International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2024/22 Volume 11, Issue 3, May – June (2024)

RESEARCH ARTICLE

Eigen Vector Based Trust Model (EVTM) for Ensuring Quality of Service (QoS) in Mobile Ad Hoc Networks

Srinivasulu Sirisala
Department of Computer Science and Engineering, CVR College of Engineering, Hyderabad, Telangana, India.
✉ vasusirisala@gmail.com

Nageswararao Sirisala
Department of Computer Science and Engineering, K.S.R.M. College of Engineering, kadapa, Andhra Pradesh, India.
nagsirisala@gmail.com

G. Rajeswarappa
Department of Computer Science and Engineering, G Pulla Reddy Engineering College, Kurnool, Andhra Pradesh, India.
rajeswarappa.cse@gprec.ac.in

Received: 03 March 2024 / Revised: 08 May 2024 / Accepted: 04 June 2024 / Published: 30 June 2024

Abstract – Mobile Ad Hoc Networks (MANETs) are the infrastructure less networks. In MANETs due to node's mobility there is frequent change of topology and nodes are provided with limited energy sources. Due to these reasons nodes may behave selfishly means they may deny forwarding other nodes' packets in order to save their energy. Hence it pivotal to compute the nodes' trust in MANETs for establishing reliable and secure communication paths. In MANETs, low trustworthiness of routes can significantly impact network performance. Therefore, it is strongly advisable to incorporate the trustworthiness evaluation of a node when considering it as an intermediate node. In this paper an Eigen Vector based Trust Model (EVTM) is proposed for ensuring QoS in establishing routing paths between source and destination. The proposed method constructs the global trust matrix and is used to compute the dominant eigen trust vector. It ranks the each intermediate node between source and destination based on node's fitness degree. Through experiments conducted in the ns-2 simulator, the method demonstrates superior performance across various metrics, including throughput, packet delivery ratio, packet delay, energy consumption, and packet drop. Notably, its consistent high performance, irrespective of the number of mobile nodes, underscores the effectiveness and scalability of the Eigen-based trust model in fostering trustworthy routing paths in MANETs.

Index Terms – Mobile Ad Hoc Networks, Trust Vector, Dominant Eigen Vector, Trust, Quality of Service (QoS), Global Trust Matrix (GTM).

1. INTRODUCTION

MANETs are composed with several collaborating nodes with limited energy and self-organizing potential. Applications for MANETs include military communications, isolated region survey, disaster assistance, and rescue, among others [1]. They understand the value of flexibility, safety, and mobility during communication [2]. In addition, MANETs require a group of collaborating nodes to self-organize into the network in order to communicate with one another and accomplish the shared objective of ensuring dependable and functional communication [3]. The packet forwarding method in this case extends the stretch of data dissemination over the single-hop networks via all the collaborative neighbour nodes [4]. Nevertheless, the mobile nodes typically have limited resources, and they occasionally might act selfishly. Secured routing has emerged as one of the main issues facing MANETs in the recent past [5]. The actions of malicious nodes within the network increase the likelihood of threats that could lead to unpredictable operations in MANETs [6]. In rare circumstances, such as the selfish behavior of mobile nodes, a reasonable node may oppose packet forwarding in order to further its own interests. The staging of network communication is severely harmed by the illogical behavior of nodes [7].Currently, it is thought to be extremely important that the mobile nodes adopt a possible packet forwarding technique. Additionally, widespread use of substantial packet

RESEARCH ARTICLE

forwarding method may increase the likelihood that transmissions over erratic channels will be successful [8]. To improve the network's life expectancy, it is required to conserve the energy depletion of the mobile nodes. At this juncture, it is required to take the node's trustworthiness [9] in to consideration in the routing process. Usually in manets node's trust is computed based on direct and indirect trust. The direct trust means, cooperation degree of a node comes to know in the direct interaction where as in-direct trust means, cooperation degree of a node comes to know through its neighbors [10]. As a result, to uphold the rate of collaboration amid the nodes, the network's maximum optimality must potentially mitigate the actions of malevolent and self-serving mobile nodes [11]. A wide range of cooperation-enforcing strategies, including game theory, probability dissemination founded trust, acknowledgement, watchdog, and game theory, have been published in the previous works. In recent decades to help potentially mitigate the impact of malicious nodes. When related to other mischievous node mitigation strategies in the literature, probability dissemination founded Trust tactics established to get an advantage [12] [13]. Usually Eigenvectors are utilized in optimization problems to find optimal solutions efficiently. Techniques like the Power Method leverage eigenvectors to approximate the dominant eigenvalue of matrices, which is useful in various optimization algorithms such as PageRank in web search ranking [14]. Eigen vector-based trust computation allows for decentralized trust management in MANETs, where nodes independently compute their trust scores based on local observations and interactions. This approach is robust to network dynamics and scalable as it does not rely on a central authority. Using Eigen vector based approach it is possible to compute the principal eigenvector of the adjacency matrix, which captures the network topology and nodes' attributes information, can be computed to derive trust scores for all nodes. Nodes with higher trust scores are deemed more reliable based on their interactions and attributes, reflecting a holistic view of trust in the network. In this paper, Eigen Vector based Trust Model (EVTM) proposed for constructing the routing paths with high trustworthiness intermediate nodes there by ensuring the QoS in the Manet. The Foremost Contributions of proposed EVTM are furnished as follows:

- It utilizes weighted sum model to compute each node trust out of the trust parameters (energy, packet drop, throughput and packet forwarding potential). It decides on weightage of each trust parameter is depends on application specific requirements.
- It uses Eigen vector-based model that consider the entire network topology and interactions among nodes, providing a global perspective on trust. This helps in forming a more accurate and comprehensive trust evaluation compared to localized models.

1.1. Motivation and Objective

MANETs are provided with inadequate resources (i.e. limited battery, memory and computational power). This limited resource constraint has the large impact on Quality of Service in MANETs. The node life time depends on its limited battery energy.

Further entire network performance goes down when node battery energy dropped below to the threshold level. Due to this reason, to remain in the network active node may behave selfishly by not supporting packet forwarding activity. This behavior of nodes leads to more packet retransmissions and ultimately effect on the routing reliability. Since it is important to judge the node's cooperative degree pertaining energy, packet delivery ratio, delay, jitter, band width, etc... Since in the proposed method trust is computed using Eigen vector approach.

Objective: Implementation of Eigen vector based trust computation method which ranks the each node based on its trust value.

1.2. Problem Statement

The intent of this research endeavor is to formulate multi attribute based approach to find cooperation degree (trust) of each node in the network thereby improve QoS in the routing path.

