INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

ORIGINAL ARTICLE

A Novel Trust Adaptability Approach for Secure Data Transmissions using Enhanced Collaborative Nodes Trustworthiness in Mobile Ad-hoc Networks

M Venkata Krishna Reddy[1,2]*, **P V S Srinivas**[3], **M Chandra Mohan**[4]

1 Research Scholar, Department of Computer Science and Engineering, Jawaharlal Nehru Technological University, Hyderabad, Telangana, 500075, India
2 Assistant Professor, Department of CSE, Chaitanya Bharathi Institute of Technology(A), Hyderabad, Telangana, 500075, India
3 Professor, Department of Computer Science and Engineering, Vignana Bharathi Institute of Technology(A), Hyderabad, Telangana, 500075, India
4 Professor, Department of Computer Science and Engineering, Jawaharlal Nehru Technological University, Hyderabad, Telangana, 500075, India

OPEN ACCESS

Received: 22-03-2022

Accepted: 04-08-2022

Published: 26-08-2022

Citation: Reddy MVK, Srinivas PVS, Mohan MC (2022) A Novel Trust Adaptability Approach for Secure Data Transmissions using Enhanced Collaborative Nodes Trustworthiness in Mobile Ad-hoc Networks. Indian Journal of Science and Technology 15(33): 1613-1623. https://doi.org/10.17485/IJST/v15i33.663

* **Corresponding author**.

krishnareddy_cse@cbit.ac.in

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Objectives: To find an efficient security routing model based on trust adaptability by considering various transmission parameters that influence the node's behavior. **Methods:** Enhanced Collaborative Trust Based Approach (ECTBA) was applied to isolate the malicious nodes from routing by computing their enhanced collaborative trust value based on the node's behavior using transmission parameters. Parameters that influence the node's behavior like the number of data packets and control packets forwarded, dropped, or misrouted by the node are quantified to compute direct trust value and neighbor reputation. Node's Enhanced Collaborative trust value was generated by the combination of direct and neighbor observations. **Findings:** The proposed strategy is compared with several cases like the Direct Trust Based Approach (DTBA), where routing involves trustworthy nodes categorized based on only direct trust, existing methods like Belief-dependent trust evolution method(BETM), Novel extended trust-dependent method (NETM) where routing is done with nodes that are categorized as trustworthy depending on direct and indirect observations and simple AODV routing performed with all the possible random nodes without any trust detection. The performance parameters of the proposed ECTBA exhibit a success rate of 10.2% in false positives detection (FPD),network throughput of 438.12 Kbps,and packet delivery ratio (PDR) of 92.3%.This method proves to be a better method when compared with the traditional trust-based security methods(BETM and NETM) in terms of efficiency. **Novelty:** This research suggested a novel and fine-tuned method for quantifying a node's trustworthiness and for secure routing that coupled the direct and indirect observations into enhanced collaborative trust based on the node's behavior by considering the transmission parameters. The present work highlights the combination of data packets forwarding behavior and control packets forwarding behavior in computing enhanced collaborative trust to decide the involvement of intermediate trustworthy nodes' which is not tried before but this study does.

Keywords: Dynamic Topology; Direct Trust; Neighbor Trust; Secure Routing; Enhanced Collaborative Trust

1 Introduction

Security is always a important factor in MANET due to frequent connection interruptions, bandwidth, resource constraint and high mobility of the wireless nodes. The nodes may behave selfishly and maliciously due to the energy constraints in forwarding other nodes' packets as they have to use their energy[1–4]. Many conventional cryptography-based approaches are in existence to resolve security issues in MANET but these approaches are inefficient in isolating the untrustworthy nodes. Several trust-dependent mechanisms are presented to isolate the malicious nodes from routing. These methods are treated as an efficient measure to encounter the security threats caused by pernicious nodes[5]. But all these trust-dependent mechanisms are computing the value of the trust using either direct or indirect observations and do not consider the network parameters while evaluating the node's trustworthiness.

