iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** I **Month of publication:** January 2017

DOI: http://doi.org/10.22214/ijraset.2017.1003

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Performance Analysis of Malicious Nodes Detection System in Manet Using Anfis Classifier

Rajeswari A. R[1], Kulothungan K[2], Ganapathy S[3], Kannan A[4]
[1,2,4]*Department of Information Science & Technology, College of Engineering , Gunidy , Anna University, Chennai. India -600025*
[4]*School of Computing Science and Engineering, VIT University-Chennai Campus, Chennai-127*

Abstract: Mobile adhoc networks (MANET) are infrastructure less networks which provide multi-hop wireless links between nodes. The main applications of MANET in real time environment are military and emergency areas where the fixed infrastructure is not required. The security is the primary concern in nodes of the MANET. Clustering and recommendation trust model based malicious node detection using classifier is proposed in this paper to increase the malicious node detection rate.The distance between node and Cluster headof an each cluster is determined by node to node center in conventional methods where as, the distance is computed by center of the sensing area of the node and Cluster head. Trust model is developed in this paper based on recommendation technique by whichthe total trust value of each node is computed from trust values of direct and indirect methods. The trust values of the normal nodea and malicious nodes are trained by Adaptive neuro fuzzy inference classifier in training mode and the nodes behaviour is tested using the test mode of the classifier and the classification results are presented. The performance of the proposed system is analyzed interms of throughput, detection rate, packet delivery ratio, average latency and energy consumption.

I. INTRODUCTION

The idea of implementation of mobile wireless devices working collectively was proposed in the 1990s, when significant amount of research activities were carried out on mobile ad hoc networks (MANETs). The Mobile Ad hoc Networks Working Group [1] was created in 1997, with the aim of standardizing routing protocols for MANETs. Two standard specifications for track routing protocol were developed by this group, namely the reactive and proactive MANET protocols. Each node in a MANET is a computer acting as both a host and a router; also having the job of forwarding the packets between two nodes which are not in direct communication with one another. Each MANET node requires a much smaller frequency spectrum that a node requires in an affixed infrastructure network [1].

A MANET is an autonomous collection of mobile user nodes communicating over wireless links, with a relative bandwidth constraint. Since the nodes are mobile, the network topology is more probable to unpredictable changes over time. A MANET is usually decentralized, i.e. all network activities including topology determination and message delivery, should be executed by the individual nodes themselves. Therefore, the routing functionality gets incorporated into the mobile nodes.

Mobile ad hoc network got outstanding success as well as tremendous attention due to certain characteristics such as self-maintenance and self-configuration. At early stages, researchers focused mostly on its user-friendly and mutual environment, however many different problems came into being; security is one of the major issues since providing secure communication between different nodes in a mobile ad hoc network environment became difficult. Finally, MANETs can be considered as an infrastructure less, multi-hop network with most importantly its self-organizing property [2].

Due to its wireless and distributed environment, the system security becomes a challenging task for the designers. In the last few years, security problems in MANETs have attracted much attention, thereby making the researchers to focus on specific security areas, like intrusion detection and response, establishment of trust infrastructure and securing routing protocols.

Intrusion detection (ID) in MANETs is more complex and challenging than in fixed networks, because of the difficulty in collecting the audit data from the network, and applying ID techniques in detecting intrusions at a low rate of false positives and an effective response to intrusion. Certain features of MANETs create implementation and operational complexities, and such additional challenges for ID schemes in MANETs are as follows:

Lack of concentration points during audit data collection and monitoring.

The routing protocols in MANET necessitate cooperation of nodes to act as routers, thereby creating opportunity for attacks.

Dynamic and unpredictable network topology due to mobility of nodes, making the process of intrusion detection complicated.

Complex ID schemes due to the limited computational ability of most of the nodes.

Section 2 states the related works and discusses the conventional algorithms in detail. Section 3 proposes the clustering back-off duration algorithm for the detection of malicious nodes in the network, during cluster formation and Section 4 shows the results and their discussion in detail. Finally, Section 5 depicts conclusion.

II. LITERATURE SURVEY

Tselikis et al. [1] developed degree-based clustering algorithm for the nodes in MANET. This method was attack-resistant without imposing significant overhead to the clustering performance. The authors extended this clustering method with a cooperative consistent algorithm which integrated security into the clustering decision achieving attacker identification and classification.