The other portions of the study are organized as, Section 2 gives a detailed literature assessment on recent trust evaluation methods, outlining their respective benefits and drawbacks. In Section 3, we delve into the computation of node trust, introducing the global matrix formulation and elucidating its updating process, subsequently exploring the determination of the fitness degree of a node. Section 4 is describes the simulation findings, while Section 5 provides a concluding summary, emphasizing the major contributions of the proposed scheme.

2. RELATED WORK

Manoranjini et al. [15] proposed an enhanced cooperation degree-based cooperation enforcing scheme aimed at improving the network's ability to detect and prevent malicious nodes. The approach focused on incorporating various trust metrics to comprehensively assess the conduct of every mobile node, relying on associations established among them. The trust metrics included QoS trust, service trait trust, and social trait trusts, collectively influencing the determination of the legitimacy of mobile nodes throughout their collaboration processes.

This scheme prioritized data privacy and underwent performance testing in diverse scenarios, evaluating trust in various dimensions. Comparative analyses between scenarios with and without trust considerations demonstrated improved

RESEARCH ARTICLE

performance across key metrics, including missed detection rate, false receiving rate, cooperation degree, energy ingesting, packet loss, and whole throughput. Although the trust-based collaboration enforcing scheme exhibited notable advancements, the level of cooperation achieved remained modest. Furthermore, it was observed that the control and overall burden of the trust approach were relatively predominant when compared to alternative approaches.

Sirisala.S et al. [16] proposed FCOPRAS-MADM approach focused on identifying the greedy and mischievous nodes based on Fuzzy Set Theory (FST) and COPRAS Model. Where FST used to generate crisp value for the neighbor node recommendations which are in the fuzzy form.

COPRAS model handled the uncertainty observed in the information as it is taken from different nodes. Despite its effectiveness in detecting selfish nodes, the impractical computational demands associated with processing fuzzy logic and conducting intricate calculations limit the overall sustainability of the fuzzy COPRAS model.

Roles & ElAarag [17] introduced a reputation approach based Bayesian Game theory for detecting mischievous nodes, specifically designed to address the challenges posed by selfish nodes in scenarios with insufficient information. Within the context of an aggressor/protector game, where the protector lacks knowledge about its opponent, policy decisions must be made based on limited evidence. Malevolent nodes strategically try to evade detection by posing normal nodes, providing seemingly beneficial network functionality.

It becomes particularly crucial in resource-constrained networks with selfish nodes. The proposed model presents a robust solution, distinct from previous approaches, demonstrating effectiveness in identifying installations inside MANETs. The defender assesses the prevalence and utility of malicious nodes based on the specific application, showcasing the model's adaptability. Notably, the proposed approach exhibits improved power consumption efficiency, a critical consideration in energy-conscious node environments is the nodes may not function collectively.

Kavitha et al. [18] introduced the Feature Extraction-based mechanism for Intruder Node Detection and Isolation (FS-INDISM) to enhance secure routing and cooperation in networks. Employing feature extraction, optimization, and classification, this mechanism discriminates between malicious and genuine nodes. It strategically utilizes trust parameters from each mobile node, optimizing them via particle swarm optimization (PSO) to achieve an optimal combination in the process of the avoiding of mischievous nodes in the path of communication.

The method integrates Neural Network (NN) as a categorizer for accurate ascertainment of intrusive nodes. Assessment of Performance, encompassing communiqué delay, energy consumption, and packet delivery attainment rate, underscores FS-INDISM's efficacy in enhancing malicious node isolation during data dissemination.

Xia et al. [19] introduced a Subjective Trust Framework (STF) characterized by its computationally efficient trust assessment and prediction processes, integrating historical node behavior into the trust evaluation for establishing the trust data sequence. Employing a weighted Markov Chain (SCGM) measure, STF enhances futuristic decision-making, particularly in the context of the baseline on-demand routing protocol (ODMRP).

Results, in comparison with FS-INDISM, affirm the significance of STF in optimizing packet transfer, throughput, network delay, and control overhead. Despite notable accomplishments, the 95.45% estimate exactness of SCGM suggests room for further enhancement.

Ponguwala and Rao [20] proposed the Secure Routing using Energy Efficiency Framework (SREEF) to ensure data reliability and safety within ad hoc networks. SREEF incorporates a validation scheme leveraging certificate-based hash chains and integrates cluster formation with a secure verification process, employing elliptic curve verification.

The model introduces a worst-case Particle Swarm Optimization (PSO)-based secure routing strategy, enhancing security through a dual-state Markov chain model. Additionally, SREEF employs a dual XOR-based Fuzzy Assessing Cipher Encryption procedure to ensure capitalize on data reliability. Comparative assessments against benchmarked approaches affirm SREEF's efficacy in improving network competence quantifiers such as packet transfer success degree, residual energy, and throughput.

H. Xia et al. [21] articulated a framework that enhances security in MANETs by evaluating and forecasting node trust based on historical behavior patterns. It integrates the SCGM (11)-weighted Markov stochastic chain for trust prediction and introduces the Dynamic Trust - Based Multicast Routing Protocol (DTMRP). This novel protocol, validated through experiments, shows marked improvements in network security.

X. Song et al. [22] improved the original artificial bee colony (ABC) algorithm by adding a mechanism to detect global optimal stagnation. When stagnation occurs, eigenvectors of the covariance matrix are employed to generate multidimensional candidate solutions, enhancing exploration. The ECMABC algorithm, evaluated using the CEC2014 function set, demonstrates superior effectiveness compared to other advanced ABC algorithms.

The Summary of literature discussed here is presented in the Table 1.

