International Journal of Applied Engineering Research ISSN 0973-4562 Volume 14, Number 17 (2019) pp. 3573-3578

An Energy Aware and Secure Fuzzy Logic Based Clustering Algorithm For Wireless Sensor Networks

Dr. A.R. Rajeswari
Associate Professor, Department of Computer Science and Engineering,
Sethu Institute of Technology, Kariapatti – 626 115, Virudhunagar – District, Tamilnadu, India.

Abstract

Energy efficient and secure transmission act as two major issues in Wireless sensor networks(WSN). Moreover, WSN consists of energy constrained sensor nodes and thus to enhance the network lifetime the energy level at the each of the node must be preserved. The clustering mechanism act as one of the primary solution to address the problem of energy consumption in the WSN. The major drawback in the existing clustering algorithms is all the nodes are considered as trustworthy nodes which are not true. However, security is one the important design issues in WSN it becomes necessary to address the security aspect during the process of clustering. Trust based mechanism is promising approach to ensure secure transmission. Hence, in this paper trust based security model is proposed to address the security issues caused by the malicious nodes and to elect a trustworthy node as Cluster Leader (CL). Therefore, an integrated trust aware and energy efficient algorithm namely Fuzzy Logic based Energy Aware Secure Clustering algorithm (FBEASC) for effective election of trustworthy and energy efficient node as Cluster leader (CL) is proposed .The simulation results shows that the proposed work provides better results in terms of enhancing network life time and secure transmission of data when compared to other existing works.

Key Words: Wireless Senor Network, Clustering, Fuzzy Inference System, Trust Management, Malicious Nodes

1. INTRODUCTION

Wireless sensor networks have tremendous development in recent years due to recent advancements in micro electromechanical systems(MEMS) technology. Usually a WSN is viewed as collection of a large number of low cost, resources constrained and battery powered wireless sensor nodes [1]. The main aim in the WSN is minimizing the energy consumption, enhance the secure transmission of data and increasing the network lifetime [2]. The clustering process act as primary source in obtaining the following goals such as energy efficiency, improving the lifetime of the network and decreasing the number of nodes that communicates with the base station (BS). Thus, developing an energy efficient and secure cluster based algorithm for WSN becomes one of the major areas of research. Thus in order to address these issues a trust based energy efficient clustering act as primary solution. Clusters are defined as group of the sensors and in each cluster, cluster members chose the node with highest energy and low cluster density node as cluster leader (CL). The CL is responsible for efficient data aggregation and transmission of data. Thus in order to enhance the network lifetime the load of CL should be balanced. In this case fuzzy logic is used for clustering process because with FIS it is possible to make uncertainty decision.

A new algorithm namely FBEASC is proposed in this work by using fuzzy logic. The working principle FBEASC consists of two parts. Firstly, a novel trust scheme is proposed in this work with an objective to detect the malicious nodes from the networks. Moreover, in this trust estimation scheme the energy level and the behavior analysis of the nodes are considered for the trust score evaluation process. Therefore, by using the estimated trust score the node with highest trust value will be selected as cluster leader. Secondly, the member nodes will join with the CL based upon the parameters such as cluster density and energy level by applying the fuzzy Inference system. The FBEASC consist of the following advantages such as enhanced secure transmission of data, the reduced energy consumption and increased lifetime.

The following is the organization of the paper. The literature review is given in Section 2. The newly developed FBEASC algorithm is discussed in Section 3. Simulation and evaluation of results are described in Section 4. Finally, Section 5 concludes this paper with future work.

2. RELATED WORK

Wireless network have wide area of application [3] such as military application, temperature sensing unit, automobile and manufacturing industries, health monitoring system and smart agriculture [4]. In recent years the WSN have such numerous applications it becomes necessary to provide secure and energy efficient communication among the nodes in the network which are not directly connected and communicated. In this section the key aspects of the few of the popular and recent trust and energy clustering algorithms in WSN are explained.