Anwar et al. presented BETM Belief-dependent trust evolution method for Mobile Adhoc Networks[6]. This mechanism differentiates the malicious nodes from good nodes. It also provides security against On–Off attacks, Denial of Service attacks, Bad-mouth attacks. This mechanism supports an estimation approach based on Bayesian formulae for calculating sensor nodes' direct and neighbor observations for secure data transmission without including the malicious nodes in routing. The drawback of this methodology is that only the packet forwarding nature of the node is considered in evaluating the trust. Syed and Shahzad[7] proposed a novel extended trust dependent method NETM for secure data transmission in the MANET. It uses a trust-dependent approach that takes into consideration both blind-direct trust and referential-neighbour trust. The drawback of this approach is that it computes trust value to classify a node's trustworthiness purely based on previous experience trust. Usha and Radha proposed a CLAODV method coupled with adaptive RSA which is used to avoid malicious nodes[8]. This method isolates the malicious nodes based on their past experiences but does not consider the present behavior which is a pitfall. A trust based security solution in Mobile ad hoc networks is given by Alrahhal et al.[9], where trust is generated based on direct and neighbor observations. The proposed method calculates trust based on only the packet transmission nature of the Node. In the Dynamic Bargain Theory metholdogy proposed by Sumathi[10], trustworthiness of data is calculated based on nodes' trustworthiness, whereas the latter is calculated using only the direct behaviour of the node. Here the drawback is that neighbor observations and other parameters are not considered for evaluating the node's trustworthiness. In the work proposed by Satheesh and Prasadh[11], a security mechanism to minimize the chances of a weak node becoming a cluster head is proposed. The method purely depends on the observations collected directly from the node which is a drawback in realty. The direct observations are computed based on the source node's observations but not considering the packet forwarding nature of the node. A energy-efficient trust-centered multipath routing scheme is presented by Alappatt et al.[12], primarily depends on direct and indirect trust and different path trust factors. In this method, trust is evaluated majorly based on the communication behavior of the nodes and does not consider any network parameters which is the strong limitation. Khan et al. presented a hybrid and a multifactor trust model which depends on sensor nodes trust value, residual energy, no of hops, and routing methodology[13]. The multifactor methodology identifies trustworthy nodes to forward data in turn to reduce energy. However, trust is generated using communication behavior of the node. Transmission parameters are not considered for computing the trust value in this approach which is a major disadvantage. A Long Short-Term Memory model (LSTM) based on adaptive trust model proposed by Du et al.[14] in which the trust is evaluated in two steps: data collection and evaluation of trust. The limitation of this method is calculating the trust using a direct strategy. Alnumayet al. discussed a quantitative method for an IoT integrated with MANET[15] that clubs both direct and neighbor trust opinions to compute the resultant trust value. Here the different trust evidence and direct trust are combined using beta probabilistic distribution. The authors claimed that this method depends on the good and bad characteristics of the node. However, a more sophisticated approach is required to compute trust value for efficient isolation of the malicious nodes. With this context, a new algorithm for routing using reputation of the nodes is proposed by Guaya-Delgado et al.[16]. The reputation values are assigned to each node in the network and based upon these values, nodes are distinguished as good/bad. The method assumes the statuary behavior of the node which is a major drawback in MANET's.

Gopala Krishnan aims to produce a power management scheme for MANET that protects energy while routing is performed based on the cluster[17]. The cluster heads may not work properly and sometimes fail causing power issues. In this method, three key elements viz. the information gathering, computing trust levels, and trust-based configuration are used to form a trust management system which coordinates with each node to maintain reliable network connections. This scheme depends only on direct observations and becomes a drawback at the time of calculating the trust factor. A new cross-layer-based rust estimation method proposed by Dhage and Vemuru provides a defense against multiple attacks[18]. The trust is evaluated based on direct observation and the major drawback of the method is not considering the network parameters in the evaluation of the trust value.

Therefore, from the previous studies, it is seen that all the existing trust-based mechanisms proposed for secure data transmission in MANETs are either dependent on direct or indirect observations for trust evaluation. It is also observed that trust evaluation is performed based on node's communication behavior as well and they are not considering all the transmission parameters for node's trust quantification. Most of the researchers are not concentrating on the isolation of malicious nodes using the trust factor. It is observed and quite necessary that an efficient and secure trust-based mechanism is required to ensure a secured routing by isolating malicious nodes using the node's trustworthiness. Node's trust value should be evaluated based upon nodes' packet forwarding behavior in terms of transmission parameters. Both the control and data packets forwarding behavior should be taken into consideration.

In this paper, a new and efficient model based on trust that combines direct and neighbor trust values is presented. The major contribution of the article is 1) to ensure a secured routing by isolating malicious nodes using trustworthiness; 2) Quantifying the trust value based on the direct and indirect observations using transmission parameters. The direct trust observations are quantified by considering transmission parameters. Neighbor trust observations are computed by considering the weights allotted to the neighbor nodes depending on their distance. The proposed enhanced collaborative scheme (ECTBA) couples direct observations of the nodes and various neighbor recommendations collected for calculating the resultant trust. To provide good performance and trustable links for the secure transmission of data, the proposed methodology believes in trust factor. The presented method is compared with existing methods, i.e., BETM, NETM, Direct Trust based approach, and simple AODV routing without any trust calculation to evaluate the performance. From the end results, it is seen that the proposed method ECTBA outperforms all the above-mentioned methods in terms of performance parameters like packet delivery ratio, throughput, and false positive detection.