RESEARCH ARTICLE

Table 1 Comparison of Trust Finding Schemes

Author	Method/Algorithm	Merits	Limitations
Manoranjini et al. [15]	Improved Trust Detection Algorithm for Black Hole Node Prevention	-Utilizes a comprehensive Trust Detection Algorithm to identify and prevent Black Hole nodes, enhancing network security. It nntegrates various trust metrics (e.g., relationship, social, service attribute, QoS) for a holistic view of node behaviour	-Effectiveness heavily depends on the accuracy of trust metrics and the reliability of the proposed detection algorithm. - May require significant computational overhead and communication cost to continuously monitor and update trust metrics.
Sirisala.S et al. [16]	FCOPRAS-NCETE Scheme for Trust Estimation in Reliable Data Dissemination	- Utilizes fuzzy COPRAS-based approach to rank intermediate nodes for trust assessment, enhancing QoS during data dissemination. - Incorporates fuzzy set theory for effective trust estimation in dynamic MANET environments.	- Complexity of fuzzy logic implementation and performance impact on resource-constrained nodes. - Requires fine-tuning of parameters and may not be easily scalable to large-scale MANETs.
Roles & ElAarag [17]	Bayesian Game Approach for Cohabitation with Mischievous and greedy nodes	- Models node perception as a Bayesian game with inadequate data, enabling identification of malicious and selfish nodes.	- Bayesian game assumptions may not fully capture the dynamic and complex behaviors of nodes in MANETs.
Kavitha et al. [18]	INDIA for Intruder Node Detection and Isolation in MANETs	- Employs feature acquisition, fine tuning, and categorization approaches for low harmful intruder identification and avoidance. - Utilizes Particle Swarm Optimization (PSO) for feature fine-tuning, enhancing accuracy of node classification.	- Performance heavily relies on the effectiveness of feature extraction and classification algorithms. - May face challenges in handling dynamic network conditions and evolving attack strategies.
Xia et al. [19]	Lightweight Subjective Trust Inference Framework in MANETs	- Proposes a novel trust inference structure based on historical behaviors and Markov chain modeling for future trust prediction. - Offers a subjective trust model that adapts to node behaviors over time, improving security and cooperation among MANET participants.	- Provides lightweight trust assessment suitable for resource-constrained MANETs. - Reliance on historical data may not fully capture real-time node behaviors and interactions.
Ponguwala and Rao [20]	E2-SR for Energy-Efficient Secure Routing in MANET-IoT	-Integrates certificate-based authentication, cluster formation, and secure communicative algorithms to safeguard MANET - IoT networks against adversaries. - Utilizes novel encryption and optimization techniques (e.g., WC-PSO, DS-MCM) for enhanced data security and integrity.	- Complexity of proposed algorithms and protocols may impact scalability and resource utilization. -Implementation overhead and computational requirements may challenge adoption in resource-limited IoT environments.

RESEARCH ARTICLE

H. Xia et al.[21]	Lightweight Subjective Trust Inference Framework Uses SCGM(11)-weighted Markov stochastic chain for trust prediction Introduces Dynamic Trust - Based Multicast Routing Protocol (DTMRP)	- Enhances security in MANETs by accurately assessing and predicting node trust - Utilizes historical behavior data for reliable trust evaluation - Demonstrates significant improvements in network security through experimental validation	- May require extensive historical data for accurate trust assessment - The complexity of implementing the SCGM(11)-weighted Markov model - Potentially higher computational overhead compared to simpler trust models
X. Song et al.[22]	Improved Artificial Bee Colony (ABC) Algorithm incorporates eigenvectors of the covariance matrix when global optimal stagnation is detected	- Improves exploration capabilities by generating multidimensional candidate solutions - Effectively utilizes elite solution information in the search process - Shows superior performance on the CEC2014 function set compared to other improved ABC algorithms	- Increased computational complexity due to the use of covariance matrix eigenvectors - May require more computational resources for managing multidimensional candidate solutions

3. PROPOSED EIGEN VECTOR BASED TRUST MODEL (EVTM)

The Eigen-based trust model for MANETs employs a mathematical approach to compute the cooperative degree of nodes within the network. This model begins with the selection of trust factors such as packet advancing ratio, throughput, energy consumption, and packet delay, which are crucial indicators of node reliability and performance. Why because, let's consider an instance of node with limited energy sources, may behave selfishly and do not support any packet forwarding activity that could benefit their neighbouring nodes. Hence for trust computation the above said parameters are pivotal. Through data collection and evaluation, a trust matrix is constructed, where rows signify source nodes and columns signify target nodes, with entries indicating the trust degrees between nodes through observed behaviors. Subsequently, the dominant eigenvector corresponding to the largest eigenvalue of the trust matrix is computed using methods like the power iteration method, providing steady-state trust values for nodes. This iterative process converges to a vector of trust values, reflecting the perceived reliability of nodes in the network. By taking direct and indirect communications into consideration, this model enables the ranking of nodes based on their computed trust values, facilitating efficient and reliable communication within the MANET. The steps of EVTM are detailed below.

3.1. Construction of Trust

Step 1: Each mobile node mn_i collects the " q " trust attributes' information of each and every other node mn_j in the network through direct and indirect interactions. The trust information of each other node is taken into a separate trust Attribute Vector represented as in Eq. (1).

$$AV_{MN_J} = [a_1, a_2, \dots \dots a_q] \quad (1)$$

Where,

mn_j(j=1,2,……n) is mobile node and a_i (i=1,2,……q) is the trust attribute value.

Step 2: Perform normalization over the trust vector to ensure all parameters are on the same scale, allowing for fair comparison and combination. Normalization is performed using Eq. (2).

$$a_i^N = \frac{original\ value(\ a_i) - Min\ value\ (a_i)}{Max\ value(a_i) - Minvalue(a_i)} \quad (2)$$

Where,

- Original Value is the raw value of the trust parameter for the node.
- Min-Value is the smallest value of the trust parameter observed across all nodes.
- Max-Value is the largest value of the trust parameter observed across all nodes.

Normalized Attribute Vector represented in Eq. (3)

$$AV_{MN_J}^N = \left[a_1^N, a_2^N, \dots . a_q^N\right] \quad (3)$$

Step 3: The trust vector of node shown in Eq. (4) is determined through weighted sum approach by taking different weights to each attribute using Eq. (5).

RESEARCH ARTICLE

$$TV_{MN_i} = [DT_{MN_1}, DT_{MN_2}, \ldots\ldots\ldots DT_{MN_n}] \quad (4)$$

Here,

$$DT_{MNj} = \frac{W_1.a_1^N + W_2.a_2^N + \cdots\ldots\ldots\ldots + W_q.a_q^N}{No.of\ Attributes} \quad (5)$$

Here,

TV_{MN_i} is the trust vector of node "i". In trust vector each entry DT_{MN_j} (j=1, 2…….n) is the aggregated degree of trust value of each node in the network. And Weights W_i (i = 1, 2…….q) are weights of trust attributes and are selected based on application specific QoS requirements. The attribute weights are represented as linguistic variables. Table 2. displays the weights of attributes within the fractional range of 0 to 1.

