Assessing Node Trustworthiness through Adaptive Trust Threshold for Secure Routing in Mobile Ad Hoc Networks

M Venkata Krishna Reddy[1]
Research Scholar, Dept. of CSE
Jawaharlal Nehru Technological University
Hyderabad
Asst. Professor
Dept. of CSE
Chaitanya Bharathi Institute of Technology (A)
Hyderabad, Telangana, India

Dr. P.V.S. Srinivas[2]
Professor, Dept. of CSE, Vignana Bharathi Institute of
Technology (A), Hyderabad, Telangana, India

Dr. M.Chandra Mohan[3]
Professor, Dept. of CSE, Jawaharlal Nehru Technological
University, Hyderabad, Telangana, India

***Abstract*—In the field of communication, Mobile Ad-hoc networks (MANET) have become popular and widely used. However, there are many security challenges in communication through these networks due to the presence of malicious nodes. The aim of this article is to present a novel adaptive threshold trust based approach for isolating malicious nodes to establish secure routing between source and destination. Many existing cryptography methods are complex and do not properly address the elimination of malicious nodes. Several trust-dependent mechanisms have been proposed that supplement old traditional cryptography- related security schemes. But it is observed that most of these trust based approaches are using direct trust and comparing with static trust threshold. This article proposes a novel method, secured trust with adaptive threshold (STAT) that uses the Adaptive threshold technique (APTT) combined along with secure trust based approach (STBA) to evaluate the node trustworthiness for efficient routing. Secure trust for a node is calculated based upon three tier observations that includes direct, neighbor, self-historical to enrich the trust factor and adaptive trust threshold is determined based upon network parameters dynamically. Node's secure trust is compared with adaptive trust threshold computed to isolate the malicious nodes from routing. The proposed method is compared with two cases where routing is performed without any trust calculation and routing with trust calculation and compared with static trust threshold approach. Results show significant performance of the proposed work in terms of metrics like packet delivery ratio, delay, throughput, false positive detection ratio and packet drop ratio. The proposed method STAT effectively isolates the malicious nodes and establishes secure routing.**

Keywords—Node trustworthiness; misbehaving nodes; secure trust; static threshold; adaptive threshold; secure routing

I. Introduction

MANET's are considered to be connected on an infrastructure that provides better linkage between the nodes and its environment [1]. These networks are considered as a part of many applications today [2]. However, though its wide application in many fields, MANET's are vulnerable to many attacks and especially due to its dynamic network topology. These attacks can be overcome using many schemes which are related to the identifying the malicious nodes. These schemes work on the principle that the trust values of the nodes are to be calculated. Later these trust value calculations are compared to the static threshold values known as trust threshold in order to make appropriate routing decision by isolating the malicious nodes. This threshold defines the tolerability of a node in a network [3]. The security challenges of MANET's are identified in the case of their scalability, resource utilization, dynamic topology, and even power consumption and usage. Other challenges are related to the secure environments of the networks [4].

Many trust based schemes proposed have actually made use of static thresholds to identify trust of the node [5]. This type of methods are prone to drawbacks like high error rates. These error rates will influence the timeframe of dropping malicious nodes from routing. Nodes due to environment glitches may drop the packets in some cases. They may also be categorized as malicious nodes due to static threshold strategy which is taken without any consideration of network behavior. Network behavior plays important role in MANET's due to its infrastructure less hierarchy. Existing trust based mechanisms are based upon the two tier observations either direct or combination of direct and indirect trust computations. All these trust based approaches are comparing the evolved trust with static threshold for identifying malicious nodes. As MANET's are dynamic in nature, there is always a need to compute adaptive trust threshold based on network parameters that change dynamically time to time for every node. Every node should have its trust threshold factor computed dynamically. Node's trust value should be compared with adaptive trust threshold to decide its trustworthiness. It is observed form the limitations of the existing methods, there is need of computing node's trust factor with more sophisticated approach and calculation of node's trust threshold using network parameters in adaptive mode.

The proposed work deals with the isolation of malicious nodes. Secure trust computation scheme is used to compute nodes trust value and it is combined with adaptive trust threshold technique (STAT). The work emphasis on adaptive trust threshold technique (APTT) instead of using static trust threshold, where first one is employed here along with sound research on the background on MANET and its challenges in the real-time applications. The study is proposed with a model which aims to design the threshold (adaptive in nature) of each and every node in the network to match the topology of the network. The research is also furnished with enough and appropriate mathematical model and formulas to introduce the Adaptive trust and proposed scheme. Satisfactory results are obtained such that it can be tested by implementing any routing protocol of choice.

Towards the end, the goal of this work is to address the challenge of adaptive trust threshold computation and combining it with three tier observations for generating secure trust in order to establish secure routing.

This article is organized with Introduction to the security challenges in MANET’s in Section I. Background research on MANETs and related work is presented in Section II, after that the proposed model is implemented in Section III along with simulation results in Section IV. The conclusions and future directions are given in Section V.

