Enhancing the Routing Security through Node Trustworthiness using Secure Trust Based Approach in Mobile Ad Hoc Networks

https://doi.org/10.3991/ijim.v16i14.30651

M. Venkata Krishna Reddy[1,2(✉)], P.V.S. Srinivas[3], M. Chandra Mohan[1]
[1]Jawaharlal Nehru Technological University, Hyderabad, India
[2]Chaitanya Bharathi Institute of Technology(A), Hyderabad, India
[3]Vignan Bharathi Institute of Technology(A), Hyderabad, India
krishnareddy_cse@cbit.ac.in

Abstract—Mobile Ad Hoc Networks, also known as MANET's are the part of many heterogeneous networks which utilizes the technologies like Internet of Things. Internet is filled with known as well as unknown sources which are still considered as a challenge. Secure routing is always a major concern in MANET's. Among all the existing and proposed cryptographic approaches to provide security to these networks seemed lengthy, complex and inefficient in eliminating malicious nodes. Many trust based approaches are proposed to replace these traditional cryptographic security methods for secure routing in MANET's. But all those trust based approaches concentrate on either direct observations or hybrid observations to determine the node's trustworthiness without taking into count network parameters. Considering the security challenges that arise due to the topology, infrastructure and bandwidth of MANET's, a novel secure trust based approach (STBA) is proposed in this article to strengthen the evolution of trust component for effective isolation of malicious nodes and secure routing. This work focuses on the computation of the node's trust factor based on network parameters and node's behavior to simulate the challenge of providing the secure transmission. The proposed method, STBA computes secure trust of a node depending on three tier observations. The performance of the proposed secure trust mechanism STBA is evaluated by comparing it with routing without any trust calculation, with existing Belief based Trust Evaluation Mechanism (BTEM) and Novel extended trust based mechanism (NETM) where routing is performed involving only with direct and indirect trust computation for node's distribution in both cases. Results show the proposed method is performing well.

Keywords—Mobile Ad Hoc networks, secure routing, node trustworthiness, direct trust, indirect trust, secure trust

1 Introduction

MANET are portable adhoc networks, which in general forms a dynamic routing virtual network. They are collection of remote self-organized nodes fueled by battery

power where other shapes of communication are unreasonable to convey [1]. They are made up of a group of portable nodes linked electronically in a self-configuring, identity system that does not rely on a wired network. Because of the distributed structure of the MANET, connection between nodes alters regularly and they are ready to roam in and around the network at their will. The node is considered as a gateway, which forwards information to all other devices in the network by dissipating its own resources. The MANET's key problem lies in equipping all these devices with the necessary information to provide services continually. Now a day they are used for monitoring the atmosphere, the house wellness, relief operations, wind defence, weaponry, drones, and other applications like accident prevention. Most of this applications demand certain security levels and raise a basic issue, especially Wireless Sensor Networks WSN is effortlessly defenseless to attacks when compared to wired systems due to its remote broadcasting characterization and constrained assets [2]. The features which make MANET's unique are Dynamic Topology, Autonomy Conduct and Resource Intervention [3].

MANET's are especially susceptible to security because of their lack of dispersed design of the encryption, wireless connectivity and centralized control. They need low latency to set up the connection, making them constantly independent. Isolation from centralized control management made MANET's more vulnerable to security.

1.1 Security issues in MANETs

MANET routing performance is affected by capabilities of mobile nodes [4]. Each unit can act as a gateway in the network as well as a server, demonstrating their independent nature. They have to dissipate their own energy resources for other node's packet forwarding which may lead to behave them as selfish and can act as malicious nodes. Isolation of malicious nodes from the routing in MANET's is always a critical security concern. A secure environment necessitates a set of well-behaving and fair nodes. Because of noise factor in the network, due to lack of centralized control, transmission and supplies are restricted. All connectivity activities, such as filtering and data packets are self-organized in a MANET [5]. Ensuring secure routing in MANET's has become difficult due to these factors.

Node Mobility is also a major security issue in MANET. Packets are routed by establishing the path with available nodes in the network [6]. Nodes may enter and exit the network at any movement and any time [7]. Secure routing is always a challenge with the presence of the malicious nodes that behave selfishly to save their energy resources from being consumed for forwarding other node's data in the network. Many existing encryption algorithms like digital signature and authentication based schemes proved to be inefficient in terms of protecting against attacks from these malicious nodes [8]. Various security solutions based on the trust idea were developed in supplement to the old cryptographic methods. By applying the trust concept in ad hoc networks context, there was a significant trend toward enhancing security in MANET. Quantifying the nodes trustworthiness plays the key role in isolating the malicious nodes thus establish the secure routing and data transmission. Trust factor evaluated confirms each node's

fair participation in routing. Many of the existing and proposed trust based methods are relying on either direct or hybrid observations in deciding the trust factor for node categorization. These methods are not considering network parameters and nodes behavior to evaluate the node's trust factor. These trust based mechanisms are proven to be inefficient in isolating the malicious nodes from their involvement in the routing.

In this article, the node trust worthiness is quantified based on three tier observations, direct, neighbour and self appraisal of the node using the method, STBA, secure trust based approach to enrich the trust factor in isolating the malicious nodes. Results obtained show the satisfactory performance of the proposed method STBA. Routing after nodes trustworthiness evolution using proposed STBA is compared with routing without any trust computation, with existing method BTEM and Novel extended trust based mechanism NETM where routing is performed after evaluating nodes trustworthiness using only direct observation and hybrid observations to show the performance of the proposed method. The main aim of the proposed STBA method in this article is to provide secure routing for data transmission by simulating the important factor node trustworthiness.