Leach[5] is a traditional and important routing protocol for WSN. Moreover leach is defined as distributed algorithm, in which the CL are elected based upon the local decision. Mhemed et al.[6] developed the clustering protocol by using the fuzzy inference system. FLCP uses the following three parameters namely residual energy level, distance to the BS and distance to the cluster head for the selection of cluster head. Rajeswari et al [7] proposed back–off clustering approach to detect the malicious nodes in MANET . Younis and Fahmy[8] proposed HEED a clustering protocol for WSN in which the residual energy of each of the sensor node act as a major factor for the election of cluster head.

Das et al.[9] proposed a trust computation model called secured trust based routing model (STRM) for enhancing secure routing. In this work, routing process is performed through agents. kim et al[10] developed the cluster head election process in distributed manner. The residual energy and distance between the cluster head and nodes act as metrics for the cluster head election process. A distributed competitive unequal clustering algorithm was proposed by Li et al[11]. The cluster head are selected by local competition. Rajeswari et al [12] developed a fuzzy based secure algorithm for effective routing in MANET. Logambigai and kannan [13] proposed a unequal cluster based routing algorithm for effective routing in wireless sensor networks.

Ganapathy et al[14] a new weighted fuzzy based C-Means clustering algorithm for grouping the nodes in networks dynamically by reorganizing the group members has been developed. Selvi et al[15] proposed a new fuzzy temporal logic for cluster formation and cluster based routing. Anupam Das et al [16] presented a novel trust computation model called Secured Trust for secure routing. Noman Mohammed et al [17] explained the methods for detection of selfish and malicious nodes in wireless environment. Li et al [18] proposed a metric to compute path trust to develop a secure routing algorithm. XueWang et al [19] designed a routing protocol based on trust for optimal routing in WSN. ZhengYan et al [20] proposed an system for trust management for developing a component based system where the trust is calculated dynamically. Rajeswari et al [21-23] proposed various detection mechanisms to detect and mitigate the malicious nodes in MANET.

3. PROPOSED WORK

The primary aim of this proposed work is to enhance the secure communication, improve the energy efficiency and in turn to maximize the lifetime of the nodes in the network. Hence, in this work fuzzy inference system is used for the process of energy efficient and secure clustering. Fuzzy inference system is a soft computing based technique in which the inputs are mapped to the outputs by using the fuzzy set theory. The proposed work consists of two main phases namely set-up and steady state phase. Moreover in the proposed work two parameters namely cluster density and residual energy are considered for the cluster formation process. The proposed work will work in rounds as in case of the traditional leach protocol. The FBEASC work in two phases namely energy efficient and secure cluster leader election process and fuzzy based cluster formation. The following subsection describes about these phases in detail.

3.1 Energy Efficient and Secure Cluster Leader Election Process

In this proposed work, among all the nodes in the network the most energy efficient and trustworthy node will be elected as Cluster Leader (CL). Thus, the cluster leader election process in carried on based upon the measured trust score and behavior analysis. The trust score computation scheme proposed in this work is elaborated in the following subsection.

3.1.1 Trust Score Computation Scheme

The trust levels of nodes are estimated based on the following two criteria. In this work, the entire nodes in the network are classified as two groups. Firstly, nodes which are authentically transmitting their acknowledgement to neighbours whenever they received the packets are treated as first group. Second, the nodes which drop more packets are considered as group two nodes. Now, the initial trust score is computed using the Eq. 1that represents the percentage of genuine acknowledgements.

$$Trust_{level1} = \frac{Numberof\ packets\ Ack}{Numberofpackets\ transmitted} X100 \quad (1)$$

The second trust level is measured based upon the rejected packets by using the Eq.2

$$Trust_{level2} = 100 - \left(\left(\frac{Number\_ofpackets\_rejected\_node}{Total\_number\_of\_packets\_rejetced\_network}\right)\right) * 100 \quad (2)$$