II. Related Work

It is found from many researches usually in their proposed trust schemes fixing a threshold value which ranges between 1 and 0 to decide the fact that the node must be given access to process towards the routing phase or not [6].

Authors in [7] proposed trust computation based on user and self evidences. They evaluated the trust between the range 1 and 0. In [8], direct observations based on probability assignment between two nodes are proposed which also uses the scale of 0 and 1 for trust evaluation. Probability centric model is used for the evaluation of trust in [9] that considers the trust within the values 0-1 and uses static trust threshold concept. A scheme is presented to append the nodes trust values of nodes, according to their behaviors in [10]. A method based on reputation using the concept of polling is proposed in [11]. A local voting trust establishment strategy based on discrete scale for mobile adhoc networks is proposed in [12]. All these approaches are considering the static trust threshold commonly for all the nodes to isolate malicious nodes from routing.

This work finds its grounds on the fact that MANET’s are known for their Dynamic Topology where a fixed calculation and pre-defined trust value doesn’t make sense [13]. Mobility is also dependent on the behavior of the network. The evaluation of the mobility is seen in many researches which show that it can be considered as a part of the proposed model [14]. Node failures associated with the link also imposes as a threat in real-time scenarios [15]. Hence, all the time considering the static trust seems ignoring the problems that arise due to MANET behavior. This forces that an adaptive nature is to be employed.

Nodes in MANET’s will move randomly time to time that leads to the raise of Node degree, a network factor. Every node in the network is linked to the fact that it is going to change for every second that can be interpreted as Rate of Link change. Average trustworthiness of the nodes in 1-hop distance is considered to compute the Adaptive threshold [16]. These are the metrics usually considered for the Topology. Hence, they do play an important role in defining the network topology as well as in secure transmission.

In the case of static methods, the threshold was based on the link as it changes in a linear fashion [17]. But in this case, every node is having its own environment which will obviously affect the link change. It is also stated by the researchers that each node might individually experience the change which is to be evaluated. These can be determined using metrics like node mobility and other parameters.

Hence, the proposed method for adaptive trust threshold computation aims towards estimating the link change at every node, node degree and average nodes trustworthiness which helps for better performance in the real-time scenarios.

III. Proposed Methdology

The proposed work computes the nodes trust based on three tier observations which are quantified into a single value to represent the secure trust factor of the node under consideration in first stage (STBA). In second phase, adaptive trust threshold is evaluated based on the network factors (APTT). In third phase, the evaluated secure trust factor is compared with adaptive trust threshold to classify the nodes category (STAT). It isolates the malicious nodes and performs secure routing only with those nodes evolved as trustworthy. The proposed approach suits to the real time environment which represents the minimum gathering in any real time scenario like a small conference. Work flow is shown the Fig. 1.

A. *Secure Trust based Approach (STBA)*

Secure Trust based approach evaluates nodes resultant secure trust value as a combination of direct, neighbor observations and nodes self-appraisal/historical trust as given in equation 1.

Resultant Secure Trust = Direct Trust + Neighbour Trust + Historical Trust/Self-appraisal of Node (1)

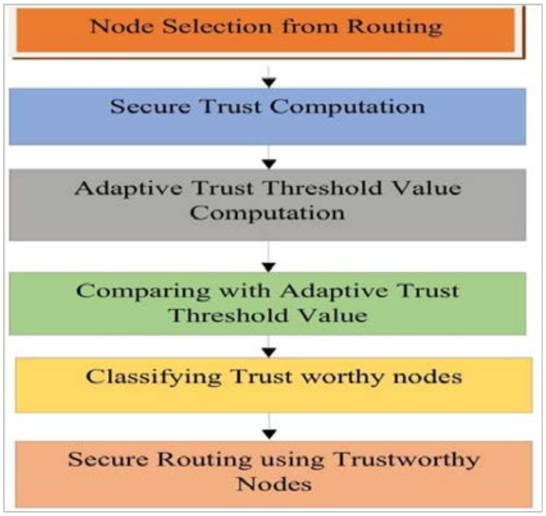
Node Selection from Routing
Secure Trust Computation
Adaptive Trust Threshold Value Computation
Comparing with Adaptive Trust Threshold Value
Classifying Trust worthy nodes
Secure Routing using Trustworthy Nodes

Fig. 1. Work Flow of the Objectives.

Direct Trust (D) : Data Packet Ratio(DF) and Control Packet Ratio(CF) is generated based on the data packets and control packets forwarding nature of the node. Direct Trust is calculated using equation 2.

Direct Trust, D = t_1 * DF + t_2 * CF (2)

Where $t_1 + t_2 = 1$, t_1, t_2 are corresponding weight given to Data Packet Ratio and Control Packet Ratio.