This work is organized as follows: Introduction and security issues of the MANET are presented in Section 1; Related Research work on MANET is described under Section 2. Section 3 discusses the proposed STBA method and in Section 4 simulation results and discussions are presented. The concluding remarks of the work and future research recommendations are given in Section 5.

2 Related work

In [9], authors presented a belief based trust evolution mechanism BETM for MANET's. This method classifies the malicious nodes and trust-worthy nodes. It defends against several attacks like Denial of Service (DoS), On–Off and Bad-mouth attacks. In this method, authors employed Bayesian estimation approach for computing direct and neighbor trust values of the sensor nodes which estimates imprecise knowledge in decision making by considering the data correlation collected over a period of time for secure transmission of data thus isolating and keeping away the malicious nodes from routing. However, this method considers only packet forwarding behavior of the node in estimating the trust. In [10], authors proposed a estimation-based trust model, Novel extended trust based mechanism NETM which aims on estimating each node's trust level in the network. This mechanism uses blind and referential trust based on previous experiences of the node. This method is not considering network parameters and packet forwarding behavior of the node in estimating the trust. Authors in [11] presented a new evaluated and administration (TEAM) paradigm that provides a distinctive template for the construction, maintenance, and assessment of Trust Models in a variety of situations and the context of malicious nodes. Various trust models (TMs) were actively developed, but presently there exists no practical process of comparing how they might perform in practice in adversarial situations. Nodes in MANET actively communicate critical data such as pre-collision signals. As a result, this data must remain secure, trustworthy and legitimate. For recognizing unscrupulous nodes and identifying the communications containing dangerous data, trust formation between nodes is essential.

Author proposed a trust based approach to ensure MANET's integrity which focus on direct observations. Similarly, authors in [12] state that wireless adhoc sensor networks (WSNs) are specialized networks with a huge number of sensor units (SNs) which are used to manage multiple natural and physical phenomena. The SNs can indeed be employed in a variety of technical, security, and agricultural purposes, such as mobility tracking and combat monitoring.

Sensors are installed on ad hoc basis and act independently in these systems; additionally, there is a growing demand for encrypted communication across SNS. The authors applied energy-efficient routing protocols (ERPSs) for isolation of selfish nodes based on trust factor where hybrid approach is taken into consideration as a result of the SNs' structure and constraints [13]. Authors in [14], proposed cluster based trust methods where the network is divided into regions. Clustering is generated based on how comparable SNs are. Each clustering seems to have a set of cluster members (CMs), with one or more designated as cluster chiefs (CHs). CHs evolutes the trustworthiness of CMs using direct observations. The data transmission effectiveness is legitimate in this method and also be analyzed through nodes trust factor. In [15] trust based mechanism is illustrated to resolve the congestion problem in the network. Nodes trust is evaluated using hybrid approach to avoid dropping of the packets due to congestion. In [16], authors presented a trust based control mechanism which depends on direct trust factor. In [17], authors proposed a methodology for secure routing taking into consideration, MANET characteristics by assessing the node's trustworthiness. It is noted that all the trust dependent approaches proposed are taking into account either direct or hybrid observations. Hence a better evaluation of Node Trustworthiness based on Node's behavior and Network parameters is required to maintain the secure transmission in wireless networks. To strengthen the computation of trust factor for establishing secure routing, a novel method based on three tier observations, STBA is presented in this article.

3 Proposed model

The proposed work STBA, Secure Trust Based Approach improvises the trustworthiness of nodes for secure transmission. It computes the secure trust value of the node depending on three level observations: direct, indirect and self appraisal.

3.1 Model for secure trust computation

The model for secure trust computation is given in Figure 1. These processes are basically dependent. The resultant secure trust is combination of three tier observations on the node under consideration. It includes direct observations, neighbor observations and nodes historical trust, Self appraisal. Secure trust value is calculated according to equation 1.

$$\textit{Resultant Secure Trust} = \text{Direct Trust} + \text{Neighbour Trust} + \text{Historical Trust}/\text{Self appraisal of Node} \quad (1)$$

The step-by-step calculations for the overall resultant trust i.e secure trust is given in Figure 1.

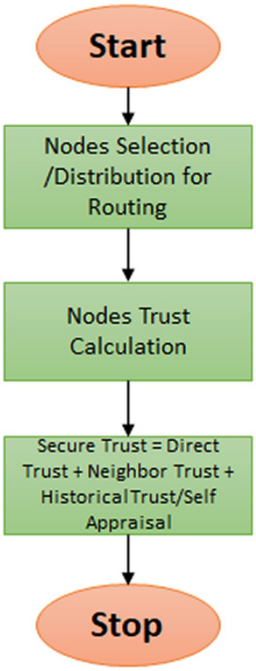

Fig. 1. Flowchart of the proposed STBA method

3.2 Direct trust calculation

Direct Trust is evaluated depending upon the direct observations on the node in the network whom trust is being calculated. Direct observations capture the nodes behavior. Several network parameters are taken into consideration here for quantifying the nodes behavior to evaluate direct trust factor. Parameters considered are

Data Packets Forwarded:

Total no of data packets received at the node = D_{td}
No of data packets forwarded correctly by the node = D_{forw}
No of data packets dropped by the node = D_{drop}
No of data packets misrouted by the node = D_{mr}
No of data packets falsely injected by the node = D_{fi}
Data Packets forwarded ratio, DFR is quantified as given in equation 2.

$$DFR = w_1*(D_{forw}/D_{td}) + w_2*(D_{drop}/D_{td}) + w_3*(D_{mr}/D_{td}) + w_4*(D_{fi}/D_{td}) \quad (2)$$

Where w1, w2, w3, w4 are the proportionate weights assigned to the packet forwarding behaviour and can be altered according to the network conditions and
$w_1 + w_2 + w_3 + w_4 = 1$

Control Packets Forwarded:

Total no of Route Request packets received at the Node = R_{treq}
Total no of Route Reply packets received at the Node = R_{trep}
Total no of Route error packets received at the Node = R_{terr}
Total no of Route acknowledgment packets received at the Node = R_{tack}
No of Route Request packets forwarded by the Node = R_{req}
No of Route Reply packets forwarded by the Node = R_{rep}
No of Route error packets forwarded by the Node = R_{err}
No of Route acknowledgment packets forwarded by the Node = R_{ack}.
Control Packets Forwarded Ratio, CFR is computed as specified in equation 3.

$$CFR = w_1 *(R_{req}/R_{treq}) + w_2 *(R_{rep}/R_{trep}) + w_3 *(R_{err}/R_{terr}) + w_4 *(R_{tack}/R_{ack}) \quad (3)$$

Where w1, w2, w3, w4 are the proportionate weights assigned to the packet forwarding behaviour and can be changed according to the network conditions and
$w_1 + w_2 + w_3 + w_4 = 1$

Direct Trust TS is calculated using Data packets forwarded ratio DFR from equation 2 and Control packets forwarded ratio CFR from equation 3, as shown in equation 4

$$TS = w_1 * DFR + w_2 * CFR \quad (4)$$

Where $w_1 + w_2 = 1$ and w1, w2 are weights assigned to DFR & CFR based on the network environment.

3.3 Neighbour trust calculation

Neighbour Trust is collective trust evolution done by all neighbouring nodes which are located in 1 hop distance from the node whose trust is being calculated by quantifying above Data packet forwarding and Control packet forwarding parameters. Weights should be assigned to all the neighbour nodes depending on where they located and distance to the node specified in the network. Weight should be calculated using coordinates. Nearest Neighbour should be assigned with more weight value depending on the total number of neighbours at time t in the network.

Neighbour Trust, TO is evaluated using equation 5 given below

$$TO = (w1*NT1 + w2*NT2 + w3*NT3 + w4*NT4\ldots. + wnNTn)/ \text{(No of Neighbour Nodes in 1 Hop distance)} \quad (5)$$

Where NT1, NT2, NT3, NT4…. NTn are the trust values calculated by the neighbour nodes by their direct observations using above mentioned parameters. And w1, w2, w3, w4…..w_n represent the weights assigned to the neighbours depending on their distance in the network.

3.4 Historical trust calculation – nodes self appraisal

Nodes under trust evaluation can have their own trust values based upon their self appraisal subjected to their performance and involvement in the fair routing in the past and present. This can be computed as Self appraisal trust factor TH. Nodes Self appraisal is calculated based on its behaviour using the below parameters.

Number of Packets correctly Forwarded (Good) = $P_{for} = \alpha$
Number of Packets dropped without forwarding (Bad) = $P_{drop} = \beta$
Number of Packets falsely injected (Bad) = $P_{fi} = \beta$
Historical Trust, Self Appraisal of node, TH is given by the equation 6.

$$TH = \alpha/(\alpha + \beta) \tag{6}$$

Final resultant, Node's secure trust calculation is computed from three tier observations Direct Trust TS, Neighbour Trust TO and Self Appraisal TH using equations 4, 5, 6 respectively.

Secure Trust, T is evaluated as shown in equation 7.

$$\text{Secure Trust, } T = \alpha TS + \beta TO + \gamma TH \tag{7}$$

Where α, β, γ are constants and assigned based on the weight factor given to the subsequent observation according to the network conditions.

The Secure trust T evaluated, falls in the range of 0 to 1.

$$0<=T<=1$$

3.5 Static threshold

Node's secure trust is computed using the equation 7 and later it is matched with the static threshold in order to decide the nodes trustworthiness. Whether a node can be included as intermediate node for secure routing or not. Static Threshold is fixed based upon the network conditions. Various levels of static trust threshold fixed are given in Table 1.

