Trust Enabled Secure Routing in Vehicular Adhoc Networks

M Venkata Krishna Reddy
Department of Computer Science and Engineering, Chaitanya Bharathi Institute of Technology, India
krishnareddy_cse@cbit.ac.in

G Kiran Kumar
Department of Computer Science and Engineering, Chaitanya Bharathi Institute of Technology, India
ganipalli.kiran@gmail.com

Panduranga Vital Terlapu
Department of Computer Science and Engineering, Aditya Institute of Technology and Management, India
vital2927@gmail.com

D. Jayaram
Department of Information Technology, Chaitanya Bharathi Institute of Technology, India
djayaram_it@cbit.ac.in

Shirina Samreen
Department of Computer Science, College of Computer and Information Sciences, Majmaah University, Saudi Arabia
s.samreen@mu.edu.sa

Abstract: *Vehicular Ad-hoc NETworks (VANETs) can improve traffic efficiency and safety on the roads by enabling real-time vehicle-infrastructure connectivity along roadways. Routing in VANETs presents major obstacles due to the continuously evolving network architecture and security risks. Trust-based routing may improve Vehicle-to-Infrastructure (V2I) communication security, reliability, and Quality of Service (QoS). Trust-based routing requires trustworthy evaluation, authentication, privacy protection, and access control for the Internet of Vehicles (IOV). IOVs' continual modification poses trust computing algorithm efficiency and scalability issues. Trust-based routing must be able to withstand Sybil attacks and poor vehicle collisions. This study introduces trust-enabled routing for VANETs. The proposed approach combines direct, indirect, situational, and experiential trust to determine node reliability. Mobility has an impact on Direct Trust (DT), which includes punishment and reward parameters, communication frequency and consistency, and delay duration. The value of feedback trust, mobility factor, and link dependability determine iN-Direct Trust (N-DT). Situational trust considers the time period of the day, location, weather, and the density of traffic between every two nodes. Effective communication builds experience and trust. We use final trust scores to select reliable routes, thereby improving network performance. This approach minimizes network latency and enables accurate assessment of trust in real-time with low false positives, enhancing network resource consumption efficiency, dependability, security, and resilience. The new Trust-Enabled Secure Routing (TESR) scheme works better than Graph-Based Trust-enabled Routing (GBTR), Obstacle Prediction-Based Routing Protocol (OPBRP), and Regression Geometric Optimization (LARgeoOPT) in terms of end-to-end delay, routing overhead, latency, dropped packet ratio, throughput, and Packet DeLivery Ratio (PDLR). It does these things by decreasing them by 2%, 2.8%, 4%, 6%, and increasing them by 6% and 7.14%, respectively. TESR improves network performance and reliability, enhances VANET security, and enables the expansion of intelligent transportation systems.*

Keywords: *Mobility, reliability, secure routing, trust, VANET.*

Received September 6, 2024; accepted March 20, 2025
https://doi.org/10.34028/iajit/22/3/13

1. Introduction

Vehicular Ad-hoc NETworks (VANETs) are emerging technologies that combine ad-hoc networks and Wireless Local Area Network (WLAN), allowing Vehicle Units (VUs) to communicate with nearby Road-Side Units (RSUs) via wireless communication, enabling users to access desired services via the internet. VANETs, wireless networks, are growing fast, connecting vehicles and enhancing road safety, traffic flow, and congestion management. Vehicle to Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications use On-Board Units (OBUs) and RSUs. VANETs include OBUs, RSUs, and trust authority. VANETs, a fascinating new wireless communication technology, has recently garnered a lot of attention. VANETs improve safety, traffic management, and infotainment by allowing vehicles to interact with each other and roadside infrastructure.

The topology of this network changes as vehicles join and leave at will. VANETs have variable network density due to traffic congestion, road conditions, and vehicle count [42, 45, 55]. Vital traffic, road risk, and emergency scenario updates can be disseminated by several forms of communication [51]. This information may improve traffic flow, reduce incidents, and improve passengers' travel experience [33]. VANETs can enhance road safety, reduce congestion, and enable new mobility amenities [56]. However, the dynamic and decentralized nature of VANETs poses substantial challenges, particularly concerning security and trust. Trust-enabled secure routing emerges as a critical area of research to ensure reliable data transmission in such networks [38].

1.1. Research Gap and Proposed Research

Research on VANETs has increased and is likely to continue because of the increasing demand for connected and intelligent vehicles. The efficiency and performance of VANETs are negatively impacted by the substantial routing problems they face. Routing systems must find effective ways via the network to minimize delay and maximize reliability, repeating communication through intermediary nodes due to limited communication range [31]. VANETs' dynamic topology and absence of central authority create security risks such as spoofing, malicious attacks, and eavesdropping, as well as internal and external attacks, compromising data interchange reliability and security [6]. Practical trust-based routing algorithms can enhance vehicle communication dependability and security and reduce security concerns in VANETs [34]. Despite the extensive research on secure routing protocols in VANETs, several gaps still need to be addressed. Existing solutions often focus on cryptographic methods, which, while essential, need to be revised to address the dynamic trust management required in highly mobile environments. Current trust models also tend to be static, failing to adapt to the constantly changing network topology and vehicle behavior. This study seeks to address these gaps by building a dynamic, trust-based, secure routing protocol that can adjust to the unique characteristics of VANETs.

1.2. Motivation and Problem Statement

This research is driven by the need to increase VANET reliability and security. In a network where vehicles make split-second decisions on incoming information, accuracy and trustworthiness are crucial. This work addresses the lack of a comprehensive mechanism to dynamically evaluate and integrate trust into secure routing protocols to safeguard data from external attacks and ensure reliability. Trust-based routing algorithms evaluate neighbors' behavior and assign trust ratings based on perceived reliability in a trusted network between vehicles [18]. Vehicles use neighbor trust values to determine routes in trust-based routing [40]. For safety and reliability, a vehicle can employ a neighbor with a high trust rating to deliver messages [39]. For security or reliability, a vehicle may stop delivering messages via a low-trust neighbor [1]. Trust-based routing methods allow VANET cars to interact with trustworthy neighbors and filter out untrustworthy ones [28, 37]. Trust-dependent VANET routing approaches are gaining popularity. Scalability, efficiency, and threat adaptation remain challenges.

1.3. Overview of Proposed Approach and Novel Contribution

Various parameters that significantly impact VANETs need to be considered for computing the trustworthiness of the vehicles for involving them in routing [17]. To address the limits of secure routing in VANETs, a unique solution is proposed that uses route request mechanisms and trust metrics to improve network stability and security [29, 49]. However, deploying the proposed method in VANETs is only possible with its potential difficulties. The efficiency and scalability of trust computation techniques are challenging. The enormous number of vehicles in VANETs and their continual motion require precise and fast trust evaluation [14]. VANETs often use heterogeneous vehicles with varied capacities and communication systems [25]. Maintaining infrastructure and vehicle compatibility proves challenging [35]. Further research is needed to fully implement Trust-Enabled Secure Routing (TESR) and improve vehicular communication security and reliability [30]. It must address VANETs' scalability, interoperability, and practical benefits. This research study presents TESR, a trust-enabled routing protocol that relies on routing decisions on trust values and the network's topology. A new trust model for VANETs uses direct, indirect, situational, and experience trust measures and mobility to improve network stability and security.

This research work targets to contribute significantly to the field of VANETs by providing a robust solution to the persistent challenge of secure and trustworthy communication, ultimately enhancing vehicular networks' overall safety and efficiency. The proposed approach involves the development of a trust-enabled secure, reliable routing method for VANETs, integrating both cryptographic security measures and dynamic trust evaluation mechanisms. The novel findings of this research study can be enumerated as follows:

1. Dynamic Trust Evaluation Mechanism.
   a) Dynamic Trust Evaluation Mechanism: introduction of a real-time Trust Evaluation System (TES) that determines the reliability of nodes depending on their behavior and interactions within the network.
2. Hybrid Trust Model: development of a hybrid trust model combining Direct Trust (DT) observations (depending on direct interactions) and iN-Direct Trust (N-DT) (depending on suggestions from other neighbor nodes) to enhance the accuracy and reliability of trust assessments.
3. Secure Routing Protocol Integration: integration of the dynamic trust model into a secure routing protocol to ensure that routing decisions are made based on both security credentials and trustworthiness.
4. Adaptive Trust Management: implement an adaptive trust management framework that adjusts trust scores based on context and environmental changes, ensuring resilience in highly mobile and dynamic VANET environments.

5. Comprehensive Security Analysis: a thorough security analysis to evaluate the effectiveness of the proposed protocol against various attack vectors, including Sybil attacks, black hole attacks, and data fabrication attacks.
6. Simulation and Real-World Testing: extensive simulations and real-world practical testing to validate the performance, reliability, and security of the proposed protocol in diverse vehicular network scenarios.

The remaining sections of the article are shown here: Section 2 provides a detailed literature review discussion. Section 3 details the proposed work that communicates between vehicles and infrastructure using VANET's trust-based routing. Section 4 discusses the methodology and inputs used in the simulation. Results and analysis of the simulation were covered in section 5. Section 6 wraps up the proposed study, followed by references.

2. Related Work and Comparative Analysis

VANETs, a type of Mobile Ad-Hoc NETwork (MANET), allow vehicles to communicate with infrastructure for traffic control, entertainment, and safety applications. Choosing the optimal route to deliver messages to their destinations is the key to reliable routing in VANETs [22]. One of the several suggested methods is graph-based routing, which uses algorithms to determine the optimal path by modeling the network topology as a graph [43]. The ever-changing nature of VANETs, including factors like vehicle mobility and network dynamics, makes traditional graph-based routing methods inadequate. This section covers current routing algorithms for VANETs, including their benefits and drawbacks.

2.1. Graph-Based Methods

Alharbi and Alsubhi [4] presented graph-based botnet detection. The proposed method detects botnets and zero-day cyberattacks. The author uses machine learning algorithms to evaluate graph-based feature section efficiency. The proposed assault detection system is practical. However, it ignores the presence of electric cars. Lightweight encryption and graph-based machine learning are used in the approach suggested by Gupta *et al*. [16] to address the authentication and security issues with Intelligent Transport Systems (ITS). This ITS smart vehicle identification and security solution employs identity-based authentication and graph-based machine learning. However, this method needs to address the scalability problem in the VANETs. Incorporating trust-based techniques, Xia *et al*. [54] propose a unique solution to multicast routing in VANETs. The authors acknowledge the significance of more effective and safe multicast transmission in VANETs for traffic control and safety services. The authors developed a trust model that considers trustworthiness and performance assessment when evaluating NDT. and Bayesian theory when evaluating DT. The suggested approach prioritizes vehicle dependability over standard multicast routing techniques, which only consider the network's structure but not node dependability. By considering VANET dynamics, Eiza and Ta [13] overcome the constraints of graph-dependent enabled routing algorithms. Along with a message-forwarding mechanism, the suggested approach incorporates an updated graph-dependent model and a reliable path-finding algorithm. Vehicle position and movement update the network topology in the developing graph model. The reliable path selection method identifies the minimal hop count and quality link path. After that, the communication system sends messages along the chosen path and adapts to network topology changes. This method needs to address the concept of private vehicles. Kamboj *et al*. [23] introduced a novel approach, reliable graph-based routing, to increase packet delivery efficiency between origin and destination nodes in VANET environments. The authors tested their suggested routing strategy in several simulation experiments using different situations, including various network sizes and densities of vehicles. They compared it to more conventional protocols such as Dynamic Source Routing (DSR) and Ad-hoc On-demand Distance Vector (AODV). This method focuses only on the dependability factor but not the node's trustworthiness.

2.2. Particle Swarm Optimization Methods

BrijilalRuban and Paramasivan [8] discussed cluster formation. Certificate revocation list highlighted attacked nodes. Certificate Authorities verify each node before secure transmission. After validation, data are delivered via the optimal route from the sender to the receiver. The path was established using enhanced OLSR routing. MPR selection is optimal with Particle Swarm Optimization (PSO). Due to the validation process's bandwidth and time consumption, overhead costs are a problem. A large-scale bi-level PSO algorithm is introduced by Jiang *et al*. [21]. This approach uses multi-particle swarms to expand the size of particle swarms and the initial population diversity. This technique addresses PSO delayed convergence and local ideal difficulties. The structural benefits of a bi-level particle swarm enable the higher-level swarm to supply decision-making data. On the other hand, particle swarm efficiency is enhanced by having lower-level working swarms operate simultaneously. Simulations have shown that 'big-scale bi-level PSO' yields good results. The proposed algorithm could be more stable in terms of data throughput.

A simple particle was presented by Tseng *et al*. [48] to solve constraints in Nonlinear Constrained Optimization (NCO) problems, drawing on the example of a slow ant in an ant colony. Modern PSO-based approaches make embedding the simple particle easier. An easy particle with sluggish ant behavior and no social or cognitive constraints can bypass constraint containment and explore unexplored areas. According to the experiments, small particles in the algorithms can decrease premature convergence and improve NCO problem performance. As needed, replenishing simple particles seems wise.