Neighbour Trust (N): All the neighbouring nodes in 1 hop distance will quantify their trust observations on the node specified for which trust is calculated using the equation 3.

Neighbour Trust,

N = (k1*T1 + k2*T2 + k3*T3+ k4*T4…. +knTN) /(Total No of Nodes within 1 Hop distance) (3)

Where T1, T2, T3, T4…. Tn are trust observations by the neighbour nodes. And k1, k2, k3, k4… are corresponding weights given to the neighbour nodes based on their distance in the network.

Nodes Self-Appraisal (H): Nodes can rate themselves with a trust value based upon their performance in terms of packet forwading. Self-Appraisal is quantified based on equation 4.

Self-Appraisal, H = No of Packets forwarded properly/Total no of packets received (4)

Then,

Secure Trust is evaluated based on equation 5.

Secure Trust (STBA), T = m1D + m2N + m3H (5)

Where m1, m2, m3 are corresponding weights assigned to the trust observations.

B. Adaptive Trust Threshold (APTT)

Adaptive trust threshold computation has to represent many different network factors. Each node in the network may encounter various conditions such as node degree variations, rate of link changes and average neighborhood.

Network Parameters to be considered are:

1) Node Degree - σ

It is defined as No of nodes in 1 hop neighbourhood. The statics are presented as follows.

Node n at time t, n(t) = 0, i.e.

Min Node Degree = 0, then it is considered as no neighbours for that node.

Max Node Degree = all are directly connected to Node μ. Node Degree has a direct impact on Trust Threshold; the higher number of nodes in its 1-hop neighbourhood. The higher is the threshold value and vice-versa. Optimal Threshold Value for the Node Degree is calculated based on the equation 6.

Optimal Threshold value

$\Sigma\sigma = \sigma n \,/\, |\, T \,|$ (6)

Where, T = total number of nodes

σn = Node Degree of node $'n$‘

and 2 Hop connectivity may be considered.

2) Rate of Link Changes – η

Neighborhood changes occur in MANETs frequently due to Network Mobility. A Node can determine its Neighbor Mobility by computing the Neighborhoods rate of link changes. Higher Mobility leads to higher rate of link changes in Nodes Neighborhood.

Rate of Link changes at Node μ is given by equation 7.

ŋ μ = λμ + μμ (7)

Where,

λ_{μ} =Number of new nodes coming in, means Neighbours of Node

μ = Total Link arrival rate at Node μ

$\mu_{\mu\ =}$ Total number of nodes moving out of Node’s μ transmission range for time interval.

Minimum Link Rate changes, ŋ $_{\mu\ min}$ = 0 = No new nodes arrival, No Link Breakages, implies Temporary Static then considered as no mobility.

Maximum Link Rate changes, ŋ $_{\mu\ max\ =}$ When all the direct neighbors are out of the transmission zone, considered as High mobility.

If the rate of change in Neighborhood is high, set Low Threshold (to avoid false positives).

If the rate of change in Neighborhood is low, set High Threshold (Network is static).

Optimal Threshold value for the Rate of link change factor is given by equation 8.

Optimal Threshold

Ƹη = 1 – $\eta\, \mu \,/ 2\sigma\mu$ [22] (8)

Where $\eta\ \mu$ = Rate of Link Changes of node ‘μ ‘

$\sigma\mu$ = Node Degree of node ‘μ ‘

3) Average Neighborhood Trustworthiness – $\boldsymbol{\tau_{avg}}$

The formula for τ_{avg} is given by equation 9.

$\tau_{\mu\ avg} = 1/\mathrm{n} \sum_{j=1}^{n} \mathrm{Tj}$ (9)

Where, Tj = Trust of all the neighbour nodes of Node μ on it, where Self-appraisal/Historical Trust of nodes is taken into consideration.

$\tau_{\mu\ avg}$ = 1: Good Nodes are available, High Trust Worthy , set High Threshold.

$\tau_{\mu\ avg}$ = 0: More Misbehaving Nodes are available, Low Trust Worthiness, set Low Threshold value.

Optimal Threshold value at node μ for malicious node isolation given be equation 10.

$$Ƹ_{T} = \tau_{\mu\ avg} \quad (10)$$

Combining all the network parameters for estimating the proposed adaptive trust threshold using equation 11.

Final adaptive trust threshold, $Ƹ_{\mu}$ is

$$Ƹ_{\mu} = (a Ƹ_{\sigma} + bƸ_{ŋ} + c Ƹ_{T}) /(a+b+c) \quad (11)$$

Where $Ƹ_{\sigma}$ = Optimal threshold value of Node Degree of the

Node

$Ƹ_{ŋ}$ = Optimal threshold value of Rate of Link.

Changes of the Node.

$Ƹ_{T}$ = Optimal threshold value of Average.

Neighbourhood Trustworthiness of the Node.

And a,b,c are constants and a+b+c is considered for higher throughput, and the Node Degree and 2 Hop connectivity are given importance. So subsequently α should have more weight.