Sandip Chakraborty et al. [2] an algorithm for addressing the problem caused by the hidden and exposed nodes wireless networks. The authors achieved 28.50 mJ of energy consumption and 88.02% average packet delivery ratio to detect the hidden and exposed nodes in MANET environment.

Jian-Ming Chang et al. [3] proposed a cooperative bait detection algorithm to detect the malicious nodes in MANET by preventing collaborative attacks. The authors attempted to resolve this issue by designing a dynamic source routing (DSR)-based routing mechanism, which is referred to as the cooperative bait detection scheme (CBDS), that integrates the advantages of both proactive and reactive defense architectures.

Xia et al. [4] developed a trust based routing algorithm for nodes in MANET using trust prediction model. Fuzzy logic rules were constructed to develop the prediction model for trust estimation of the node. The security of the information exchange was analyzed using this prediction model and this algorithm was also used to detect the malicious nodes. Li et al. Proposed a trust model based on the behaviour of nodes. They have evaluated the trust as a weighted sum of forwarding ratio and the path trust is estimated in terms of product of the node trust. The main advantages with their model were flexibility and feasibility in selecting the trustworthy shortest path from the source to the destination. Denko et al (6) developed a trust management scheme for pervasive computing environments. By using they model it is possible to mitigate the malicious device by employing the effective and trustworthy recommendation from the neighbour devices in the network.

Renyong Wu et al. [7] proposed a anamaly node detection in networks using trust based authentication algorithm.The anamaly nodes were detectd based on fuzzy theory and revised evidence theory. By monitoring the behaviors of the evaluated nodes with multidimensional characteristics and integrating these pieces of information, the malicious nodes in a network can be identified and the normal operation of the whole network can be verified.Syed Syed Muhammad Sajjada et al. [8] proposed intrusion detection model based on neighbor node trust estimation process to detect the malicious nodes from the network. Each node will estimate the trust value of it neighbouring nodes by using both the direct and indirect trust estimation. Depending upon the measured trust value the nodes can be classified either as trustworthy or malicious node. Moreover the trustworthy nodes are updated the forwarding engine for the packet forwarding activity. The main advantages of their model is to detect the hello flood attack, jamming attack and selective forwarding attack by analyzing the malicious activity of the nodes and the network statistics.

III. PROPOSED METHODOLOGIES

A. *Clustering Nodes In Manet*

The nodes in the MANET are grouped into cluster which reduces the energy consumption to improve the performance of the MANET environment. MANET may have number of clusters based on the density of the nodes in network and each cluster has cluster head (CH) to control the behaviour of the nodes belonging to their sensing area. The following procedure is adopted for clustering the nodes.

Step 1: The length (L) and width (W) of the MANET environment is determined and the center point of the network is located at (L/2, W/2). Divide the entire network into four quadrant regions based on this center point.Each quadrant is named as cluster. At this stage, we have four clusters. The nodes may be placed over the boundary of the separation quadrant as shown in Figure 1.

Step 2: Select any node in each cluster at random manner and assumed as CH.

Step 3: The newly selected CH sends the cluster_join_request signal to all the nodes within this cluster area as shown in Fig.3. The nodes at boundary may receive the cluster_join_request signal from both CH as shown in Fig.3 and it will compute the signal strength of the request receiving from both CH, using the following Equation.

Volume 5 Issue I, January 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

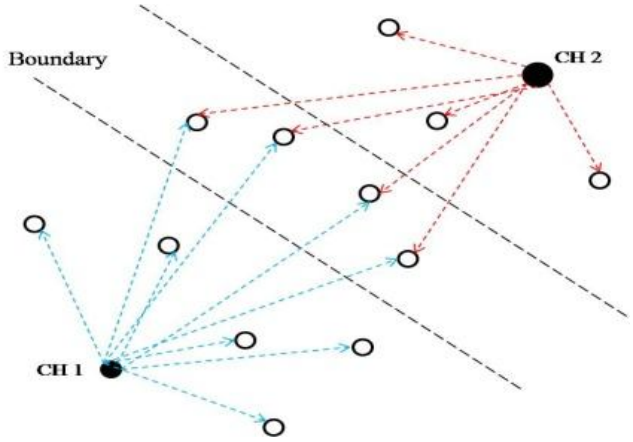


Figure 1 Configuration of nodes at boundary

Step 4: The node at boundary take CH-joining-decision based on the signal strength and joined to the corresponding CH as shown in Figure 2.
Step 5: Each CH updates the node details in their corresponding CH table.