2.3. Trust-Based Routing Protocols

In their study, Mahi *et al.* [32] identified fraudulent nodes in VANETs using data-centric, entity, and recommendation trust. This method synthesizes direct and NDT. via the analysis of neighbor proposals and the computation of local trust. In [26], a Distrust-based Misbehavior Vehicle (DMV) technique was created to identify vehicle misbehavior using distrust value in a cluster architecture. It enhances vehicle misbehavior prediction and outperforms at high speeds by ensuring stability. However, this work does not consider the dynamic motion of vehicles. By distributing dishonest nodes in VANET, Bousbaa *et al.* [7] showed that a Trust and Reputation-based Opportunistic Vehicle Routing (TROUVE) methodology could find the nearest, fastest, secure route to a destination. The above work needs to concentrate on efficiently computing the node's trust. According to Bangotra *et al.* [5], a Trust-enabled Energy-based Routing Protocol (TERP) can detect and remove problematic nodes from the routing path. This routing technique considers intermediary node energy levels to select shorter paths with less interference, resulting in reduced delay, routing load, and increased throughput.

Yao *et al.* [57] created a trusted method for dynamic entity centers depending on weights, considering the levels of node authority. These works do not focus on multitier trust computation to enhance the secure routing. The Privileged Infrastructure for Vehicular Communication Architecture (PIVCA) was first developed by De Francesco *et al.* [11] to reduce end-to-end latency by message broadcasting. This technique takes into account the predicted transmission range. Here in this study, nodes' trustworthiness is not taken into consideration. While Wang *et al.* [52] provided a trust framework for opportunistic mobile social networks, they neglected to account for social proximity or resemblance. Service management in-vehicle networks have seen the development of several distributed models. One of these is the Vehicular Trusted Third Party (VTTP) idea, laid out in [27], enabling drivers to take advantage of various services. The methods proposed above only deal with the trustworthiness of the nodes after involving them in routing for communication. In their work in [44], authors integrate trust-based methods to propose an innovative approach. While conventional multicast routing algorithms merely take network structure into account, the suggested method shifts the emphasis to the dependability of vehicles. After determining the vehicles' trust values using a fuzzy logic-based method, they choose the most reliable intermediary nodes to pass messages. The proposed method here concentrates only on the DT factor for the computation of trustworthiness.

2.4. Hybrid Methods

According to Naeem *et al.* [36], the proposed method can improve network routing stability and average transfer rate. The Sugeno model fuzzy inference system evaluates Cluster Heads (CH) considering the distance to the base station, concentration, node degree, local distance, and residual energy. The revised routing protocol and channel model improve the link rate in VANETs with a stable network size. This model increases end-to-end delay, thus degrading network performance. This method does not address the isolation of malicious vehicles. The method addressed by Choksi and Shah [9] proposes a Dynamic Clustering Algorithm (DCA) based on Fuzzy c-Means (FM) machine learning for selecting dependable vehicles for energy-efficient multi-hop routing taking into account mobility characteristics such as position, direction, speed, and energy. Another approach is to use residual power with FM including distance to determine constant CHs that can enhance data dissemination to the destination. This proposal won't consider the trust factor in the isolation of malicious nodes. In addition, those methods can potentially increase network overhead to routing algorithms. To circumvent these limitations, a new VANET routing protocol that is trust-enabled should feature trust models that are efficient, lightweight, scalable, and trustworthy and that correctly assess both indirect and DT values. The system must be resilient to new threats and adaptable to complex network conditions.

2.5. Comparative Analysis

VANETs have garnered substantial research interest, particularly concerning secure routing protocols. This section critically examines the existing body of work comparatively, highlighting the strengths and weaknesses of various approaches. Table 1 presents the comparative analysis of the existing work.

2.6. Identifying Research Gaps

Despite the progress in secure routing for VANETs, several critical gaps remain: Static trust models: Many existing trust-based protocols use static models that do not adapt to the dynamic nature of VANETs. Integration challenges: Combining cryptographic methods with trust evaluation often results in high complexity and computational overhead. Limited Real-World Validation: Most proposed protocols need extensive real-world testing and validation, relying primarily on simulations.

2.7. Addressing Research Gaps

This article proposes a novel solution to overcome the limitations of scalable and secure routing in VANETs. The proposed TESR computes the node's trust using several parameters to isolate the malicious nodes. It implements a route mechanism to choose energy-efficient and secure routes for safe communication. The proposed trust-enabled secure routing protocol aims to address these gaps through the following innovations:

1. Dynamic Trust Evaluation: unlike static trust models, the proposed protocol continuously evaluates the trustworthiness of nodes in real-time, allowing for adaptive and responsive trust management.
2. Hybrid Trust Model: by combining direct and NDT assessments, the protocol improves the accuracy and reliability of trust evaluations, enhancing the robustness of routing decisions.
3. Seamless Integration: the integration of the trust model into the secure routing protocol is designed to minimize computational overhead while maximizing security and trust.
4. Extensive Validation: the proposed protocol will undergo rigorous simulation and real-world testing to ensure its effectiveness and reliability in various vehicular network scenarios.

Table 1 summarizes research on secure routing methods in VANETs.

Table 1. Comprehensive review analysis.

Ref.	Author	Approach	Strength	Weakness	Scope in proposed method
[2]	Akter *et al.*	The method modifies the network structure based on vehicle position and navigation needs.	The message-forwarding system guides messages and adjusts to network changes.	This method fails in recognizing malicious nodes.	Using the TRUST threshold, malicious nodes can be identified.
[46]	Sumithra and Vadivel	Graph-based metrics to detect insider threats in VANETs.	The main idea focuses on authorizing entities via a public key infrastructure.	This strategy does not address authorized insider attacks.	Prevents insider attacks by detecting and isolating malicious nodes.
[47]	Temurnikar *et al.*	This method considers dynamic topology, sporadic connectivity, and high mobility.	Depends on topological changes	High Mobility of the nodes is the major concern	Considers Hop to hop trust evaluation and dissemination.
[19]	Husain *et al.*	Three routing methods, ZRPgeoOPT, LARgeoOPT, and DREAMgeoOPT created utilizing PSO	PSO's fitness function improved throughput, PDLR, reduced delays, routing load, and packets lost.	Causes convergence issues or scalability issues due to swarm optimization	TRUST-based evaluation minimizes packet loss by isolating malicious vehicles.
[24]	Kandali *et al.*	Combination of three algorithms: Continuous Hopfield Network, Maximum Stable Set Problem, and modified K-means clustering	Enhancing data transmission in dense, mobile VANETs is the major goal of KMRP	Choosing CH is always challenging	Enhances secure data transmission by choosing a secure path
[41]	Shokrollahi and Dehghan	Trust-Based Geographic Routing Protocol	A vehicle monitoring system updates trust, tracks packet forwarding rate, and resends missed packets	Neighbor recommendation trust may not be accurate in all conditions	Neighbour trust is evaluated with consideration to network conditions
[53]	Wu *et al.*	GeoDTN+Nav-based trusted routing protocol	It uses opportunistic routing and Bayesian trust management to establish secure pathways	Complex computation	Uses direct and NDT factors for evaluation
[15]	Gazdar *et al.*	The framework relies on observing neighbors to establish trust and employs a level-based strategy to minimize harm	Improve the data delivery rate	These works do not focus on multitier trust computation to enhance the secure routing	Uses multitier trust computation for robust isolation
[20]	Jaballah *et al.*	This technique considers the predicted transmission range	Reduces end-to-end latency by message broadcasting	The trustworthiness of nodes was not considered in the study	Based on trustworthy evolution
[10]	Choksi and Shah	Gree AODV, low-power vehicle ad hoc routing protocol	Efficiently selects the optimal route in a VANET by evaluating power consumption between sender and receiver	Vulnerable to the attacks	Isolates the malicious behaviors
[3]	Alam *et al.*	Graph-based trust-enabled routing (GBTR)	Assesses mobility and indirect, direct, and contextual trust using graph-based topology and trust measures.	This method does not address the isolation of malicious vehicles	A strong TES to identify and separate malicious vehicles.
[12]	Diaa *et al.*	OPBRP-obstacle forecast-oriented routing method	Route dependability and PDR are improved by vehicle kinematics and mobility forecasts.	Network overhead	Comparatively less network overhead
[50]	Venkatamune and PrabhaShankar	Q-Learning based collision warning Prediction and Safety message Dissemination (QCP-SD)	pliable Q-learning based collision prediction and Safety alert message dissemination	Next-hop disseminators selected based on a multi-attribute cost value	Collision risk factor

3. Proposed Work

The proposed methodology for trust-enabled secure routing in VANETs involves the development of a dynamic trust-based secure routing method. This section details the algorithms used, the trust-evaluation procedure, and the overall framework, illustrated with comprehensive figures to understand the approach clearly. Addressing the mentioned constraints of trustworthy routing in VANETs, a new method of routing, TESR, that improves network security and reliability by using trust metrics is proposed in this article. The proposed one is an innovative contribution to the domain of VANETs. Building and testing a trust-dependent routing procedure that considers both the network's topological parameters and trust values while making route selections is the main novelty of the study, TESR. Below is a concise rundown of the most significant scientific advancements.

- TESR is a new approach to trust in VANETs that improves network security and dependability by combining various topological parameters with many trust metrics like direct, indirect, situational, and experience trust, all of which have an excellent mobility factor.
- Successful communication frequency among the nodes, punishment/reward, consistency, and latency are the factors that, when combined with the mobility factor, can lead to DT.
- The NDT observation is used to derive the mobility factor's effect on connection dependability and the feedback trust value.
- Situational Trust is evaluated using local and environmental information in trust calculation.
- Experience Trust is evaluated considering successful communications made by the node in the network.
- The proposed TESR, a trust-enabled routing protocol that considers vital vehicle trustworthiness when deciding where to send traffic, is tested. A Route-Finding System (RFS) and a Route Maintenance System (RMS) are constituent parts of the suggested routing protocol.
- Error in route recovery and detection are the two primary parts of the Road Maintenance Management (RMM) system in TESR. Repairing the route locally and fixing it globally are the two main components of route error recovery.
- TESR uses a new trust updating methodology that promotes stability, fairness, cooperation, and trustworthiness through fewer rewards and more penalties. To make the network more equitable, a scheme of rewards and penalties can be implemented to guarantee that every node is treated fairly.
- Nodes that act responsibly are rewarded, whereas nodes that act maliciously are punished. Network stability can be enhanced using a reward and penalty structure, encouraging nodes to behave consistently. This lessens the possibility of unexpected behavior changes that could cause network disruptions.
- The proposed protocol outperforms conventional routing protocols in the veins simulator regarding network throughput, normalized routing load, end-to-end delay, Packet Data loss Rate (PDR), and Packet DeLivery Ratio (PDLR). These findings indicate that trust-enabled routing may be essential in improving the general performance and safety of future VANETs, which has significant consequences for their design.

The proposed method TESR performs operations as follows: TES, RFS, RMS, Trust Update (TU), Energy-Efficient, Trusted, and Secure routing (ETS).

Figure 1 describes the proposed approach framework. It shows the major components of the proposed method: Trust evaluation process, route finding system, RMS, and route selection and secure routing. Trust evaluation process includes direct, indirect, situational, and experience trust. Figure 2 explains the detailed components used in the trust evolution sub-system.

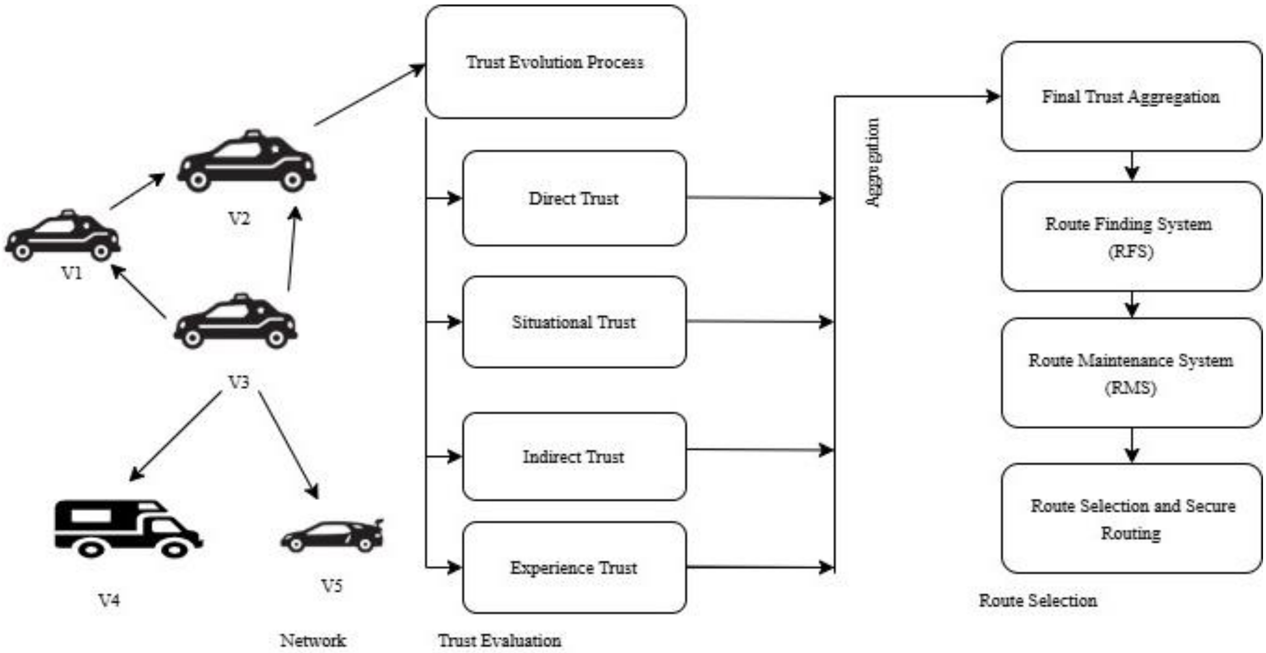

Figure 1. Proposed trust enabled secure routing framework with four sub-systems for evolving trust and finding a secure path.