Then Decision of isolating a node depends upon.

T, Trust Evaluated of the node >= Adaptive Trust Threshold - $Ƹ_{\mu,}$ Node is decided as Trusted Node.

T, Trust Evaluated < Adaptive Trust Threshold - $Ƹ_{\mu,,}$ Node is decided as Un Trusted Node, then, isolate the node from routing.

C. Proposed Algorithm for Adaptive Trust Threshold

Considering the 2-hop connectivity an algorithm is proposed for the adaptive trust threshold as follows:

Algorithm Optimal adaptive trust threshold computation

```
procedure Secure Trust(T, D, N, H)
{
// T = Secure trust of the Node
// D= Direct Trust of the Node
// N=Neighbor Trust of the Node
// H=Historical Trust/Self Appraisal of the Node
Step:1 Node trustworthiness is initiated, for each and every node
Step:2 Data Packet Forward ratio is
    $DF = w_1 *( D_{forw}/ D_{td}) + w_2 *( D_{drop}/ D_{td}) + w_3 *( D_{mr}/ D_{td}) + w_4 *( D_{fi}/ D_{td})$
Step:3 Control Packet Forward Ratio is
    $CF= w_1 *( R_{req} / R_{treq}) + w_2 *( R_{rep} / R_{trep}) + w_3 *( R_{err} / R_{terr}) + w_4 *( R_{tack}/ R_{ack})$
Step:4 Driect Trust, $D = t_1 * DF + t_2 * CF$
Step:5 Neighbour Trust, N = (k1*T1 + k2*T2 + k3*T3+ k4*T4…. +knTN) /(Total No of Nodes within 1 Hop distance)
Step:6 Self-Appraisal, H = No of Packets forwarded properly/Total no of packets received
Step:7 Secure Trust(STBA), T = m1D + m2N + m3H
}
end procedure

procedure Network Parameters ($T_{avg,}$ Ɛ σ , Ƹ ŋ )
{
//$T_{avg}$ = Average Neighborhood Trustworthiness
// Ɛ σ = Optimal Threshold value of Node Degree
//Ƹ ŋ= Optimal Threshold value of Rate of Change in Linkage
Step:1 if new node appears then$\tau_{avg} = \tau_{avg}$+ Threshold of new node.
Step:2 Calculating the optimal threshold through node degree using $Ɛ \sigma = \sigma n / | T |$
Step:3 Based on the mobility of the network calculate the total Change of rate of linkage using $Ƹ ŋ = 1 – ŋ \mu /2\sigma\mu$
Step:4 if$\tau_{\mu\ avg}$=0 then consider it as Malicious node.
Step:5 The threshold for malicious node is calculated
    $Ƹ_{T} = \tau_{\mu\ avg.}$
}
end procedure

procedure Adaptive Threshold ($Ƹ_{\mu}$ , $Ƹ_{\sigma}$, $Ƹ_{ŋ}$, $Ƹ_{T}$)
{
// $Ƹ_{\mu}$ = Adaptive Trust Threshold
//$Ƹ_{\sigma}$ = Optimal Trust Threshold of Node Degree
// $Ƹ_{ŋ}$ = Optimal Trust Threshold of Rate of Link Changes
//$Ƹ_{T}$ = Optimal Trust Threshold of Average Node Trustworthiness
Step:1 Overall Adaptive Trust Threshold is calculated using
    $Ƹ_{\mu} = ( a Ƹ_{\sigma} + bƸ_{ŋ} + c Ƹ_{T} ) /( a+b+c)$
}
end procedure

procedure Routing Decision ($T_{\mu}$ , $Ƹ_{\mu}$)
{
// $T_{\mu}$ = Secure trust of the Node μ
// $Ƹ_{\mu}$ = Adaptive Trust Threshold of the Node μ
if ($T_{\mu} < Ƹ_{\mu}$ ) then malicious node, isolate the node
else
Trustworthy node, Involve in routing process
end if
}
end procedure
```

IV. Experiment and Result Analysis

Network Simulator 2 (NS2) is used for simulation of desired network. The network traffic is maintained with a size of 512Bytes with a packet rate of 200 and 100 packets per second. The malicious Nodes are defined in the physical layers. Hence, considering the parameters for configuration, the trust and other metrics are calculated. To analyze the results, the network configuration parameters and simulation parameters are given in Table I.

TABLE I. SIMULATION PARAMETERS

Simulation tool	NS2
Number of Nodes	100
Malicious Nodes	18
Propagation Model	Two ray ground
Malicious Nodes Declaration	0t
Topography	700*500(M)
Simulation Time	500s
Mobility(r)	5m/s

The simulations are carried out for three design goals in which the last scenario is the proposed method where calculations are obtained from the Adaptive trust threshold.