2 Materials and Methods

2.1 Proposed Model

In this proposed model, enhanced collaborative trust is computed based on direct and indirect observations using network parameters such as nodes data, control packets forwarding count, drop ratio, and misrouted number. Further enhanced collaborative trust of the node is mapped with the threshold value to identify malicious nodes and later they are isolated for efficient routing.

The existing methods BETM and NETM compute the trust of the node based on only the node's packet forwarding behavior. In these existing methods, neighbor node locations in the network are ignored while computing the neighbor observations. The proposed model ECTBA computes the trust value for isolation of the misbehaving nodes based on transmission parameters considering both direct and neighbor observations. While computing neighbor observations, neighbor nodes are given weights based on their location in the network.

2.2 Trust Model

The trust model explained in Fig.1 illustrates the generation of trust, propagation, node categorization, and routing decision. Trust is generated based on direct and indirect observations using transmission parameters. Trust generated for all the nodes is propagated across the network. A node is categorized into malicious and trustworthy based upon the threshold value. Threshold value is fixed considering the network parameters.

The routing decision is completely based on the node categorization, and the node categorization depends on trust calculation.

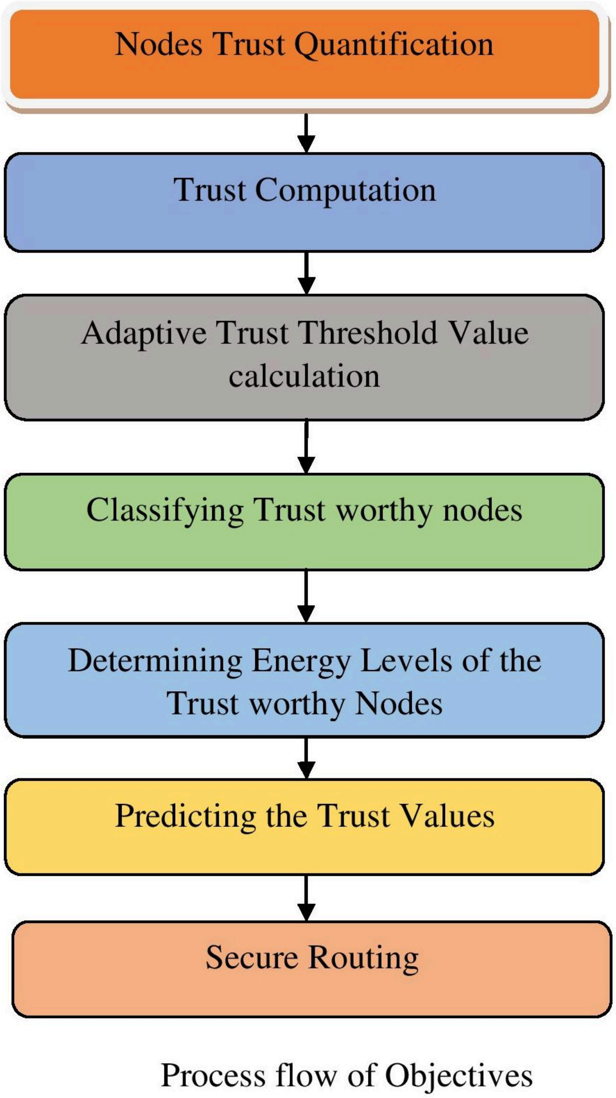
Nodes Trust Quantification
Trust Computation
Adaptive Trust Threshold Value calculation
Classifying Trust worthy nodes
Determining Energy Levels of the Trust worthy Nodes
Predicting the Trust Values
Secure Routing
Process flow of Objectives

Fig 1. Framework for Trust Calculation and Routing Decision

2.3 Trust Calculation

2.3.1 Direct Trust Based Approach (DTBA)

A node records all its observations on the trustee node intended for trust calculation directly. Based on the behavior of the node, it records all its findings directly. The packet forward behavior of the nodes is taken into consideration for evolving the trust using DTBA.