B. Determination of distance (d) from each node to CH

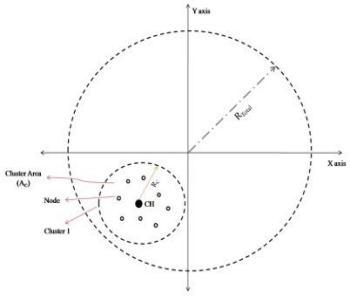


Figure 2 MANET Architecture

The appropriate distance between each cluster member to CH is computed using Equation 1, by considering that CH is located at the center of the cluster.

$$d_i = \iint \sqrt{(x_i - x_c)^2 + (y_i - y_c)^2}.\rho(x_i.y_i)dx.dy \quad (1)$$

Where, (x_i,y_i) represents the coordinates of cluster member within the cluster and (x_c,y_c) represents the coordinates of the CH, which is considered as x_c = 0 and y_c =0, at initial condition.

$$d_i = \iint \sqrt{x_i^2 + y_i^2}.\rho(x_i.y_i)dx.dy \quad (2)$$

The Cartesian coordinate system is now converted to polar coordinate system and by substitute $r = \sqrt{x_i^2 + y_i^2}$ in Equation (2), we get,

$$d_i = \iint r.\ \rho(r,\theta).r.dr.d\theta \quad (3)$$

$$d_i = \rho(r,\theta) \iint r^2.dr.d\theta \quad (4)$$

Let 'n' be the number of clusters in MANET and 'R_c' be the radius of each cluster. Let 'A_c' be the cluster Area 'R_{Total}' be the total area of the network and 'ρ' be the densiti of nodes in the cluster. The cluster radius is computed as,

$$R_c = \frac{R_{Total}}{\sqrt{n}} \quad (5)$$

$$d_i = \rho \int_0^{2\pi} \int_0^{\frac{R_{Total}}{\sqrt{n}}} r^2 .\, dr .\, d\theta \quad (6)$$

$$= \rho \int_0^{2\pi} \left(\frac{r^3}{3}\right)_0^{\frac{R_{Total}}{\sqrt{n}}} d\theta \quad (7)$$

$$d_i = \frac{2\pi\rho R_{Total}^3}{3\pi\sqrt{n}} \quad (8)$$

The distance between centers of sensing area of the node to CH is determined as,

$$d_{center} = \frac{d_i}{r_{node}} \quad (9)$$

$$d_{center} = \frac{2\pi\rho R_{Total}^3}{3 r_{node} n\sqrt{n}} \quad (10)$$

Where, 'r_{node}' is the radius of the sensing area of each node.

C. Trust Model

The trust model is used to compute the trust of each node in each cluster of the MANET.In this paper, the following trust model is used to estimate the trust of the node in MANET and they are categorized into Recommendation based trust model and Overhearing based trust model.

In this paper, the recommendation based trust model is used to estimate the trust value of the nodes in MANET environment. It is based on the total trust of each node in cluster and it is categorized into direct trust and indirect trust deterimination. They can be determined using positive observation rate (α) and negative observation rate (β). The number of forwarded packets by a node is represented by positive observation rate and the number of dropped packets by a node is represented by negative observation rate.

The direct trust value T_d (i,j) of a node I (CH) about node j(node 2) is computed using the following equation as,

$$Td\,(i,j) = \frac{\alpha(i,j)}{\alpha(i,j)+\beta(i,j)} \quad (11)$$

At time t=0, $\alpha\,(i,j)$=1 and $\beta(i,j)$=0. Therefore, the total trust value of a node is 1, which indicates high trust value. If node j is an falsy node, then $\alpha\,(i,j)$=1 and $\beta(i,j)$=1, which implies the total trust value of a node is 0.5. This indicates low trust value of node j by node i.