Finally, the overall trust level of the individual node are measured by using Eq. 3.

$$Overall\_Trust\_Level = \frac{Trust_{level1}}{Trust_{level2}} \quad (3)$$

3.1.2 Identifying the malicious nodes from the network

The $Trust_{Threshold}$ is measured based on the mean value of the overall trust score by applying Eq. 4

$$Trust_{Threshold} = \sum_{i=1}^{n} \frac{Overall\_Trust\_Level}{n} \quad (4)$$

The Selection_Score for selection of nodes in the routing process is computed by applying Eq 5.

$$\text{Selection\_Score} = \frac{(W1XOverall\_Trust\_Level + W2XREL)}{(W1+W2)} \quad (5)$$

where REL is the residual energy level

W1+w2=1

Thus, if the measured choice level of the node is less than the $Trust_{Threshold}$ then the node will be identified as the malicious nodes else the node will be identified as trustworthy node and given a chance to act as a cluster leader.

3.2 Fuzzy Based Cluster Formation Process

This Section describes about the fuzzy based cluster formation process. The remaining nodes in the network find and join with the suitable CL by measuring the member choice of each CL by applying the FIS. In this work the member nodes will chose the appropratied CL by using the following two parameters namely energy level of the cluster leader and cluster density. The system diagram of the proposed work is shown in the Figure 1.

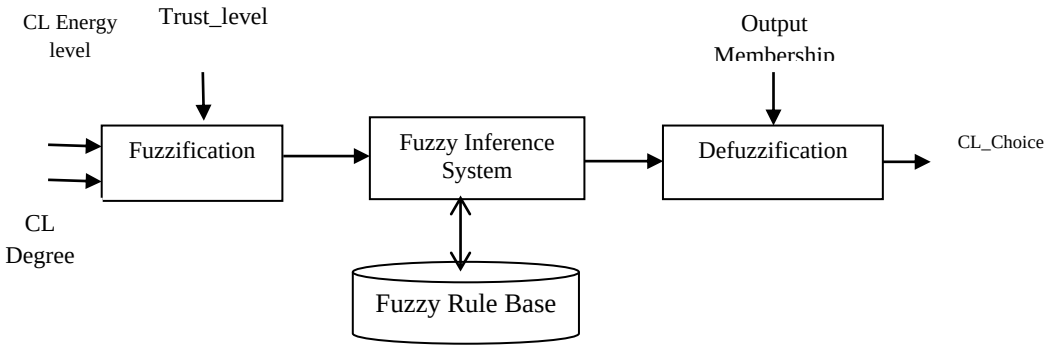

Figure 1. System Architecture

3.2.1 Cluster Leader Degree

The number of member nodes in acluster is defined as a load of cluster or cluster density. Thus, the cluster densityacts as primary metrics for load balancing in a cluster. Cluster Leader degree is measured by using the Eq.(6)

$$Cluster\ Leadrer\_degree = \frac{Number\ of\ nodes\ in\ the\ clusters}{total\ number\ of\ nodes\ in\ the\ network} \quad (6)$$

3.2.2 Energy Model

The energy model used in our work is similar to [5] is given in (7) and (8). The Eelec, εfs and εmp are the electronics energy and the amplifier energy in free space and multipath respectively.

The transmission energy required for an l-bit message over a distance d is as follows:

$$E_T(l,d) = \begin{cases} lE_{elec} + l\varepsilon_{fs}d^2 ford < d_0 \\ lE_{elec} + l\varepsilon_{mp}d^4 ford \geq d_0 \end{cases} \quad (7)$$

The reception energy required for an l-bit message is as follows given in Eq(8).

$$E_R(l) = lE_{elec} \quad (8)$$

3.2.3 Fuzzy Membership Functions

In the FIS, the triangular and trapezoidal membership functions as in [6] used to present input parameters are given in Eq (9) and (10).