Table 2 Attribute Weights their Ranges

Attribute Weights	Range
Very Low (VL)	[0.0 - 0.1]
Low (L)	[0.1 - 0.3]
Medium Low (ML)	[0,3 - 0.4]
Medium (M)	[0.4 - 0.5]
Medium High (MH)	[0.5 - 0.6]
High (H)	[0.6 - 0.9]
Very High (VH)	[0.9 - 1.0]

Step 4: Construct the Global Trust Matrix (GTM) from all nodes trust vector and is represented in Eq. (6).

$$GTM = \begin{bmatrix} DT_{MN_{11}} & DT_{MN_{12}} & \cdots & DT_{MN_{1n}} \\ DT_{MN_{21}} & DT_{MN_{22}} & \ldots & DT_{MN_{2n}} \\ \vdots & \vdots & \vdots & \vdots \\ DT_{MN_{n1}} & DT_{MN_{n2}} & \cdots & DT_{MN_{nn}} \end{bmatrix} \quad (6)$$

- Rows represent the source nodes (the nodes from which trust is being evaluated).
- Columns represent the target nodes (the nodes to which trust is being evaluated).

Each entry in the trust matrix denotes the trustworthiness of a target node from the perspective of a source node. For example, if we consider node A as the source node, the entries in the first row of the matrix represent the trust values of node A towards remaining nodes in the network.

3.2. Construction of Dominant Eigenvector

In the context of the trust matrix, the dominant eigenvector represents the steady-state trust values of nodes. Each element of the eigenvector corresponds to the trust value of a specific node in the network. The dominant eigenvector captures the relative trustworthiness of nodes as perceived by the network, considering both direct and indirect trust relationships. The eigenvalue associated with the dominant eigenvector indicates the rate of convergence of the iterative process used to compute the eigenvector. A larger eigenvalue signifies faster convergence and stronger influence of the corresponding eigenvector on the trust values.

Steps involved in the computation of Dominant Eigen vector as follows:

Step1: The vector "V" represents an approximation of the dominant eigenvector at each iteration k. This vector indicates the current estimate of the steady-state trust values of nodes in the network as perceived by node A and is represented using Eq. (7).

$$V_k = [1 \quad 1 \quad \ldots. \quad 1] \quad (7)$$

Initial vector V_0 chosen as a vector of all ones (the highest trust value).

Step 2: The power iteration method is an iterative algorithm used to find the dominant eigenvector of a global trust matrix. Throughout the iterations of the power iteration method, the vector "V" is updated based on the trust matrix's multiplication with Vector V and normalization until convergence. The final vector obtained after convergence represents the dominant eigenvector, providing insights into the relative trustworthiness of nodes in the network.

In each iteration global trust matrix – vector (V) product is performed and the resulting current estimate of the steady-state dominant eigenvector is shown in Eq. (8).

$$V_k = [tv_{kMN1} \quad tv_{kMN2} \quad \ldots\ldots \quad tv_{kMNn}] \quad (8)$$

Here, tv_{kMNi} (i=1,2…n) is current estimate of dominant eigenvector value of each mobile node in iteration "k" and is computed using Eq. (9)

$$tv_{kMNi} = DT_{MN_{ij}}.tv_{k-1MNi} + DT_{MN_{ij}}.tv_{k-1MNi} + \ldots\ldots\ldots\ldots + DT_{MN_{ij}}.tv_{MNi} \quad (9)$$

In Eq. (9) DT_{MNij} (for every i = 1, 2 … n. j varies 1, 2, … n).

After performing above product, in the power iteration method for computing the dominant eigenvector, normalization is typically performed after each iteration. The normalization step ensures the resulting vector maintains a consistent magnitude or unit length, allowing for a stable convergence towards the dominant eigenvector. It helps prevent any single component of the vector from dominating the others, ensuring a balanced representation of trust values.

In normalization process resulting vector (V_k) each element divided by the vector's Euclidean norm (magnitude). This ensures that the vector's length remains 1 (unit length) after

RESEARCH ARTICLE

normalization. After normalization updated vector is expressed using Eq. (10).

$$\hat{V} = \frac{V_k}{\|V_k\|} \quad (10)$$

Where $\|V_k\|$ denotes the Euclidean norm of the vector V_k, calculated as the square root of the sum of its elements.

For the next iteration $\hat{V}$ will act as vector "V".

Step 3: Once the change in the vector elements or the dominant eigenvalue falls below the specified threshold (i.e. updating of vector happens until difference between V_K and V_{k-1} is significantly very less (i.e. less than 0.05), the iterative process is considered to have converged, and the computed vector is accepted as the dominant eigenvector approximation.

Based on final dominant eigenvector trust values each node is given with rank in the order of their trust values high to low and low ranked nodes (less than 40%) are isolated during path construction between source and destination nodes there by ensuring the QoS in the network. The pseudo steps are detailed in the Algorithm 1.

1. Input: Global Trust Matrix
2. Output : Dominant Eigenvector with steady-state trust values of nodes.
3. initialize vector V with random values or ones
4. set convergence_threshold //i.e. difference between V_K and V_{k-1} is significantly very less (i.e. less than 0.05)
5. iteration = 0
6. // Iteration
7. repeat until convergence or max_iterations reached:
   a. // Compute matrix-vector product
   b. vector Mv = trust_matrix * V
   c. // Normalize resulting vector
      vector v_next = normalize(Mv)
   d. // Check for convergence
      if ||v_next - v|| < convergence_threshold:
         break
      else
         // Update vector for next iteration
         V = v_next
      iteration += 1

Algorithm1 Dominant_Eigenvector

Figure 1 details the Steps entailed in the proposed EVTM.

3.3. Example

Let us consider a Manet with four nodes A, B, C, and D. And Trust parameters as Energy consumption, throughput, Packet forwarding ratio, and delay.

Step1: For ex, A node collects trust information of B, C, D into a vector using Eq. (1).

$$AV_{MN_B} = [6, 10, 70, 4]$$

$$AV_{MN_C} = [7, 14, 80, 3]$$

$$AV_{MN_D} = [5, 11, 60, 2]$$

Step 2: Normalization takes place in this step to bring different ranged parameters' values into a common range (0 to1) as the target trust usually measured in the range of (0 to1). Normalization performed using Eq. (2).