Table 1. Levels and rankings for the trust value

Level	Resultant Secure Trust Value	Ranking
1	–1	Complete Distrust
2	0	New or Unknown
3	0.2	Very Low Trust
4	0.4	Low Trust
5	0.6	Average Trust
6	0.8	High Trust
7	1	Absolute Trust

The average static trust threshold value considered is

$$TH_{threshold} is = 0.6 – Average\ Trust$$

Nodes trustworthiness is classified based on the average static threshold.
Node's Classification – $T >= TH_{threshold}$ = Trustworthy Node
$T < TH_{threshold}$ = Untrustworthy Node

3.6 Algorithm (Secure Trust Based Approach-STBA)

Procedure Direct Trust (TS, N1, N2, DFR, CFR)
//TS is the Direct Trust
//N1 is the node and N2 is its neighbor node
//Data packets forwarded ratio is DFR
//Control Packets Forwarded Ratio CFR
//Direct Trust TS
{
Step 1: if N1 initiates finding trustworthiness on N2 node
then the process starts.
Step 2: Data Packet Ratio is calculated as
$DFR = w_1 *(D_{forw}/ D_{td}) + w_2 *(D_{drop}/ D_{td}) + w_3 * (D_{mr}/D_{td}) + w_4 *(D_{fi}/ D_{td})$
Step 3: Control Packet Ratio is calculated using
$CFR = w_1 *(R_{req}/R_{treq}) + w_2 *(R_{rep}/R_{trep}) + w_3 * (R_{err}/R_{terr}) + w_4 *(R_{tack}/ R_{ack})$
Step 4: Then Direct Trust factor, TS is calculated from
$TS = w_1 * DFR + w_2 * CFR$
}
end procedure

Procedure Neighbor Trust (TO, N1, N2)
//TO is the Neighbor Trust
//N1 is the node of which trust to be evaluated and N2 is its neighbor node
//Neighbor Trust TO
{
Step 1: If all the neighbors in 1-hop distance initiates finding the node trustworthiness of the node N1 under consideration based on their direct observations. Then the process starts.
Step 2: Neighbor Trust, TO is calculated using
TO = (w1*NT1 + w2*NT2 + w3*NT3 + w4*NT4…. + wnNTn)/ (No of Neighbour Nodes in 1 Hop distance)
Step 3: Weights are assigned depending on location and the distance of the neighbor nodes in the network.
}
end procedure

Procedure Self Trust (TH, N1, PF, PD)
//TH is the Historical/Self Appraisal Trust
//N1 is the node
//Data packets forwarded – PF
//Data packets dropped – PD
//Self Appraisal Trust TH
{
Step 1: Node N1 evaluates its own trust based upon the packets routing, process starts.
Step 2: Packets forwarded PF = PF + 1 – α
Step 3: Packets dropped PD = PD-1 – β
Step 4: Self Appraisal Trust, TH is calculated from
TH = α/(α + β)
}
end procedure

Procedure Secure Trust (T, TS, TO, TH, N1, N2)
//TS is the Direct Trust
//TO is the Neighbor Trust
//TH is the Historical/Self Appraisal Trust
//T is resultant Secure Trust
{
Step 1: If node N1 gets TS, TO, TH on a node N2 whose trust is being evaluated then computes the resultant secure trust value.
Secure Trust, T = αTS + βTO + γTH and 0<=T<=1
else
Step 2: set final secure trust value, T to 0
end if
}
end procedure

Procedure Secure Routing (T, $TH_{threshold}$)
//T is resultant Secure Trust
//$TH_{threshold}$ is the Static trust threshold
//Secure Routing
{
Step 1: Average static trust threshold is 0.6
Step 2: If T>= $TH_{threshold}$, Node is classified as Trustworthy
else
T<= $TH_{threshold}$, Node is classified as malicious and isolated.
end if
Step 3: Perform secure Routing involving only trustworthy nodes as intermediate nodes.
}
end procedure

4 Results and discussions

4.1 Simulation

Simulation is performed on Network Simulator NS2. The components in the different layers are: Wireless Physical layer followed through MAC 802.11 Data link layer and AODV for the network layer and finally, the UDP (User data gram protocol) for Transport layer. These settings are made in the Network Simulator 2 (NS2). The constant bit rate traffic is fixed with 512 bytes size for 200 and 100 packets per second i.e., packet rate. Simulation parameters considered can be seen in Table 2 and parameters for network configuration are given under Table 3 [9] [12].

Table 2. Parameters illustrating network configuration

Simulation tool	NS2
Total Number of Nodes used for Simulation	100
Malicious Nodes Inserted	15
Propagation Model used	Two ray ground
Malicious Nodes Declaration time	0t
Topography used	700*500(M)
Simulation Time	500s
Mobility(r)	5m/s

Table 3. Network configuration parameters

Parameter	Value
Simulation tool	NS2
Version	2.35 (base)
Operating System	Fedora 11
Channel	Wireless channel
Type of Network Interface	Wireless Physical
Medium Access Control Protocol	MAC 802.11
Type of Interface Queue	Drop Tail
Interface Queue Length	50
Type of Antenna	Omni Directional
Network Layer Protocol	AODV (Ad-hoc On-demand Distance Vector)
Random Motion	Disabled
Carrier Sense Threshold	4.21756e-11
Receiving threshold	4.4613e-10
Capture Threshold	75.0
Transmission Power	0.2818
Frequency	2.4e+9
Initial Energy	500u
Transmission Power	0.9u
Receiving Power	0.5u
Idle Power	0.45u
Sleep Power	0.05u

Simulations are performed for the four design goals in order to generate the performance of the proposed STBA method. The first case is the proposed STBA method where routing is performed involving the trustworthy nodes whose trust is calculated depending on three level observations. Second goal is existing NETM method and third goal is existing BETM method where in both cases routing is performed by involving the trustworthy nodes which are classified based on only direct & indirect trust computations. The last one is the simple AODV routing protocol where routing performed involving all the available nodes without any trust computation. Below are the performance parameters used to analyze the results and efficiency of the proposed work.

Packet Delivery Ratio: It is defined as total number of packets received at the destination divided by the total number of packets sent from the source in the network [18][19].

Packet Drop Rate: It is the ratio of the total number of dropped packets divided by the total number of sent packets by the source [20].

Malicious Node Detection Ratio: Malicious, bad behaviour Nodes detected out of total nodes present in the network [21].

False Positive Detection: The ratio defined as the total count of good behavior nodes wrongly designated as malicious one's to the total count of nodes present in the network is called as 'False positive detection' [22].

Throughput: It refers to how much data can be transferred in the network from source to destination within a given timeframe [23].

Delay: Time delay taken to transfer data packets from Source to Destination [24][25].

4.2 Results

After performing the simulations, results are analyzed. Node's Trustworthiness is evaluated based on the proposed method, secure trust based approach STBA. This method uses three tier observations for computation of trust factor. Direct, Neighbour and Self appraisal trusts are calculated using above mentioned equations. Results obtained and calculations carried out for secure trust computation from the simulation are tabulated in Table 4.

Table 4. Sample secure trust value computation

Node No.	Direct Trust Calculation	Neighbor Trust Calculation	Historical Trust Calculation	Node Secure Trust Value
N0	0.92	0.4323	0.83	0.84352
N1	0.71	0.3667	0.987	0.73265
N2	0.23	0.4591	0.89	0.21477
N3	0.31	0.5238	0.91	0.24725
N4	0.12	0.4791	0.60	0.28965
N5	0.22	0.3956	0.71	0.77864
N6	0.34	0.13274	0.89	0.79326
N7	0.05	0.725	0.79	0.3231
N8	0.62	0.5571	0.89	0.65326

(Continued)

Table 4. Sample secure trust value computation *(Continued)*

Node No.	Direct Trust Calculation	Neighbor Trust Calculation	Historical Trust Calculation	Node Secure Trust Value
N9	0.81	0.13674	0.889	0.532524
N10	0.69	0.513	0.99	0.74651
N11	0.56	0.3195	1	0.72689
N12	0.43	0.3535	0.95	0.73418
N13	0.61	0.3894	0.89	0.78865
N14	0.43	0.262	0.79	0.5982
N15	0.3	0.2238	0.73	0.64714
N16	0.62	0.2748	0.84	0.65444
N17	0.75	0.519	0.81	0.6057
N18	0.76	0.5815	0.79	0.63045
N19	0.42	0.528	0.75	0.6104
N20	0.28	0.375	0.88	0.6805

The proposed STBA method identifies and isolates the malicious nodes using Node's Secure Trust computation as shown in Table 5.

Table 5. Sample malicious nodes identification and isolation

Node	Node Secure Trust	Static Trust Threshold	Decision
N0	0.84352	0.6	Trustworthy
N1	0.73265	0.6	Trustworthy
N2	0.21477	0.6	Malicious
N3	0.24725	0.6	Malicious
N4	0.28965	0.6	Malicious
N5	0.77864	0.6	Trustworthy
N6	0.79326	0.6	Trustworthy
N7	0.3231	0.6	Malicious
N8	0.65326	0.6	Malicious
N9	0.532524	0.6	Malicious
N10	0.74651	0.6	Trustworthy
N11	0.72689	0.6	Trustworthy
N12	0.73418	0.6	Trustworthy
N13	0.78865	0.6	Trustworthy
N14	0.5982	0.6	Malicious
N15	0.64714	0.6	Trustworthy
N16	0.65444	0.6	Trustworthy
N17	0.6057	0.6	Trustworthy
N18	0.63045	0.6	Trustworthy
N19	0.6104	0.6	Trustworthy
N20	0.6805	0.6	Trustworthy

The interpretations are made through the evaluations of the metrics. The efficiency of proposed STBA method is demonstrated using below performance parameters.

Packet delivery ratio. From the simulation results, it was noted that for 100pkts/s, 47012 packets received out of 50000 packets sent, so Packet Delivery Ratio is 94.9% for the proposed STBA method, 89.1% for NETM, 87.2% for the existing BTEM where routing involved with direct & indirect trust computation, 52.9% in case of fourth design goal where routing is performed without any prior trust computation. For 200pkts/s, in case of proposed STBA method 75016 packets received out of 100000 packets sent, Packet Delivery Ratio is 76.3%, in case of NETM and BTEM, it is 75.6% and 74.2% respectively and fourth case it is 31.2%. Figure 2 depicts packet delivery ratio for all the cases. It shows how the delivery of the packets is affected through the presence of malicious nodes.

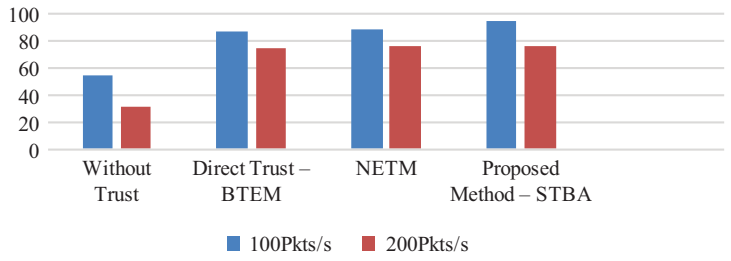

Fig. 2. Packet delivery ratio

False positives detection ratio (FPD Ratio). In case of proposed method for 100 packets, False Positive Detection Rate is 44%, whereas 36% for the second case NETM and 32% for third case BTEM where routing involved with direct & indirect trust. Figure 3 shows the comparison of False Positive Detection Rate of proposed method with NETM and BTEM method.