$$\mu_{A1}(x) = \begin{cases} 0 & x \leq a1 \\ \frac{x-a1}{b1-a1} & a1 \leq x \leq b1 \\ \frac{c1-x}{c1-b1} & b1 \leq x \leq c1 \\ 0 & c1 \leq x \end{cases} \quad (9)$$

$$\mu_{A1}(x) = \begin{cases} 0, & x \leq a2 \\ \frac{d2-x}{d2-c2}, & c2 \leq x \leq d2 \\ 1, & b2 \leq x \leq c2 \\ \frac{d2-x}{d2-c2}, & c2 \leq x \leq d2 \\ 0, & d2 \leq x \end{cases} \quad (10)$$

3.2.4 Fuzzy Rules

In this work, mamdani Fuzzy inference system is used. 2 input variables and each input has 3 levels are used. Table 1show about the fuzzy input variables.

Table 1. Fuzzy variables and Levels

PARAMETERS	LEVELS
CL energy level	*low, medium and high*
CL degree	*low, medium and high*
Trust_level	*low, medium and high*

So, 3^2=9 possible member choice values are computed using fuzzy if-then rules. For member CL_Choice output variable, 9 levels such as very weak, weak, medium, high medium, strong and very strong. The triangular and trapezoidal functions are used to represent CL_Choicelevels. The fuzzy if-then rules used in our system are listed in Table 2.

Table 2. Fuzzy "If-then" Rules

Set of Fuzzy Rules
*Case 1: If (CL Energy Level is **low**) and (CL Degree is **High**) and (Trust_level is **low**) then (CL_Choice is **weak**)*
*Case 2: If (CL Energy Level is **high**) and (CL Degree is **low**)and (Trust_level is **high**) then (CL_Choice is **strong**).*
*Case 3: If (CL Energy Level is **High**) and (CL Degree is **medium**) and (Trust_level is **high**) then (CL_Choice is **medium**).*

In this work, the mamdani inference system is used and the defuzzification act as final step in the system model. Moreover, Center of Area (COA) method which is given in Eq. (11).

$$COA = \frac{\int \mu_A(x).xdx}{\int \mu_A(x)dx} \quad (11)$$

4. SIMULATION RESULTS

The performances of Fuzzy logic based energy aware secure clustering (FBEASC) is evaluated using Fuzzy Logic Toolbox in MATLAB. The performance of FBEASC is compared with the LEACH and STRM. For experiment, 50-250 sensors are randomly placed in an area of (500 x 500) meter square. Initially, all the nodes are deployed with equal energy of 2 J .Simulation time for each round is 20s. The simulation parameters used for designing FBEASC are given in Table 3.

Table 3. Simulation Parameters

Parameters	Value
Area	500m x 500m
No of Sensor nodes	50-250
Basic routing protocol	LEACH
Initial energy	2 J
E_{elec}	50 nJ/bit
Packet Size	1024 bits
Mobility model	Random way mobility
Mobility Speed	10 m/s to 40 m/s

Figure 2 depict the packet delivery rate analysis. From the figure 2, it is observed that the packet delivery rate of the proposed work is more when compared to the existing work LEACH and STRM. This is due to the fact that the packet drop caused by the malicious nodes is eliminated in the FBEASC by utilizing the novel trust scheme. Hence, this leads to the increase in the packet delivery rate of the FBEASC.