A node should listen to its neighbor nodes to estimate the trust. Due to the distributed characteristics of mobile ad-hoc networks, a node can monitor the neighbor node to evaluate its behavior during their direct communications in a passive mode. The proposed scheme uses direct observations to calculate direct trust-related values (D$_{Trust}$) of neighbor nodes by applying the below parameters.

a. Number of data packets forwarded(considered as Good)

b. Number of data packets dropped (considered as Bad)

Node A collects the information regarding the above parameters for calculating trust by observing traffic that goes through each neighbor of Node B. Then Node A uses the above information to generate the direct trust value in a time period (τ_{Time}). After running out of each time period(τ_{Time}), the trust parameters information is gathered again and direct trust value (D$_{Trust}$) is evaluated. Trust is calculated time to time due to the adhoc nature of MANETs and the nodes are grouped depending on their good and bad characterizations.

After gathering the information about the good and bad behaviors of the nodes, the direct trust can be calculated by Node A on Node B using Equation 1.

D$_{Trust\,=}$ $\alpha/(\alpha+\beta)$ (1)

where α represents Good behavior, β represents Bad behavior, and $0 \leq$D$_{Trust}\leq 1$, α, β>0

2.3.2 DTBA Algorithm

The algorithm for DTBA considers the following steps:

Step 1: Consider the node for which trust should be calculated.

Step 2: Observe the behavior of the node using parameters like packet forwarding and packet dropping.

Step 3: Compute the direct trust based on equation 1.

Step 4: Direct trust value can be propagated to all the nodes.

Step 5: Compare the trust value evaluated with a threshold value fixed based upon network performance.

Step 6: Node categorization can be done based on Step 5.

Step 7: Repeat the procedure for all the nodes to be involved in routing.

Step 8: Routing will be performed only with those nodes categorized as trustworthy.

2.3.3 Proposed Enhanced Collaborative Trust-Based Approach (ECTBA)

The proposed enhanced collaborative trust can be computed based upon the direct and neighbor observations on that node.

For computing, the proposed scheme, the following parameters are taken into consideration.

1. For Data Packets

- Total no of data packets received at the node (D$_t$)
- Number of data packets forwarded correctly by the node (D$_f$)
- Numberof data packets dropped by the node (D$_d$)
- Numberof data packets misrouted by the node (D$_m$)

2. Control Packets Forwarded

- Total no of Route Request packets received at the Node (R$_{tr}$)
- Total no of Route Reply packets received at the Node (R$_{tp}$)
- Number of the Route Request packets forwarded by the Node (R$_r$)
- Number of the Route Request packets forwarded by the Node (R$_p$)

After gathering the information using the above parameters regarding the node, the data packets and control packets ratio can be estimated by Node A on Node B using Equation 2 and Equation 3.

Data packets ratio, DR

$$DR = w_1\left(\frac{D_f}{D_t}\right)+w_2\left(\frac{D_d}{D_t}\right)+w_3\left(\frac{D_m}{D_t}\right)$$

where,$w_1+\ w_2+w_3=1$

Control packets ratio, CR

$$CR = w_1\left(\frac{R_r}{R_{tr}}\right)+w_2\left(\frac{R_p}{R_{tp}}\right)$$

where,$w_1+\ w_2=1$

$D_{Trust} =$ Direct Trust and then,

$$DTrust = w_1 \times DFR + w_2 \times CFR$$

where, $w_1 + w_2 = 1$

2.3.4 Neighbor Node Reputation Trust Calculation

In the process of trust evolution on Node B, Node A also considers the recommendations of neighboring nodes on Node B in the 1-Hop distance[19]. The Neighbor Node Trust(ND_{Trust}) is calculated through Equation 5.

$$ND_{Trust} = \sum_{i=1\ to\ n} (w_i \times D_{Trust})$$

Where w_i is weights allotted to the nodes based on their location in 1-Hop,$0 \leq w_i \leq 1$,and D_{Trust} represents the Direct Trust Observations of the Neighboring Nodes on Node B.

2.3.5 Enhanced Collaborative Trust

The final enhanced collaborative trust (C_T) of a node is computed using Direct Trust D_{Trust} and Neighbor Node Trust Calculation ND_{Trust} (20) through Equation 6.

$C_T = w_1 \times D_{Trust} + w_2 \times ND_{Trust}$

where,$w_1 + w_2 = 1$

2.3.6 ECTBA Algorithm

Algorithm for Enhanced Collaborative Trust Based Approach (ECTBA)

```
Step 1: Consider the node for which trust should be calculated.
Step 2: Observe the behavior of the node in terms of parameters: Data Packets and Control Packets
Step 3: Compute the Data Packet ratio and Control Packet ratio using equations 2& 3 respectively.
Step 4: Compute the Direct trust based on Equation 4.
Step 5: Compute Neighbor Trust based on Equation 5
Step 6: Compute Enhanced Collaborative Trust using Equation 6.
Step 7: Final Enhanced Collaborative trust value computed can be propagated to all the nodes.
Step 8: Compare final trust value evaluated with threshold value fixed based upon network performance.
Step 9: Node categorization can be done based on Step 7.
Step 10: Repeat the procedure for all the nodes to be involved in routing.
Step 11: Routing will be performed only with those nodes categorized as trustworthy.
```

2.4 Trust Propagation

Once the trust is evaluated on target node by any of the nodes, the resources used for recomputation of trust by other nodes can be minimized if the evaluated trust gets propagated in the network.