For ex: parameter (energy Consumption) value of node B is normalized as follows.

$$AV^N_{MNB} = (6-5)/(7-5) = 0.2$$

Similarly all other parameters normalized values will be computed. After all, Attribute vectors of all nodes seems to be as follows

$$AV_{MN_B} = [0.2, 0, 0.2, 1]$$

$$AV_{MN_C} = [1, 1, 1, 0.2]$$

$$AV_{MN_D} = [0, 0.25, 0, 0]$$

Step 3: Weighted trust values of nodes [B, C, and D] are computed using Eq. (4) by taking weights as per application requirements. For ex: for military operation application the weights of parameters [Energy, throughput, Packet forwarding ratio, delay] are [High (0.9), High (0.9), High (0.9), and low (0.3)].

$$DT_{MN_B} = 0.9 * 0.2 + 0 * 0.9 + 0.2 * 0.9 + 1 * 0.3 = 0.66$$

Similarly the other nodes C and D weighted trust values (0.69, 0.05) will be calculated and represented through following Trust Vector of node A.

$$TV_{MN_A} = [0.66 \quad 0.69 \quad 0.05]$$

Similarly, Trust vectors of B, C, and D will be computed.

Step 4: Using above computed Trust Vectors of every node, the Global Trust Matrix (GTM) is computed using Eq. (5).

$$GTM = \begin{bmatrix} 0.78 & 0.66 & 0.69 & 0.05 \\ 0.7 & 0.56 & 0.49 & 0.55 \\ 0.62 & 0.79 & 0.81 & 0.69 \\ 0.56 & 0.74 & 0.81 & 0.88 \end{bmatrix}$$

Here GTM represents the every node's trust perception on other nodes in the network. i.e. first row gives node A trust

RESEARCH ARTICLE

opinion on itself and B, C, and D. similarly B, C and D nodes' trust opinion on other nodes represented in other rows respectively.

Step 5: Deriving Dominant Vector:

Take initial vector $V_0 = [1, 1, 1, 1]$

Here V_0 represents the vector of trust values of each node assumed to be with highest trust. Further each node's trust is updated through the operations: product of GTM and V_k and normalization. This updating process takes place in iterations till we get a steady state of dominant vector computed.

Product operation of GTM and V_k (where "k" represents iterations 0 to k) is done using Eq. (8).

Iteration 1:

$$\begin{bmatrix} 0.78 & 0.66 & 0.69 & 0.05 \\ 0.7 & 0.56 & 0.49 & 0.55 \\ 0.62 & 0.79 & 0.81 & 0.69 \\ 0.56 & 0.74 & 0.81 & 0.88 \end{bmatrix} .[1, 1, 1, 1] = [2.66, 2.3, 2.91, 2.99]$$

Normalization: in this operation trust values of nodes (i.e. vector values) are divided by Euclidean norm using Eq. (9). This normalization process ensures the cooperative degree values fall in the range of 0 to 1.

Here Euclidian norm is the square root taken for the sum of the trust values.

For ex: normalized value of 2.66 is

$(2.66/\sqrt{}\ (2.66+2.3+2.91+2.99)=0.80.$

Similarly other values are computed. Therefore, after iteration 1 the dominant trust vector V1 =[0.80,0.69 ,0.88,0.90].

This process of updating vector happens until difference between V_K and V_{k-1} is significantly very less (i.e. less than 0.05) and this state considered as study state of convergence.

With the current example after three iterations the vector has reached a study state and it is required dominant vector representing trust values of each node.

Dominant trust Vector = [0.65 0.42 0.86 0.88]

Using this Dominant trust vector nodes are ranked. i.e. the nodes with trust value greater than 0.40 are considered and they ranked in the order of their trust values highest to lowest.

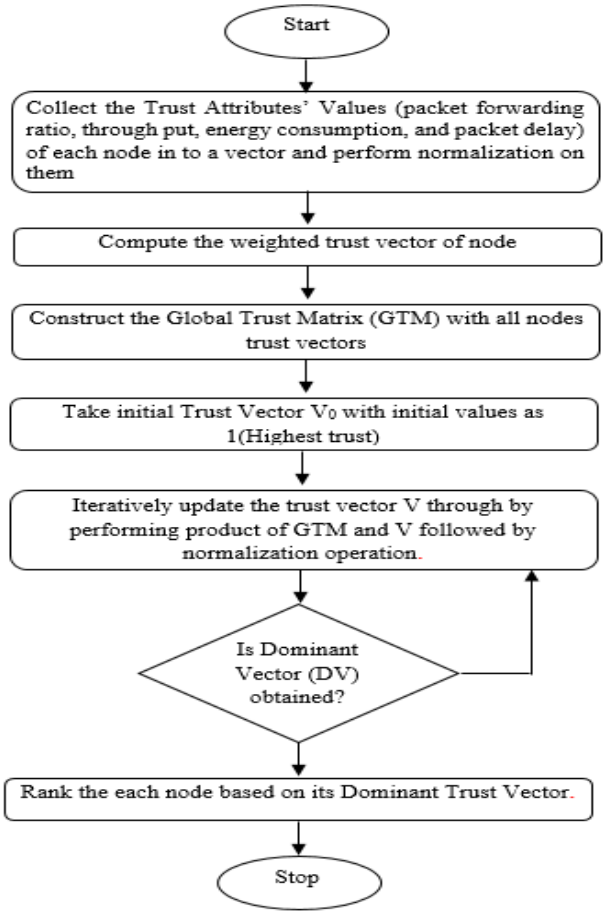

Figure 1 Flow Chart of Proposed EVTM

International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2024/22 Volume 11, Issue 3, May – June (2024)

RESEARCH ARTICLE

4. SIMULATION RESULTS AND DISCUSSION

The simulation outcomes of the proposed Eigen Vector Founded Trust Model (EVTM) and the FS-INDISM, SREEF, and FCOPRAS approaches, conducted using the ns-2.34. Results are crucial for understanding the efficacy of EVTM in MANET scenarios. The AODV protocol [23, 24] served as the foundational routing protocol within the MANET architecture, facilitating dynamic decision-making processes. In this simulation environment, 100 mobile nodes traversed a terrain area of 1000 x 1000 square meters.

The varying presence of malicious nodes, ranging from 5 to 50, allowed for an exploration of their impact on the performance of the EVTM scheme. These malicious nodes were programmed to drop packets at rates between 60% and 80%. The simulation incorporates a direct cooperation mechanism among 40 source and destination pairs. It adopts a constant bit rate traffic model, maintaining a steady pace of five packets per second.

Furthermore, a pause time of 50 seconds is employed in the simulation settings. The entire implementation of the proposed Eigen Vector Based Trust Model (EVTM) spans a simulation time of precisely 13.45 minutes. The Experimental setup used is furnished in Table 3.