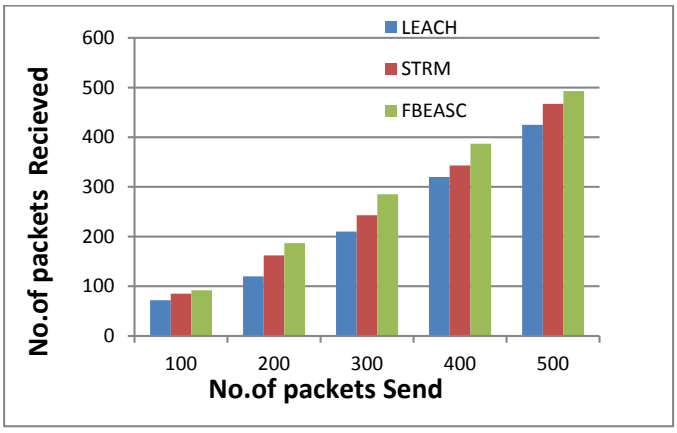

Figure 2. Packet delivery Analysis

Figure 3 shows the energy consumption analysis of the proposed work FBEASC, LEACH and HEED. In the proposed work energy level acts as one of key factor in Cluster Leader choice selection. Moreover, numbers of malicious nodes are identified and removed from the network is more in case of the proposed work when compared to the existing work. Therefore, the energy utilized by the malicious nodes is saved and this leads to decrease in energy consumption by the proposed work FBEASC.

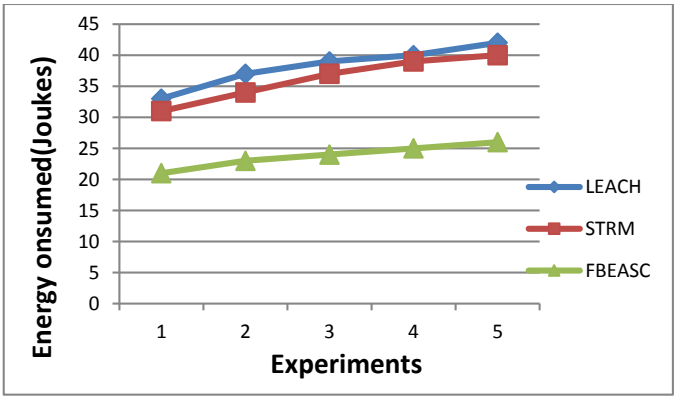

Figure 3. Energy consumption Analysis

Figure 4 shows the detection rate of the proposed work in comparison with STRM. In the proposed work the trust score of nodes are evaluated based upon the energy level and behavior analysis of the nodes with each other. Hence, more number of malicious nodes is detected in FBEASC.

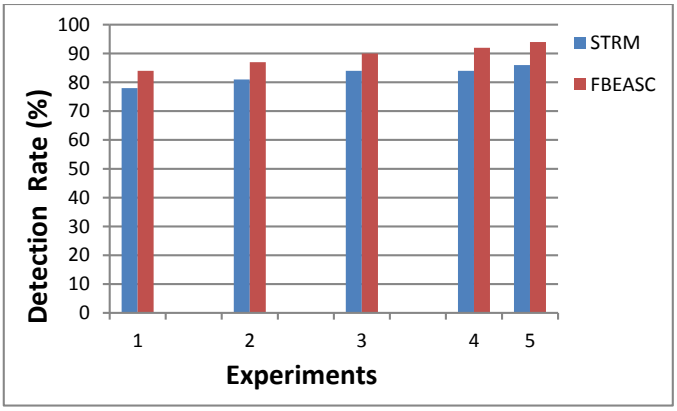

Figure 4. Malicious Node Detection Rate

Table 4 shows the delay analysis comparison of proposed with LEACH and STRM. From table 4, it is observed that the delay in FBEASC is comparatively less when compared to LEACH and STRM. This is due to fact that the delay in transmission caused by the malicious nodes is reduced to larger extent in the proposed work when compared to LEACH, STRM. This is because in the proposed work the energy efficient and trustworthy node alone can act as a cluster leader and through these chosen CL the data are transmitted. Therefore, delay caused by the malicious nodes is reduced in FBEASC.

