Mobile Networks and Applications
https://doi.org/10.1007/s11036-023-02274-9

Efficient and Secure Graph-Based Trust-Enabled Routing in Vehicular Ad-Hoc Networks

Intyaz Alam[1] · Manisha Manjul[2] · Vinay Pathak[3] · Vajenti Mala[4] · Anuj Mangal[5] · Hardeo Kumar Thakur[6] · Deepak Kumar Sharma[7]

Accepted: 13 November 2023

Abstract
Vehicular Ad hoc Networks (VANETs) have gained significant recognition as a prospective technology for augmenting road safety and optimizing traffic efficiency through facilitating instantaneous communication between vehicles and roadside infrastructure. However, routing in VANETs faces significant challenges due to the dynamic network topology and security threats. In this context, trust-based routing offers an effective solution by improving reliability, security, and quality of service (QoS) in vehicle-to-infrastructure communication. However, trust-based routing in IOVs requires reliable trust evaluation mechanisms, privacy preservation, authentication, and access control. Challenges arise from the dynamic nature of IOVs, necessitating scalable and efficient trust computation algorithms. Moreover, ensuring the resilience of trust-based routing against malicious attacks, such as Sybil attacks or collusion among malicious vehicles, is an issue of great importance that necessitates attention and resolution. This research paper proposes a novel Graph-Based Trust-Enabled Routing (GBTR) scheme specifically designed for VANETs. The scheme incorporates direct trust, indirect trust, and contextual trust to evaluate the trustworthiness of participating nodes. Direct trust is determined based on factors such as frequency and consistency of successful communication, communication delay, and a mobility factor that incorporates punishment/reward parameters. Indirect trust is calculated using feedback trust value and link reliability, also considering the mobility factor. The contextual trust incorporates factors like location, time of day, weather conditions, and traffic density for each node pair. Routing decisions are made based on the final trust scores obtained from these trust evaluations. The route request/reply mechanism and route maintenance mechanism ensure the selection of the most reliable and trustworthy routes, thereby improving network performance. Additionally, a trust update algorithm with a concept of less reward and more penalty is employed to periodically update the trust values of participating vehicles. This approach enhances security, reliability, robustness, and efficiency of network resource usage, reducing congestion and enabling real-time trust evaluation while minimizing false positives. The simulation results substantiate that the GBTR scheme, as proposed, surpasses existing routing schemes across various performance metrics, including packet delivery ratio (PDR%), dropped packet ratio (DPR%), end-to-end delay (ms), throughput (Kbps), and normalized routing load (packets/sec). These outcomes underscore the efficacy of the proposed scheme in enhancing network performance and bolstering reliability. Overall, the graph-based trust-enabled routing scheme presented in this research contributes to enhancing the reliability and security of VANETs, thereby supporting the development of intelligent transportation systems.

Keywords Trust · Security · Routing · Graph · VANET

1 Introduction

In recent years, Vehicular Ad Hoc Networks (VANETs) have emerged as a significant and innovative wireless communication technology, garnering considerable attention. Specifically designed for vehicles, VANETs aim to enhance traffic safety, traffic efficiency, and passenger comfort [1]. In VANETs, vehicles are equipped with communication devices enabling inter-vehicle and vehicle-infrastructure interactions, creating a dynamic mobile ad hoc network. This network exhibits a constantly changing topology as vehicles join and depart at will. Through this communication, crucial information regarding traffic conditions, road hazards, and emergency situations can be shared [2]. Leveraging this information, traffic flow can be improved, accidents can be reduced, and passengers can enjoy an enhanced travel

Extended author information available on the last page of the article

Published online: 11 January 2024

experience [3]. Notably, VANETs exhibit highly variable network density, influenced by factors such as traffic congestion, road conditions, and the number of vehicles present [4]. The research on VANETs has experienced rapid growth in recent times, with further expansion expected in the future due to the surging popularity of smart cars and connected vehicles. Dedicated Short Range Communication (DSRC), operating on the 5.9 GHz frequency band, serves as the communication medium for data transmission within VANETs, facilitating high-speed and low-latency data transfer.

