coherent matching algorithm stated in this paper achieved 70.46% of detection rate and also achieved 94.84% of packet delivery ratio as average value from the simulation results.

References

[1] *Atakli, I.M.; Hu, H.; Chen, Y.; Ku, W.-S.; Su, Z. Malicious Node Detection in Wireless Sensor Networks Using Weighted Trust Evaluation. In Proceedings of the 2008 Spring Simulation Multiconference, Ottawa, Canada, 14-17 April 2008; pp. 836–842.*

[2] *Sung Yul Lim and Yoon-Hwa Choi, "Malicious Node Detection Using a Dual Threshold in Wireless Sensor Networks", J. Sens. Actuator Netw. 2013, 2, 70-84;*

[3] *D. I. Curiac, O. Banias, F. Dragan, C. Volosencu and O. Dranga, "Malicious Node Detection in Wireless Sensor Networks Using an Autoregression Technique,"* Networking and Services, 2007. ICNS. Third International Conference on*, Athens, 2007, pp. 83-83.*

[4] *M.A.M. Vieira, D.C. da Silva Jr., C.N. Coelho Jr., and J.M. da Mata., "Survey on Wireless Sensor Network Devices," Emerging Technologies and Factory Automation (ETFA03), September 2003.*

[5] *Gopalakrishnan, S. and Kumar, P. (2016) Performance Analysis of Malicious Node Detection and Elimination Using Clustering Approach on MANET. Circuits and Systems, 7, 748-758.*

[6] *Wooseong Kim, "Adaptive Resource Scheduling for Dual Connectivity in Heterogeneous IoT Cellular Networks", International Journal of Distributed Sensor Networks, Vol 12, Issue 4, 2016.*

[7] *Chakib Bekara, "Security Issues and Challenges for the IoT-based Smart Grid", Procedia Computer Science Volume 34, 2014, Pages 532-537.*

[8] *Attlee M. Gamundani, "An Algorithmic Framework Security Model for Internet of Things". International Journal of Computer Trends and Technology (IJCTT) V12 (1):16-20, June 2014.*

[9] *H. Ko, J. Jin and S. L. Keoh, "Secure Service Virtualization in IoT by Dynamic Service Dependency Verification," in IEEE Internet of Things Journal, vol. 3, no. 6, pp. 1006-1014, Dec. 2016.*