The Enhanced Collaborative Trust (C_T) determined for the target node is broadcasted across the network so that the other nodes can update.

2.5 Node Categorization

A node is said to be a bad one if it randomly drops packets intentionally but not for intrinsic network issues. The nodes are clustered into two groups Good or Bad, depending on their Direct Trust evaluated using Equation 3 and compared with Trust threshold (TH). These threshold limits are fixed depending on network configuration. Static trust threshold value is taken into consideration and average threshold trust value of 0.6 is used to isolate malicious nodes.

Good: if $C_T \geq$TH

Bad: if $C_T <$TH

2.6 Routing Decision

Source finds trusted nodes using the proposed scheme to establish the secure route to the destination. Each node consists of a list of dependable(trusted) neighbor nodes as well as their latest calculated trust values. Good nodes are used to form path between source and destination.

3 Simulation Carried

The performance of the proposed ECTBA is evaluated by comparing it with the existing BETM, NETM, Direct Trust-based approach, and simple AODV routing without any trust calculation. The proposed model of this article computes the enhanced collaboration trust value of a node by looking into its data transmission nature. Various transmission parameters like the number of data packets and control packets forwarded or dropped are considered for the resultant trust calculation. In this proposed solution, the resultant enhanced collaborative trust is evaluated using a computable approach by considering the direct and other trust observations on the node using network parameters. Simulation is carried out in a 700 × 500 m^2 network area and IEEE 802.11 MAC for 500s with 100 nodes[6,21]. Table 1 summarizes the simulation parameters.

Table 1. Simulation Parameters

Simulation Parameter	Value
Simulator	NS2.34
No of Nodes	100
Network area	700 x 500
Packet Size	512 bytes
No. of malicious nodes	05
Traffic Type	CBR/UDP
Mobility	4–25 m/s
Pause Time	5s
Simulation Time	500s

4 Results and Discussions

4.1 Results

The performance of the proposed model when mapped with methods BETM and NETM are shown in Table 2 with computed trust values for the proposed and existing models.

Table 2. Trust Value Computations of proposed ECTBA, DTBA, BETM and NETM

	ECTBA			DTBA	BETM	NETM
Node No.	**Direct Trust Calculation**	**Neighbor Trust calculation**	**Node enhanced collaborative Trust Value**	**Direct & Final Trust Calculation**	**Final Trust Value**	**Final Trust Value**
Node1	0.89	0.39	0.81	0.78	0.79	0.75
Node2	0.67	0.37	0.71	0.64	0.73	0.34
Node 3	0.44	0.56	0.65	0.45	0.54	0.65
Node 4	0.27	0.49	0.23	0.31	0.65	0.61
Node5	0.39	0.56	0.69	0.36	0.52	0.61
Node6	0.19	0.37	0.73	0.25	0.65	0.32
Node7	0.09	0.15	0.29	0.69	0.35	0.67
Node8	0.02	0.71	0.32	0.12	0.65	0.69
Node9	0.59	0.56	0.66	0.55	0.52	0.53
Node10	0.79	0.15	0.54	0.65	0.53	0.57
Node11	0.65	0.52	0.75	0.63	0.63	0.73
Node12	0.57	0.33	0.73	0.59	0.69	0.66
Node13	0.45	0.32	0.65	0.67	0.61	0.72
Node14	0.58	0.35	0.77	0.55	0.54	0.24
Node15	0.49	0.32	0.65	0.52	0.61	0.32

The proposed ECTBA method classifies the malicious nodes and trustworthy nodes depending on the computed enhanced collaborative trust value. Here average trust threshold value taken into consideration based on network conditions. Node classification details are shown in Table 3.