VANETs have many potential applications, including improving road safety, reducing traffic congestion, and enabling new mobility services [5–7]. VANETs can be used to exchange information about road conditions, such as accidents, road closures, and weather conditions. This information can be used by drivers to make more informed decisions about their driving, which can help reduce accidents and save lives [8, 9]. VANETs can also be used to implement cooperative collision avoidance systems, where vehicles can communicate with each other to avoid collisions. Furthermore, VANETs can also be used to implement intelligent transportation systems (ITS), contribute to effective traffic management by facilitating improved traffic flow and delivering real-time traffic information to drivers, allowing them to choose the most efficient routes [10]. For example, ITS can be used to control traffic lights based on real-time traffic conditions, which can help reduce wait times at intersections [11]. VANETs can also enable new mobility services, such as ride-sharing and on-demand public transportation [12]. By providing real-time information about vehicle availability and location, VANETs can help connect riders with drivers, making it easier to share rides and reduce the number of vehicles on the road [13, 14]. In summary, VANETs are a promising technology that has the potential to revolutionize the way we travel and enhance the safety and efficiency of transportation. However, several challenges need to be addressed, including the design of efficient communication protocols, ensuring the security and privacy of the network [15], routing, scalability [16], QoS, reliability, interoperability, energy efficiency [17], cost, and the development of various applications [18]. Addressing these challenges is critical to ensure the successful deployment and operation of VANETs in the future.The remainder of the introduction section is structured as follows: firstly, we examine the significance of diverse routing issues in VANETs. Subsequently, we delve into potential routing attacks in VANETs. Following that, we explore the efficiency of trust-based routing algorithms for VANETs. Then, we discuss various topologies for VANETs and emphasize the key features of the most suitable topology, supported by justification. Finally, we present an overview of the research work, along with the methodology employed.

Routing is a critical aspect of VANETs as it determines the transmission of messages between nodes in the network [19]. The efficiency and reliability of communication rely on routing protocols that can adapt to the dynamic network topology, optimize resource utilization, and support Quality of Service (QoS) requirements while ensuring communication security [8, 20, 21]. VANETs face several key routing challenges that greatly impact their performance and effectiveness. The dynamic topology [22] of VANETs, with constantly moving vehicles, necessitates communication protocols that can handle frequent topology changes and maintain reliable connectivity. Limited communication range [23] requires routing protocols to select efficient paths through the network, minimizing delay and maximizing reliability by relaying messages through intermediate nodes. Resource constraints, such as limited bandwidth and energy consumption, necessitate the optimization of resource usage to mitigate their impact on network performance [24]. VANETs must also support diverse QoS requirements, prioritizing safety-critical messages and ensuring reliable and timely communication in challenging environments [25]. Security is a paramount concern, with routing protocols requiring robust authentication, encryption, and trust mechanisms to safeguard message integrity and confidentiality while preventing unauthorized access and tampering. Privacy mechanisms are necessary to protect sensitive information exchanged in VANETs [26]. The implementation of appropriate security measures is crucial to prevent and mitigate internal attacks, ensuring the safety, privacy, and security of vehicles and their occupants within the VANET environment. Table 1 shows the list of Routing attacks in VANETs [27–31].

Trust-based routing algorithms can be efficient for VANETs because they can improve the reliability and security of the communication between vehicles, and help to mitigate security threats [22]. Trust-based routing algorithms rely on a network of trust between vehicles, where vehicles evaluate the behaviour of their neighbours and assign trust values to them based on their perceived reliability [23]. In a trust-based routing algorithm, vehicles can select routes based on the trust values of their neighbours [24]. For example, a vehicle may choose to route its messages through a neighbour with a high trust value because it is more likely to deliver the message reliably and securely. Conversely, a vehicle may avoid routing messages through a neighbour with a low trust value because it is less reliable or less secure. Furthermore, Trust-based routing algorithms can also help to mitigate security threats in VANETs, such as attacks from malicious nodes or impersonation attacks. By using trust values to determine the reliability of neighbors, vehicles can identify and avoid malicious or compromised nodes, thereby preventing them from disrupting the network or compromising the security of the communication [25].