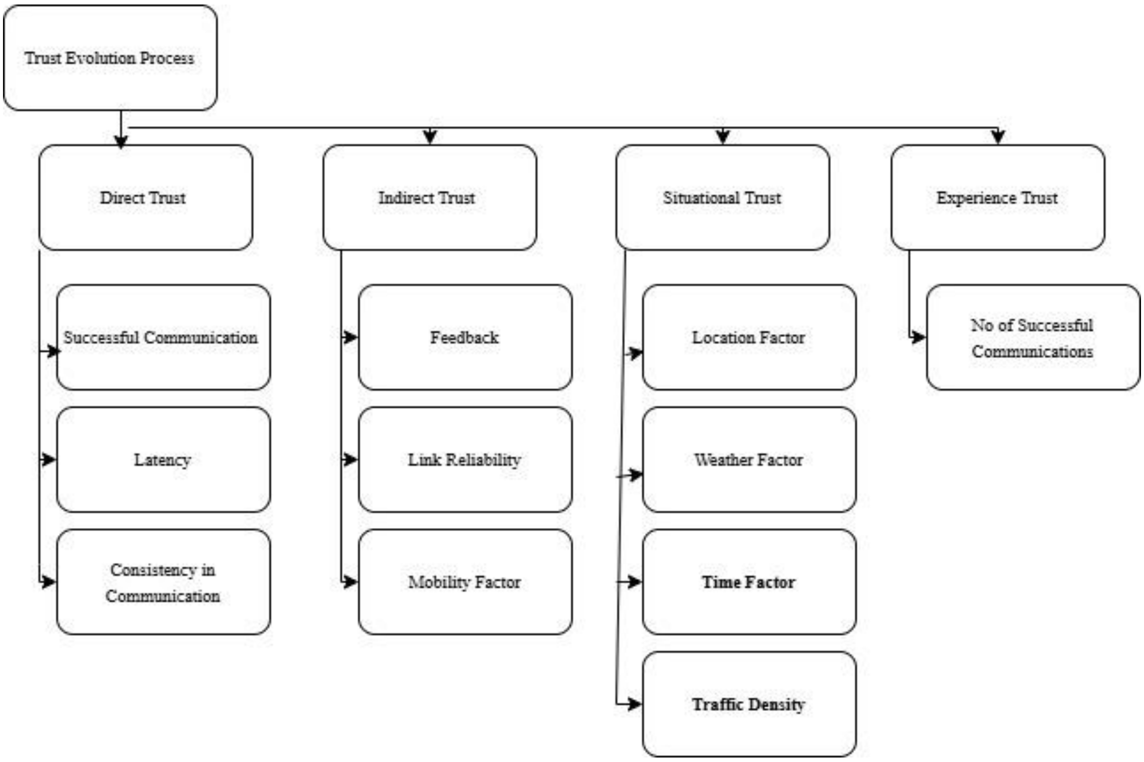

Figure 2. Detailed description of trust evolution sub-component in trust enabled secure routing framework.

3.1. Trust Evolution System (TES)

The first step in the proposed TESR for the source node is to use the suggested trust assessment scheme to determine whether its neighbors can be trusted. When trustworthy nodes are not present in the neighborhood, and issues with vehicle-to-vehicle trust along with unstable Internet connectivity via RSUs lead to many limitations like longer transmission delays, inflexibility, nonresponse to dynamic changes in crucial information parameters, and lower PDLR because of fast topology-change. The transmission of information between untrusted vehicles also affects safety. So, the trustworthiness of nodes needs to be evaluated for secure and efficient routing. Using metrics like situational, direct, experience, and NDT, the trust evaluation scheme finds the most reliable and efficient nodes to route data.

- The source node should have trust in the node to which it has direct communication. The node's confidence in another node in the network is determined by its prior interactions with that node or by its own experiences. Hence, DT is taken as a trust metric.
- The node determines trustworthiness by considering the recommendations and views of its nearby peers in the network. The opinion of other nodes in the network matters as the source node should rely on intermediate vehicles for data transfer to the destination node in the network. Here, NDT plays a significant part in finalizing the final trust score.
- Nodes often determine trust by looking at past interactions with other nodes and considering their experience. This allows experience trust to be included in trust calculation.
- The node's proximity metrics, such as time, distance, location, etc., are also part of the network's trusted formula. As these network parameters consistently affect.

The network environment and the vehicle's performance are taken into consideration as trust metrics and situational trust for the final trust score. Including direct, indirect, situational, and experience trust strengthens the evaluation of the final trust value of a node. A node's trustworthiness needs to be evaluated to decide its involvement in the routing.

A trusted node enhances the security and efficiency of routing through fair data transmission. Node's final trust combines indirect, direct, situational, and experience trust.

- DT is quantified using parameters of successful communication, latency communication, and communication consistency of the node under consideration.
- Direct value and the reliability of links are used to measure NDT.
- Location parameters, including time of delay, position, traffic density, and weather, are used to quantify the Situational Trust.

At the end of the trust assessment, the source node that started the process chooses the most reliable node to utilize as the subsequent link in the path. This section introduces a reliable trust evaluation method for VANETs that outlines route finding, maintenance, and optimal path selection mechanisms. A trust-based routing strategy assigns a trust score to each vehicle in the network depending on its prior behavior and contacts with others. This score assesses the vehicle's trustworthiness and reliability. When routing messages, a vehicle can consider a trust score when choosing a vehicle for communication. VANET may be seriously affected if dishonest vehicles, such as Man in the Middle (MITM) attackers, were to be present in the network and spread harmful content. So, in a VANET, more trustworthy node routing can improve authenticity, privacy, accuracy, and security. This proposed method is designed and implemented with the following initial assumptions:

- The assumption is that all vehicles' power, processing capacity, and range of communication are severely constrained. Therefore, the routing method must account for the range of communication while picking the next hop for packet forwarding.
- The network is assumed to have homogeneous vehicles with similar hardware and communication. The accuracy of the localization mechanism impacts trust metrics and routing performance.
- Each vehicle's trust value starts at five and reaches a maximum of 10.
- The decentralized network has no central authority governing or controlling its actions.
- The network may have 10-50% misbehaving nodes that impede interaction and launch attacks on other nodes.
- Additionally, broadcast communication examines whether the message is sent to the transmission range nodes of the source.

By replying to the message, the receiving node confirms its identity. Trust assessment considers the above factors. The final trust includes recommendations and the prior performance/trust value. To fully demonstrate the behavior of a node, it is crucial to take its historical performance and trust value into account while estimating its trustworthiness in the context of a selective forwarding attack. It could be helpful as an inherent safeguard against a selective forwarding attack. To illustrate the point, let's say that the node dropped a few packets during the last trust estimation period but is now forwarding the packets. Hence, combining trust values from these two periods is better for detecting malicious nodes. This enhances the trust's accuracy. Recommendations, experience, and Situational factors are paired to form the final trust value with direct observations to obtain comprehensive trust value. As such, it helps detect coordinated attacks and shows the true nature of node behavior. This composition of evaluating the final trust value of a node in the proposed method can face the challenges of the attacks to some extent. The integration of situational and experience-based trust metrics involves the collection and analysis of potentially sensitive data. Cryptographic tools will protract the data collected here; however, further research is required to comply with relevant legal and ethical standards.

3.2. Direct Trust

Successful communication frequency, latency, and consistency contribute to DT. Using Equation (1), calculate the DT among the nodes *x*, *y* at *t* time factor,

$$DT(x - y) = [\, w_1 + w_2 SC + w_3 DC + w_4 CC] \qquad (1)$$

Where, Baseline trust score=W_1, Successful Communication (*SC*) metric weight=W_2. Delay of Communication (*DC*) weight=W_3. Communication Consistency (*CC*) weight=W_4. And SC-successful communication. DC-latency of communication. *CC*-communication consistency.

A predefined number or the node's historical behavior can be used to modify the baseline trust score (w_1). Establishing trust between vehicles helps enhance VANET security and dependability. Furthermore, it is used as a foundation for determining the reliability of every vehicle in the system. For example, to determine the vehicle's trustworthiness, the baseline trust score can consider its reputation, past behavior, or other pertinent attributes. Over time, each vehicle's reliability can be enhanced by its communication with other vehicles in the network. Vehicles may be able to trust or avoid other vehicles based on their baseline trust score. Successful Communication, *SC* is the ratio of successful Packets Received (*RP*) to Total Packets transmitted (*TP*) within a certain period, as mentioned in Equation (2).

$$SC = \frac{(RP + R)}{(TP + P)} \qquad (2)$$

Where *R* is Reward and *P* is Punishment. *SC*'s reward and punishment parameters can be changed according to the node's historical behavior, i.e., no successful packet transfers over total packets. A node may be penalized by increasing its *P* value if it fails to send and receive packets and rewarded by increasing its *R*-value if it can transmit successfully.

Time elapsed between a node's packet transmission and reception averaged over all successful communication events, is termed Communication Delay (DC) as given in Equation (3).

$$DC = \sum_i^n (TR_i - TS_i) \qquad (3)$$

The Communication Consistency (CC) of a node is determined by comparing the sum of all time slots (*M*) available for communication between the node and its neighbors, divided by the no. of time slots (*N*) in total, available during that period as given in Equation (4).

$$CC = \frac{(M\ \text{-}\ PM)}{(N + PN)} \qquad (4)$$

Where *M*=the number of time slots available for communication between the node and its neighbors. *N* is the total number of available time slots, *PN* is Punishment, and *PM* is Reward. Modifying the *CC* parameters for punishment (*PN*) and reward (*PM*) is possible depending on the past behavior of the node. The node may be rewarded with a decrease in PM if its immediate neighbors are always reachable and punished with an increase in PN if they are infrequently reachable.

3.3. In-Direct Trust

According to Equation (5), the NDT value is determined by integrating the feedback trust, link dependability, and mobility factor.

$$NDT = \left[(W_1)*(1/n)*\sum_{1}^{n} DT + W_2*link\_reliability \right] \quad (5)$$

Link reliability is critical in establishing a trust paradigm for VANETs. Achieving accurate and effective trust metrics in VANETs requires evaluating the quality of communication links due to their dynamic and unexpected character. High connection reliability improves trust model integrity, network performance, and security, while low link reliability might result in inaccurate trust evaluations and routing decisions.

Where *DT* is the DT value, each measure has weights w_1 and w_2, which can be adjusted to achieve the required balance and efficiency in assessing reliability for the intended application. The NDT evaluation vehicle count is *n*.

3.4. Situational Trust

Situational trust in VANETs involves incorporating local environmental information into trust calculations. Essentially, situational trust considers the specific context of network nodes, including time of delay, position, traffic density, weather, and other characteristics. Considering location data in the trust computation methodology improves VANET precision, dependability, and security by refining the trust evaluation method. Nodes *x* and *y*'s operational context is reflected in the situational trust factor. Position, traffic density, and weather are some of the factors that might be considered for this purpose. To determine contextual trust for node pair (*x*, *y*), integrate the following elements using a weighted sum approach as given in Equation (6).

$$SituationalTrust\ \mathrm{ST} = \left\{ \begin{array}{l} \left(W_1*Location\ Factor\right) + \\ \left(W_2*Time\ of\ \ Day\ Factor\right) + \\ \left(W_3*Wether\ \ Factor\right) + \\ \left(W_4*Traffic\ Density\ Factor\right) \end{array} \right\} \quad (6)$$

The influence of each component on the overall situational factor is controlled by the weight factors w_1, w_2, w_3, and w_4. The significance of each element for the application determines weight parameters. The factors involved in the above computation are determined below.

- Nodes' locations: are determined by the location factor, calculated using GPS coordinates. This can be determined using GPS coordinates or RSUs for position data. When expressed as a binary value, the location factor shows whether nodes are in heavily populated or sparsely populated regions.
- The period of the day value indicates whenever nodes are operational. To describe the scenario, a binary number can indicate whether nodes operate throughout peak or non-peak hours.
- The factor representing weather conditions measures the atmospheric circumstances during node operation. This binary number might indicate whether nodes function in perfect or adverse weather.
- The density factor of traffic measures traffic during node operation. A binary number can express whether nodes operate in heavy traffic or less-populated areas.

3.5. Experience Trust

This trust is generated depending on the previous nature of the vehicle node in VANET. This can be evaluated as the number of successful communications over the total no. of communications. Equation (7) gives experience trust.

$$ET\ \ (Experience\,Trust) = \left(\frac{(Number\ of\ \ Successful\ Communications)}{(Total\ no\ of\ \ Communications)} \right) (7)$$

The ultimate trust score is calculated using Equation (8).

$$FT\ \ (Final\ \ Trust)\ \ = \left(\frac{((W_1\ *\ DT)\ +\ (W_2\ *\ NDT)\ +(\ W_3\ *ST)\ +\ (W_4\ *\ ET))}{4} \right) \quad (8)$$

Where Direct Trust is (*DT*), Indirect Trust is (*NDT*), is Situational Trust (*ST*), and is Experience Trust (*ET*). w1, w2, w3, and w4 are the weights assigned subsequently with gaining importance for the four trusts calculated. The final trust value is crucial in VANETs for informing routing decisions. The routing algorithm protects against attacks and malicious behavior while delivering messages efficiently by exploiting node trustworthiness. The final trust calculated for each vehicle is compared with the trust threshold value to decide whether the car is trustworthy and eligible for routing.

3.6. Route Finding System

This subsection introduces the trust-enabled routing RFS for VANETs, which includes a route request/reply mechanism. As part of the proposed TESR method to maximize energy efficiency and security, it uses a RFS to identify trustworthy and efficient nodes. This sub-method reduces network energy usage while providing secure and reliable message delivery. RFS begins with the source node assessing the trustworthiness of its neighbors using a proposed scheme, the TES. The trust assessment method considers indirect, direct, experience, and situational trust features to determine the most reliable and efficient routing nodes. Once the source node has evaluated the nodes” trustworthiness, it identifies the most reliable node as the next hop. Upon receiving a route request message from the source node, the node examines its neighbors’ trustworthiness and chooses the next stage in the path. After reaching the destination node, the source node gets an efficient, safe, and secure message about route replies to confirm the safe and efficient routing. The route response message specifies the most reliable vehicles to consider for routing and the finest energy-saving way to reach the receiver vehicle. After deciding on the most reliable and energy-efficient route, the source vehicle begins delivering the messages to the destination vehicle.

3.7. Route Maintenance System (RMS)

The RMS ensures the route choice remains trustworthy over time. The main aim of RMS is to find and handle network changes that can affect route reliability and choose an alternate if needed. The relevance matching model TESR-RMM has two key stages: Route recovery and route error detection. In the process of detecting route errors, a sender vehicle continuously examines the trustworthiness of vehicles along a selected path while transmitting data to the target vehicle. If a vehicle’s trustworthiness level goes behind the threshold, then the sender vehicle considers a route error and initiates the recovery procedure. The route error recovery technique entails local and global repairs.

Algorithm 1: Final Trust Evaluation.

```
Input: ViD (Vehicle ID), PP (Position Parameters), VV
(Vehicle Velocity), FT (Trust Factor), TH (Trust Threshold),
T (Current Time), RT (Routing Table)
Output: TR (Trust-Based Route)
Deploy the vehicles onto the network.
Locate the M to the S at time t.
    S = Source Vehicle
    M = Current Vehicle
if (M == Empty)
    Announce 'No Neighbors'
    Return();
  else if (S → D and D(T) > TH)
      Establish a direct route between
      S → D
      Announce ('Success and message sent
      directly').
    Return()
  else
    Compute FTs.m Δt of M using Eq (8).
      If (FTs.m Δt (M) > TH)
        Identify M as a trustworthy
        node
      Else
        Note M is a malicious
        node and
        Eliminate it from routing
      end if
end if
Repeat the process until the next hop.
Apply Route Finding System (RFS)
    S sends the RREQ (Route Request) message to
    its neighbor M.
The M with valid, shortest, energy-efficient,
trustworthy paths reply to the RREQ to the S.
Route is established with trusted vehicles between S
and D.
    Data transfer occurs.
End Algorithm
```

Local repair stage: To fix the route locally, the source vehicle first chooses an alternate vehicle within its range of transmission with a higher trustworthiness rating than the error-causing node. Upon discovering a car, the sender vehicle revises the route details and transfers information along the restored route. The sender vehicle will begin the global repair if the local repair does not work. Global repair stage: The sender node sends a route request for a new path to reach its neighbors. The most recent route request message updates the error details and asks for alternative routes to the destination vehicle. Nearby vehicles evaluate each other’s reliability in response to a new route request and then respond with a reliable, energy-effective path to the receiver node. The message is posted to the receiver vehicle by the sender vehicle after it has chosen the most energy-effective and reliable way. Below are the steps of the suggested method TESR, as shown above in Algorithm (1).

3.8. Trust Update (TU)

As a vital part of trust-dependent routing in VANET, a TU system improves the efficiency, effectiveness, and security of VANETs. It makes decisions about routes based on trust evaluation in real-time. The trust-update system uses the final trust value, and known status plays a role in updating the trust value. TU system maintains three lists, “trust_list,” “known list,” and “Blacklist,” which are constantly updated with the latest value of trust and known status, respectively. As per the TU system,

1. If the node is a known vehicle and the trust value, FT>=Trust Threshold, i.e., trustworthy, then TU will reward the node with one point. Update Trust Value of the node = Final Trust Value +1.
2. If the node is a known vehicle and the trust value, FT<Trust Threshold, i.e., untrustworthy, TU will punish the node with 1.5 points. Update Trust Value of the node=Final Trust Value-1.5.
3. If the node is an unknown vehicle and the trust value is FT>=Trust Threshold, i.e., trustworthy, then TU will add the node to its known list and set its default trust value.
4. If the node is an unknown vehicle and the trust value, FT<Trust Threshold, i.e., untrustworthy, then TU will add the node to its blocklist, delete the message, and notify ID to its neighbors.

Enhancing the trust updating process in the proposed routing Algorithm (2) with a reward and punishment system adds value to the proposed method. An incentive and punishment system can strengthen the reliability and safety of the network by rewarding good conduct, punishing bad behavior, and fostering equity and consistency among nodes in the network. This method will reduce the false positives and further enhance the security and efficiency of the network. The final trust value evaluated for a node is a combination of direct observations, including successful transmissions, indirect, experience, and situational trust factors. Final Trust is compared with the trust threshold to isolate the malicious nodes. Here, direct observations of the source vehicle on the node under consideration will restrict the false reports of Trust and thus help to detect the false positives in the network. The trust threshold will be taken from 1 to 10 on a scale, and the average trust threshold will be considered 0.5. This proposed method's essential components of the Trust updating mechanism are blocklists and known lists. This TU mechanism incorporated in the proposed method for real-time trust evaluation lowers false positives, improves security, promotes fairness, and minimizes network congestion. It is possible to update trust measures in real-world circumstances at regular intervals according to a periodic schedule.

Algorithm 2: Trust Components Evolution.

```
Input: Direct Observations ($O_{ij}$): Trustworthiness evaluation
of node j by node i based on direct interaction Network
Parameters Neighbors (M)
Output: DT: Direct Trust table, NDT: Indirect Trust table, ST:
Situational Trust table, ET: Experience Trust table,
FTs.m(Δt): Final Trust of Neighbor 'M' at time difference Δt.
Initialize Trust Table
    T = {}
for each node i in the network:
    Initialize direct trust, DT(i) = 0
    Initialize indirect trust, NDT(i) = 0
    Initialize situational trust, ST(i) = 0
    Initialize experience trust, ET(i) = 0
end for;
for each packet received from node j by node i:
    Evaluate direct observations: $DT_{ij.}$
    Calculate DT(i) = f($O_{ij}$) // Function f aggregates
    direct observations
end for;
Loop: Collect recommendations from
      neighbouring nodes: $R_k$(j) where
      k != i
    i.   Calculate NDT(i) = g($R_k$(j))
             // Function aggregates indirect trust
    ii.  Calculate ST(i) = h(ST(j))
           // Function h calculates situational
            trust
    iii. Calculate ET(i) = h(ET(j))
             //Function h calculates experience
              trust
end loop;
Compute FTs.m Δt of M using DT, NDT, ST, and ET:
    FTs.m Δt = f(DT(s.m), NDT(i), ST(i), ET(i))
      //Function f computes final trust
      score
End Algorithm
```

Updating the system regularly entails re-computing the trust metrics given the most recent information and feedback. Regular updates make it possible to reevaluate trust metrics at specific intervals systematically. With enough up-to-date data considered, this method can give a more thorough and fair evaluation of trustworthiness. This feature detects long-term behavior changes and guarantees that trust values are updated consistently. In situations where consistency and general behavior patterns are inconsistent, periodic updates can be helpful. By utilizing the suggested scheme to calculate and update trust scores in general circumstances, VANETs can improve communication reliability, security, and performance. This is achieved by successfully analyzing node trustworthiness and making intelligent routing decisions. The trust computation process Algorithm (3) is complex in large-scale networks. Trust can be computed by dividing the large-scale networks into smaller hubs. The final trust value of each vehicle can be propagated in the network so that the source vehicle that wants to assess the Trust will be able to know the trust value. So that the complexity can be reduced. This approach also reduces the computational overhead, enhancing the suggested method's performance. Algorithm (4) details the RMS while Algorithm (5) shows the TU system process.

Algorithm 3: Secure Routing.

```
Input:  FTs.m Δt, RREQ
Output: RREP, R
Initialize Routing Table
    R = {}
for each node i initiate a route request to node j:
    Broadcast Route Request (RREQ) packet
    including trust threshold TH
for each intermediate node k receiving RREQ:
    Check trust score FT(k)
    If FT(k) >= TH
        Forward RREQ
      else
        Discard RREQ
    end If
Upon receiving Route Reply (RREP) from node j:
    Verify the FT of all nodes in the route.
    If all nodes FT >= TH
        Update Routing Table R with
        the new route
      else
        Initiate a new route discovery
        process
    end If
End Algorithm
```

Algorithm 4: Route Maintenance System.

```
Input:  FTs.m Δt, RREQ
Output: Route, New Node
Source continually monitors the vehicles that
participated in the current routing process
    If FT(k) < TH
Then, Apply the route recovery process.
```

```
        If FT(k) >= TH and transmission range<=
        range, select this new vehicle as next_hop and
        update the new route
        Else
        Broadcast RREQ message to neighbors.
    Neighbors will evaluate the trust level of the sender
    node
        If the sender is trustworthy, then
            Neighbors will provide a better route
            to the sender

    If the message is broadcasted for a predefined
    number of times, then
        Terminate the search and repeat the steps
        until the destination is reached.
    end If
    End Algorithm
```

Algorithm 5: Trust Update.

```
Input:  FTs.m Δt, TH, Known List, Black List
Output: Update Trust value
    If sender 'k' is a known vehicle and FT(k) >= TH,
    then.
        Update the Trust value of the sender by
        adding 1
        New Trust value = Old Trust value + 1
    Else If sender 'k' is a known vehicle and FT(k) < TH,
    then
        Update the Trust value of the sender by
        subtracting 1
        New Trust value = Old Trust value - 1
    Else If sender 'k' is an unknown vehicle and FT(k)
    >= TH, then.
        Add the sender to the known list and assign
        default trust value – 1
    Else If sender 'k' is unknown vehicle and FT(k) <
    TH, then
        Add the sender to the blacklist and discard
        the message, further broadcasting the ID of
        the malicious vehicles to the neighbors.
    end If
    End Algorithm
```

The proposed system utilizes a secure, trusted communication architecture that meets authentication, and privacy requirements. Digital signature and certificate systems use asymmetric keys. This is the most common infrastructure-based trust method. Vehicles are assigned Public/Private key pairs to digitally sign messages and authenticate with receivers. Every network message has a digital signature and certificate for authentication and integrity.

Vehicle Public Key Infrastructure (VPKI) is mostly used for self-trust management. Digital certificates necessitate centralization. Each vehicle is registered with a national/regional authority and given an Electronic License Plate (ELP) identity. Electronic identification is utilized for vehicle tracking. In PKI, a vehicle's private key is used to sign a message, which includes the CA's certificate. *V* is the sending vehicle, * represents all recipients, *M* is the message, *T* is the time-stamp for message validity, *PrKv* is the private key, and *Certv* is the public key certificate of *V*. Equation (9) shows the key,

$$V \rightarrow *: < M, SignP\,rKv\,[M|T\,], CertV > \qquad (9)$$

To maintain anonymity, vehicles must keep a large key/certificate set and alter it periodically for cryptographic security. A Tamper-Proof Device (TPD) stores all secret information (public/Private key pair) to prevent unauthorized duplication and modification. Keys in the Trustworthy Platform Module (TPM) [27, 44] are physically protected and cannot be manipulated or read by unauthorized parties. Additionally, it signs all outgoing communications. This device is only accessible to authorized users. VANET has no global trusted entity. Trust is established by individual VANET nodes. They sign certificates for each other's keys and determine the trustworthiness of the issuer. If a node I have interacted with issuing entities before, it will be aware of their public keys and trustworthiness. 'i' can accept j's key or not. Otherwise, trust relationships are self-organized. Node i calculates trust values for one-hop neighbors, then two hops, and so on till the destination is reached.

3.9. Energy Efficient, Trusted and Secure Routing (ETS)

The source node evaluates the trustworthiness of the nodes in the network and chooses energy-efficient and trustworthy nodes for routing. Thus, VANETs can improve communication performance, security, and reliability by making more secure routing decisions based on trust metrics that are computed and updated in real-world scenarios according to the suggested method. The proposed approach is detailed in the algorithms below. Algorithm (1) explains the process of final trust evaluation. Algorithm (2) demonstrates the evolution of trust components. Algorithm (3) showcases the process of secure routing.

4. Simulation Results

This section covers the simulation setup and findings obtained from simulations using the Veins 3.0 simulator [44]. The widely used OMANeT+ simulator is the foundation for Veins, an open-source event-driven model of vehicular networks. The research and development area utilized this tool heavily since it simulates communication in VANETs among vehicles and infrastructure along the roadside. Users can simulate realistic vehicle network situations with Veins, including vehicle behavior, wireless communication channels, and road infrastructure. The system involves many mobility models, such as the SUMO traffic simulator, which replicates the movement of vehicles on road networks. Mobility models and communication models, such as 3G/4G LTE and IEEE 802.11p, are available from Veins to simulate a variety of protocols and technologies used in vehicle networks. The simulator supports various routing protocols, including DSR, Greedy Perimeter Stateless Routing (GPSR), and AODV [36]. The proposed work involves 10 to 100 vehicles ranging from

10 to 100 kmph. The road length is 5 km, and the mobility model utilized is SUMO. The vehicle's dimensions are 5 meters in length and 1024 bytes in width. The simulation lasts 240 s and has a maximum transmission range of 400 m. The MAC protocol is IEEE802.11p, with a trusted range of 0-10 and a threshold of 5. With the weight assignment method, 50 packets are queued, each with an equal weight. Figure 3 shows a simulation experiment evaluating the proposed method, with nodes representing vehicles distributed across the network. This visualization provides insight into the method's performance in a simulated environment, aiding in understanding its effectiveness and behavior. Figure 4 shows the proposed model's experimentation process and trust computation, which uses direct, indirect, situational, and experience observations to evaluate node trustworthiness. Figure 5 shows how to identify malicious nodes in secure routing protocols for VANETs.

39
40
43
7
41
42
34
35
38
6
37
36
45
44
8
46
48
47
29
30
31
5
11
12
10
1
13
9
0
33
32
24
25
28
4
26
27
14
15
18
2
16
17
19
20
23
3
21
22

Figure 3. Sample simulation settings for the proposed work.

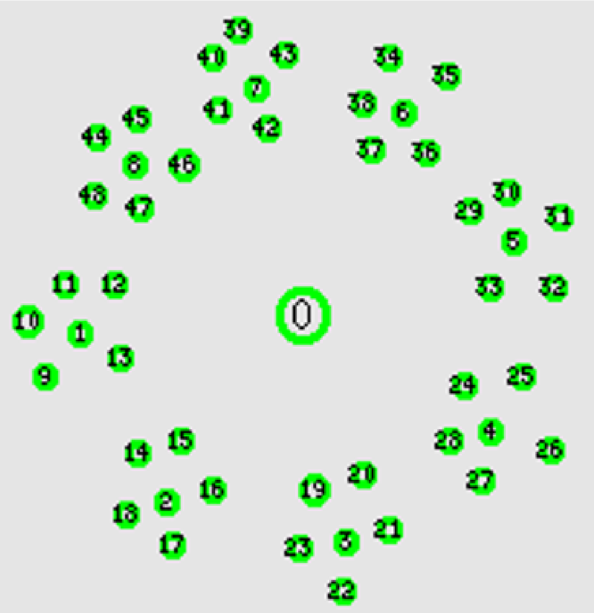

Figure 4. Experimentation and trust computation.

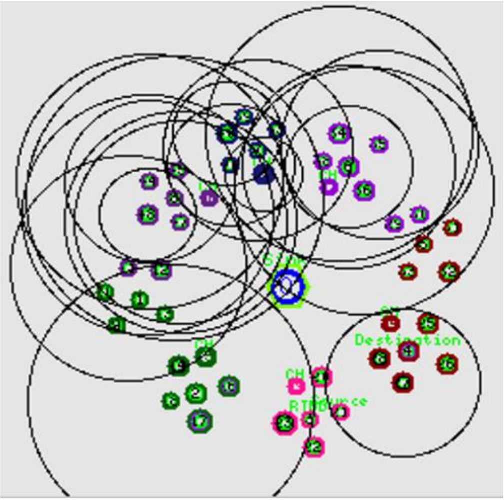

Figure 5. Identification of malicious nodes.

Figure 6 shows how malicious nodes are isolated in trust-dependent secure routing in VANETs. Table 2 presents simulation settings for trust-enabled secure routing in VANETs. The settings include simulation area, vehicle speed, mobility model, and communication protocols. The simulation area is 500m x 500m. The number of vehicles ranges from 10 to 100, and a maximum transmission range of 400m.

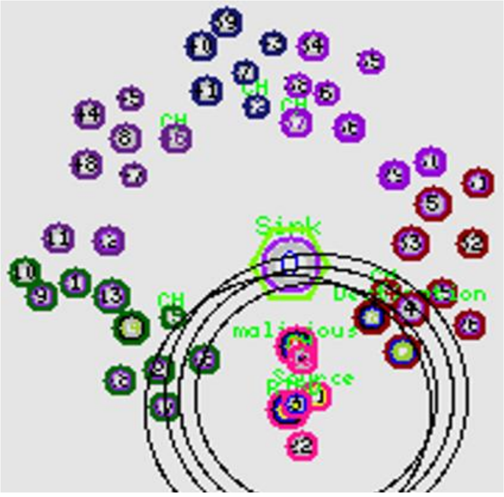

Figure 6. Isolation of malicious nodes.

Table 2. Simulation settings.

Parameter name	Value
Simulation area	500 m *500 m
Number of vehicles	[1-100]
Speed range of vehicles	(10-100) kmph
Mobility model	SUMO-traffic simulator
Road-length	5 km
Size of vehicle	5
Size of packet	1024 Bytes
Simulation time	240 s
Maximum transmission range	400 m
Mac protocol	IEEE802.11p
Range of trust value	[0 to 10]
Trust threshold value	5m
Strategy for weights assignments	Equal weights
Size of queue in packets	50
Network structure	Graph-based
Channel type	Wireless
Communication mode	Broadcast
The rate at which data sent	2 Mbps

5. Result Analysis

The outcomes of the simulations are being investigated. The proposed approach, TESR, is used to determine the trustworthiness of nodes and select trustworthy paths for routing messages. Table 3 displays the results and computations of the simulation for calculating the consequent trust and isolation of untrustworthy nodes. The equations above are used during the simulation to calculate the direct, indirect, situational, and experience trust observations. The routing process excludes untrustworthy nodes. The performance of the suggested TESR scheme is evaluated by comparing it with the existing and proposed methods, Regression Geometric Optimization (LARgeoOPT), Obstacle Prediction-Based Routing Protocol (OPBRP), and GBTR, in terms of performance metrics viz PDLR, Packet Drop Ratio, Throughput, Latency, Overhead, end-to-end delay. Equations (10), (11), (12), (13), and (14) demonstrate the performance metrics used for evaluating the proposed method in comparison with the existing methods.

$$PDLR(\text{Packet Delivery Ratio}) = \left(\frac{\text{Number of Packets Received}}{\text{Number of Packets Sent}}\right)\text{X100} \quad (10)$$

$$\text{PDR (Packet Drop Ratio PDR)} = \left(\frac{\text{Number of Packet Dropped}}{\text{Total Number of Packets generated}}\right)\text{X100} \quad (11)$$

$$\text{End to End Delay (EED)} = \left(\frac{\text{Total time taken for packets deliver}}{\text{Total Number of Packets generated}}\right)\text{X100} \quad (12)$$

$$\text{Throughput} = \left(\frac{\text{Number of packets transferred in a time period}}{\text{Total Number of Packets generated}}\right)\text{X100} \quad (13)$$

$$\text{Overhead} = (\text{Excess Resources utilized for transferring the packets}) \quad (14)$$

The outcomes of the simulations are examined. The proposed approach, TESR, determines the node’s trustworthiness. Table 3 displays the results of the simulation as well as the computations for the consequent trust and isolation of malicious nodes. The equations calculate the direct, indirect, situational, and experience trust observations during the simulation.

Table 3. Resultant trust comparison.

Vehicle	Direct observations–Trust (DT)	Indirect observations–Trust (NDT)	Situational observations-Trust (ST)	Experience observations–Trust (ET)	Resultant Final Trust value (FT)	Classification
V1	0.82	0.3842	0.75	0.832	0.657	Trustworthy
V2	0.68	0.3972	0.878	0.735	0.665	Trustworthy
V3	0.25	0.5464	0.865	0.656	0.612	Trustworthy
V4	0.33	0.5432	0.854	0.545	0.433	Un Trustworthy
V5	0.71	0.5879	0.623	0.498	0.313	Un Trustworthy
V6	0.36	0.4248	0.76	0.865	0.468	Un Trustworthy
V7	0.44	0.1566	0.78	0.845	0.842	Trustworthy
V8	0.55	0.7832	0.86	0.461	0.736	Trustworthy
V9	0.63	0.4924	0.83	0.687	0.548	Trustworthy
V10	0.83	0.2356	0.81	0.683	0.665	Trustworthy

5.1. Packet Delivery Ratio

Figure 7 illustrates how vehicle density affects PDLR. Increasing vehicle numbers result in higher PDLR for suggested TESR compared to GBTR, LARgeoOPT, and OPBRP. The proposed TESR steadily increases PDLR, while other schemes see fluctuations as vehicle numbers increase. Moreover, with 100 vehicle density, proposed TESR, GBTR, LARgeoOPT, and OPBRP have PDLRs of 96%,89%, 88%, and 86%, respectively. Table 4 shows the PDLR of all four methods. Greater PDLR values indicate better performance. TESR has the greatest PDLR compared to the four algorithms, followed by GBTR, OPBRP, and LARgeoOPT. The percentage enhancement of TESR versus GBTR, LARgeoOPT, and OPBRP was 7.14%, 8.16%, and 10.72%, respectively. TESR outperforms GBTR, LARgeoOPT, and OPBRP in PDLR, with the most significant improvement over OPBRP. The exceptional performance is due to a reliable trust model that provides precise trust values for efficient routing.

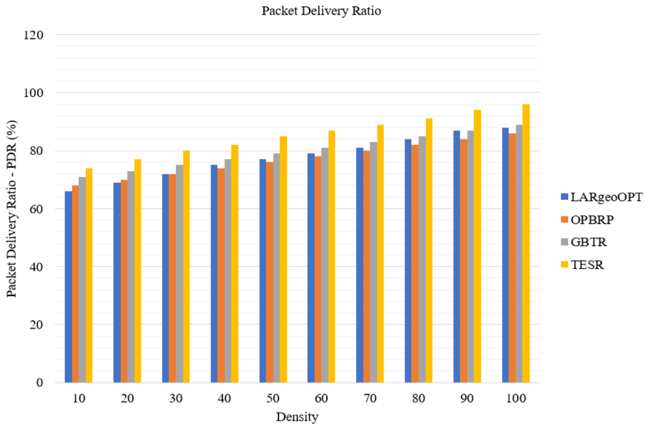

Figure 7. PDLR against density of vehicles.

Table 4. PDLR of proposed vs existing methods.

No	LARgeoOPT	OPBRP	GBTR	TEST
10	66	68	71	74
20	69	70	73	77
30	72	72	75	80
40	75	74	77	82
50	77	76	79	85
60	79	78	81	87
70	81	80	83	89
80	84	82	85	91
90	87	84	87	94
100	88	86	89	96

The trust model eliminates untrustworthy nodes and reduces redundant data transmission, resulting in better packet delivery inside dense networks.

5.2. Packet Drop Ratio

Table 5 and Figure 8 compare PDR for suggested TESR, GBTR, LARgeoOPT, KMRP, and OPBRP. Increased vehicle density leads to lower PDR (%) as more vehicles generate and use the channel, causing packet drops owing to congestion. TESR has a lower PDR (%) than GBTR, LARgeoOPT, and OPBRP. At 100 vehicle density, the PDR of proposed TESR, GBTR, OPBRP, and LARgeoOPT are 6%, 9%, 12%, and 15%, respectively. In this circumstance, TESR outperforms other methods in dropped packet ratio, with a 25-30% improvement. Moreover, for 80 vehicle density, the DPR of suggested TESR, GBTR, LARgeoOPT, and OPBRP are 11%, 14%, 16%, and 18%, respectively. Furthermore, under all circumstances, the TESR scheme achieves the lowest dropped packet ratio, with GBTR, OPBRP, and LARgeoOPT closely following.

Table 5. Packet drop ratio of proposed vs existing methods.

No	LARgeoOPT	OPBRP	GBTR	TESR
20	46	41	38	35
40	33	29	26	21
60	24	21	18	15
80	18	16	14	11
100	15	12	9	6

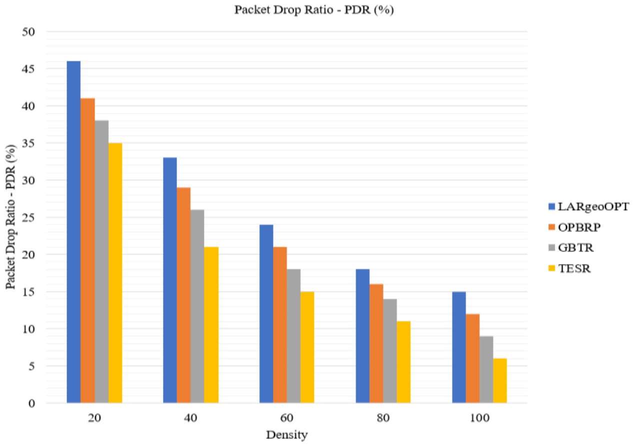

Figure 8. Dropped packets ratio vs density of vehicles.

5.3. Throughput

Figures 9 and 10 illustrate how vehicle velocity and density affect suggested TESR, LAR-geoOPT, OPBRP, and GBTR throughput. TESR outperforms GBTR, LARgeoOPT, and OPBRP in all vehicle density and velocity scenarios because of its efficient routing algorithm and trust concept, resulting in higher throughput and improved PDLR. The throughput parameter is used to measure the performance of the proposed method in terms of impact on scalability. A receiver's throughput is the sum of all data from the sender until the last packet transmission ends. As the number of vehicles increases, congestion and network collapses.

The proposed method handles scalability by calculating the trust of the vehicles hop by hop. The throughput of the proposed method decreases as the number of vehicles increases in the network, impacting scalability. However, the throughput of the proposed method is far better compared to the existing protocols regarding the number of vehicles. Even if vehicles increase abnormally, creating a dense network may lead to severe congestion.

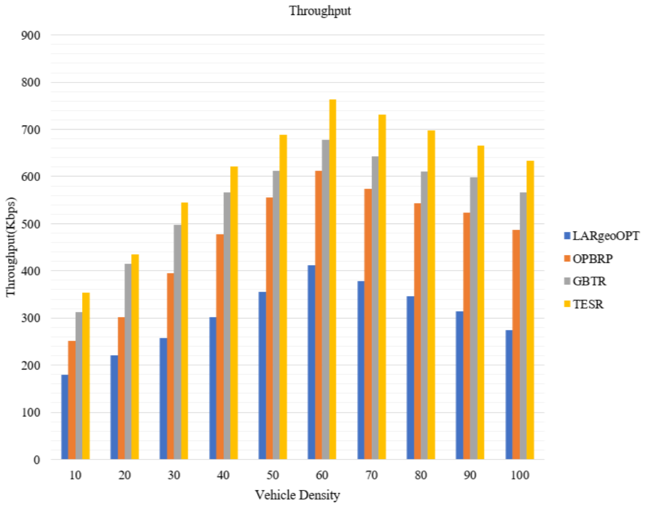

Figure 9. Throughput vs density of vehicles.

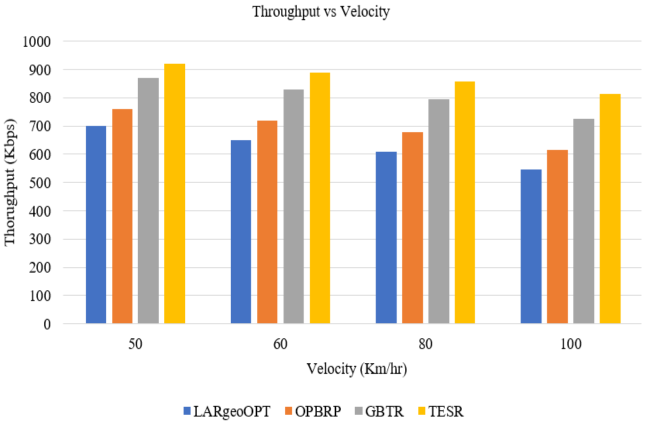

Figure 10. Throughput vs velocity of vehicle.

The throughput variation in scalability for the proposed and existing algorithms is shown in Figure 9. As vehicle velocity increases, throughput falls for all methods due to VANET's dynamic nature and link failure likelihood. While all methods experience diminishing throughput with increasing velocity, the suggested strategy TESR outperforms GBTR, LARgeoOPT, and OPBRP due to link reliability factor incorporation during NDT evaluation. The suggested system TESR improves throughput by achieving good PDLR and reduced latency. Tables 6 and 7 depict the throughput states compared to vehicles' velocity and density. Assuming 80 km/h vehicle velocity, suggested TESR, GBTR, OPBRP, and LARgeoOPT have throughputs of 858, 795, 678, and 610 kbps, respectively. Assuming 100 km/h vehicle velocity, suggested TESR, GBTR, OPBRP, and LARgeoOPT have throughputs of 812, 725, 615, and 545 kbps, respectively. Moreover, at 120 km/h vehicle speed, proposed TESR, GBTR, OPBRP, and LARgeoOPT achieve throughputs of 756, 686, 558, and 495 kbps, respectively. TESR surpasses GBTR, OPBRP, and LARgeoOPT by 60%, 74%, and 90%, respectively.

Table 6. Throughput of proposed and existing methods w.r.t density of vehicles.

No	LARgeoOPT	OPBRP	GBTR	TESR
10	179	252	312	354
20	221	302	415	435
30	258	395	498	545
40	302	478	567	622
50	356	556	612	689
60	412	612	678	764
70	378	574	643	732
80	346	543	610	698
90	314	523	598	665
100	275	487	567	634

Table 7. Throughput of proposed and existing methods w.r.t velocity of vehicles.

No	LARgeoOPT	OPBRP	GBTR	TESR
50	700	760	870	920
60	650	720	830	890
80	610	678	795	858
100	545	615	725	812
120	495	558	686	756

5.4. End-to-End Delay

Table 8 and Figure 11 illustrate how vehicle density affects end-to-end delay (E2E-D) for suggested TESR, GBTR, LARgeoOPT, and OPBRP. TESR has a lower end-to-end delay than GBTR, LARgeoOPT, and OPBRP in all vehicle density scenarios because of its lightweight trust model and rapid routing algorithm, which selects reliable routes with fewer link failures.

Table 8. End-to-end delay of proposed and existing methods w.r.t density of vehicles.

No	LARgeoOPT	OPBRP	GBTR	TESR
10	2.8	2.55	2.43	2.36
20	2.3	2.21	2.03	1.97
30	1.9	1.85	1.54	1.35
40	1.4	1.34	1.21	1.01
50	1.1	1.02	0.98	0.78
60	1.35	1.29	1.24	1.16
70	1.98	1.76	1.64	1.35
80	2.4	2.21	1.98	1.65
90	2.7	2.56	2.34	1.95
100	2.9	2.68	2.45	2.25

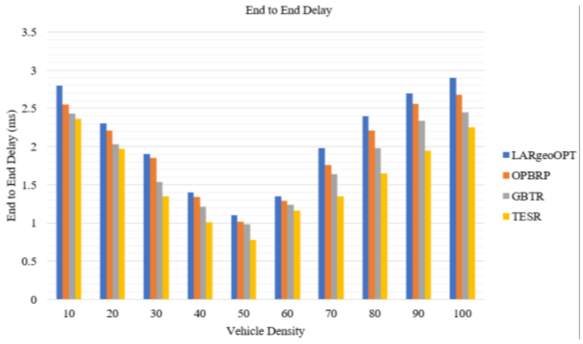

Figure 11. End-to-end delay vs density of vehicles.

The proposed scheme evaluates NDT by considering link reliability to reduce failure chances. At 100 vehicle density, the E2E-D of suggested TESR, LARgeoOPT, OPBRP, and GBTR are 2.25, 2.45, 2.9, and 2.68 ms, respectively. TESR surpasses other systems, such as E2E-D, by 4.15 to 28.29 percent. The suggested TESR, GBTR, LARgeoOPT, and OPBRP have E2E-D values of 1.95 ms, 2.34 ms, 2.7 ms, and 2.56 ms, respectively, with a vehicle density of 90. Additionally, the TESR scheme has the lowest E2E-D across all scenarios, followed by GBTR, OPBRP, and LARgeoOPT. The proposed TESR supports a faster message transmission technique compared to existing methods.

5.5. Overhead

The effect of vehicle density on routing load (RL) is seen in Figure 12 and Table 9. All schemes show that RL increases as the number of vehicles increases because a greater number of vehicles share the same wireless channel. But in every instance, the RL value in the suggested system TESR is lower than that of GBTR, LARgeoOPT, and OPBRP. The current routing protocols treat every vehicle on the network as an equal and allow any vehicle to take part in routing packets. Even if some vehicles aren't dependable, this can cause the network to have more load to forward packets. To solve this problem, the proposed TESR employs a trust-based routing strategy, in which each vehicle's reputation is built up by its interactions with other vehicles and its previous actions in the network. Next, the routing options are decided on the trust values, ensuring that only the most trustworthy and dependable routes are chosen to forward packets. Reduced network routing burden is achieved by TESR by a combination of utilizing only the most trustworthy connections and minimizing the number of vehicles involved in packet routing. By limiting routing to trusted vehicles only, network efficiency is enhanced, and the risk of malicious attacks or data tampering is reduced. The routing load of the suggested TESR, GBTR, LARgeoOPT, and OPBRP systems, with a vehicle density of 100, are 278, 376, 624, and 390 packets/sec, respectively. Compared to GTBR, LARgeoOPT, and OPBRP, TESR significantly outperforms them in this worst-case scenario, with improvements of 28.50%, 21.46%, and 18.65%, respectively. The proposed TESR method required less network behavior and route discovery information, reducing computational overhead and making it suitable for dynamic and ascendable networks. Here the trust values, once computed over a period of time are broadcasted to all the nodes. The same can be used by the nodes for further route discovery in terms of trusted vehicles. This reduces computational overhead significantly.

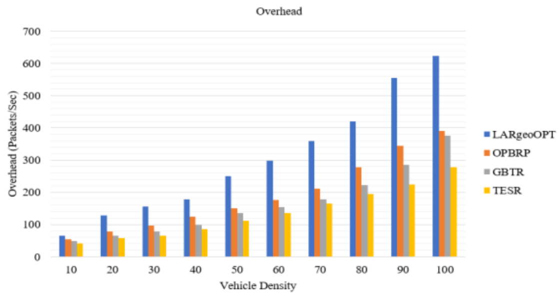

Figure 12. Routing overhead vs density of vehicles.

Table 9. Routing overhead of proposed and existing methods w.r.t velocity of vehicles.

No	LARgeoOPT	OPBRP	GBTR	TESR
10	65	54	48	42
20	128	78	65	58
30	156	96	78	65
40	178	125	98	85
50	250	150	135	112
60	298	176	154	135
70	359	212	178	165
80	420	278	223	194
90	556	345	286	225
100	624	390	376	278

5.6. Latency

The network latency also increases slightly but not significantly for the proposed method compared to the existing protocols. The effect of vehicle density on latency is seen in Figure 13 and Table 10. All methods show that latency increases as the number of vehicles increases. But in every instance, the latency value in the suggested system TESR is lower than that of GBTR, LARgeoOPT, and OPBRP. The latency of the suggested TESR, GBTR, LARgeoOPT, and OPBRP systems, with a vehicle density of 100, are 34, 46, 57, and 122 ms, respectively. Compared to GTBR, LARgeoOPT, and OPBRP, TESR significantly outperforms them in this worst-case scenario.

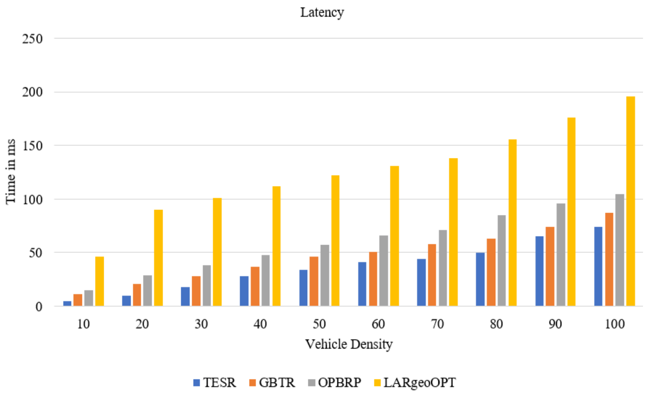

Figure 13. Latency vs density of vehicles.

Table 10. Latency of proposed and existing methods w.r.t density of vehicles.

No	TESR	GBTR	OPBRP	LARgeoOPT
10	5	11	15	46
20	10	21	29	90
30	18	28	38	101
40	28	37	48	112
50	34	46	57	122
60	41	51	66	131
70	44	58	71	138
80	50	63	85	156
90	65	74	96	176
100	74	87	105	196

5.7. Performance on Networks with Higher Density of Vehicles (Urban Areas)

The performance analysis of the proposed TESR on networks with a higher density of vehicles in urban areas is depicted in Figure 14 and Table 11. The four metrics of these tests had average values of 84% PDLR, 67.63% Throughput, 32% PDR, and 3.6% latency.

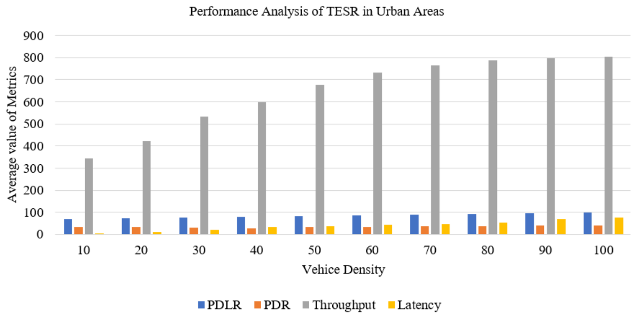

Figure 14. Performance analysis of TESR in urban areas.

Table 11. Performance analysis of TESR in Urban areas.

No	PDLR	PDR	Throughput	Latency
10	71	35	345	5
20	74	32	423	11
30	76	30	534	19
40	78	28	598	32
50	84	32	676	36
60	85	34	732	43
70	89	37	765	45
80	93	38	789	53
90	96	40	798	68
100	98	41	803	76

5.8. Real-World Application Case Study

The suggested Trust Enabled Secure Routing (TESR), is also tested on a real-world traffic model derived from a street map in Hyderabad city, India, which helps to bridge the gap between virtual and physical settings. This implementation of a real-world application uses the real-world traffic model [12] included in the ns-3 distribution to simulate the starting position, mobility, and speed of cars. It takes 300 seconds and offers three different settings for traffic density: low, medium, and high. Table 12 details the simulation parameters that differ from Table 2.

Table 12. Real-world traffic model simulation parameters.

Parameter name	Value
Simulation area	4.6 km x 3.0 km street map
Number of vehicles	110 (low), 220 (medium), 330 (high)
Speed range of vehicles	(10-100) kmph
Mobility model	real-world traffic data model
Size of packet	1024 Bytes
Simulation time	240 s
Maximum transmission range	400 m
Mac protocol	IEEE802.11p
Range of trust value	[0 to 10]
Trust threshold value	5m
Strategy for weights assignments	Equal weights

The four metrics of these tests had average values of 80.68% PDLR, 70.3% Throughput, 18% PDR, and 3.6% latency. The model performs admirably on a real-world traffic model, as demonstrated by these test results as well. Additionally, the suggested TESR protects the real-world traffic model from false information assaults and has practical applications. Figure 15 and Table 13 demonstrate the real word testing performance of the proposed method TESR.

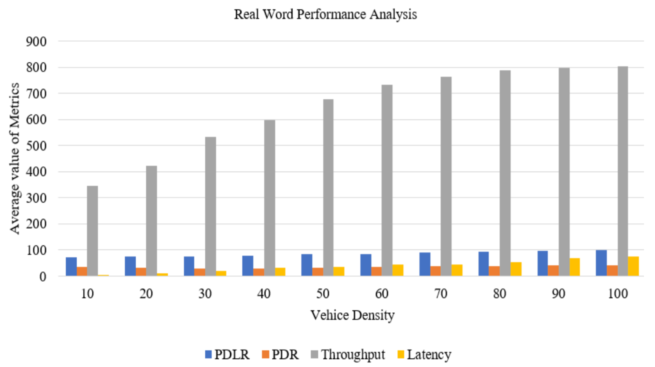

Figure 15. Performance analysis of TESR in real-world traffic model.

Table 13. Real-world traffic model performance analysis of TESR.

No	PDLR	PDR	Throughput	Latency
10	70		345	7
20	74	39	423	13
30	76		534	21
40	77	30	612	32
50	81		643	36
60	83	18	732	45
70	84		704	48
80	86	15	687	54
90	88		635	68
100	91	10	624	77

6. Conclusions

VANETs allow vehicles to communicate with each other and with roadside infrastructure. VANETs rely heavily on trust-based routing to improve vehicle-to-vehicle communication efficiency, security, and dependability. In this research, Trust Enabled Secure Routing (TESR) for VANETs, which evaluates nodes' trustworthiness using four types of trust: direct, indirect, situational, and experience, is proposed.

DT considers frequency, consistency, communication, mobility, and latency. Link dependability, feedback trust value, and mobility comprise NDT. When building trust between node pairs, weather, traffic density, and time of day are considered. Successful node communication affects experience trust. Without losing sensitive data, the routing algorithm identifies the trustworthy path using the final trust score. The request/reply and route management methods of the routing algorithm provide VANET data transmission reliability. End-to-end delay (ms), throughput (Kbps), normalized routing load (packets/sec), PDLR%, and Packet Dropped Ratio (PDR%), are the performance metrics used to evaluate the proposed scheme TESR through veins (3.0) simulator. Experimental results demonstrate that the proposed system TESR improves previous methods by ensuring VANET security and reliability. Addressing the failures of the suggested routing strategy should be the focus of future research. This includes better ways for selecting trustworthy paths and updating the dynamic trust model. Another field that needs more research is how to use sensor fusion and machine learning to make vehicle position and movement data more accurate and trustworthy. Furthermore, future studies need to investigate methods for dealing with routing constraints in highly crowded or interfering situations.

Acknowledgment

The authors would like to thank Deanship of Scientific Research at Majmaah University for supporting this work under Project Number R-2025-1636.

References

[1] Abdalla A. and Salamah S., "Performance Comparison between Delay-Tolerant and Non-Delay-Tolerant Position-Based Routing Protocols in VANETs," *International Journal of Communications, Network and System Sciences*, vol. 15, no. 1, pp. 1-14, 2022. file:///C:/Users/user/Downloads/Performance_Comparison_between_Delay-Tolerant_and_.pdf

[2] Akter S., Shahriar Rahman M., Bhuiyan M., and Mansoor N., "Towards Secure Communication in CR-VENTs through a Trust-Based Routing Protocol," *in Proceedings of the IEEE INFOCOM-IEEE Conference on Computer Communications Workshops*, Vancouver, pp. 1-6, 2021. https://doi.org/10.1109/infocomwkshps51825.2021.9484515

[3] Alam I., Manjul M., Pathak V., Mala V., Mangal A., ThakurH., and Sharma D., "Efficient and Secure Graph-based Trust-Enabled Routing in Vehicular Ad-Hoc Networks," *Mobile Networks and Applications*, pp. 1-21, 2024. https://link.springer.com/article/10.1007/s11036-023-02274-9

[4] Alharbi A. and Alsubhi K., "Botnet Detection Approach Using Graph-based Machine Learning," *IEEE Access*, vol. 9, pp. 99166-99180, 2021. https://doi.org/10.1109/access.2021.3094183

[5] Bangotra D., Singh Y., Selwal A., Kumar N., and Singh P., "A Trust-Based Secure Intelligent Opportunistic Routing Protocol for Wireless Sensor Networks," *Wireless Personal Communications*, vol. 127, no. 2, pp. 1045-1066, 2022. https://doi.org/10.1007/s11277-021-08564-3

[6] Belamri F., Boulfekhar S., and Aissani D., "A Survey on QoS Routing Protocols in Vehicular Ad Hoc Network (VANET)," *Telecommunication Systems*, vol. 78, no. 1, pp. 117-153, 2021. https://doi.org/10.1007/s11235-021-00797-8

[7] Bousbaa F., Kerrache C., Lagraa N., Hussain R., Yagoubi M., and Tahari A., "Group Data Communication in Connected Vehicles: A Survey," *Vehicular Communications*, vol. 37, pp. 100518, 2022. https://doi.org/10.1016/j.vehcom.2022.100518

[8] BrijilalRuban C. and Paramasivan B., "Energy Efficient Enhanced OLSR Routing Protocol Using Particle Swarm Optimization with Certificate Revocation Scheme for VANET," *Wireless Personal Communications*, vol. 121, pp. 2589-2608, 2021. https://doi.org/10.1007/s11277-021-08838-w

[9] Choksi A. and Shah M., "Machine Learning Based Centralized Dynamic Clustering Algorithm for Energy Efficient Routing in Vehicular Ad Hoc Networks," *Transactions on Emerging Telecommunications Technologies*, vol. 35, no. 1 pp. e 4914, 2024. https://doi.org/10.1002/ett.4914

[10] Choksi A. and Shah M., "Neural Network-based Dynamic Clustering Model for Energy Efficient Data Uploading and Downloading in Green Vehicular Ad-Hoc Networks," *International Journal of Next-Generation Computing*, vol. 14, no. 3, pp. 502-521, 2023. file:///C:/Users/user/Downloads/PublishedIJNGC Paper.pdf

[11] De Francesco C., Palazzi C., and Ronzani D., "Fast Message Broadcasting in Vehicular Networks: Model Analysis and Performance Evaluation," *IEEE Communications Letters*, vol. 24, no. 8, pp. 1669-1672, 2020. https://doi.org/10.1109/lcomm.2020.2993006

[12] Diaa M., Khalid I., Mohamed I., and Hassan M., "OPBRP-Obstacle Prediction-Based Routing Protocol in VANETs," *Ain Shams Engineering Journal*, vol. 14, no. 7, pp. 101989, 2023. https://doi.org/10.1016/j.asej.2022.101989

[13] Eiza M. and Ta V., "An Indirect Social Trust Model for Vehicular Social Networks Using Evolving Graph Theory," *arXiv Preprint*, vol. arXiv:arXiv:2206.13144v1, pp. 1-6, 2022. https://doi.org/10.48550/arXiv.2206.13144

[14] Fatemidokht H., Rafsanjani M., Gupta B., and Hsu C., "Efficient and Secure Routing Protocol Based on Artificial Intelligence Algorithms with UAV-Assisted for Vehicular Ad Hoc Networks in Intelligent Transportation Systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 4757-4769, 2021. https://doi.org/10.1109/tits.2020.3041746

[15] Gazdar T., Alboqomi O., and Munshi A., "A Decentralized Blockchain-based Trust Management Framework for Vehicular Ad Hoc Networks," *Smart Cities*, vol. 5, no. 1, pp. 348-363, 2022. https://doi.org/10.3390/smartcities5010020

[16] Gupta B., Gaurav A., Marin E., and Alhalabi W., "Novel Graph-based Machine Learning Technique to Secure Smart Vehicles in Intelligent Transportation Systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 8, pp. 8483-849, 2023. https://doi.org/10.1109/TITS.2022.3174333

[17] Gupta M., Gera P., and Mishra B., *Inventive Communication and Computational Technologie*, Springer Nature Singapore, 2022. https://link.springer.com/book/10.1007/978-981-19-4960-9

[18] Hamdi M., Al-Dosary O., Alrawi., Mustafa A., Abood M., and Noori M., "An Overview of Challenges for Data Dissemination and Routing Protocols in VANETs," *in Proceedings of the 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications*, Ankara, pp. 1-6, 2021. https://doi.org/10.1109/hora52670.2021.9461396

[19] Husain A., Singh S., and Sharma S., "PSO Optimized Geocast Routing in VANET," *Wireless Personal Communications*, vol. 115, pp. 2269-2288, 2020. https://doi.org/10.1007/s11277-020-07681-9

[20] Jaballah W., Conti M., and Lal C., "Security and Design Requirements for Software-Defined VANETs," *Computer Networks*, vol. 169, pp. 107099, 2020. https://doi.org/10.1016/j.comnet.2020.107099

[21] Jiang J., Wei W., Shao W., Liang Y., and Qu Y., "Research on Large-Scale Bi-Level Particle Swarm Optimization Algorithm," *IEEE Access*, vol. 9, pp. 56364-56375, 2021. https://doi.org/10.1109/access.2021.3072199

[22] Kadam M., Vaze V., and Todmal S., "TACR: Trust Aware Clustering-Based Routing for Secure and Reliable VANET Communications," *Wireless Personal Communications*, vol. 132, no. 1, pp. 305-328, 2023. https://doi.org/10.1007/s11277-023-10612-z

[23] Kamboj S., Mann K., and Kaur S., "An Optimized Multiple Malicious Node Detection Method for Detection of Security Attacks in VANETs," *in Proceedings of the 2nd International Conference on Computational Methods in Science and Technology*, Mohali, pp. 152-157, 2021. https://doi.org/10.1109/iccmst54943.2021.00041

[24] Kandali K., Bennis L., and Bennis H., "A New Hybrid Routing Protocol Using a Modified K-Means Clustering Algorithm and Continuous Hopfield Network for VANET," *IEEE Access*, vol. 9, pp. 47169-47183, 2021. https://doi.org/10.1109/access.2021.3068074

[25] Kaur G. and Kakkar D., "Hybrid Optimization Enabled Trust-Based Secure Routing with Deep Learning-based Attack Detection in VANET," *Ad Hoc Networks*, vol. 136, pp. 102961, 2022. https://doi.org/10.1016/j.adhoc.2022.102961

[26] Kchaou A., Abassi R., and Guemara S., "Towards the Performance Evaluation of a Clustering and Trust-Based Security Mechanism for VANET," *in Proceedings of the 15th International Conference on Availability, Reliability and Security*, Ireland, pp. 1-6, 2020.

https://doi.org/10.1145/3407023.3407071

[27] Khadim S., Riaz F., Jabbar S., Khalid S., and Aloqaily M., "A Non-Cooperative Rear-End Collision Avoidance Scheme for Non-Connected and Heterogeneous Environment," *Computer Communications*, vol. 150, pp. 828-840, 2020. https://doi.org/10.1016/j.comcom.2019.11.002

[28] Kudva S., Badsha S., Sengupta S., La H., Khalil I., and Atiquzzaman M., "A Scalable Blockchain-Based Trust Management in VANET Routing Protocol," *Journal of Parallel and Distributed Computing*, vol. 152, pp. 144-156, 2021. https://doi.org/10.1016/j.jpdc.2021.02.024

[29] Luong N. and Hoang D., "BAPRP: A Machine Learning Approach to Blackhole Attacks Prevention Routing Protocol in Vehicular Ad Hoc Networks," *International Journal of Information Security*, vol. 22, no. 6, pp. 1547-1566, 2023. https://doi.org/10.1007/s10207-023-00705-y

[30] Mahalakshmi G., Uma E., Senthilnayaki B., Devi A., Rajeswary C., and Dharanyadevi P., "Trust Score Evaluation Scheme for Secure Routing in VANET," *in Proceedings of the IEEE International Conference on Mobile Networks and Wireless Communications*, Karnataka, pp. 1-6, 2021. https://doi.org/10.1109/icmnwc52512.2021.9688475

[31] Mahdi H., Abood M, and Hamdi M., "Performance Evaluation for Vehicular Ad-Hoc Networks-Based Routing Protocols," Bulletin of Electrical Engineering and Informatics, vol. 10, no. 2, pp. 1080-1091, 2021. https://doi.org/10.11591/eei.v10i2.2943

[32] Mahi M., Chaki S., Ahmed S., Biswas M., Shamim Kaiser M., Islam M., Sookhak M., Barros A., and Whaiduzzaman M., "A Review on VANET Research: Perspective of Recent Emerging Technologies," *IEEE Access*, vol. 10, pp. 65760-65783, 2022. https://doi.org/10.1109/access.2022.3183605

[33] Maria A., Rajasekaran A., Al-Turjman F., Altrjman C., and Mostarda L., "BAIV: An Efficient Blockchain-based Anonymous Authentication and Integrity Preservation Scheme for Secure Communication in VANETs," *Electronics*, vol. 11 no. 3, pp. 1-20, 2022. https://doi.org/10.3390/electronics11030488

[34] Michael O., Tambuwal A., Chemebe C., Noor R., and Distefano S., "VANETs QoS-based Routing Protocols Based on Multi-Constrained Ability to Support ITS Infotainment Services," *Wireless Networks*, vol. 26, pp. 1685-1715, 2020. https://doi.org/10.1007/s11276-018-1860-7

[35] Muzammal S., Murugesan R., and Jhanjhi N., "A Comprehensive Review on Secure Routing in the Internet of Things: Mitigation Methods and Trust-based Approaches," *IEEE Internet of Things Journal*, vol. 8, no.6 pp. 4186-4210, 2020. https://doi.org/10.1109/jiot.2020.3031162

[36] Naeem A., Rizwan M., Alsubai S., Almadhor A., Akhtaruzzaman M., Islam S., and Hameedur Rahman., "Enhanced Clustering Based Routing Protocol in Vehicular Ad-Hoc Networks," *IET Electrical Systems in Transportation*, vol. 13, no. 1, pp. 1-15, 2023. https://doi.org/10.1049/els2.12069

[37] Reddy M., Srinivas P., and Chandra Mohan M., "Energy Efficient Routing with Secure and Adaptive Trust Threshold Approach in Mobile Ad Hoc Networks," *The Journal of Supercomputing*, vol. 79, no. 12, pp. 13519-13544, 2023. https://doi.org/10.1007/s11227-023-05187-2

[38] Reddy M., Srinivas P., and Mohan M., "Enhancing the Routing Security through Node Trustworthiness Using Secure Trust Based Approach in Mobile Ad Hoc Networks," *International Journal of Interactive Mobile Technologies*, vol. 17, no. 14, pp. 152-170, 2022. https://doi.org/10.3991/ijim.v16i14.30651

[39] Shafi S. and Ratnam D., "A Trust-Based Energy and Mobility Aware Routing Protocol to Improve Infotainment Services in VANETs," *Peer-to-Peer Networking and Applications*, vol. 15, no. 1, pp. 576-591, 2021. https://doi.org/10.1007/s12083-021-01272-6

[40] Shafi S. and Venkata Ratnam D., "An Efficient Cross-Layer Design of Stability Based Clustering Scheme Using Ant Colony Optimization in VANETs," *Wireless Personal Communications*, vol. 126, no. 4, pp. 3001-3019, 2022. https://doi.org/10.1007/s11277-022-09849-x

[41] Shokrollahi S. and Dehghan M., "TGRV: A Trust-Based Geographic Routing Protocol for VANETs," *Ad Hoc Networks*, vol. 140, pp. 103062, 2023. https://doi.org/10.1016/j.adhoc.2022.103062

[42] Shrikant T., Manvi S., and Lorenz P., "Trust Management Scheme Based on Hybrid Cryptography for Secure Communications in VANETs," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 5, pp. 5232-5243, 2020. https://doi.org/10.1109/tvt.2020.2981127

[43] Shrivastava P. and Vishwamitra L., "Comparative Analysis of Proactive and Reactive Routing Protocols in VANET Environment," *Measurement: Sensors*, vol. 16, pp. 100051, 2021. https://doi.org/10.1016/j.measen.2021.100051

[44] Soni M., Dhiman G., Rajput B., Patel R., and Tejra N., "Energy-Effective and Secure Data Transfer Scheme for mobile Nodes in Smart City Applications," *Wireless Personal Communications*, vol. 127, no. 3, pp. 2041-2061, 2022. https://doi.org/10.1007/s11277-021-08767-8

[45] Speiran J. and Shakshuki E., "Understanding the

Effect of Physical Parameters on Packet Loss in Veins VANET Simulato," *Procedia Computer Science*, vol. 201, pp. 359-367, 2022. https://doi.org/10.1016/j.procs.2022.03.048

[46] Sumithra S. and Vadivel R., "Ensemble Miscellaneous Classifiers-based Misbehavior Detection Model for Vehicular Ad-Hoc Network Security," *International Journal of Computer Networks and Applications*, vol. 8, no. 2, pp. 90-107, 2021. https://doi.org/10.22247/ijcna/2021/208890

[47] Temurnikar A., Verma P., and Dhiman G., "A PSO Enable Multi-Hop Clustering Algorithm for VANET," *International Journal of Swarm Intelligence Research*, vol. 13, no. 2, pp. 1-14, 2022. https://doi.org/10.4018/ijsir.20220401.oa7

[48] Tseng H., Chu P., Lu H., and Tsai M., "Easy particle Swarm Optimization for Nonlinear Constrained Optimization Problems," *IEEE Access*, vol. 9, pp. 124757-124767, 2021. https://doi.org/10.1109/access.2021.3110708

[49] Velayudhan N, Anitha A., and Madanan M., "An Optimization-Driven Deep Residual Network for Sybil Attack Detection with Reputation and Trust-Based Misbehavior Detection in VANET," *Journal of Experimental and Theoretical Artificial Intelligence*, vol. 36, no. 5, pp. 721-744, 2022. https://doi.org/10.1080/0952813X.2022.2104387

[50] Venkatamune N. and PrabhaShankar J., "A VANET Collision Warning System with Cloud Aided Pliable Q-Learning and Safety Message Dissemination," *The International Arab Journal of Information Technology*, vol. 20, no. 1, pp. 113-124, 2023. https://doi.org/10.34028/iajit/20/1/12

[51] Wahid I., Tanvir S., Ahmad M., Ullah F., AlGhamdi A., Khan M., and Alshamrani S., "Vehicular Ad Hoc Networks Routing Strategies for Intelligent Transportation System," *Electronics*, vol. 11, no. 15, pp. 1-36, 2022. https://doi.org/10.3390/electronics11152298

[52] Wang R., Li Y., Xu Y., Xie H., Lui J., and He S., "Toward Fast and Scalable Random Walks over Disk-Resident Graphs via Efficient I/O Management," *ACM Transactions on Storage*, vol. 18, no. 4, pp. 1-33, 2022. https://doi.org/10.1145/3533579

[53] Wu J., Fang M., Li H., and Li X., "RSU-Assisted Traffic-Aware Routing Based on Reinforcement Learning for Urban VANETs," *IEEE Access*, vol. 8, pp. 5733-5748, 2020. https://doi.org/10.1109/access.2020.2963850

[54] Xia H., Zhang S., Li B., Li L., and Cheng X., "Towards a Novel Trust-based Multicast Routing for VANETs," *Security and Communication Networks*, vol. 2018, no. 1, pp. 1-12, 2018. https://doi.org/10.1155/2018/7608198

[55] Xia Z., Wu J., Wu L., Chen Y., Yang J., and Yu P., "A Comprehensive Survey of the Key Technologies and Challenges Surrounding Vehicular Ad Hoc Networks," *ACM Transactions on Intelligent Systems and Technology*, vol. 12, no. 7, pp. 1-30, 2021. https://doi.org/10.1145/3451984

[56] Xu S., Li H., Li T., and Li S., et al., "Neutrophil Extracellular Traps and Macrophage Extracellular Traps Predict Postoperative Recurrence in Resectable Nonfunctional Pancreatic Neuroendocrine Tumors," *Frontiers in Immunology*, vol. 12, pp. 1-9, 2021. https://doi.org/10.3389/fimmu.2021.577517

[57] Yao X., Farha F., Li R., Psychoula I., Chen L., and Ning H., "Security and Privacy Issues of Physical Objects in the IoT: Challenges and Opportunities," *Digital Communications and Networks*, vol. 7, no. 3, pp. 373-384, 2021. https://doi.org/10.1016/j.dcan.2020.09.001

M Venkata Krishna Reddy was born in Hyderabad, Telangana, India in 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. He received his Ph.D.in CSE from JNTUH, Hyderabad. Currently, he is doing research in the field of Mobile ad hoc networks, the Internet of Things, and Cloud Computing. He has more than 17 years of teaching experience. He published more than 40 publications in reputed international journals and conferences. He is working as an Assistant, Professor in the Computer Science Engineering Department, Chaitanya Bharathi Institute of Technology CBIT(A), Gandi pet, Hyderabad, India.

G Kiran Kumar (Member, IEEE) received his PhD from Acharya Nagarjuna University, Andhra Pradesh, India, and an M.Tech from Osmania University, Hyderabad, India. He works as an Associate Professor at Chaitanya Bharathi Institute of Technology, Hyderabad. He has more than 20 years of teaching experience. He published more than 20 publications in international journals and conferences of repute. His research interests include Data Mining, Machine Learning, Deep Learning, and Image processing.

Panduranga Vital Terlapu obtained his Bachelor of Science in Computer Science from Andhra University in A.P, India, in 1995 and completed his Master of Computer Application from Andhra University in 1998. He pursued his M. Tech in Computer Science and Engineering from Acharya Nagarjuna University in A.P., India. He completed his PhD in Computer Science and Engineering from GITAM University in A.P., India. With 24 years of teaching and 18 years of research experience, he currently holds the position of Professor in the Department of Computer Science and Engineering at Aditya Institute of Technology and Management (AITAM), India. Dr. Terlapu is an esteemed member of the Association for Computing Machinery (ACM) and holds Lifetime Memberships from the International Computer Science and Engineering Society (ICSES), USA, and the Indian Society for Technical Education (ISTE), New Delhi, India, and has five reputed memberships with the close Association. Dr. Terlapu has contributed to the field of computer science with over 72 research papers published in reputed international journals, including SCI, SCOPUS-indexed journals, and conferences published by IEEE, Springer, Elsevier and available online. He also reviews reputable journals from Springer, Elsevier, and IEEE databases. His primary research focuses on Machine Learning, Image Processing and Deep Learning, Data Mining, Data and Big Data Analytics, IoT and Computational Intelligence, Voice Analysis and Voice Processing, signal processing, and Bioinformatics.

D. Jayaram (Member, IEEE) received the Master of Computer Applications degree from Andhra University, Visakhapatnam, India, in 1998, the M. Tech. Degree in CSE from Osmania University, Hyderabad, India, in 2007, and the Ph.D. degree from JNTU, Hyderabad, in 2022. He is currently an Assistant Professor at the Department of Information Technology, Chaitanya Bharathi Institute of Technology (A), Hyderabad. He has more than 23 years of teaching experience. His research interests include machine learning, deep learning, image processing, and natural language processing. He has published two patents and over 25 publications in various international journals and conferences. He is a Life Member of ISTE.

Shirina Samreen is an Associate Professor in the Department of Computer Science, College of Computer and Information Sciences, Majmaah University, Kingdom of Saudi Arabia. She received her Ph.D in Computer Science and Engineering from JNTUH, India in 2016. She received best paper awards twice for her research papers at IEEE ICCIC, a renowned international conference. She is a reviewer for IEEE Access, IEEE Wireless Communication Magazine, Journal of Engineering and Applied Sciences (JEAS), and numerous other peer-reviewed International Journals. She has over 40 research papers to her credit in various IEEE International conferences and SCI/Scopus indexed Journals. Currently, her research interests include Cyber Security, Applied machine learning, and Deep learning.