Table 3 Simulation Environment of the Proposed EVTM

Simulation Metric	Value
mobile nodes count	100
Routing protocol	AODV
Experiment duration	13.45 min
source- destination sets	40
Packet loss rate	60 % - 80 %
Packet – length	512 B
Pause time	50 Sec
Degree of movement	15 m/s
Mobility extent	1000 x1000 Sqm
Span of communication	250 m
Speed	2 Kbps
Movement model	Random Way Point model
Model of traffic	Constant Bit Rate (CBR)

4.1. Parameters – Metrics

The performance of EVTM against the other benchmark methods is compared through various attributes. Those parameters and their metrics are listed in the Table 4.

Table 4 Attributes – Metrics

Attribute	Metric
Energy	Jouls
Packet forwarding ratio	Percentage (%)
Through put	KBPS (Kilo Bytes Per Second)
Mean Delay	Milli Seconds

The proposed method EVTM is compared against the bench mark approaches FS-INDISM, SREEF, and FCOPRAS in regard to diverse amount of nodes and mischievous nodes. Figure 2, 3, and 4 show evaluation involved assessing the performance of EVTM alongside FS-INDISM, SREEF, and FCOPRAS concerning metrics such as packet dissemination ratio, through put, and energy ingestion under varied amount of nodes.

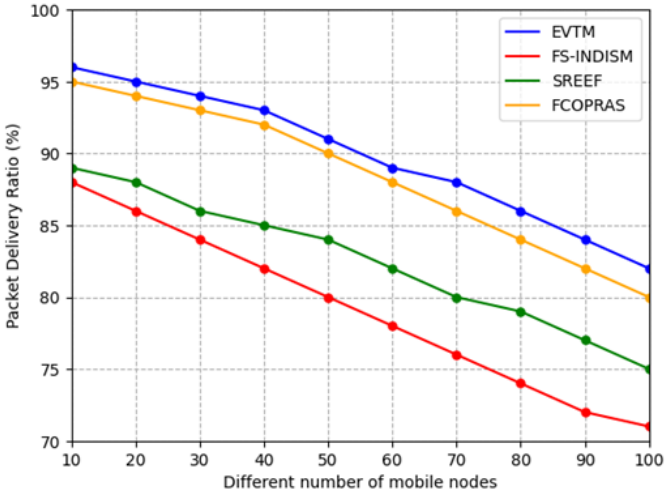

Figure 2 Proposed EVTM-Packet Delivery Rate for Varied Amount of Nodes

In Figure 2 the packet dissemination rates of both the EVTM and former considered tactics decrease with the amount of mobile nodes due to increased packet generation and forwarding requirements. However, the proposed EVTM maintains a consistently high delivery rate compared to baseline schemes. EVTM shown an improvement of packet delivery ratio 9.09%, 7.87%, and 1.05% with FS-INDISM, SREEF, and FCOPRAS.

Figure 3 illustrates the throughput observed through proposed EVTM and benchmarked approaches across varying numbers of nodes. The average throughput in EVTM shows a systematic decline with increasing mobile nodes. Nonetheless, EVTM manages to sustain throughput at acceptable levels compared to FS-INDISM, SREEF, and FCOPRAS. EVTMT

RESEARCH ARTICLE

is approximately 16.09%, 12.23%, and 11.05% better than FS-INDISM, SREEF, and FCOPRAS in terms of throughput.

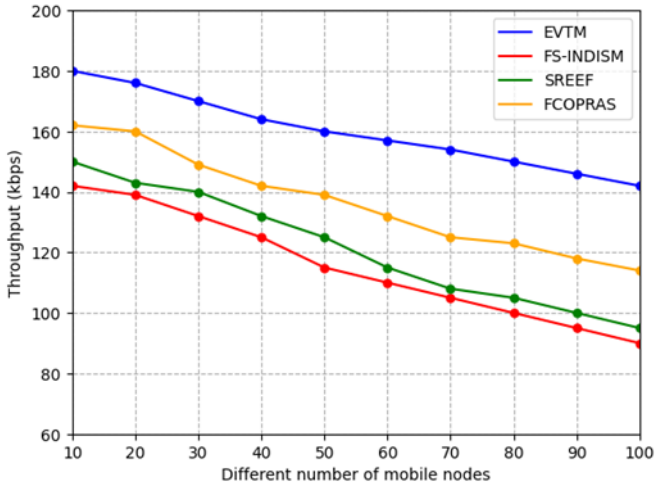

Figure 3 Proposed EVTM-Throughput for Varied Amount of Nodes

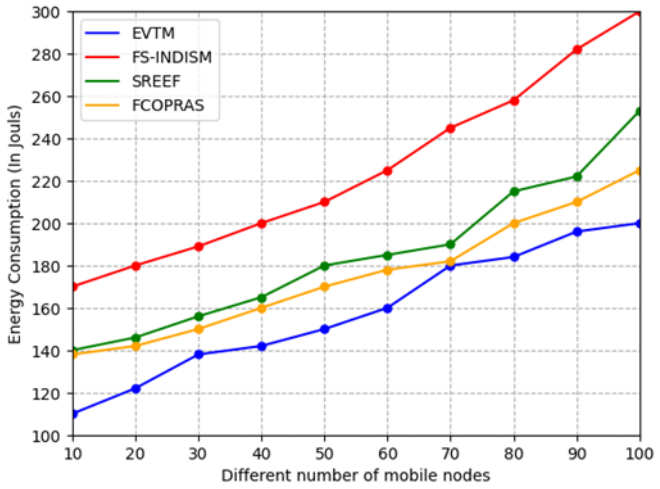

Figure 4 Proposed EVTM-Energy Consumption for Varied Amount of Nodes

Figure 4 demonstrates the performance of EVTM against the approaches FCOPRAS, SREEF, FS-INDISM pertaining to energy ingesting. From the results it is observed that, the amount of nodes is augmented in the network the energy consumption of EVTM has gradually increased along with other approaches. But the energy consumption is confined to the moderate levels. EVTM is approximately exhibits an improvement of 11.11%, 14.24%, and 16.76% with FCOPRAS, SREEF, and FS- INDISM respectively.

Further it was analysed the performance of proposed EVTM against the benchmarked techniques with increased amount of malicious nodes.