Table 4. Delay Analysis

Methods	Number of Packets Sent			
	4000	5000	6000	7000
Delayin LEACH(ms)	0.75	1.94	2.8	3.2
Delay in STRM(ms)	0.71	1.85	2.5	2.7
Delay in FBEASC(ms)	0.65	1.20	1.68	1.8

Figure 5 shows the network life time analysis of the proposed work with LEACH and STRM. From the Figure .5 it is observed that the FBEASC performs better that LEACH and STRM. This is because in the proposed work during the process of cluster formation. Energy level of CL and CL degree are considered as parameters. Moreover, based on the cluster leader degree the new member node will join with the CL. This leads to increase in network lifetime of the proposed work when compared to LEACH and STRM

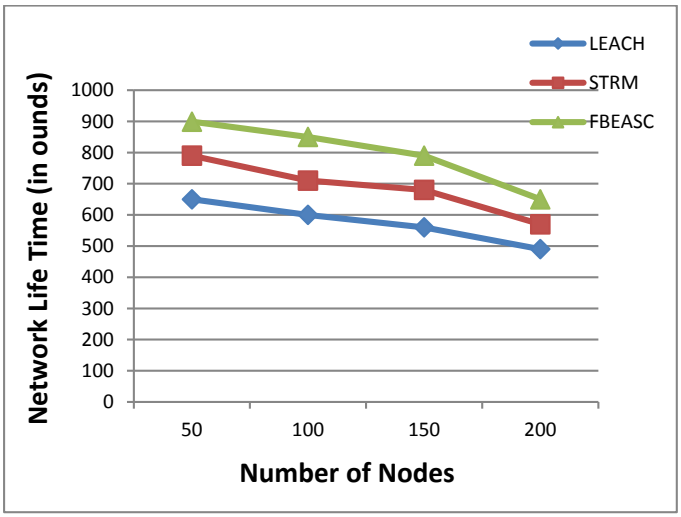

Figure 5. Network Lifetime

5. CONCLUSION

In this work, a new fuzzy based energy aware trust based secure clustering approach is proposed. In this paper a new trust score evaluation scheme is proposed to mitigate the malicious nodes form the network and to elect the trust aware node as CL. Moreover, after the CL is elected, the cluster members will join with the suitable CL by applying the FIS. In this work the four parameters namely cluster density, residual energy level, distance between the node and sink and distance between the node and BS are considered as parameters for the cluster formation. The key advantages of the proposed work is that enhanced security and improved energy efficiency. Form the experiment conducted and the simulation results the proposed work is compared with LEACH and STRM the results shows that the proposed work gives better results in terms of energy consumption and network lifetime. The further work in this direction is to address the security issues by using the cryptographic techniques.

REFERENCES

[1] Yick, J., Mukherjee, B., &Ghosal, D. (2008). Wireless sensor network survey. Computer Networks, 52(12), 2292–2330.

[2] Potdar, V., Sharif, A., & Chang, E. (2009). Wireless sensor networks: A survey. In International conference on advanced information networking and applications workshops, 2009. WAINA'09 (pp. 636–641). IEEE.

[3] Al-Karaki, J. N., & Kamal, A. E. (2004). Routing techniques in wireless sensor networks: A survey.*IEEE Wireless Communications, 11,* 6–28.

[4] Akyildiz, I. F., &Vuran, M. C. (2010). *Wireless sensor networks* (pp. 131–141). Hoboken: Wiley.

[5] Heinzelman, W. R., Chandrakasan, A., Balakrishnan, H. (2000). Energy-efficient communication protocol for wireless micro sensor networks. In *Proceedings of the 33rd annual Hawaii international conference on system sciences, IEEE* (pp. 1–10).

[6] Mhemed, R., Aslam, N., Phillips, W., &Comeau, F. (2012). An energy efficient fuzzy logic cluster formation protocol in wireless sensor networks. *Procedia Computer Science, 10*, 255–262.

[7] Rajeswari, A.R., Kulothungan, K., Ganapathy, S., & Kannan, A. (2016) Malicious Nodes Detection in MANET Using Back-Off Clustering Approach. Circuits and Systems 7 (8), 2070-2079.