The indirect trust value T_{in} (i,j) of node I (node 1) about node j (node 2) is computed using the following equation as,

$$Tin\,(i,j) = \frac{\alpha(i,j)}{\alpha(i,j)+\beta(i,j)} \quad (12)$$

Let T_{di} (i, j) and T_{in} (i, j) be the direct and indirect trust value of node 2, respectively. The total trust value of node 2 is the based on the direct and indirect trust values and it is given by,

$$T_t = w_{di}\,(i,j) * T_{di}\,(i,j) + w_{in}\,(i,j) * T_{in}\,(i,j) \quad (13)$$

Total trust value of each node in cluster is the addition of direct trust value of that particular node and the indirect trust value of that particular node by other node.

$$wdi\,(i,j) = \begin{cases} b_{N2} \times |y_{d2} - y| + b_{max}, & x_{d2} - x < 0 \\ b_{N2}, & else \end{cases} \quad (14)$$

$$win\,(i,j) = \begin{cases} b_{N1} \times (y_{d2} - y) + b_{max}, & y_{d2} - y > 0 \\ b_{N1}, & else \end{cases} \quad (15)$$

Where, b_{N1} and b_{N2} represents the bandwidth of the node 1 and node 2, respectively.(x_{d2}, y_{d2}) represents the coordinates the node 2 and (x,y) represents the coordinates the node 1. The maximum bandwidth of the node is noted as b_{max}.

Table 1 Trust computation

Nodes	Direct trust value	Indirect trust value	Total trust value
1	0.32	0.45	0.77
2	0.13	0.25	0.38
3	0.25	0.65	0.90
4	0.56	0.32	0.88
5	0.37	0.27	0.64
6	0.27	0.38	0.65
7	0.38	0.32	0.70
8	0.37	0.29	0.66
9	0.32	0.21	0.53
10	0.31	0.26	0.57

Table 1 shows the estimated trust values of the nodes in MANET environment. The trust value of a particular node is computed by adding the trust values of direct and indirect methods. The total trust value of 10 nodes in MANET is given in Table 1.The node with lowest trust value is noted as malicious node and it is blacklisted in cluster table of CH.

D. Classification of nodes behaviour

A multi layer Adaptive Neuro Fuzzy Inference System (ANFIS) classifier is used in this paper to classify the behaviour of the node. This classifier differentiates the behaviour of the normal node from malicious node. It consists of an input layer, three hidden layers and an output layer, is used in this paper for classification of nodes behaviour in MANET. The input layer of the ANFIS classifier is constructed with number of neurons which is equal to the size of the extracted trust values of normal nodes and malicious nodes. The hidden layer with different number of neurons is tested and finally 4 hidden layers are configured for obtaining the optimal classification rate. In this paper, 4 hidden layers and each hidden layer with 20 neurons are configured. The output layer consist a single neuron and thus produces a single binary output 0 (Normal node) or 1 (Malicious node).

The ANFIS classifier is operated into two modes as training and testing mode. In training mode of the classifier, the features (trust values) of the normal nodes and malicious nodes are trained by the classifier which generated trained pattern. In testing mode of the classifier, trust values of each node are tested with trained pattern of this classifier.

IV. RESULTS AND DISCUSSION

The performance of the proposed malicious node detection system is analyzed using Network simulator-2 (version 2.34) under open source operating system environment. The carrien sense multiple access protocol is configured to transmit and receive the packets between nodes in MANET. The area of the simulated system is 1000 m (width) and 1000 m (height). The distance between two nodes in simulated area is set 250 m at an initial stage. The nodes in this environment are dynamic which indiactes the location of the nodes are not fixed at a particular point over a two way propagation radio channel. The initial simulation parameters are illustrated in Table 2.

Table 2 Network simulation parameters

Parameter	Initial value
Number of nodes	100,200,300
Network Area	1000m*1000m
Packet size	512 bytes
Routing protocol	DSR(Dynamic Source Routing)
Energy	1000 J
Data rate	1 Mbps
Pause time	10 s
Mobility type	Random model
MAC	802.11
Trust threshold(antesar et al.,)	0.4
Simulation time	700 s

The proposed clustering based malicious nodes detection in MANET achieves higher performance in terms of the following performance evaluation parameters [10].