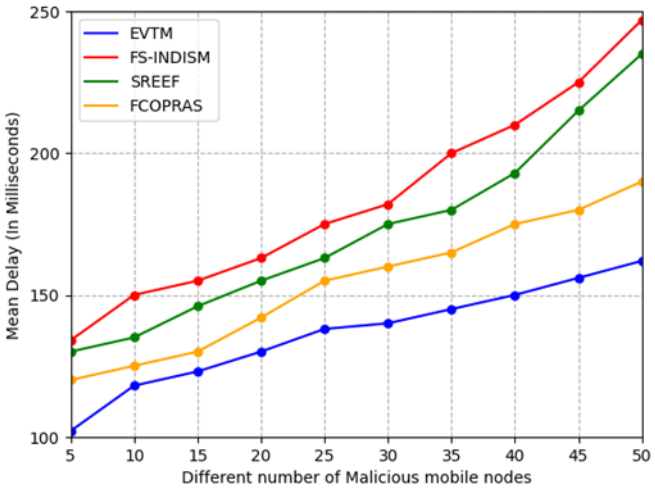

Figure 5 Proposed EVTM-Mean Delay for Varied Amount of Mischievous Mobile Nodes

Figure 5 depicts average delay increases with the amount of malicious nodes, as more malicious nodes lead to higher packet drop rates and increased forwarding time. However, EVTM, leveraging power iteration method for rapid malicious node detection, sustains delay similar to baseline approaches, ensuring network performance remains stable. EVTM showcases a significant improvement of 11.74%, 13.49%, and 14.79 % with FCOPRAS, SREEF, and FS-INDISM respectively.

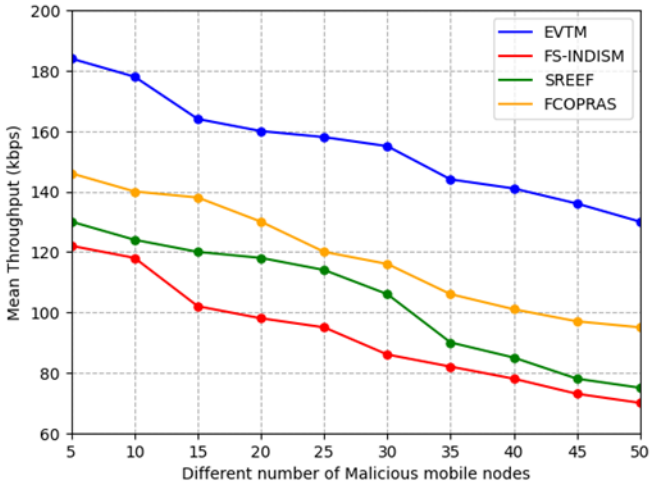

Figure 6 Proposed EVTM-Mean Throughput for Varied Amount of Malicious Nodes

Figure 6 illustrates the average throughput of the EVTM and former FS - INDISM, SREEF, and FCOPRAS tactics across varying numbers of mischievous nodes. EVTM exhibits a systematic decrease in throughput with increasing malicious nodes, attributed to intentional or selfish packet drops.

RESEARCH ARTICLE

However, it maintains throughput at an acceptable level compared to the benchmarks.

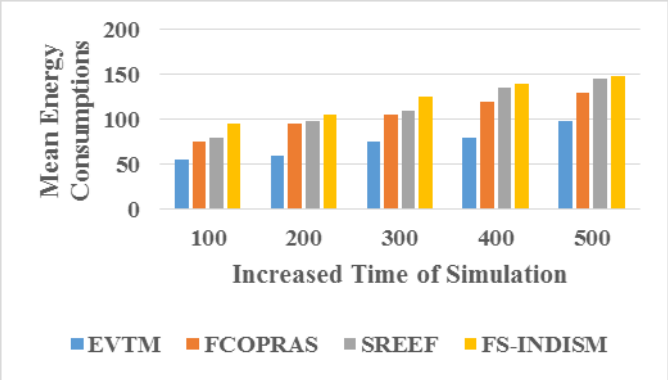

Figure 7 Proposed EVTM-Mean Energy Consumption with Increased Time of Simulation

Figure 7 illustrates the average energy feastings of the EVTM and the earlier FS-INDISM, SREEF, and FCOPRAS approaches as the simulation time increases. Results consistently show that the energy consumption in EVTM remains lower regardless of the simulation duration. This reduced consumption is attributed to EVTM's efficient approach to trust computation, enabling accurate conjecturing of node behaviour in the paths of communication.

In results the projected EVTM performance is tested using the attributes packet dissemination degree, throughput and energy ingesting with increased amount of mobile nodes in the network and average throughput, delay and energy consumption with increased amount of malicious nodes in the network. In these two scenarios EVTM outperformed than other approaches, as it is considering every node's opinion (global) while assessing nodes trust along with that power iteration method used to achieve steady state of trust.

5. CONCLUSION AND FUTURE WORK

The Eigen Vector based Trust Model (EVTM) proposed a robust framework for ensuring QoS in MANETs by accurately evaluating the trustworthiness of network nodes. By incorporating key trust parameters viz.: packet dissemination rate, throughput, energy utilization, and packet delay, EVTM constructs a global trust matrix and computes the dominant eigenvector, providing steady-state trust values for nodes. By comparing EVTM against benchmarked approaches FS-INDISM, SREEF, and FCOPRAS, it becomes evident that EVTM consistently outperforms pertaining to packet dissemination rate, throughput, energy utilization, and average delay. Even in scenarios with increased amount of nodes and mischievous actors, EVTM demonstrates robustness and scalability, maintaining network performance at acceptable levels. Further research into dynamic trust adaptation may involve leveraging machine learning approaches to compute node trust, incorporating past behavior as a key factor in the trust evaluation process.