[8] Younis, O., &Fahmy, S. (2004). HEED: A hybrid energy-efficient, distributed clustering approach for Ad Hoc sensor Networks. *IEEE Transaction on Mobile Computing, 3,* 366–379.

[9] Das, A., & Islam, M. M. (2012). Secured trust: A dynamic trust computation model for secured communication in multiagent systems. *IEEE Transactions on Dependable and Secure Computing, 9*(2), 261–274.

[10] J. Kim, S. Park, Y. Han, T. Chung, CHEF: cluster head election mechanism using fuzzy logic in wireless sensor networks, in: Proceedings of the ICACT, 2008, 654– 659.

[11] C. Li, M. Ye, G. Chen, J. Wu, An energy-efficient unequal clustering mechanism for wireless sensor networks, in: IEEE International Conference on Mobile Ad Hoc and Sensor Systems Conference, 2005, p. 8.

[12] Rajeswari, A.R., Kulothungan, K., Ganapathy, S., & Kannan, A. (2019). Trust Aware Svm Based Ids For Mitigating The Malicious Nodes In Manet .International Journal of Innovative Technology and Exploring Engineering .8(8) .185- 197.

[13] Logambigai, R., &Kannan, A. (2016). Fuzzy logic based unequal clustering for wireless sensor

networks. *Wireless Networks, 22,* 945–957.

[14] Ganapathy, Kulothungan, Yogesh, Kannan, " A Novel Weighted Fuzzy C-Means Clustering Based on Immune Genetic Algorithm for Intrusion Detection", Proceeding Engineering, Elsevier, vol. 38, pp. 1750-1757, 2012.

[15] Selvi, M., &Nandhini, C., Thangaramya, K., Kulothungan, K., &Kannan, A. (2016). HBO based clustering and energy optimized routing algorithm for WSN. In *Proceedings of the eighth international conference on advanced computing (ICoAC)* (pp. 89–92).

[16] Das, A., & Islam, M. M. (2012). Secured trust: A dynamic trust computation model for secured communication in multiagent systems. *IEEE Transactions on Dependable and Secure Computing, 9*(2), 261–274.

[17] Mohammed, N., Otrok, H., Wang, L., Debbabi, M., & Bhattacharya, P. (2011). Mechanism designbased secure leader election model for intrusion detection in MANET. *IEEE Transactions on Dependable and Secure Computing, 8*(1), 89–103.

[18] Li, F., & Wu, J. (2010). Uncertainty modeling and reduction in MANETs. *IEEE Transactions on Mobile Computing, 9*(7), 1035–1049.

[19] Wang, X., Ding, L., & Wang, S. (2011). Trust evaluation sensing for wireless sensor networks. *IEEE Transactions on Instrumentation and Measurement, 60*(6), 2088–2095.

[20] Yan, Z., &Prehofer, C. (2011). Autonomic trust management for a component-based software system. *IEEE Transactions on Dependable and Secure Computing, 8*(6), 810–823.

[21] Rajeswari, A.R., Kulothungan, K., Ganapathy, S., & Kannan, A. (2019). Trust Aware Svm Based Ids For Mitigating The Malicious Nodes In Manet .International Journal of Innovative Technology and Exploring Engineering .8(8) .185- 197.

[22] Rajeswari, A.R., Kulothungan, K., & Kannan, A. (2016) .GNB-AODV: Guard Node Based –AODV to Mitigate Black Hole Attack in MANET International Journal of Scientific Research in Science, Engineering and Technology 2(6) . 671-677

[23] Rajeswari, A.R., Kulothungan, K., Ganapathy, S., & Kannan, A. (2017) . Performance Analysis of Malicious Nodes Detection System in Manet Using Anfis Classifier International Journal for Research in Applied Science & Engineering Technology 5(1) .14-21