Table 3. Classification of the Nodes

Node	ECTBA - Node enhanced collaborative Trust Value	Static Trust Threshold	Decision
Node1	0.81	0.6	Trusted Node
Node2	0.71	0.6	Trusted Node
Node 3	0.65	0.6	Trusted Node
Node 4	0.23	0.6	Malicious Node
Node5	0.69	0.6	Trusted Node
Node6	0.73	0.6	Trusted Node
Node7	0.29	0.6	Malicious Node
Node8	0.32	0.6	Malicious Node
Node9	0.66	0.6	Trusted Node
Node10	0.54	0.6	Malicious Node
Node11	0.75	0.6	Trusted Node
Node12	0.73	0.6	Trusted Node
Node13	0.65	0.6	Trusted Node
Node14	0.77	0.6	Trusted Node
Node15	0.65	0.6	Trusted Node

It is noticed that around 22% of the packets (non-intentional-malicious drops) are found lost because of the environmental glitches in the network. For the performance evolution of the proposed model, metrics like Packet Delivery Ratio (PDR), Detection of False Positives, and Throughput are considered.

4.2 False Positive Detection Ratio

FPD ratio is the count of good nodes falsely identified as malicious nodes to the total available number of nodes in the network. It is used to calculate the(False positive)[22]. False positive detection ratio of the nodes for DTBA and proposed ECTBA with existing BETM and NETM methods as shown in Figure 2. From the graph it is seen that 10.6% of nodes are falsely detected as false positives, malicious when 25% of packet collisions occur in ECTBA, 9.2% false positive detection in BETM, 8.6% false positive detection in NETM, and 4.8% nodes are wrongly detected as false positives in DTBA. However, the results also show that ECTBA is efficient in case of False positives detection.

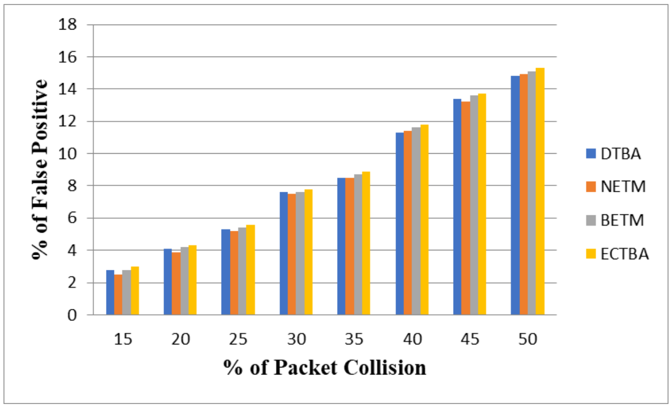

Fig 2. False Positive Detection Ratio

4.3 Packet Delivery Ratio

Figure 3 depicts how packet delivery is affected by the presence of malicious nodes. The graph depicts the mapping between the routing protocol without any trust, DTBA, NETM, BETM,and the proposed model ECTBA. It shows high Packet Delivery Ratio. In the presence of 5% of malicious nodes, packet delivery ratio for the routing protocol without any trust calculation is 72.2%, 82% for DTBA, 85% for NETM, 87.2% for BETM and 92.3% for ECTBA. It is observed that in the proposed scheme ECTBA is detecting malicious nodes using enhanced collaborative trust evaluation efficiently and avoiding them in routing thus increasing the packet delivery ratio.