A. Throughput

It is defined as the total number of packets correctly delivered by the intermediate nodes in MANET over a particular period of time. The throughput of any node in MANET is given in Equation (16),

$$Throughput = \frac{number\ of\ packets\ correctly\ transmitted}{Time\ taken\ by\ a\ node} \times 100\ \% \quad (16)$$

The throughput should be high for a best malicious nodes detection system of MANET. The unit of the throughput is bits/second.

Table 3.Performance Analysis of proposed methodology in terms of Throughput.

Methodology	Throughput (Mb/s)						
	Number of malicious nodes (%) in MANET						
	10	20	30	40	50	60	Average
Proposed work	18.2	17.6	15.9	14.76	12.01	11.2	14.94
Fatima Zohra et al. [4]	16.3	16.1	14.67	13.65	11.92	9.63	13.71
Murad Abusubaih [6]	15.9	15.7	13.28	12.97	10.36	8.79	12.83
Jian-Ming Chang et al.[8]	16.1	15.9	12.75	11.65	10.24	6.73	12.22
Sandip Chakraborty et al. [9]	17.2	16.9	11.65	10.26	9.84	5.75	11.93

B. Detection rate

It is defined as the total number malicious nodes correctly identified by the proposed algorithm in MANET over a particular period of time. The detection rate of any node in MANET is given in Equation (17),

$$Detection\ rate = \frac{number\ of\ malicious\ nodes\ correctly\ identified}{Total\ number\ of\ malicious\ nodes\ in\ network} \times 100\ \% \quad (17)$$

The detection rate hould be high for a best malicious nodes detection system of MANET.

Table 4. Performance Analysis of proposed methodology in terms of Packet delivery ratio.

Methodology	Detection rate(%)						
	Number of malicious nodes (%) in MANET						
	10	20	30	40	50	60	Average
Proposed work	92	89	85	82	79	71	83
Fatima Zohra et al. [4]	89	86	82	79	72	67	79.16
Murad Abusubaih [6]	87	85	78	76	69	61	76
Jian-Ming Chang et al.[8]	85	78	69	71	61	58	70.33
Sandip Chakraborty et al. [9]	75	73	64	62	59	53	64.33

C. Packet Delivery Ratio (PDR)

It determines the percentage of packets correctly received at the destination node and it is defined as the ratio between the number of packets correctly received at the destination node and the total number of packets transmitted from the source node.

Volume 5 Issue I, January 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

$$PDR = \frac{number\ of\ packets\ correctly\ received}{total\ number\ of\ packets\ transmitted\ from\ the\ source\ node} \times 100\ \% \quad (18)$$

The value of PDR lies between 0 and 100. Higher PDR indicates the performance of the MANET is high. In our experiment, number of malicious nodes are randomly generated and distributed among the nodes in MANET. The performance of the proposed system is analyzed in terms of PDR against number of malicious nodes and PDR values for different number of malicious nodes is stated in Table 2. The proposed method achieves 89.35% of PDR while the conventional methods Fatima Zohra et al. [8], Murad Abusubaih [9], Jian-Ming Chang et al. [10] and Sandip Chakraborty et al. [11] achieved PDR are 84.36%, 86.50%, 87.92% and 88.02%, respectively.

Table 5. Performance Analysis of proposed methodology in terms of Packet delivery ratio

Methodology	Packet delivery ratio (%)						
	Number of malicious nodes (%) in MANET						
	10	20	30	40	50	60	Average
Proposed work	94.27	93.99	92.10	89.37	88.26	79.37	89.56
Fatima Zohra et al. [4]	92.18	88.97	86.18	84.1	82.87	71.9	84.36
Murad Abusubaih [6]	93.89	92.10	89.87	85.79	83.18	74.19	86.50
Jian-Ming Chang et al.[8]	94.17	93.19	91.10	88.76	85.15	75.15	87.92
Sandip Chakraborty et al. [9]	95.65	93.17	91.0	87.19	85.5	75.64	88.02

In some methodologies [9, 10-11], PDR values are slightly higher than the proposed method at the case of 60% malicious nodes. However, the proposed method in this paper achieves higher average PDR than the conventional methods due to its robust and stability of the algorithm.