The parameters used to evaluate the results are Packet Delivery Ratio (PDR): It is defined to be the ratio denoting the number of packets received at the destination and the number of packets sent from the source [18].

Packet Drop Rate (PPR): It is defined as a ratio of the number of lost packets to the total number of sent packets [19].

False Positive Detection (FPR): It denotes the ratio the count of good nodes wrongly identified as malicious to the total available count of nodes. It is also used to calculate the FPR (False positive rate) [20, 21].

Malicious Node Detection Ratio (MDR): it gives the ratio of malicious/misbehaving nodes from the total nodes from the network [20, 21].

Throughput (T): It usually defines the amount of data transferability of a network through a period of time [20,21].

Delay (D): This shows the time frame from delivering the packets through source and destination. [22].

These parameters are considered to evaluate the performance of three occurrences, where the first occurrence routing without any prior trust calculation.

The second occurrence considers the routing with nodes trust computation using the methodology Secure trust based approach (STBA) but compared with static trust threshold factor for node isolation.

Third occurrence is the proposed work, routing with Secure trust combined with Adaptive Trust threshold (STAT) which is the combination of Computation of Secure trust (STBA) and Computation of Adaptive trust threshold (APTT). More emphasis is on computation and comparison of Adaptive trust threshold. Results proved the proposed scheme with adaptive trust threshold comparison performs well over other two occurrences mentioned.

A. *Result and Analysis*

1) Secure Trust Based Approach Computation (STBA): Secure Trust is computed based upon the three tier observations using the above mentioned equations. Results obtained for secure trust are tabulated in Table II.

2) Adaptive Trust Threshold Computation (APTT): Adaptive Trust Threshold is computed based upon network parameters Node Degreeσ, Rate of Link changes ŋ, Average Node Behavior τ_{avg} using above mentioned equations. Results generated are tabulated in Table III. Identification of malicious nodes and their isolation using proposed STAT method with Node's Secure Trust computation and comparison with Adaptive Trust Threshold is shown in Table IV.

TABLE II. SECURE TRUST THRESHOLD COMPUTATION

Node	**Direct Trust**	**Neighbor calculation**	**Historical Trust Calculation**	**Node Secure Trust**
0	0.93	0.3417	0.94	0.75451
1	0.75	0.2788	1	0.63364
2	0	0.3792	0.78	0.11376
3	0	0.5238	0.87	0.15714
4	0	0.5992	0.78	0.17976
5	0	0.2955	0.67	0.08865
6	0	0.03075	0.76	0.009225
7	0.03	0.624	0.87	0.2052
8	0.69	0.4672	0.91	0.55416
9	0.83	0.04975	0.995	0.612425
10	0.72	0.414	1	0.6562
11	0.49	0.4096	0.79	0.81688
12	0.47	0.4636	0.86	0.82108
13	0.67	0.2895	0.83	0.88885
14	0.31	0.179	0.85	0.4397

TABLE III. ADAPTIVE TRUST THRESHOLD ξ_{μ} COMPUTATION

Node	#1hop Neighbor -	Node Degree Value σ	Rate of Link Changes	2sigma	d/e	Link change η	Average Neighborhood Trustworthiness - τ_{avg}	Adaptive trust Threshold - ξ_{μ}
0	12	0.5714286	2	24	0.083333	0.916667	0.4792	0.665777
1	11	0.5238095	5	22	0.227273	0.772727	0.4822	0.594324
2	13	0.6190476	4	26	0.153846	0.846154	0.4215	0.667425
3	11	0.5238095	4	22	0.181818	0.818182	0.5268	0.61242
4	13	0.6190476	3	26	0.115385	0.884615	0.5914	0.695953
5	11	0.5238095	5	22	0.227273	0.772727	0.4866	0.594764
6	14	0.6666667	8	28	0.285714	0.714286	0.5489	0.669176
7	15	0.7142857	3	30	0.1	0.9	0.5578	0.754351
8	10	0.4761905	6	20	0.3	0.7	0.5422	0.549934
9	10	0.4761905	3	20	0.15	0.85	0.4911	0.589824
10	11	0.5238095	5	22	0.227273	0.772727	0.4474	0.590844
11	15	0.7142857	3	30	0.1	0.9	0.5781	0.756381
12	15	0.7142857	2	30	0.066667	0.933333	0.5512	0.763691
13	14	0.6666667	2	28	0.071429	0.928571	0.4719	0.725761
14	3	0.1428571	1	6	0.166667	0.833333	0.5144	0.387154

TABLE IV. MALICIOUS NODE ISOLATION

Node	Node Secure Trust	Adaptive trust Threshold - ξ_{μ}	Decision
0	0.75451	0.665777	Trustworthy
1	0.63364	0.594324	Trustworthy
2	0.11376	0.667425	Malicious
3	0.15714	0.61242	Malicious
4	0.17976	0.695953	Malicious
5	0.08865	0.594764	Trustworthy
6	0.009225	0.669176	Malicious
7	0.2052	0.754351	Malicious
8	0.55416	0.549934	Trustworthy
9	0.612425	0.589824	Trustworthy
10	0.6562	0.590844	Trustworthy
11	0.81688	0.756381	Trustworthy
12	0.82108	0.763691	Trustworthy
13	0.88885	0.725761	Trustworthy
14	0.4397	0.387154	Trustworthy