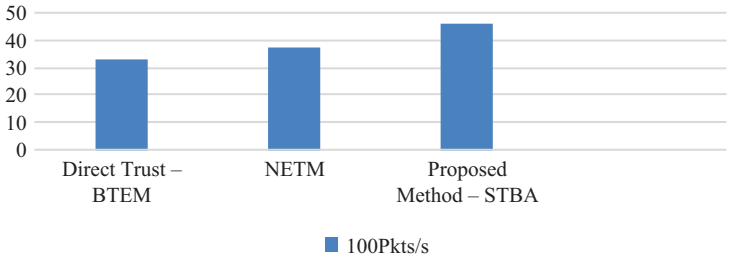

Fig. 3. False positive detection ratio of STBA

Packet drop ratio. Simulation results show that for 100pkts/s, 2990 packets lost out of 50000 packets sent, Packet Drop Ratio is 5.8% for the STBA method, it is 8.4% for NETM, 9.7% for the existing method BTEM where routing involved with Direct & Indirect trust computation, in case of fourth design goal, it is 43.3% where

routing is done without any trust calculation. For 200pkts/s, 24068 packets lost out of 100000 packets sent, Packet Drop Ratio is 21.124% in case of proposed STBA method, whereas for NETM it is 24.5%, BTEM it is 25.6%, and for fourth design goal it is 69.4%. Comparison of the above four cases in terms of the Packet drop ratio is shown in Figure 4.

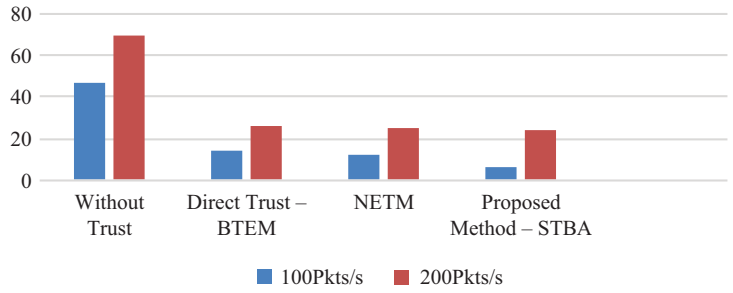

Fig. 4. Packet drop ratio

Malicious node detection. Malicious Node Detection rate for the proposed method is 26%, 24% for NETM and 22% for BTEM where routing is involved with direct & indirect trust. Figure 5 shows the comparison and efficiency of the proposed method in terms of malicious node detection.

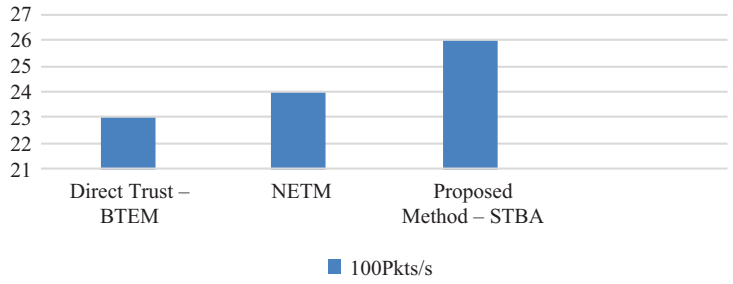

Fig. 5. Detection of malicious nodes

Throughput. Simulation results show that throughput for 100pkts/s is 389.1kbps for the proposed STBA method, 362.2kbps for the NETM, 356.3kbps for the existing BTEM, whereas it is 210.5kbps for the fourth design goal which involves routing without any trust calculation and in case of 200pkts/s, Throughput is 602.9kbps for proposed STBA method, whereas it is 591.4kbps, 587.6kbps, 228.3kbps for NETM, BTEM and fourth design goal respectively. Figure 6. Illustrates the throughput efficiency of the proposed method compared with other cases.

Basically, throughput shows the efficient delivery of packets. Hence, it can be interpreted that the proposed method performs very well in terms of throughput.

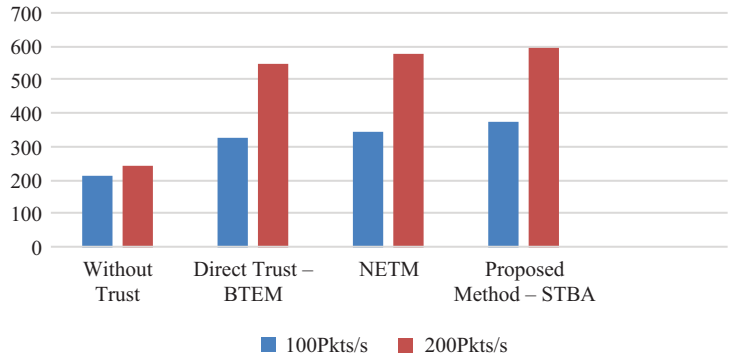

Fig. 6. Throughput comparison

Delay. From the results, in case of proposed method STBA, for 100pkts/s delay is noted as 192ms, 196ms for the second case NTEM, 198ms for the BTEM, where routing involved with direct & indirect trust, 221ms in fourth case where trust calculation is not done before routing and delay is 283ms for 200pkts/s in case of proposed STBA method, it is 291ms for NTEM, 293ms for BTEM and 298ms for fourth case. Efficiency of the proposed method in terms delay is shown in Figure 7.