D. Latency

It is defined as the total time taken to deliver the packet from source node to destination node in MANET environment. The latency is affected by malicious nodes due to the wastage of transmission through these nodes. It is estimated in milliseconds (ms). Lower latency indicates the performance of the MANET is high. The performance of the proposed system is analyzed in terms of latency against number of malicious nodes and latency values for different number of malicious nodes is stated in Table 3. The proposed method achieves 36.2 ms latency while the conventional methods Fatima Zohra et al. [8] , Murad Abusubaih [9], Jian-Ming Chang et al. [10] and Sandip Chakraborty et al. [11] achieved latency are 37.47 ms, 36.98 ms, 37.49 ms and 37.40 ms, respectively.

Table 6. Performance Analysis of proposed methodology in terms of Latency.

Methodology	Latency (ms)						
	Number of malicious nodes (%) in MANET						
	10	20	30	40	50	60	Average
Proposed work	22.16	31.76	32.17	33.52	40.16	42.15	33.65
Fatima Zohra et al. [4]	29.75	33.90	35.17	38.67	42.19	45.15	37.47
Murad Abusubaih [6]	29.62	32.87	34.14	37.16	41.99	46.13	36.98
Jian-Ming Chang et al. [8]	28.19	33.78	35.67	38.38	42.98	45.96	37.49
Sandip Chakraborty et al. [9]	28.97	33.10	35.1	37.98	42.19	47.10	37.40

Table 7.Performance Analysis of proposed methodology in terms of Energy Consumption.

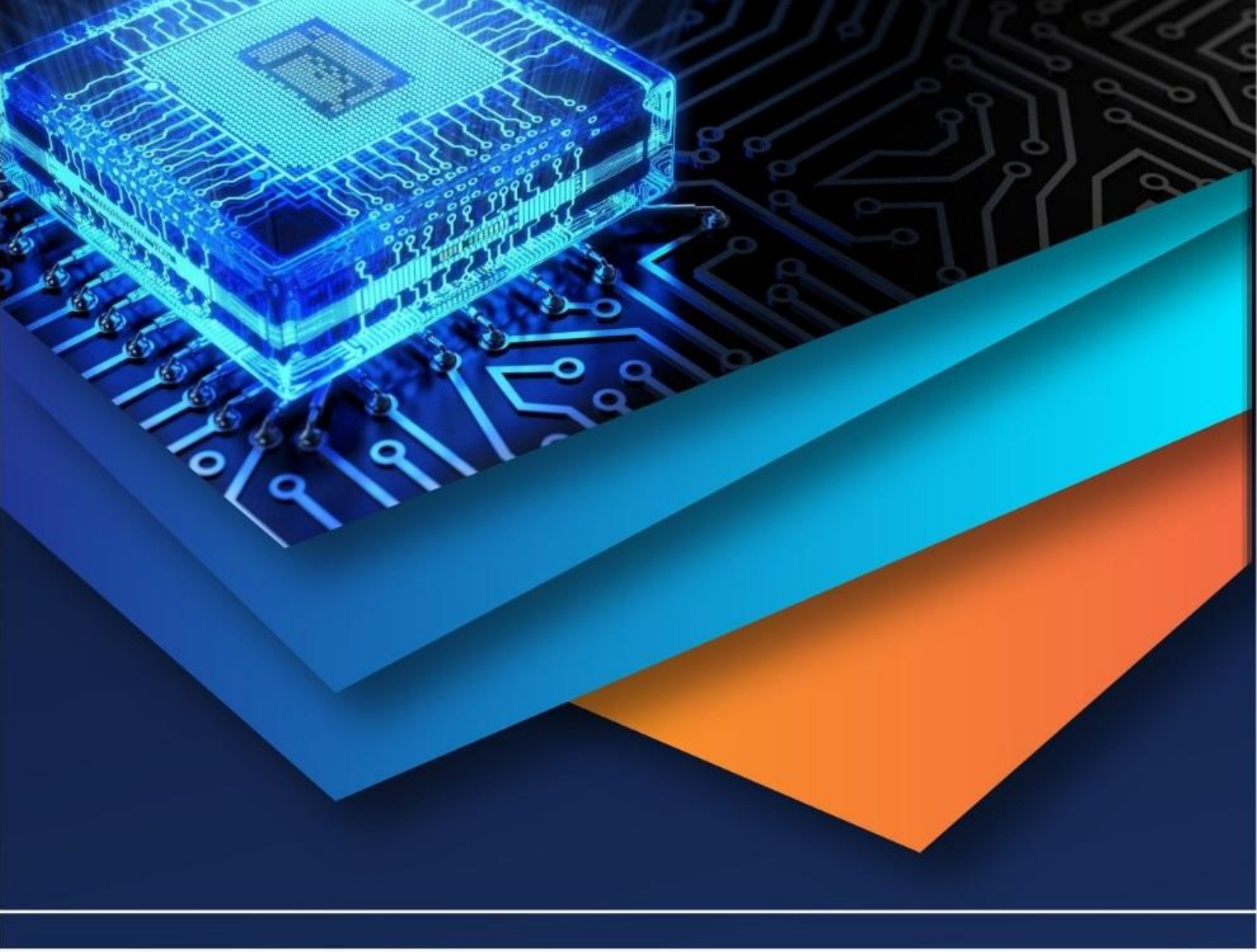
Methodology	Energy Consumption (mJ)						
	Number of malicious nodes (%) in MANET						
	10	20	30	40	50	60	Average
Proposed work	15	25	41	72	85	121	59.83
Fatima Zohra et al. [4]	45	29	47	79	89	145	72.83
Murad Abusubaih [6]	42	39	56	82	93	165	79.5
Jian-Ming Chang et al. [8]	37	34	52	85	92	154	75.66
Sandip Chakraborty et al. [9]	32	29	53	81	91	143	71.5