Table 1 Routing attacks in VANETs [32–36]

Sybil attack	In this attack, a malicious node creates multiple identities or pseudonyms, which it uses to disrupt the network by creating false routing information. This can lead to message loss, incorrect routing, and DoS
Blackhole attack	In this attack, a malicious node falsely claims to have the shortest path to a destination and drops all messages it receives. This can lead to message loss, incorrect routing, and DoS
Wormhole attack	In this attack, two or more malicious nodes create a virtual tunnel between them and use it to forward messages. This can lead to incorrect routing and message loss
Grayhole attack	In this attack, a malicious node selectively drops some messages while forwarding others, leading to message loss and incorrect routing
Routing table attacks	In this type of attack, a malicious node modifies the routing table of a vehicle, resulting in incorrect routing of messages. This can lead to message loss, incorrect routing, and DoS
Packet dropping attacks	In this attack, a malicious node selectively drops packets, leading to message loss, incorrect routing, and DoS
Delayed forwarding attacks	This attack involves a malicious node forwarding messages with a delay, which can cause incorrect routing and message loss
False routing information attacks	In this attack, a malicious node provides false routing information, causing vehicles to route messages to incorrect destinations. This can lead to message loss, incorrect routing, and DoS
Jamming attacks	This attack involves a malicious node transmitting a large amount of noise or interference on the communication channel, preventing vehicles from communicating with each other. This can lead to message loss, incorrect routing, and DoS

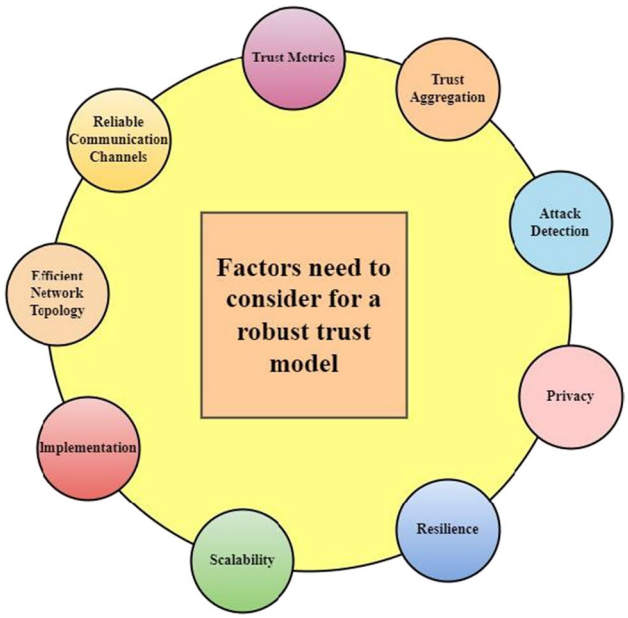

Fig. 1 Factors for a robust trust model in VANET

Figure 1 shows the vital factors for a robust trust model in VANET. The topology of a VANET has a significant effect on its performance. However, the network topology can impact various aspects of VANETs, including scalability, resilience, routing efficiency, network latency, and overall network performance. There are several existing topologies that have been proposed for VANETs, including the mesh, cluster, and hybrid topologies [11, 20]. In Mesh topology, each node communicates directly with every other node in the network to provide a high degree of connectivity and redundancy, but may incur substantial overhead due to the large number of connections that need to be established and maintained. In Cluster Topology, nodes are organized into clusters, with a cluster head acting as a central node that coordinates communication within the cluster. This topology can reduce overhead and improve network scalability, but it can also create a single point of failure in the network. Hybrid topology combines elements of both mesh and cluster topologies, with nodes organized into clusters that are connected through a mesh network. This topology provides a good balance between connectivity and efficiency, but it can be more complex to implement than the other two topologies. Graph-based topologies provide a robust and efficient framework for managing communication in VANETs, enabling effective attack detection and successful routing [6]. Graph-based topologies have emerged as a promising approach for VANETs due to their scalability, resilience, attack detection, routing efficiency, flexibility, decentralization, redundancy, efficiency, and security benefits. Graph-based topologies can handle a large number of nodes without performance degradation, quickly adapt to changes in the network topology, detect and mitigate attacks, optimize routing, and improve network efficiency. They are flexible and easily adaptable to different requirements, while also providing redundancy and enhancing network resilience. Graph-based topologies also enable secure communication between nodes, enhancing network security [5]. Therefore, they are a well-suited approach for modeling and analyzing VANETs, providing a flexible and scalable framework for developing productive and proficient routing algorithms. In this paper, we use the graph-based topology with trust model to ensure reliable routing. Graph-Based Trust-Enabled Routing is an important concept in VANETs that has gained increasing attention in recent years. It refers to a routing protocol that utilizes a graph-based approach and trust management mechanisms