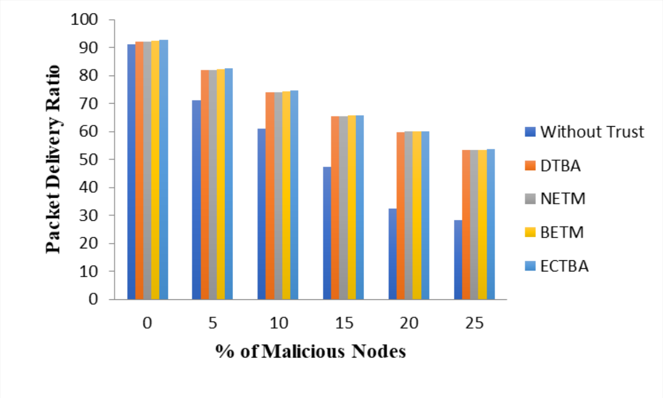

Fig 3. Packet delivery ratio mapped with number of malicious nodes

4.4 Throughput

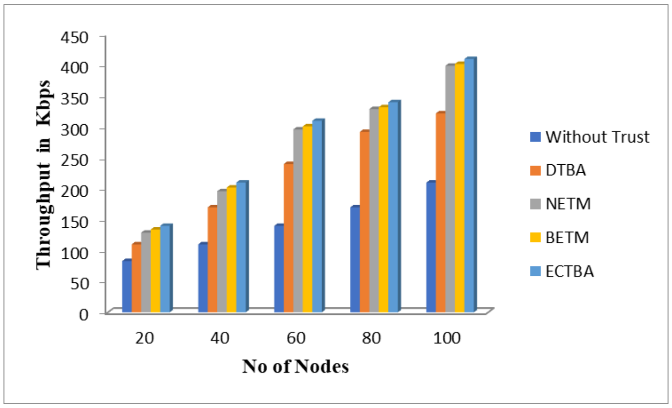

Fig 4. Throughput comparison

Throughput of the routing protocol without any trust computation, Direct Trust-based approach DTBA, NETM, BETM, and proposed method ECTBA with enhanced collaborative trust calculations are shown in Figure 4. Throughput is the number of units delivered in a stipulated time. The graph shows that the proposed method ECTBA has a throughput performance of 438.12 Kbps, BETM has 432.2 Kbps, and NETM has 428.24Kbps. whereas the scheme DTBA has 422.72 Kbps and the scheme without any trust calculation has 349.34 Kbps. It shows that the presented scheme is efficient throughput wise.4.5

Discussion

The proposed model ECTBA is compared with existing methods BETM and NETM. Existing methods compute the trust value using only the node's packet forwarding behavior. The proposed ECTBA estimated the node's trust value depending on network parameters and assigns weights for the neighbor nodes while computing neighbor observations. The performance metrics comparison between proposed and existing methods is tabulated and shown in Table 4 .

Table 4. Comparison of results – Efficiency of the proposed method ECTBA

S.No	Performance Parameter	Proposed Method – ECTBA (%)	DTBA (%)	NETM (%)	BETM (%)	Without any Trust Calculation(AODV) (%)
1	Packet Delivery Ratio	92.3	82	85	87.2	71
2	False Positive Detection Ratio	10.6	4.8	8.6	9.2	-
3	Throughout	438.12 Kbps	422.72 Kbps	428.24 Kbps	432.2 Kbps	349.34 Kbps

The proposed method ECTBA shows a high packet delivery ratio when compared with the existing methods BETM and NETM. It clearly shows more than a 5% of increment in packet delivery ratio. The proposed ECTBA detects false positives at the rate of 10.6 % when compared with existing methods. It shows increased throughput of 438.12 kbps and exhibits high performance.

5 Conclusion

This paper presents a quantitative trust model ECTBA by the integration of various data and control packets, and network parameters using direct and neighbour observations in calculating collaborative trust. The proposed trust method calculates resultant trust using the combination of data packets and control packets ratio along with indirect observations. Results obtained from simulation show that the model performs with good efficiency with respect to performance metrics like false positive detection, packet delivery ratio, and throughput as compared to the routing protocol without any trust calculation for DTBA or other existing NETM and BETM methods. Based on the comparison, the proposed model ECTBA has achieved a 10.2% success rate in False Positives detection,438.12 Kbps Throughput, and 92.3% Packet Delivery Ratio. This shows that trustworthy nodes can be easily detected through this method efficiently. So the path between source and destination is connected with the identified trusted nodes.

In the future, this method can be used in making efficient routing decisions. The enhanced collaborative trust factor after computation can be compared with the adaptive threshold for secured and efficient routing decisions. The proposed trust scheme can be applied to provide security in mobile ad-hoc networks.

6 Acknowledgement

The authors thank all the members for having provided their continuous support to this work.

References

1) Zhihan LV, Song H. Trust Mechanism of Feedback Trust Weight in Multimedia Network. *ACM Transactions on Multimedia Computing, Communications, and Applications*. 2021;17(4):1–26. Available from: https://doi.org/10.1145/3391296.

2) Kotteeswaran C, Patra I, Nagaraju R, Sungeetha D, Kommula BN, Algani YMA, et al. Autonomous detection of malevolent nodes using secure heterogeneous cluster protocol. *Computers and Electrical Engineering*. 2022;100:107902–107902. Available from: https://doi.org/10.1016/j.compeleceng.2022.107902.

3) Mbarek B, Ge M, Pitner T. An adaptive anti-jamming system in HyperLedger-based wireless sensor networks. *Wireless Networks*. 2022;28(2):691–703. Available from: https://doi.org/10.1007/s11276-022-02886-1.

4) Mohammadi V, Rahmani AM, Darwesh AM, Sahafi A. Trust-based recommendation systems in Internet of Things: a systematic literature review. *Human-centric Computing and Information Sciences*. 2019;9:1–61. Available from: https://doi.org/10.1186/s13673-019-0183-8.

5) Yang H. A Study on Improving Secure Routing Performance Using Trust Model in MANET. *Mobile Information Systems*. 2020;2020:1–17. Available from: https://doi.org/10.1155/2020/8819587.

6) Anwar RW, Zainal A, Outay F, Yasar A, Iqbal S. BTEM: Belief based trust evaluation mechanism for wireless sensor networks. *Future generation computer systems*. 2019;96:605–621. Available from: https://doi.org/10.1016/j.future.2019.02.004.