B. Performance Metrics

1) Packet delivery ratio: It was observed that for 100pkts/s, out of 50000 packets sent, 47550 packets received, Packet Delivery Ratio is 95.1% for the proposed method, 91.1 % for the second case where trust is compared with static trust threshold, 53.2 % in case of third design goal where routing involved without trust calculation and for 200pkts/s**,** out of 100000 packets sent, 79235 packets received, Packet Delivery Ratio is 79.2%. In case of proposed method, 75.3%, 30.1%. In case of second and third case, respectively whereas in Fig. 2, shows the Packet Delivery ratio of all the three design goals.

C. Packet Drop Ratio

From the simulation, it was observed that for 100pkts/s, out of 50000 packets sent, 2451 packets lost, Packet Drop Ratio is 4.9% for the proposed method, 5.8 % for the second case where trust is compared with static trust threshold, 43.3 % in case of third design goal where routing involved without trust calculation and for 200pkts/s**,** out of 100000 packets sent, 20785 packets lost, Packet Drop Ratio is 20.765%. In case of proposed method, whereas it is 23.4%, 69.2% for second and third design goal. Fig. 3 shows the Packet drop ratio for the three cases compared.

D. Throughput

From the simulation, it was observed that for 100pkts/s, Throughput is 380.4kbps for the proposed method, 358.2kbps for the second case where trust is compared with static trust threshold, 211.6kbps in case of third design goal where routing involved without trust calculation and for 200pkts/s**,** Throughput is 633.4kbps in case of proposed method, whereas it is 603.5kbps, 229.2kbps for second and third design goal. In Fig. 4, throughput efficiency of the proposed method STAT is shown.

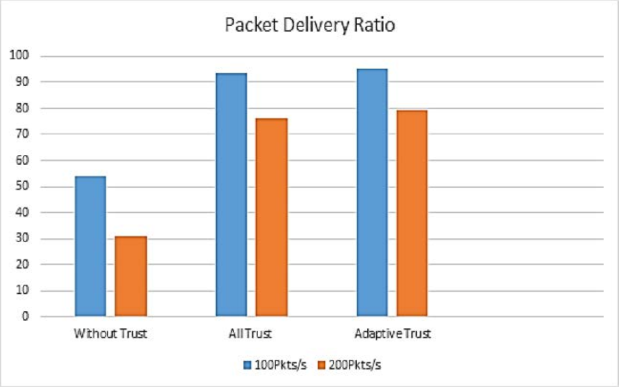

Fig. 2. Packet Delivery Ratio Analysis.

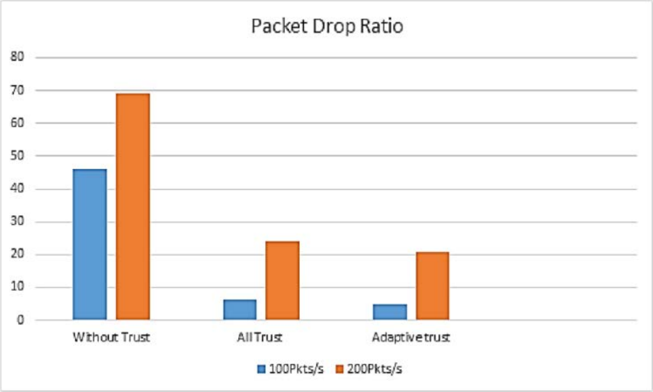

Fig. 3. Packet Drop Ratio Analysis.

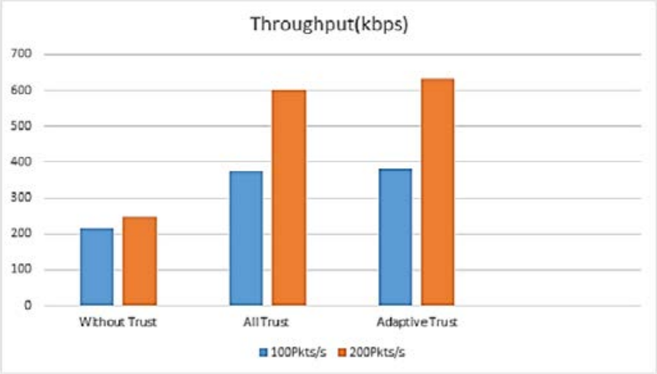

Fig. 4. Analysis of Throughput.

E. Delay

Delay is observed as 187ms for 100pkts/s in case of proposed method, 198ms for the second case where trust is compared with static trust threshold, 232ms in case of third design goal where routing involved without trust calculation and for 200pkts/s**,** Delay is 270ms in case of proposed method, whereas it is 287ms, 302ms for second and third design goal. Fig. 5 depicts the delay parameter in case of three scenarios mentioned and proves the efficacy of the proposed method. Delay in the network in case of packet delivery is illustrated as follows.

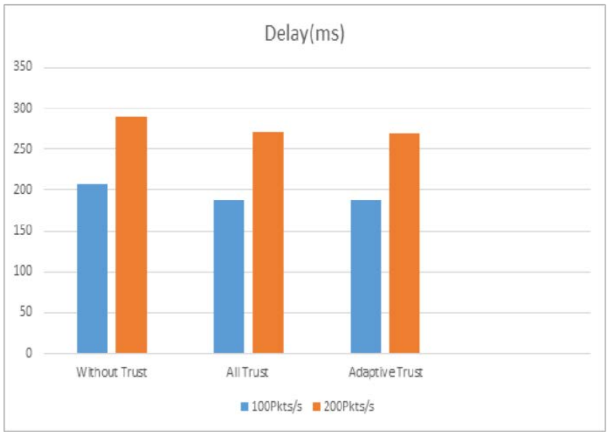

Fig. 5. Delay in the Network.

F. False Positive Detection Rate

False Positive Detection Rate is found as 52% in case of proposed method, 44% for the second case where trust is compared with static trust threshold. In Fig. 6, False Positive Detection Rate is shown for the proposed method.

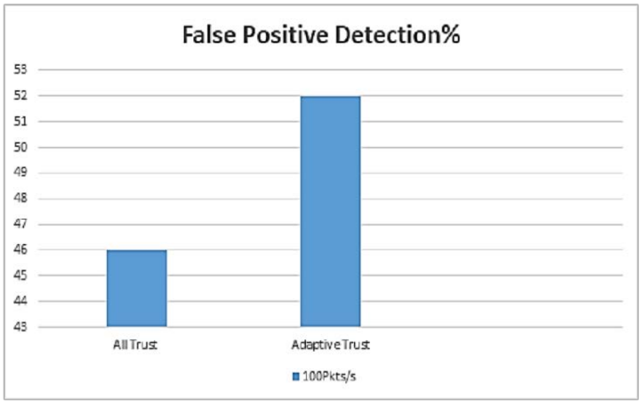

Fig. 6. False Positive Detection Ratio Analysis.

G. Malicious node Detection Rate

Malicious node Detection Rate is found as 23% in case of proposed method, 21% for the second case where trust is compared with static trust threshold. In Fig. 7, proposed method is performing better compared with the secure trust (static threshold) in terms of malicious node detection rate.

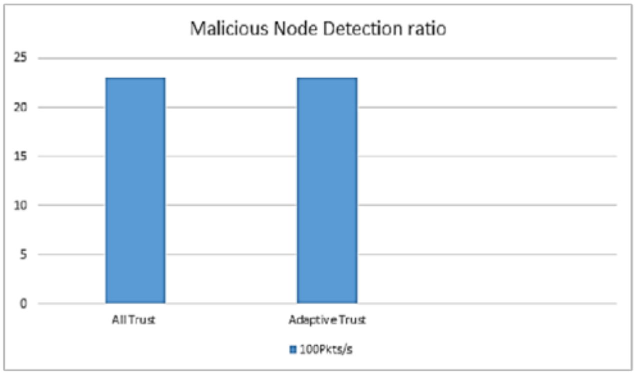

Fig. 7. Detection of Malicious Nodes.

From results, it is interpreted that computation of adaptive trust threshold based on the network parameters when combined with secure trust mechanism, efficiently identifies the malicious nodes which are dropping packets and good natured nodes which are delivering packets and can be used for mobilization.

V. Conclusion

The work presented here shows a strategy which can be used to detect the nodes which are misbehaving in a network by considering the network parameters which plays an important role in network. The results evaluated and shown in Fig. 2 to 7 prove the efficacy of the proposed work STAT. The Packet delivery ratio for the method proposed (Adaptive trust Threshold) shows significant growth along with less packet loss ratio as well which makes it easy to consider the technique proposed in the real-time traffic networks. The proposed method is evaluated and seemed better performing than other methods in particular with methods that uses static trust threshold. Results proves the efficiency of the proposed method when compared with other approaches like routing without trust calculation and routing with trust computation and static threshold approaches. The further scope of the work will be extended by considering the Power consumption scenarios in the networks in case of trustworthy nodes.

ACKNOWLEDGMENT

The authors acknowledge the support and cooperation rendered by all the members directly and indirectly.

REFERENCES

[1] B.V.S Uma Prathyusha, K.Ramesh Babu, ”A Node Monitoring Agent based Handover Mechanism for Effective Communication in Cloud-Assisted MANETs in 5G”, International Journal of Advanced Computer Science and Applications(2022), Vol. 13, No. 1, 2022, 128-136.

[2] Ahmed, Malik N., et al. "F3TM: Flooding Factor based Trust Management Framework for secure data transmission in MANETs." *Journal of King Saud University-Computer and Information Sciences* 29.3 (2017): 269-280.

[3] AlKhatieb, Anas, Emad Felemban, and Atif Naseer. "Performance evaluation of ad-hoc routing protocols in (FANETs)." *2020 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*. IEEE, 2020.

[4] H C Ramaprasad , S.C. Lingareddy , “A Novel Integrated Scheme for Detection and Mitigation of Route Diversion Attack in MANET”, International Journal of Advanced Computer Science and Applications(2022), Vol. 12, No. 11, 2021, 374-381.

[5] Chakraborty, Arpita, Jyoti Sekhar Banerjee, and Abir Chattopadhyay. "Malicious node restricted quantized data fusion scheme for trustworthy spectrum sensing in cognitive radio networks." *Journal of mechanics of continua and mathematical sciences* 15.1 (2020): 39-56.

[6] Jain, Ashish Kumar, Vrinda Tokekar, and Shailendra Shrivastava. "Security enhancement in MANETs using fuzzy-based trust computation against black hole attacks." *Information and Communication Technology*. Springer, Singapore, 2018. 39-47.

[7] Saidi, Ahmed. "Trust evaluation method for Wireless Sensor Networks based on behavioral similarity and similarity coefficient." *2021 International Conference on Networking and Advanced Systems (ICNAS)*. IEEE, 2021.

[8] Khan, Burhan Ul Islam, et al. "A survey on MANETs: architecture, evolution, applications, security issues and solutions." *Indonesian Journal of Electrical Engineering and Computer Science* 12.2 (2018): 832-842.

[9] Zhang, De-gan, et al. "Novel approach of distributed & adaptive trust metrics for MANET." *Wireless Networks* 25.6 (2019): 3587-3603.

[10] Daly, Elizabeth M., and Mads Haahr. "The challenges of disconnected delay-tolerant MANETs." *Ad Hoc Networks* 8.2 (2010): 241-250.

[11] Abdel-Fattah, Farhan, et al. "Security challenges and attacks in dynamic mobile ad hoc networks MANETs." *2019 IEEE jordan international joint conference on electrical engineering and information technology (JEEIT)*. IEEE, 2019.

[12] G. A. S. T. ME, and M. Manikandan. "Trust threshold-based neighborhood-Trustworthy with node certified public key Management scheme in MANET." pp. 28-33. International Journal of Science and Technology, 2019.

[13] Divyashree, H. B., C. Puttamadappa, and KS Nandini Prasad. "Performance Analysis and Enhancement of QoS Parameters for Real-Time Applications in MANETs-Comparative Study." *2020 International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT)*. IEEE, 2020.

[14] Jhaveri, Rutvij H., et al. "A composite trust model for secure routing in mobile ad-hoc networks." *Adhoc Networks* 2 (2017): 19-45.

[15] Koul, Ajay, and Harinder Kaur. "Quality of Service Oriented Secure Routing Model for Mobile Ad hoc Networks." *Proceedings of the 2017 International Conference on Intelligent Systems, Metaheuristics & Swarm Intelligence*. 2017.

[16] M. Ebrahimi, N. , N. Ho, T. Nguyen, and J. Stolmeier. "Evaluation of parameters affecting the performance of routing protocols in mobile ad hoc networks (MANETs) with a focus on energy efficiency." In Future of information and communication conference, pp. 1210-1219. Springer, Cham, 2019.

[17] Saudi, Nur Amirah Mohd, et al. "Mobile ad-hoc network (MANET) routing protocols: A performance assessment." *Proceedings of the third international conference on computing, mathematics and statistics (iCMS2017)*. Springer, Singapore, 2019.

[18] Tamilselvi, P., and C. Ganesh Babu. "An efficient approach to circumvent black hole nodes in manets." *Cluster Computing* 22.5 (2019): 11401-11409.

[19] Anwar, Raja Waseem, et al. "BTEM: Belief based trust evaluation mechanism for wireless sensor networks." *Future generation computer systems* 96 (2019): 605-616.

[20] Sethuraman, Priya, and N. Kannan. "Refined trust energy-ad hoc on demand distance vector (ReTE-AODV) routing algorithm for secured routing in MANET." *Wireless Networks* 23.7 (2017): 2227-2237.

[21] Oubabas, Sarah, et al. "Secure and stable vehicular ad hoc network clustering algorithm based on hybrid mobility similarities and trust management scheme." *Vehicular Communications* 13 (2018): 128-138.

[22] Patel, Surabhi, and Heman Pathak. "A mathematical framework for link failure time estimation in MANETs." *Engineering Science and Technology, an International Journal* 25 (2022): 100984.