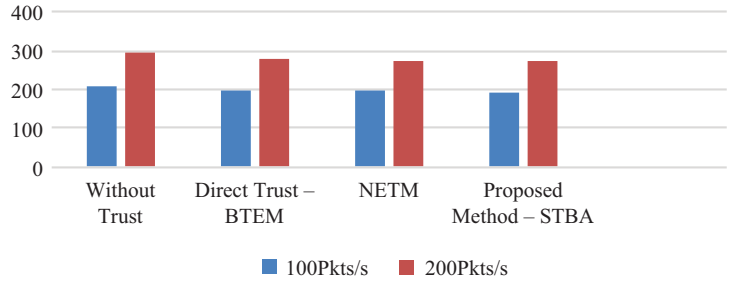

Fig. 7. Delay in milliseconds

Discussions. The proposed STBA method performs secure routing efficiently by evaluating trust factor for identifying the trustworthy nodes and isolating the malicious nodes. Secure trust value of a node is computed using factors, direct, indirect observations and self appraisal of the node. The proposed method STBA is compared with the existing NETM, BTEM mechanism and routing without trust calculation, simple AODV protocol. Simulation results prove the proposed STBA method is performing well. The comparison between the proposed and existing methods in terms of performance metrics are tabulated below in Table 6.

Table 6. Comparison of results – efficiency of the proposed method STBA

S. No	Performance Parameter	Proposed Method – STBA (%)		NETM (%)		BETM (%)		Without any Trust Calculation (AODV) (%)	
		100 Pkts/Sec	200 Pkts/Sec	100 Pkts/Sec	200 Pkts/Sec	100 Pkts/Sec	200 Pkts/Sec	100 Pkts/Sec	200 Pkts/Sec
1	Packet Delivery Ratio	94.9	76.3	89.1	75.6	87.2	74.2	52.9	31.2
2	Packet Drop Ratio	5.8	21.12	8.4	24.5	9.7	25.6	43.3	69.4
3	False Positive Detection Ratio	44		36		32		–	
4	Malicious Node Detection	24		24		22		–	
5	Throughout	389.1 kbps	602.9 kbps	362.2 kbps	591.4 kbps	356.3 kbps	587.6 kbps	210.5 kbps	228.3 kbps
6	Delay	192 ms	283 ms	196 ms	291 ms	198 ms	293 ms	221 ms	298 ms

5 Conclusion

From this paper, a quantitative model Secure Trust based Approach STBA is proposed to show the effective transfer of packets for communication in wireless networks using node's trustworthiness with three tier observations. The method successfully isolates the malicious nodes. This work is proved to be efficient when compared with other existing approaches like NETM and BETM where both uses hybrid observations for evolution of trustworthiness and isolation of malicious nodes. The aim is achieved through calculating the trust worthiness of the nodes and packet metrics. The appropriate results and evidences were pointed to show the effective combination of three tier observations for calculating node's trustworthiness and for secure transmission. This research can be extended in future by considering the factor of Adaptive trust threshold. The adaptive growth of the proposed model can be seen by implementing an adaptive threshold technique in place of static trust threshold factor to compare the secure trust calculated.

6 Acknowledgment

Special thanks to the members involved for support and knowledgeable efforts towards simulations directly and indirectly.

7 References

[1] Wheeb, Ali H., and Nadia Adnan Shiltagh Al-Jamali. "Performance analysis of OLSR protocol in Mobile Ad Hoc networks." *iJIM* 16.01 (2022): 107. https://doi.org/10.3991/ijim.v16i01.26663

[2] Almalkawi, Islam, et al. "A novel and Efficient priority-based cross-layer contextual unobservability scheme against global attacks for WMSNs." *iJIM* 15.03 (2021): 43–69. https://doi.org/10.3991/ijim.v15i03.18327

[3] Sultan, Shahid, et al. "Collaborative-trust approach toward malicious node detection in vehicular ad hoc networks." *Environment, Development and Sustainability* (2021): 1–19. https://doi.org/10.1007/s10668-021-01632-5

[4] Alnabhan, Mohammad. "Advanced GPSR in Mobile Ad-hoc Networks (MANETs)." *iJIM* 14.18 (2020): 107–131. https://doi.org/10.3991/ijim.v14i18.16661

[5] Sheikh, Muhammad Sameer, Jun Liang, and Wensong Wang. "Security and privacy in vehicular Ad Hoc network and vehicle cloud computing: a survey." *Wireless Communications and Mobile Computing* 2020 (2020). https://doi.org/10.1155/2020/5129620

[6] Srivastava, Vikas, et al. "Energy efficient optimized rate based congestion control routing in wireless sensor network." *Journal of Ambient Intelligence and Humanized Computing* 11.3 (2020): 1325–1338. https://doi.org/10.1007/s12652-019-01449-1

[7] Dwivedi, Ashutosh Dhar, et al. "A decentralized privacy-preserving healthcare blockchain for IoT." *Sensors* 19.2 (2019): 326. https://doi.org/10.3390/s19020326

[8] Elhoseny, Mohamed, and K. Shankar. "Reliable data transmission model for Mobile Ad Hoc network using signcryption technique." *IEEE Transactions on Reliability* 69.3 (2019): 1077–1086. https://doi.org/10.1109/TR.2019.2915800