REFERENCES

[1] S. Vassilaras, D. Vogiatzis, and G. S. Yovanof, "Security and Cooperation in clustered mobile ad hoc networks with centralized supervision", IEEE Journal on Selected Areas in Communications, 2006, Vol. 24, No. 2, pp. 329-342.
[2] G. Dhananjayan and J. Subbiah, "T2AR: trust-aware ad-hoc routing protocol for MANET", SpringerPlus, , 2016, Vol. 5, 995.
[3] M. S. Khan, M. I. Khan, S. Malik, O. Khalid, M. Azim, and N. Javaid, "MATF: A multi-attribute trust framework for MANETs", EURASIP Journal on Wireless Communications and Networking, 2016.
[4] Y. Li and X. Wu, "Cooperative packet-forwarding strategies in mobile ad hoc networks with unreliable channels: An evolutionary game approach", International Journal of Distributed SensorNetworks, 2019.
[5] K. RahimiZadeh and P. Kabiri, "Trust-based routing method using a mobility-based clustering approach in mobile ad hoc networks", Security Comm. Networks, 2014, Vol. 7, pp. 1746-1763.
[6] S. NageswaraRao and C. Shobabindu, "Uncertain Rule Based Fuzzy Logic QoS Trust Model in MANETs", International Conference on Advanced Computing and Communications -ADCOM, 2015,,pp. 55-60.
[7] A. Dorri, "An EDRI-based approach for detecting and eliminating cooperative black hole nodes in MANET", Wireless Netw. , 2014,Vol. 23, pp. 1767-1778.
[8] L. G. Delgado, E. P. Segarra, and A. M. Mezher, "A novel dynamic reputation-based source routing protocol for mobile ad hoc networks", J Wireless Com Network 2019, Vol. 77.
[9] J. -H. Cho, A. Swami and I. -R. Chen, "A Survey on Trust Management for Mobile Ad Hoc Networks," in IEEE Communications Surveys & Tutorials, vol. 13, no. 4, pp. 562-583, Fourth Quarter 2011, doi: 10.1109/SURV.2011.092110.00088.
[10] Sirisala, Nageswara & Chigarapalle, Shoba. (2017). "A novel QoS trust computation in MANETs using fuzzy petri nets". International Journal of Intelligent Engineering and Systems. 10. 116-125. 10.22266/ijies2017.0430.13.
[11] Sirisala, Srinivasulu & Ramakrishna, S.. "Survey: Enhanced Trust Management for Improving QoS in MANETs": AICC 2018. 2019, 10.1007/978-981-13-1580-0_25.
[12] N. Ramya and S. Rathi, "Detection of selfish Nodes in MANET - a survey," 2016 3rd International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2016, pp. 1-6, doi: 10.1109/ICACCS.2016.7586378.
[13] S. Janakiraman and B. B. Jayasingh, "A Hyper Exponential Factor-Based Semi-Markov Prediction Mechanism for Selfish Rendezvous Nodes in MANETs", Wireless Pers Commun., 2019,Vol. 108, pp. 1493-1511
[14] Savita, Verma, A. Eigen Vector Centrality (EVC) Routing for Delay Tolerant Networks: A Time Associated Matrix-Based Approach. Wireless Pers Commun 128, 2023, 1217–1233
[15] J. Manoranjini, A. Chandrasekar, and S. Jothi, "Improved QoS and avoidance of black hole attacks in MANET using trust detection framework", Automatika, 2019, pp. 274-284.
[16] Sirisala, S., Rama Krishna, S.: Fuzzy COPRAS-based Node Cooperation Enforcing Trust Estimation Scheme for enhancing Quality of Service (QoS) during reliable data dissemination in MANETs. Int. J. Commun. Syst. 34(7), e4767 (2021). https://doi.org/10.1002/dac.4767
[17] Roles A, ElAarag H. Coexistence with malicious and selfish nodes in wireless ad hoc networks: A Bayesian game approach. J Algorithm Comput Technol. 2017;11(4):353-365.
[18] T. Kavitha, K. Geetha, and R. Muthaiah, "India: Intruder Node Detection and Isolation Action in Mobile Ad Hoc Networks Using Feature Optimization and Classification Approach", J Med Syst., 2019,Vol. 43.
[19] H. Xia, Z. Li, Y. Zheng, A. Liu, Y. Choi, and H. Sekiya, "A Novel Light-Weight Subjective Trust Inference Framework in MANETs",

RESEARCH ARTICLE

IEEE Transactions on Sustainable Computing, 2020, Vol. 5, No. 2, pp. 236-248.
[20] M. Ponguwala and S. Rao, "E2-SR: a novel energy-efficient secure routing scheme to protect MANET-IoT", IET Communications, , 2019, Vol. 13, No. 19, pp. 3207-3216.
[21] H. Xia, Z. Li, Y. Zheng, A. Liu, Y. -J. Choi and H. Sekiya, "A Novel Light-Weight Subjective Trust Inference Framework in MANETs," in IEEE Transactions on Sustainable Computing, 2020, vol. 5, no. 2, pp. 236-248.
[22] X. Song, Y. Fu and M. Zhao, "Improved Artificial Bee Colony Algorithm Based on Eigenvectors of Covariance Matrix," 2023 2nd International Conference on Computing, Communication, Perception and Quantum Technology (CCPQT), Xiamen, China, 2023, pp. 39-45, doi: 10.1109/CCPQT60491.2023.00013.
[23] W. G. Kumar, K. S. Kumar, and S. K. Mutto, "Trust framework for attack resilience in MANET using AODV", Journal of Discrete Mathematical Sciences and Cryptography, 2020, pp. 209-220.
[24] Bairwa, A.K., Joshi, S. (2022). An Improved Scheme in AODV Routing Protocol for Enhancement of QoS in MANET. In: Nanda, P., Verma, V.K., Srivastava, S., Gupta, R.K., Mazumdar, A.P. (eds) Data Engineering for Smart Systems. Lecture Notes in Networks and Systems, vol 238. Springer, Singapore. https://doi.org/10.1007/978-981-16-2641-8_17.

Authors

Dr. Srinivasulu Sirisala has received his Master of Technology Degree in Computer Science and Engineering in 2012 from JNT University Anantapuramu, AP, India. In 2022 he completed his Ph.D in Computer Science from Sri Venkateswara University, Tirupati. He has more than 12 years of teaching experience. He has published more than 12 papers in international, national journals, workshops, books and conference proceedings. His Current area of interest includes Manets, Internet of Things, Artificial Learning and Machine Learning.

Dr. Nageswararao Sirisala, has 16 years of Experience in teaching and research. He received Ph.D in the Dept of Computer Science and Engineering (CSE), from JNT University Anantapuramu, AP, India. He has published more than 20 research papers in international conferences and journals. His area of interest is computer networks, Mobile adhoc networks, algorithms, soft computing methods, distributed systems, mathematical foundation of computer science, designing of data base and programming languages.

Dr .G. Rajeswarappa has Completed his Bachelor of Technology from G Pulla Reddy Engineering College, Kurnool, Received M.Tech from Sree Vidyanikethan Engineering College,Tirupati, and Ph.D degree from JNTUA University, Anantapur, Andhra Pradesh. He has 16 years of teaching experience and published papers in reputed journals. His Research interests includes wireless sensor networks, Network security, Big data, Cloud Computing, Artificial Intelligence and Machine Learning.

How to cite this article:

Srinivasulu Sirisala, Nageswararao Sirisala, G. Rajeswarappa, "Eigen Vector Based Trust Model (EVTM) for Ensuring Quality of Service (QoS) in Mobile Ad Hoc Networks", International Journal of Computer Networks and Applications (IJCNA), 11(3), PP: 351-362, 2024, DOI: 10.22247/ijcna/2024/22.