V. CONCLUSION

In this paper, a new efficient mechanism for the detection of malicious nodes in MANET is proposed. The nodes in MANET environment are grouped as cluster. The malicious nodes are detected in this paper using ANFIS classifier. The trust values are extracted from both normal and malicious nodes and these values are trained by training mode of the classfier.Further, the behaviour of each node in MANET is tested by testing mode of the classfier. The ANFIS classfier increases the malicious node detection rate and reduces the energy consumption. The proposed method achieves 89.56% of packet delivery ratio, 33.65ms latency and 59.83mJ of energy consumption.

REFERENCES

[1] Tselikis, C., Mitropoulos, S., Komninos, N., and Douligeris, C. (2012) Degree-Based Clustering Algorithms for Wireless Ad Hoc Networks Under Attack. IEEE Communications Letters, 16(5).
[2] Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai. (2015) Defending Against Collaborative Attacks by Malicious Nodes in MANETs: Cooperative Bait Detection Approach. IEEE Systems Journal, 9(1).
[3] Sandip Chakraborty, Sukumar Nandi and Subhrendu Chattopadhyay. (2016) Alleviating Hidden and Exposed Nodes in High-Throughput Wireless Mesh Networks. IEEE Transactions on Wireless Communications, 15(2).
[4] H. Xia, Zhiping Jia, Xin Li, Lei Ju, Edwin H.-M. Sha,"Trust prediction and trust-based source routing in mobile ad hoc networks, Ad Hoc Netw. (2012).
[5] X. Li, Z. Jia, P. Zhang, R. Zhang, H. Wang, Trust-based on-demand multi path routing in mobile ad hoc networks', IET Special Issue on Multi-Agent & Distributed Information Security 4 (4) (2010) 212– 223.
[6] Mieso K. Denko, Tao Sun, Isaac Woungang," Trust management in ubiquitous computing: A Bayesian approach", Computer Communications 34 (2011) 398–406.
[7] Renyong Wu, Xue Deng, Rongxing Lu, and Xuemin (Sherman) Shen, "Trust-Based Anomaly Detection in Emerging Sensor Networks," International Journal of Distributed Sensor Networks, vol. 2015, Article ID 363569, 14 pages, 2015.
[8] Syed Muhammad Sajjada, Safdar Hussain Boukb, Muhammad Yousaf, "Neighbor Node Trust Based Intrusion Detection System for WSN", Procedia Computer Science 63 (2015) 183 – 188.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY