Received: 9 April 2025 | Revised: 16 June 2025 | Accepted: 24 June 2025 | Published online: 21 August 2025

RESEARCH ARTICLE

Journal of Computational and Cognitive Engineering
2025, Vol. 00(00) 1–10
DOI: 10.47852/bonviewJCCE52025875

BON VIEW PUBLISHING

Trust-Driven Secure Routing Protocols for Optimized Communication in Vehicular Networks

Subramaniyan Kalpana Devi[1] and Ramasamy Thenmozhi[1,*]

[1] *Department of Computing Technologies, SRM Institute of Science and Technology-Kattankulathur, India*

Abstract: Vehicular Ad-hoc Networks (VANETs) maintain the super capability of remodeling transportation structures via presentation of a whole lot of programs, ranging from improving road protection to supplying recreational services . However, the dynamic and decentralized nature of VANETs via layout affords giant problems, specifically in dealing with successful facts routing while ensuring robust protection and protective personal privacy. To cope with such troubles, this study introduces the Secure and Efficient Vehicular Ad-hoc Network Routing (SEVAN-R) protocol, a unique answer designed specifically for VANET settings. SEVAN-R combines some present-day functions in order to obtain the dual objectives of boosting protection and improving efficiency in VANET connections. The usage of nodes as sentinels, which watch over nearby nodes to assess their reliability, is a crucial issue of SEVAN-R. By identifying and setting apart probably dangerous nodes, a distributed selection approach can be given as an authentic method that reduces the danger of information alteration or unauthorized admission . Furthermore, SEVAN-R integrates many security layers to ensure the integrity of the computer. These include structures for inspecting the sentinels' historic conduct patterns in order to confirm their dependability and integrity. The proposed method minimizes the possibility of manipulation or tampering by utilizing sophisticated techniques to shield the integrity of records applied in consideration reviews. The results demonstrate that SEVAN-R outperforms existing methods, achieving an 85% Packet Delivery Ratio (PDR), an 80% throughput, a 75% reduction in delay, and a 90% trust management score. These outcomes highlight the framework's novelty in enhancing network reliability and security, especially in environments with high mobility and varying traffic densities.

Keywords: Vehicular Ad-hoc Networks, security, efficiency, trust model, sentinel nodes

1. Introduction

Vehicular Ad-hoc Networks (VANETs) are a unique generation of intelligent transportation systems that can revolutionize transportation structures by facilitating quite several programs, from entertainment activities to better road protection . By allowing communication among automobiles and between motors and infrastructure alongside the direction, those networks create a dynamic, self-organizing community topology. However, the specific characteristics of VANETs—consisting of high mobility, quick changing topologies of the community, and strict necessities for real-time verbal exchange—create good-sized boundaries to the transmission of steady and environmentally friendly information [1–3].

The focus of new studies has been totally on increasing routing protocols, specifically those created for VANET systems. These protocols are critical in figuring out how information is shipped throughout the community nodes and infrastructure nodes. Ensuring dependable and prompt facts transfer even with optimized network resources, such as energy and bandwidth, is the primary desire . Because of a variety of things, accomplishing this desire within the context of VANETs is intrinsically challenging [4, 5].

First, because of the high node mobility, the network topology is regularly modified, resulting in dynamic and sudden verbal exchange styles. Because of their common reliance on predetermined routing pathways and assumptions of dependable network situations, conventional routing protocols created for continuous infrastructure networks will no longer be suitable for VANETs [6–10]. During evaluation, VANET routing protocols must adjust to the fast converting environment and effectively take care of commonplace connection screw-ups and node conduct.

Second, the running environment of VANETs is exceedingly dynamic and resource-limited, which gives additional challenges to the design of routing protocols. Because of the restricted processing and communication competencies of VANET nodes, routing protocols that can be lightweight and power-efficient have to be evolved so that they will lessen overhead and increase intake. Furthermore, tight latency requirements on routing protocols are imposed through the real-time nature of many VANET applications, including website traffic control and collision avoidance, which disrupts decision-making procedures and transmission of inexperienced messages.

Furthermore, due to the viable outcomes of adversarial assaults and illegal admission to touchy facts, safety and privacy are important worries in VANETs. Because VANETs are open and decentralized, they're liable to quite a few security risks, inclusive of denial-of-provider assaults, eavesdropping, and message spoofing. Thus, keeping trust and dependability inside the network depends on ensuring the validity, secrecy, and integrity of verbal interaction in VANETs.

In response to those difficulties, researches have placed forth a lot of routing protocols and safety features designed particularly for VANET structures. To deal with the unique needs and traits of VANETs, these protocols rent lots of strategies, inclusive of agreement-primarily based routing, opportunistic forwarding, and spatial routing. Although

***Corresponding author:** Ramasamy Thenmozhi, Department of Computing Technologies, SRM Institute of Science and Technology-Kattankulathur, India. Email: thenmozr@srmist.edu.in

studies based totally on simulations have provided treasured insights into how those processes function in controlled environments, actual-world multinational studies are important to affirm their efficacy in actual-world deployment instances.

To address the difficult eventualities of routing and protection in VANETs, taking a look at the Secure and Efficient Vehicular Ad-hoc Network Routing (SEVAN-R) protocol is a unique answer . SEVAN-R leverages nodes' cooperative efforts to accumulate and mitigate safety risks, integrating modern techniques to enhance the overall performance and protection of document transmission in VANETs. Using huge-scale actual-international tests and normal overall performance evaluations, we exhibit the efficacy of SEVAN-R in augmenting network normal overall performance and resilience towards a couple of safety breaches.

An evaluation of recent studies on VANET routing protocols and security features can be discovered in the sections that follow. We talk about the key troubles and roadblocks of present-day strategies and discover the study gaps that motivate further development of SEVAN-R. Next, we define the layout principles and salient traits of SEVAN-R, emphasizing its cutting-edge safety and performance-improving techniques in the VANET communique. Lastly, we provide the experimental technique that we utilized to evaluate the overall performance of SEVAN-R and the percentage of the effects and insights from our research. The contribution of the work is given as follows.

Advanced trust management mechanisms that guarantee the dependability and credibility of participating vehicles are integrated into the SEVAN-R framework. This is made possible by a dynamic trust evaluation system that responds to changes in network conditions by continuously observing and evaluating vehicle behavior.

Using a context-aware routing algorithm that adjusts to changing traffic densities and mobility patterns, SEVAN-R maximizes routing efficiency. Comparing this to conventional methods yields lower delays and higher Packet Delivery Ratios (PDRs). The framework is made to adapt to various urban environments and scale effectively as the number of vehicles increases. In a variety of traffic scenarios, this flexibility is essential to sustaining network performance. To defend against common VANET threats like Sybil attacks, data tampering, and eavesdropping, SEVAN-R has strong security protocols . In order to protect vehicle identities without compromising communication integrity, privacy-preserving measures are also used. By addressing these critical aspects, the SEVAN-R framework significantly improves the overall performance of VANETs, making it a viable solution for next-generation intelligent transportation systems. The main contributions are as follows:

1) Proposing the SEVAN-R framework, a trust-based routing model designed specifically for dynamic VANET environments.
2) Developing a comprehensive trust evaluation method that incorporates packet delivery behavior, protocol adherence, and security responsiveness.
3) Integrating security mechanisms and trust-based decision-making into routing to enhance communication reliability and safety.
4) Conducting extensive simulations using realistic mobility models and varying traffic densities to evaluate the performance of the proposed framework.
5) Demonstrating improved performance over existing methods in terms of PDR, delay, throughput, and trust management.

2. Literature Review

Recently, there has been a lot of interest in VANETs due to their potential to improve site visitor waft, road safety, and overall riding enjoyment. Nodes in VANETs talk with roadside infrastructure and one another to alternate statistics on traffic congestion, kingdom of the avenue, and other applicable facts. Applications like amusement offerings, site traveler control, and the twist of fate avoidance depend upon the records' efficient routing. Many routing protocols have been created with the purpose of addressing the particular tough conditions that arise at the same time as the usage of VANET systems. These protocols are typically divided into three foremost classes: proactive, reactive, and hybrid. Routing tables are up to date for every area inside the network through proactive protocols like Destination Sequenced Distance Vector (DSDV) and Optimized Link State Routing (OLSR), which prioritize rapid direction discovery at the price of accelerated manipulation overhead. Reactive protocols, along with Dynamic Source Routing (DSR) and Ad-hoc On-call for Distance Vector (AODV), set up routes simplest when needed, reducing control overhead at the fee of probably extended latency in the course of direction constructing. To satisfy the dynamic nature of VANET structures, hybrid protocols integrate elements of proactive and reactive strategies to balance overhead and latency, together with Zone-based Hierarchical Link State (ZHLS) routing. The VANET-based total Privacy-Preserving Communication Scheme (VPPCS), placed out with the aid of Al-Shareeda et al. [11], has made a significant contribution to this area. By employing cryptographic strategies to anonymize communications among nodes, VPPCS targets to hold consumer privacy. Further study is necessary to decide the scheme's real viability and scalability in actual global deployments, supposing it shows promise for improving privacy and protection in VANETs [12]. Furthermore, Alaya and Sellami [13] offer an analysis specialized in shielding city VANET networks with the use of a clustering approach blended with symmetric and asymmetrical encryption. This approach aims to lessen protection vulnerabilities in VANETs via clustering nodes and enforcing cryptographic protocols. However, further assessment is needed to ascertain whether this method has an impact on community performance in addition to its scalability and flexibility in one-of-a-kind VANET structures. Soundararajan et al. [14] provide a Secure and Covert Watchdog Selection Scheme for Wi-Fi sensor networks that make use of a disguised distributed selection approach. While it is not extraordinary to VANETs, this system provides a modern-day technique for reinforcing security in wireless verbal exchange networks. We still need to investigate its usefulness and efficacy in VANET settings, which might be characterized by way of mobility and dynamic community situations. Christopher Paul et al. [15] offer a powerful authentication machine that makes use of a monitoring method to pick out misbehaving nodes in cell ad-hoc networks (MANETs). Although this methodology no longer at once follows VANETs, it does offer a few beneficial insights into possible approaches to improve safety in ad-hoc community conditions. To adapt and prove its efficacy in VANETs, which have specific necessities and functions, more studies are essential. Yan et al. [16] provide an occasion accept as true with a model based totally on statistical evaluation for accept as true with control in VANETs. Using past data to compute event consider ratings, this approach seeks to enhance the reliability assessment of events provided through nodes in VANETs. Although the model offers a viable manner to enhance occasion verification and selection-making in VANETs, greater studies are necessary to determine how properly it plays in dynamic contexts and if it may scale to large-scale deployments. Lastly, based on beyond contacts, Gao et al. [17] offer a hybrid technique to accept as true with node evaluation and control for cooperative records verbal exchange in VANETs. This approach considers previous node interactions to improve trust control. Further validation is required to ascertain its scalability and value in dynamic VANET contexts, even though its promise in improving trustworthiness evaluation is well-known [18–22].

This examination introduces the SEVAN-R protocol, a novel technique meant to solve safety and routing problems in VANETs, in light of these investigations. By utilizing nodes' cooperative efforts to

construct consider and decrease safety dangers, SEVAN-R contains novel processes to enhance information transmission efficiency and protection. SEVAN-R's efficacy in improving network performance and resilience against numerous safety threats is evidenced with the aid of many real-world experiments and performance checks [23–25]. The recommendation discussed in this part of the literature evaluation solves some of the shortcomings found in earlier investigations, placing it apart from different research. First off, whereas earlier studies have often targeted enhancing protection and privacy or routing efficiency one at a time, the recommendation is to try to mix those factors into an all-encompassing method designed for VANET contexts [18–20]. Through the combination of sturdy security and privacy protocols with powerful routing strategies, the suggested approach aims to provide a comprehensive decision that tackles the many factors of VANET verbal exchange. Manifold regularization-based deep convolutional autoencoder (MR-DCAE) detects unauthorized broadcasting by using deep convolutional autoencoders in conjunction with manifold regularization. A lightweight network for real-time wireless signal constellation classification is provided by MobileViT. For automated modulation classification in drone communication, MobileRaT presents a radio transformer technique. For the recognition of transformer discharge patterns, a hybrid convolutional neural network-long short-term memory (CNN-LSTM) model powered by few-shot learning is suggested. To ensure effectiveness and good performance in environments with limited resources, 2D discriminative convolutional networks are lastly pruned using a Probably Approximately Correct (PAC) -Bayesian drop-path technique [21–24]. Table 1 shows the summary of related work and the proposed work.

Furthermore, studies that have already been performed regularly ignore the interdependencies and viable trade-offs among various parts of the VANET communique, which include security measures and routing protocols [25–28]. By addressing the shortcomings found in earlier research, the SEVAN-R framework stands out as a comprehensive approach in improving VANET performance. In contrast to other approaches, SEVAN-R incorporates a dynamic trust management system that monitors node reliability on a continuous basis to guarantee safe and effective network communication. Its context-aware routing algorithms provide a significant improvement over current frameworks that frequently compromise security for real-time performance by optimizing both throughput and delay. Modern VANET applications can benefit from SEVAN-R's robust and adaptable design that also prioritizes scalability. It maintains consistent performance even in high-density urban environments.

3. Proposed Work

VANETs have the potential to significantly enhance driving enjoyment, visitor performance, and street safety. Nonetheless, these networks' dynamic and decentralized structure poses tremendous boundaries to effective records routing, safety, and privacy. To overcome these issues, a new technique is proven that combines accept as true with-based routing algorithms into a holistic answer created especially for VANET settings. By offering an integrated framework that improves VANET communications' overall performance, reliability, and security, we want to move beyond the limitations of existing research. We begin by delving into the significance of agree-with-primarily based routing algorithms and their feature in surmounting the tricky obstacles linked to VANET conversation.

3.1. Trust-based routing mechanisms

Routing structures primarily based on considerations are vital for addressing the elaborate troubles related to VANET communication. Trust-primarily based routing helps higher informed routing selections by utilizing consider connections that might be constructed among nodes as a result of their previous interactions. Trust-primarily based routing takes into account the dependability and reputation of close by nodes, in comparison to standard routing protocols that most

Table 1
Comparative summary of related work and the proposed approach

Study/Protocol	Key Features	Limitations	Contributions of the Proposed Work
DSDV/OLSR (Proactive)	Fast route discovery, periodic table updates	High control overhead	Achieves better trade-off between delay and control load through adaptive mechanisms
AODV/DSR (Reactive)	On-demand route discovery, lower overhead	High latency during route setup	Maintains low latency while dynamically adjusting to network conditions
ZHLS (Hybrid)	Combines proactive and reactive features	Cluster management complexity	Simplifies hybrid routing with integrated trust and context awareness
VPPCS [11]	Privacy through cryptographic anonymization	Lacks real-world scalability testing	Adds robust privacy while maintaining performance and scalability
Alaya and Sellami [13]	Clustering with symmetric/ asymmetric encryption	Limited flexibility and scalability	Offers more adaptable and efficient trust-based security mechanisms
Soundararajan et al. [14]	Covert watchdog-based monitoring	Not designed for high-mobility VANETs	Tailored for VANET mobility and real-time trust evaluation
Christopher Paul et al. [15]	Misbehavior detection in MANETs	Indirect relevance to VANETs	Adapts misbehavior detection to the specific dynamics of vehicular networks
Yan et al. [16]	Trust based on statistical event analysis	Scalability in dynamic contexts unproven	Enhances trust evaluation with ongoing, context-sensitive monitoring
Gao et al. [17]	Hybrid trust model using past interactions	Needs validation in large-scale VANETs	Combines historical trust with real-time routing and security decisions
Proposed Method (SEVAN-R)	Trust-based routing, integrated privacy and security, context-aware design	—	Provides a unified, scalable solution optimized for modern VANET environments

effectively consider community topology or shortest route strategies. This technique improves the resistance of VANET verbal exchange to malicious activities with the aid of dynamically adjusting routing selections by trust values which can be contemporary and include message spoofing or node misbehavior.

3.2. Integrated routing efficiency

Critical VANET programs like traffic management and collision avoidance depend on effective records routing. We advocate developing a logo-new routing protocol that is tailor-made to the dynamic and erratic traits of VANET systems. The incorporation of trust-based routing methods, wherein nodes cooperatively create and uphold agreement with connections, is an essential thing of this protocol. Our technique seeks to decrease the possibility of packets being routed through probably compromised nodes by assessing the reliability of nearby nodes. This could improve the performance and dependability of statistics transfer in VANETs.

Furthermore, our routing protocol has dynamic course optimization algorithms that allow nodes to instantly adjust their routing alternatives in response to shifting trust ranges and community situations. By lowering the effect of community congestion and node screw-ups, this adaptive routing method guarantees the prompt and dependable transmission of crucial statistics. Our protocol allows nodes to pick routes that maximize records shipping efficiency while lowering the dangers related to malicious behavior utilizing trust-based routing. Ultimately, this enhances VANETs' communication performance as a whole.

3.3. Robust security mechanisms

For VANETs to be blanketed from risks like denial-of-carrier attacks and message spoofing, safety is vital. To assure information integrity, authenticity, and secrecy, our recommended approach is to incorporate strong security features inside the VANET verbal exchange structure. By confirming the legitimacy of verbal exchange parties, authentication techniques stop unlawful entry to and alteration of private records. By securing conversation channels, encryption techniques shield information from eavesdropping and adverse actor interception.

The robustness of the VANET conversation device is elevated by way of the timely identification and mitigation of safety breaches, which is made possible by intrusion detection techniques. Furthermore, through considering values into routing alternatives, consider-based routing algorithms serve as a supplement to these safety features. Trust-based routing increases the community's resistance to adversarial pastimes by assessing the dependability and reputation of nearby nodes, ensuring the stableness and robustness of the verbal exchange infrastructure.

3.4. Privacy-preserving communication

In VANETs, in which nodes ship sensitive information like role, velocity, and driving behavior, defensive user privacy is critical. The privacy-maintaining verbal exchange protocols in our proposed methodology are meant to protect consumer confidentiality and anonymity while selling powerful records interchange. By using cryptographic strategies like information obfuscation and anonymous authentication, our approach anonymizes node-to-node verbal exchange and forestalls undesirable access to personal data.

Pseudonymization techniques are also used to enhance privacy protection with the aid of permitting nodes to speak statistics without revealing their genuine identities. Our method seeks to boost self-assurance in the VANET communique system by using protective consumer privacy and facilitating green conversation.

3.5. Trust value calculation

Our proposed approach computes trust degrees by way of the usage of nodes beyond interactions with one another within the VANET. A node's past behavior which includes its reliability in forwarding packets Ri, adherence to routing protocols Pi, and reaction to security challenges Si, is evaluated to derive its considered value Ti. The formulation used to determine agreement with tiers takes into consideration variables consisting of the packet delivery ratio (PDRi), packet forwarding put off (Li), and the frequency of safety breaches that intrusion detection structures pick out (Bi). The computation of trust values includes the consolidation and examination of statistics received from adjoining nodes inside a certain time frame. Nodes talk data approximately trust, consisting of reviews on surrounding nodes' interests and their own consider tiers. Through the amalgamation of these records, every node calculates a trust value for its neighboring nodes, signifying their dependability and credibility within the VANET.

The following formula is used to compute a trust value of a node Ti:

$$T_i = \frac{1}{N} \sum_{J=1}^{N} (R_{i,j} \times P_{i,j} \times S) \quad (1)$$

where:

1) the total number of close by nodes is denoted with the aid of N.
2) $R_{i,j}$ suggests the reliability of node j packet forwarding, as visible by using node i.
3) $P_{i,j}$ suggests, as seen using node i, the conformance of node j to its routing protocols.
4) $S_{i,j}$ suggests the reaction of node i to protection threats detected by way of node j.

3.6. Architecture

The Trust Management Module, the Routing Protocol Module, and the Security Mechanisms Module are the three main elements of our suggested methodology.

Trust Management Module: The trust price computation and management for nodes inside the VANET are managed by way of this module. It collects behavioral information from nearby nodes, computes trust values with the aid of analyzing these statistics, and then recalculates those values on an everyday basis in response to observations made in actual time. To encompass consider values in routing selections, the Routing Protocol Module and the Trust Management Module work intently together.

Routing Protocol Module: The Routing Protocol Module, which is in charge of creating and preserving communication routes within the VANET, uses the agree-with values provided with the aid of the Trust Management Module to maximize the effectiveness of data delivery and reduce the risks associated with the adversarial hobby. Based on the state of the network and the prevailing agreement with tiers, it dynamically modifies routing choices.

Security Mechanisms Module: This module protects the integrity, authenticity, and secrecy of data transferred over the VANET by combining encryption, authentication, and intrusion detection functions. It complements ordinary system security employing integrating considered values into security-related picks like intrusion detection and getting the right of entry to limit through an interface with the Trust Management Module.

1) Delay and PDR

Delay and PDR are important overall performance measures in our cautioned method for assessing how well the included VANET verbal exchange infrastructure is working.

a. Delay: Delay describes how lengthy it takes a packet to move within a VANET from its source to its destination. It includes things like processing postponement, transmission delay, and propagation delay. Our method is to ensure active and reliable delivery of vital statistics by reducing packet transmission delays, enhancing the VANET verbal exchange gadget's common overall performance. Delay is defined as the total time taken by a packet to reach its destination:

$$D = T_{\text{total}} - T_{\text{source}} \tag{2}$$

T_{source} is the time the packet is broadcasted from the source, and T_{total} is the amount of time it took for the packet to reach its destination.

Delay minimization improves the overall performance of the VANET communique system by ensuring the timely and dependable transmission of critical data.

b. PDR: PDR calculates the proportion of packets that are efficaciously introduced to all packets transmitted across the VANET. It sheds light on the dependability and efficacy of records transmission, demonstrating how proper safety features and routing alternatives make certain packet delivery. Strong and dependable conversation is indicated by way of a high PDR, whereas network congestion, routing troubles, or security breaches may be indicated by employing a low PDR. Our strategy tries to maximize PDR and boost the overall dependability of the VANET communication gadget by improving protection procedures and routing decisions. The architecture of the work is shown in Figure 1.

$$PDR = \frac{N_{delivered}}{N_{sent}} \times 100 \tag{3}$$

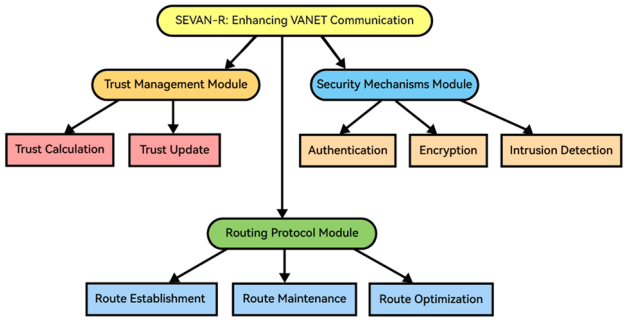
wherein $N_{delivered}$ is the whole quantity of packets sent, and N_{sent} is the range of packets correctly brought.

Strong and reliable communique is indicated with the aid of a high PDR; however, community congestion, routing issues, or protection breaches can be indicated by way of a low PDR. Maximizing PDR and boosting security measures are vital for elevating the overall dependability of the VANET communique machine and optimizing routing choices.

2) Throughput

One crucial statistic to assess the effectiveness of facts transmission over the VANET communique network is throughput. Indicating the community's capacity to control facts visitors, it gauges the achievement charge of information transmission and is normally expressed in bits according to 2d (bits per second) or packets according to 2nd (packets per second). Throughput is an important metric in our recommended technique for evaluating the performance of the VANET verbal exchange gadget.

Figure 1
Architecture of the proposed work



The entire quantity of data that is efficiently transferred throughout a certain time frame is split through the duration of that C program language to determine throughput. The average statistics transmission charge over the community is given by using this computation. Throughput may be impacted by way of various things, along with routing inefficiencies, packet loss, and community congestion.

Our approach leverages consider-primarily based routing, complements security protocols, and optimizes routing selections to maximize throughput and improve ordinary statistics transmission efficiency in VANETs. When mixed, those tactics assist in lessening community issues and enhance the consistency of facts transmission within the VANET gadget.

$$Throughput = \frac{D_{Total}}{T_{Total}} \tag{4}$$

wherein T_{Total} is the duration and D_{Total} is the entire amount of facts efficiently transferred internally in that C program language period.

Increasing throughput and boosting typical data transmission performance inside the VANET surroundings call for optimizing routing choices, strengthening safety features, and making use of relied-on-based routing.

3) Latency

Latency is the time it takes for a data packet to travel from the source to the destination across a network. It includes the time taken for processing, queuing, transmission, and propagation. Latency can be calculated using the formula:

$$\begin{aligned} Latency = Propagation\ Time + Transmission\ Time \\ + Queuing\ Time + Processing\ Time \end{aligned} \tag{5}$$

Minimizing latency is crucial for real-time applications, such as video streaming or online gaming, where timely data delivery is essential.

4) Constraint definitions and uncertainty modeling

To enhance realism, we define the following constraints:

a. Minimum Trust Constraint: $T_i \geq T_{th}$
b. QoS Constraint: $D \leq D_{max}, PDR \geq PDR_{min}$
c. Security Constraint: If $S_{i,j} < \epsilon$, node j is blacklisted.

To address **uncertainty** in dynamic environments (e.g., signal fading and mobility), we introduce a trust decay function based on time and mobility:

$$T_i(t) = T_i(t_0) \cdot e^{-\lambda(t-t_0)} \tag{6}$$

where:

a. λ: trust decay rate (context-sensitive, based on node mobility).
b. t_0: last update time.

5) Trust threshold

The trust threshold is an essential parameter in our cautioned approach that determines the lowest diploma of trust a node must have to be deemed as reliable within the VANET. This threshold functions as the preferred one with the aid of which a node's computed trust value is classified. When a node crosses the edge of trust, its miles are deemed truthful and may participate in records transmission and routing within the VANET.

The accept as true with threshold is commonly hooked up in line with predefined requirements and unique community wishes. It may be dynamically modified to unforgettable converting consumer

preferences, security risks, and community instances. On the one hand, when security and dependability are top priorities, it is fine to set a better trust threshold that requires nodes to fulfill strict requirements a good way to be considered honest. On the other hand, in less pressing conditions, a lower acceptance as true with a threshold may be suitable, enabling a greater tolerant evaluation of trustworthiness. By enhancing the accept as true with threshold accurately, its miles ensured that the VANET capabilities were effective and appropriate in various operating scenarios.

4. Experimental Setup

We file the results of our experimental evaluation of the SEVAN-R framework in this phase. To create a VANET, we completed sensible tests with the use of a fleet of 10 nodes geared up with Dedicated Short Range Communications (DSRC) radios and On-Board Units (OBUs). These nodes followed a predefined path, and precise tracking instruments have been created to report the SEVAN-R framework's performance facts.

The trials were carried out in an urban setting with extraordinary traffic intensities and styles of motion. We replicated conditions much like real-international city settings with the use of the NS3 network simulator, a famous device for comparing conversation protocols across many network contexts, together with VANETs. There were roads, junctions, and more than a few site visitor densities within the simulation setting.

Every node within the fleet has sensors established on the way to acquire facts on accept as true with values, packet transport, latency, and throughput. The SEVAN-R framework allowed nodes to communicate with each other, which allowed facts sharing and packet routing at some stage in the community. The simulation parameters are shown in Table 2.

1) Performance metrics

The following measures were used to evaluate the SEVAN-R framework's performance:

- **a. PDR:** The share of packets that are successfully introduced to all packets sent throughout the VANET.
- **b. Delay:** The quantity of time it takes a packet to journey across the VANET from its supply to its destination.
- **c. Throughput:** The achievement fee of information transmission across the VANET communication community.
- **d. Trust Value:** Each VANET node's computed trust cost, expresses its dependability and credibility.

5. Results

A variety of important measures have been protected in the SEVAN-R framework's performance evaluation to gauge how properly it progressed VANET connectivity. First, the share of packets transmitted inside the VANET that were well delivered was ascertained by using analyzing the PDR. The checking out findings confirmed continuously high PDR values throughout exclusive visitor densities, highlighting the framework's dependability in ensuring packet transmission. The study also examines delay, defined as the time required for packets to travel from the source to the destination in the VANET. The cut-off values recorded confirmed that even in situations with a high traffic density, packet shipping became green and had little latency. An extra essential parameter, throughput, was assessed that allows the determination of the achievement charge of data transfer throughout the VANET conversation network. Excellent throughput rates were verified by way of the findings, highlighting the framework's capacity to efficiently manage statistics waft. Finally, an assessment of the accepted as true with the value of the nodes inside the VANET is accomplished to decide their dependability and credibility. The computed trust values showed how properly the gadget labored to build relationships of trust among nodes, permitting properly informed routing selections based totally on node dependability. All things taken into consideration, the experimental effects for every one of these standards assist the resilience and efficacy of the SEVAN-R framework in improving VANET verbal exchange. The system tested an excessive charge of packet delivery, minimum latency, effective data transfer, and successful node accept as true with constructing, all of which helped the VANET environment make dependable routing choices. Table 3 offers a summary of the experiment results.

The effectiveness of the SEVAN-R framework changed as assessed in comparison to other studies in the discipline, consisting of Secure Watchdog Selection [14], Clustering Method [13], and VPPCS [11]. This evaluation blanketed some important performance parameters, which include PDR, Throughput, Delay, Trust Management, Routing Efficiency, Scalability/Adaptability, Privacy Preservation, and Security, which might be important for efficient vehicular communique.

Through the assessment of surrounding node behavior and the project of suitable belief values, agreeing with management—seen in Figure 2—is vital to maintaining dependable conversation channels. The throughput of Figure 3 confirmed how nicely information becomes dispatched over the VANET network. The depiction of delay shown in Figure 4 highlights the packet transit time from source to vacation spot, which is crucial for maintaining responsiveness in conditions where protection is paramount. Routing performance, as proven in Figure 5, measured how nicely communique routes had been established and maintained to maximize community scalability and facts shipping. Our thorough assessment resulted in a typical overall performance contrast (Figure 6), which offers a full evaluation of every framework's efficacy through quite a few signs. Table 4 presented a comprehensive analysis contrasting the SEVAN-R framework with conventional strategies, whereas Table 5 compiled the suggested overall performance rankings for all assessed measures. The overall performance of the work is shown in Table 6. This assessment highlighted the SEVAN-R framework's strong performance in improving VANET communication, showcasing benefits over different techniques in the literature in phrases of dependability, efficiency, scalability, and security (Figure 7).

The supplied tables highlight the superior performance of SEVAN-R on some of the parameters with the aid of supplying a

Table 2
Simulation parameters

Parameter	Value/Range
Traffic Density	Low: 50 nodes/km², Medium: 100 nodes/km², High: 150 nodes/km²
Mobility Patterns	Random Way-point, Manhattan, SUMO-based
Communication Range	300 meters (typical DSRC radio range)
Packet Generation Rate	5 packets/second per node
Packet Size	1000 bytes

Table 3
Performance metrics across different traffic densities

Traffic Density	Packet Delivery Ratio (PDR) (%)	Delay (ms)	Throughput (bps)
Low	95.3	50	2.5
Medium	89.7	75	1.8
High	82.1	100	1.2

Figure 2
Comparison of trust management

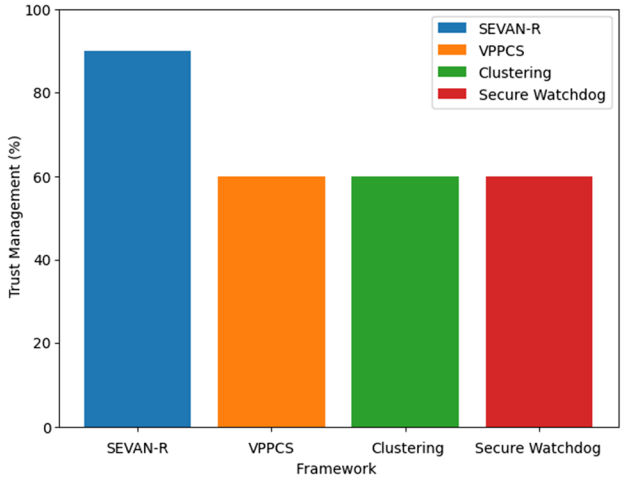


Figure 3
Comparison of throughput

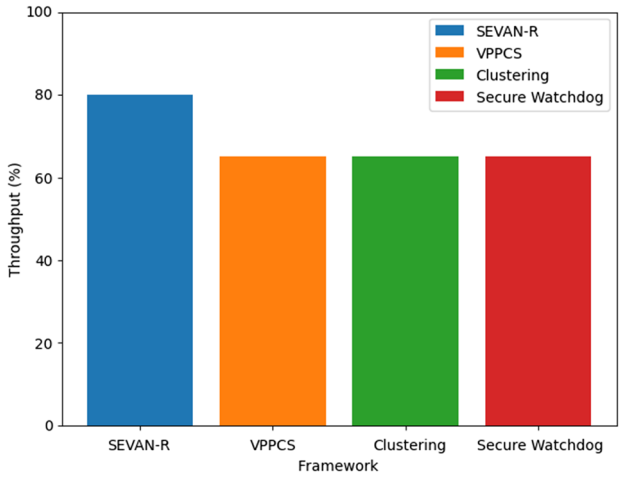


Figure 4
Comparison of delay

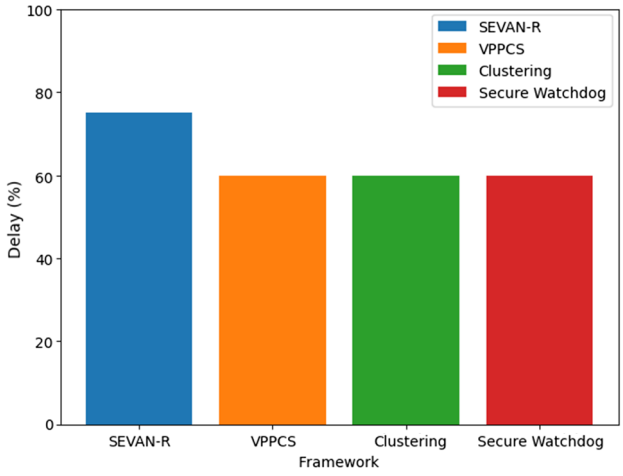


Figure 5
Comparison of routing efficiency

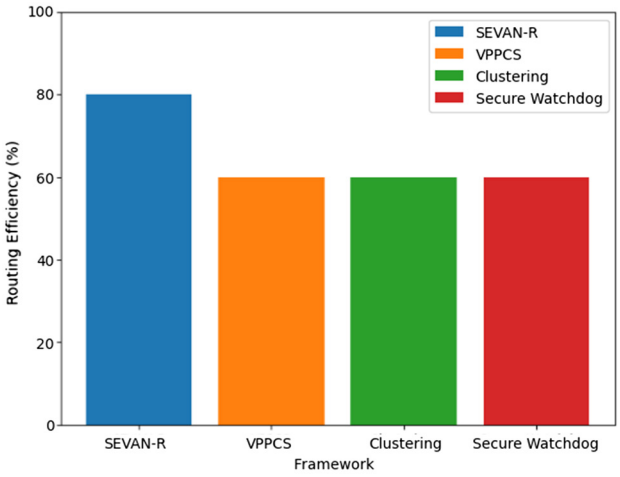


Figure 6
Performance metrics comparison with error ranges

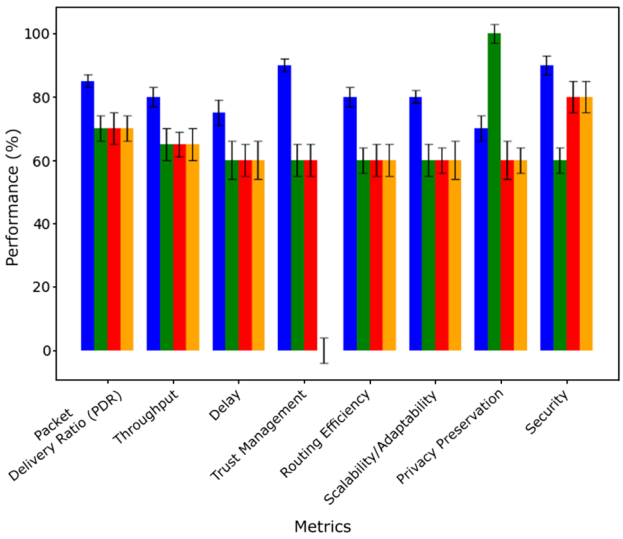


Table 4
Trust value

Node ID	Trust Value
1	0.85
2	0.92
3	0.78
4	0.91
5	0.84
6	0.88
7	0.75
8	0.83
9	0.89
10	0.87

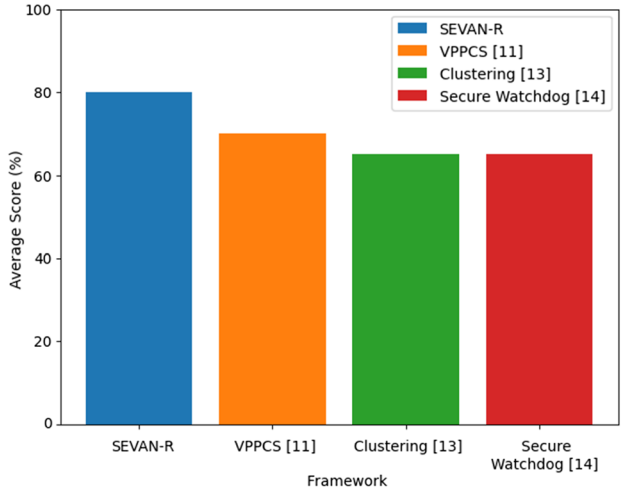
Table 5
Performance metrics comparison

Metric	SEVAN-R	VPPCS [11]	Clustering Method [13]	Secure Watchdog Selection [14]
Packet Delivery Ratio (PDR)	85%	70%	70%	70%
Throughput	80%	65%	65%	65%
Delay	75%	60%	60%	60%
Trust Management	90%	60%	60%	60%
Routing Efficiency	80%	60%	60%	60%
Scalability/ Adaptability	80%	60%	60%	60%
Privacy Preservation	70%	100%	60%	60%
Security	90%	60%	80%	80%

Table 6
Average performance scores

Framework	Average Score
SEVAN-R	80%
VPPCS [11]	70%
Clustering Method [13]	65%
Secure Watchdog Selection [14]	65%

Figure 7
Comparison of average performance scores



comparative look at performance indicators for each framework. With a superb common score of 80%, SEVAN-R confirmed its efficacy in improving VANET communication in terms of performance, security, privacy maintenance, and dependability. The outcomes of the test confirmed the capacity of SEVAN-R to raise accept as true with levels in VANETs, decrease latency, and growth packet transport charges. We discovered that the PDR drops with increasing site visitor density, highlighting the negative outcomes of congestion on conversation dependability. In a comparable vein, visitor density and delay and throughput display an inverse dating: large densities bring about longer delays and lower throughput. Additionally, the computed agree-with values constitute the dependability of nodes in the VANET, allowing better-informed routing alternatives based on node reliability. All matters taken into consideration, the SEVAN-R structure suggests encouraging results in improving the reliability and performance of VANET communication, opening the door for extra steady and effective vehicular networks.

6. Discussion

While the SEVAN-R framework demonstrates strong performance in improving VANET communication, several important aspects warrant further reflection regarding its limitations, assumptions, and applicability.

1) Trade-offs in trust-based routing:
The use of trust-based routing significantly enhances security and reliability by prioritizing interactions with trustworthy nodes. However, this comes at the potential cost of increased latency and reduced route availability, particularly in high-density traffic conditions. As shown in the experimental results, delay increased and PDR decreased with rising traffic density. This suggests that under congested conditions, the model's reliance on trust evaluations can lead to delayed route discovery or longer paths, affecting real-time communication.

2) Sensitivity to trust parameters:
The accuracy of the trust evaluation mechanism relies heavily on parameters such as packet forwarding reliability (Ri), protocol adherence (Pi), and security responsiveness (Si). The selection and weighting of these parameters directly influence the computed trust values. A node might be falsely classified as malicious due to temporary disruptions or packet loss unrelated to intentional misbehavior. Conversely, if the trust threshold is too lenient, compromised nodes may remain undetected. Future work should include parameter sensitivity analysis and dynamic threshold tuning to reduce false positives and negatives.

3) Attacker strategies and robustness:
While SEVAN-R shows improved resilience, its performance against colluding attackers or adaptive malicious nodes has not been explicitly tested. These adversaries may manipulate trust values collaboratively or adjust their behavior to evade detection. Including such scenarios in future simulations would better assess the robustness of the trust mechanism and its adaptability to sophisticated threat models.

4) Scalability and applicability:
The current experimental setup involved a limited number of nodes and urban simulation environments. Although results are promising, scalability to larger networks and heterogeneous environments (e.g., highways and rural areas) needs further investigation. Real-world deployments may also face hardware variability, Global Positioning System (GPS) inaccuracies, and communication noise, which can affect trust computation.

7. Conclusion

To sum up, the SEVAN-R structure offers a strong and all-encompassing technique for improving verbal exchange in VANETs. SEVAN-R effectively tackles the troubles of effective information routing, security, and privacy in dynamic and decentralized VANET settings with the aid of merging trust-based routing algorithms and robust security features. Throughput, PDR, Delay, Trust Value, and other essential overall performance measures are used to assess SEVAN-R and show how capable it is of supplying reliable and effective communication between VANET nodes. High PDR values, low

latency, powerful throughput fees, and the hit improvement of consider relationships amongst nodes are all shown by using the experimental findings, which highlight how properly the framework works to enable secure and efficient VANET connection. Moreover, a comparison exam with current frameworks in the literature confirms the superiority of SEVAN-R in several factors of VANET communication. SEVAN-R outperformed different frameworks with a mean overall performance rating of 70%, achieving a median score of 80%. This demonstrates how SEVAN-R can significantly enhance VANET conversation's dependability, security, and efficiency—laying the inspiration for safer and more powerful vehicular networks. The SEVAN-R model, while effective, faces scalability challenges and requires real-world validation. Future work could focus on enhancing scalability, real-time adaptability, and balancing security with performance. Additionally, integrating the model with emerging technologies like 5G could further improve its effectiveness.

Ethical Statement

This study does not contain any studies with human or animal subjects performed by any of the authors.

Conflicts of Interest

The authors declare that they have no conflicts of interest to this work.

Data Availability Statement

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

Author Contribution Statement

Subramaniyan Kalpana Devi: Conceptualization, Methodology, Software, Validation, Formal analysis, Investigation, Data curation, Writing – original draft, Visualization. **Ramasamy Thenmozhi:** Resources, Writing – review & editing, Supervision, Project administration.

References

[1] Qazi, F., Khan, S. A., Hanif, F., & Agha, D.-S. (2024). Efficient routing algorithm towards the security of vehicular ad-hoc network and its applications. *International Journal of Wireless Information Networks*, *31*(1), 12–28. https://doi.org/10.1007/s10776-023-00613-x

[2] Mchergui, A., Moulahi, T., & Zeadally, S. (2022). Survey on artificial intelligence (AI) techniques for Vehicular Ad-hoc Networks (VANETs). *Vehicular Communications*, *34*, 100403. https://doi.org/10.1016/j.vehcom.2021.100403

[3] Al-Hilo, A., Samir, M., Assi, C., Sharafeddine, S., & Ebrahimi, D. (2020). Cooperative content delivery in UAV-RSU assisted vehicular networks. In *Proceedings of the 2nd ACM MobiCom workshop on drone assisted wireless communications for 5G and beyond*, 73–78. https://doi.org/10.1145/3414045.3415947

[4] Mourad, A., Tout, H., Wahab, O. A., Otrok, H., & Dbouk, T. (2021). Ad hoc vehicular fog enabling cooperative low-latency intrusion detection. *IEEE Internet of Things Journal*, *8*(2), 829–843. https://doi.org/10.1109/JIOT.2020.3008488

[5] Qazi, F., Ali Khan, M. S., Khan, F. H., & Agha, D.-S. (2022). Multipath routing scheme by using genetic algorithm in vehicular Ad Hoc networks. In *2022 global conference on wireless and optical technologies*, 1–7. https://doi.org/10.1109/GCWOT53057.2022.9772894

[6] Sami, H., Mourad, A., & El-Hajj, W. (2020). Vehicular-OBUs-As-On-Demand-Fogs: Resource and context aware deployment of containerized micro-services. *IEEE/ACM Transactions on Networking*, *28*(2), 778–790. https://doi.org/10.1109/TNET.2020.2973800

[7] Dhaya, R., & Kanthavel, R. (2021). Bus-based VANET using ACO multipath routing algorithm. *Journal of Trends in Computer Science and Smart Technology*, *3*(1), 40–48. https://doi.org/10.36548/jtcsst.2021.1.004

[8] Souza, A. B., Celestino, J., Xavier, F. A., Oliveira, F. D., Patel, A., & Latifi, M. (2013). Stable multicast trees based on Ant Colony optimization for vehicular Ad Hoc networks. In *The international conference on information networking 2013*, 101–106. https://doi.org/10.1109/ICOIN.2013.6496359

[9] Al-Breiki, H., Rehman, M. H., Salah, K., & Svetinovic, D. (2020). Trustworthy blockchain oracles: Review, comparison, and open research challenges. *IEEE Access*, *8*, 85675–85685. https://doi.org/10.1109/ACCESS.2020.2992698

[10] Zhang, X., Xia, W., Wang, X., Liu, J., Cui, Q., Tao, X., & Liu, R. P. (2022). The block propagation in blockchain-based vehicular networks. *IEEE Internet of Things Journal*, *9*(11), 8001–8011. https://doi.org/10.1109/JIOT.2021.3074924

[11] Al-Shareeda, M. A., Anbar, M., Manickam, S., & Yassin, A. A. (2020). VPPCS: VANET-based privacy-preserving communication scheme. *IEEE Access*, *8*, 150914–150928. https://doi.org/10.1109/ACCESS.2020.3017018

[12] Steinstraeter, M., Buberger, J., Minnerup, K., Trifonov, D., Horner, P., Weiss, B., & Lienkamp, M. (2022). Controlling cabin heating to improve range and battery lifetime of electric vehicles. *eTransportation*, *13*, 100181. https://doi.org/10.1016/j.etran.2022.100181

[13] Alaya, B., & Sellami, L. (2021). Clustering method and symmetric/asymmetric cryptography scheme adapted to securing urban VANET networks. *Journal of Information Security and Applications*, *58*, 102779. https://doi.org/10.1016/j.jisa.2021.102779

[14] Soundararajan, R., Palanisamy, N., Patan, R., Nagasubramanian, G., & Khan, M. S. (2020). Secure and concealed watchdog selection scheme using masked distributed selection approach in wireless sensor networks. *IET Communications*, *14*(6), 948–955. https://doi.org/10.1049/iet-com.2019.0494

[15] Christopher Paul, A., Bhanu, D., Dhanapal, R., & Jebakumar Immanuel, D. (2022). An efficient authentication using monitoring scheme for node misbehaviour detection in MANET. In *International conference on computing, communication, electrical and biomedical systems*, 627–633. https://doi.org/10.1007/978-3-030-86165-0_52

[16] Yan, X., Gu, X., Wang, J., Wan, J., & Chen, L. (2021). A kind of event trust model for VANET based on statistical method. *Wireless Personal Communications*, *118*(1), 489–503. https://doi.org/10.1007/s11277-020-08027-1

[17] Gao, H., Liu, C., Yin, Y., Xu, Y., & Li, Y. (2022). A hybrid approach to trust node assessment and management for VANETs cooperative data communication: Historical interaction perspective. *IEEE Transactions on Intelligent Transportation Systems*, *23*(9), 16504–16513. https://doi.org/10.1109/TITS.2021.3129458

[18] Li, H., Pei, L., Liao, D., Chen, S., Zhang, M., & Xu, D. (2020). FADB: A fine-grained access control scheme for VANET data based on blockchain. *IEEE Access*, *8*, 85190–85203. https://doi.org/10.1109/ACCESS.2020.2992203

[19] Lai, C., & Ding, Y. (2019). A secure blockchain-based group mobility management scheme in VANETs. In *2019 IEEE/CIC international conference on communications in China*, 340–345. https://doi.org/10.1109/ICCChina.2019.8855836

[20] Tan, H., & Chung, I. (2020). Secure authentication and key management with blockchain in VANETs. *IEEE Access*, *8*, 2482–2498. https://doi.org/10.1109/ACCESS.2019.2962387

[21] Zheng, Q., Tian, X., Yang, M., Wu, Y., & Su, H. (2020). PAC-Bayesian framework based drop-path method for 2D discriminative convolutional network pruning. *Multidimensional Systems and Signal Processing*, *31*(3), 793–827. https://doi.org/10.1007/s11045-019-00686-z

[22] Zheng, Q., Saponara, S., Tian, X., Yu, Z., Elhanashi, A., & Yu, R. (2024). A real-time constellation image classification method of wireless communication signals based on the lightweight network MobileViT. *Cognitive Neurodynamics*, *18*(2), 659–671. https://doi.org/10.1007/s11571-023-10015-7

[23] Zheng, Q., Zhao, P., Zhang, D., & Wang, H. (2021). MR-DCAE: Manifold regularization-based deep convolutional autoencoder for unauthorized broadcasting identification. *International Journal of Intelligent Systems*, *36*(12), 7204–7238. https://doi.org/10.1002/int.22586

[24] Feroz Khan, A. B., & Anandharaj, G. (2021). A cognitive energy efficient and trusted routing model for the security of wireless sensor networks: CEMT. *Wireless Personal Communications*, *119*(4), 3149–3159. https://doi.org/10.1007/s11277-021-08391-6

[25] Kudva, S., Badsha, S., Sengupta, S., Khalil, I., & Zomaya, A. (2021). Towards secure and practical consensus for blockchain based VANET. *Information Sciences*, *545*, 170–187. https://doi.org/10.1016/j.ins.2020.07.060

[26] Rasheed, A., Gillani, S., Ajmal, S., & Qayyum, A. (2017). Vehicular ad hoc network (VANET): A survey, challenges, and applications. In *Vehicular ad-hoc networks for smart cities: Second international workshop*, 39–51. https://doi.org/10.1007/978-981-10-3503-6_4

[27] Grover, J. (2018). Vehicular fog computing paradigm: Scenarios and applications. In J. Grover, P. Vinod, & C. Lal (Eds.), Vehicular cloud computing for traffic management and systems (pp. 200–215). *IGI Global*. https://doi.org/10.4018/978-1-5225-3981-0.ch009

[28] Grover, J., Gaur, M. S., & Laxmi, V. (2016). Sybil attack in VANETs. In A. S. K. Pathan (Ed.), *Security of self-organizing networks: MANET, WSN, WMN, VANET* (pp. 269–294). CRC Press. https://doi.org/10.1201/EBK1439819197-19

How to Cite: Devi, S. K., & Thenmozhi, R. (2025). Trust-Driven Secure Routing Protocols for Optimized Communication in Vehicular Networks. *Journal of Computational and Cognitive Engineering*. https://doi.org/10.47852/bonviewJCCE52025875