7) Syed SA, Ali S. Enhanced dynamic source routing for verifying trust in mobile ad hoc network for secure routing. *International Journal of Electrical and Computer Engineering (IJECE)*. 2022;12(1):425–425. Available from: https://doi.org/10.11591/ijece.v12i1.pp425-430.

8) Usha S, Radha S. Detection and avoidance of node misbehavior in MANET based on CLAODV. *Indian Journal of Science and Technology*. 2011;4(10):1340–1346. Available from: https://doi.org/10.17485/ijst/2011/v4i10.12.

9) Alrahhal H, Jamous R, Ramadan R, Alayba AM, Yadav K. Utilising Acknowledge for the Trust in Wireless Sensor Networks. *Applied Sciences*. 2022;12(4):2045–2045. Available from: https://doi.org/10.3390/app12042045.

10) Sumathi AC, Akila M, De Prado RP, Wozniak M, Divakarachari P. Dynamic Bargain Game Theory in the Internet of Things for Data Trustworthiness. *Sensors*. 2021;21(22):7611–7611. Available from: https://doi.org/10.3390/s21227611.

11) Satheesh N, Prasadh K. Improvements in Cluster-Based Routing to Protect Malicious Node Attacks on TAODV Routing Protocol using MANET. *Applied Mathematics & Information Sciences*. 2019;13(6):899–911. Available from: https://doi.org/10.18576/amis/130603.

12) Alappatt V, M JPP. Trust-Based Energy Efficient Secure Multipath Routing in MANET Using LF-SSO and SH2E. *International Journal of Computer Networks and Applications*. 2021;8(4):400–400. Available from: https://doi.org/10.22247/ijcna/2021/209706.

13) Khan T, Singh K, Manjul M, Ahmad MN, Zain AM, Ahmadian A. A Temperature-Aware Trusted Routing Scheme for Sensor Networks: Security Approach. *Computers & Electrical Engineering*. 2022;98:107735–107735. Available from: https://doi.org/10.1016/j.compeleceng.2022.107735.

14) Du J, Han G, Lin C, Martinez-Garcia M. LTrust: An Adaptive Trust Model Based on LSTM for Underwater Acoustic Sensor Networks. *IEEE Transactions on Wireless Communications*. 2022;p. 1–1. Available from: https://doi.org/10.1109/TWC.2022.3157621.

15) Alnumay W, Ghosh U, Chatterjee P. A Trust-Based Predictive Model for Mobile Ad Hoc Network in Internet of Things. *Sensors*. 2019;19(6):1467–1467. Available from: https://doi.org/10.3390/s19061467.

16) Guaya-Delgado L, Pallarès-Segarra E, Mezher AM, Forné J. A novel dynamic reputation-based source routing protocol for mobile ad hoc networks. *EURASIP Journal on Wireless Communications and Networking*. 2019;2019(1):1–6. Available from: https://doi.org/10.1186/s13638-019-1375-7.

17) Krishnan CG, Nishan AH, Gomathi S, Swaminathan GA. Energy and Trust Management Framework for MANET using Clustering Algorithm. *Wireless Personal Communications*. 2022;122. Available from: https://doi.org/10.1002/dac5138.

18) Dhage MR, Vemuru S. Trust based Secure Routing using Cross layer for Heterogeneous Environment in WSN. *International Journal of Emerging Trends in Engineering Research*. 2020;8(7):3241–3246. Available from: https://doi.org/10.30534/ijeter/2020/59872020.

19) Mukhedkar MM, Kolekar U. Hybrid PSGWO Algorithm for Trust-Based Secure Routing in MANET. *Journal of Networking and Communication Systems (JNACS)*. 2019;2(3). Available from: https://doi.org/10.46253/jnacs.v2i3.a1.

20) Kumar N. Battery power and trust based routing strategy for MANET. *In2014 IEEE International Conference on Advanced Communications, Control and Computing Technologies*. 2014;p. 1559–1562. Available from: https://doi.org/10.1109/icimia48430.2020.9074870.

21) Sarbhukan VV, Ragha L. Establishing Secure Routing Path Using Trust to Enhance Security in MANET. *Wireless Personal Communications*. 2020;110(1):245–255. Available from: https://doi.org/10.1007/s11277-019-06724-0.

22) Wahi C, Chakraverty S, Vandana Bhattacherjee. A trust-based secure AODV routing scheme for MANET. *International Journal of Ad Hoc and Ubiquitous Computing*. 2021;38(4):231–231. Available from: https://doi.org/10.1504/ijahuc.2021.119853.