[9] Anwar, Raja Waseem, et al. "BTEM: Belief based trust evaluation mechanism for wireless sensor networks." *Future generation computer systems* 96 (2019): 605–616. https://doi.org/10.1016/j.future.2019.02.004

[10] Syed, Salman Ali, and Ali Shahzad. "Enhanced dynamic source routing for verifying trust in Mobile Ad Hoc network for secure routing." *International Journal of Electrical and Computer Engineering* 12.1 (2022): 425. https://doi.org/10.11591/ijece.v12i1.pp425-430

[11] Jamal, Tauseef, and Shariq Aziz Butt. "Malicious node analysis in MANETS." *International Journal of Information Technology* 11.4 (2019): 859–867. https://doi.org/10.1007/s41870-018-0168-2

[12] Mukhedkar, Moresh Madhukar, and Uttam Kolekar. "Trust-based secure routing in Mobile Ad Hoc network using hybrid optimization algorithm." *The Computer Journal* 62.10 (2019): 1528–1545. https://doi.org/10.1093/comjnl/bxz061

[13] Selvi, M., et al. "A rule based delay constrained energy efficient routing technique for wireless sensor networks." *Cluster Computing* 22.5 (2019): 10839–10848. https://doi.org/10.1007/s10586-017-1191-y

[14] Abbas, Fakhar, and Pingzhi Fan. "Clustering-based reliable low-latency routing scheme using ACO method for vehicular networks." *Vehicular Communications* 12 (2018): 66–74. https://doi.org/10.1016/j.vehcom.2018.02.004

[15] Ahmad, Farhan, Virginia NL Franqueira, and Asma Adnane. "TEAM: A trust evaluation and management framework in context-enabled vehicular ad-hoc networks." *IEEE Access* 6 (2018): 28643–28660. https://doi.org/10.1109/ACCESS.2018.2837887

[16] Draz, Umar, et al. "Evaluation based analysis of packet delivery ratio for AODV and DSR under UDP and TCP environment." *2018 international conference on computing, mathematics and engineering technologies (iCoMET)*. IEEE, 2018. https://doi.org/10.1109/ICOMET.2018.8346385

[17] Khan, Muhammad Asghar, et al. "Dynamic routing in flying ad-hoc networks using topology-based routing protocols." *Drones* 2.3 (2018): 27. https://doi.org/10.3390/drones2030027

[18] Vaibhav, Akash, et al. "Security challenges, authentication, application and trust models for vehicular ad hoc network-a survey." *International Journal of Wireless and Microwave Technologies* 7.3 (2017): 36–48. https://doi.org/10.5815/ijwmt.2017.03.04

[19] Arshdeep Kaur. " Vehicular Ad-hoc Network: A Survey." *International Journal of Computer Science Research* 5.2 (2017): 35–37.

[20] Airehrour, David, Jairo Gutierrez, and Sayan Kumar Ray. "Secure routing for internet of things: A survey." *Journal of Network and Computer Applications* 66 (2016): 198–213. https://doi.org/10.1016/j.jnca.2016.03.006

[21] A. Ouaddah, A. A. Elkalam, and A. A. Ouahman. "FairAccess: a new Blockchain-based access control framework for the Internet of Things." *Security and communication networks* 9, no. 18 (2016): 5943–5964. https://doi.org/10.1002/sec.1748

[22] Li, Wenjia, and Houbing Song. "ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks." *IEEE transactions on intelligent transportation systems* 17.4 (2015): 960–969. https://doi.org/10.1109/TITS.2015.2494017

[23] Ho, Quang-Dung, et al. *Wireless communications networks for the smart grid*. Springer International Publishing, 2014.

[24] Rahul Misra, and Prashant Sharma. " Challenges in Mobile Ad Hoc Network for Secure Data Transmission." *International Journal of Electrical & Electronics Research*, 1.1 (2013):8–12. https://doi.org/10.37391/IJEER.010103

[25] Bartoli, Andrea. "Security protocols suite for machine-to-machine systems." (2013).

8 Authors

M Venkata Krishna Reddy was born in Hyderabad, Telangana, India on 1982. He received his B.Tech in Computer Science and Engineering from JNTUH in 2005. He received his M.Tech in Computer Science and Engineering in 2009 from JNTUH. Currently, he is doing Ph.D. in the field of Mobile Adhoc Network from JNTUH. He is working as Asst, Professor in Computer Science Engineering Department, Chaitanya Bharathi Institute of Technology CBIT(A), Gandipet, Hyderabad, India. His researches focus on the trust computation for secure routing in MANETs.

Dr. P.V.S. Srinivas was born in Andhra Pradesh, India. He recievd his Ph.D in Computer Science and Engineering from JNTUH, Hyderabad,India. His research areas are Mobile Adhoc Networks, Machine Learning. Currently, he is working as Principal and Professor in CSE, Vignana Bharathi Institute of Technology(A), Hyderabad, India.

Dr. M.Chandra Mohan was born in Andhra Pradesh, India. He recievd his Ph.D in Computer Science and Engineering from JNTUH, Hyderabad, India. His research areas are Image Processing, Pattern Recogition and Software Engineering. Currently he is working as Director of Evaluation and Professor in CSE, Jawaharlal Nehru Technological University-JNTUH, Hyderabad, India.

Article submitted 2022-03-04. Resubmitted 2022-05-08. Final acceptance 2022-05-08. Final version published as submitted by the authors.