to ensure secure and efficient communication between vehicles and infrastructure. Some key benefits of Graph-Based Trust-Enabled Routing in VANETs are that it provides a more efficient and secure means of routing as well as optimize the network topology to reduce the number of hops required for communication between nodes. This helps to reduce routing overhead, minimize packet loss, and enhance the overall Quality of Service (QoS) of the VANETs. Additionally, Graph-Based Trust-Enabled Routing enhances security in VANETs by incorporating trust management mechanisms. These mechanisms evaluate the trustworthiness of vehicles and infrastructure nodes based on their behavior and past interactions. Such routing prioritizes nodes with higher trust levels, while actively avoiding nodes with lower trust levels, in order to maintain network integrity and security. This helps to prevent attacks from malicious nodes, such as Sybil attacks, spoofing attacks, and routing attacks. Another important benefit of Graph-Based Trust-Enabled Routing is its adaptability to changing network conditions. Since VANETs are highly dynamic and prone to frequent topology changes, the routing protocol must be able to adjust quickly to ensure efficient communication. By using a graph-based approach, the routing protocol can quickly reconfigure the network topology to accommodate changes such as node additions or removals [2–4].

Implementing Graph-Based Trust-Enabled Routing (GBTR) in VANETs offers several practical implications and potential challenges. Practically, GBTR enhances the reliability and security of VANETs by incorporating trust evaluation mechanisms. By considering direct trust, indirect trust, and contextual trust, GBTR provides a comprehensive evaluation of the trustworthiness of participating nodes. This enables the selection of more reliable and trustworthy routes for communication between vehicles and infrastructure, improving overall network performance. GBTR's incorporation of factors such as successful communication frequency, delay, consistency, and mobility parameters ensures a more accurate assessment of trust, leading to more efficient routing decisions. Additionally, the use of privacy preservation mechanisms safeguards sensitive information during trust evaluation, enhancing the privacy of vehicle users. However, challenges may arise during the implementation of GBTR in VANETs. One major challenge is the scalability and efficiency of trust computation algorithms. VANETs are characterized by a significant number of vehicles with dynamic movements, which necessitates fast and accurate trust evaluation. Developing efficient algorithms that can handle the scale and dynamics of VANETs is crucial. Moreover, ensuring the resilience of trust-based routing against malicious attacks, such as Sybil attacks or collusion among malicious vehicles, poses a significant challenge. Robust security measures need to be implemented to detect and mitigate such attacks, as they can undermine the trust evaluation process and compromise the integrity of routing decisions. Another challenge is the practical deployment of GBTR in real-world scenarios. VANETs often involve heterogeneous vehicles with different capabilities and communication technologies. Ensuring compatibility and interoperability among various vehicles and infrastructure units can be complex. Standardization efforts and protocols need to be established to facilitate the implementation of GBTR across different VANET deployments. Overall, while GBTR brings practical benefits to VANETs, addressing the challenges related to scalability, security, and interoperability is essential to enable its successful implementation and realize its full potential in enhancing the reliability and security of vehicular communication.

2 Motivation

Are expected to have a pivotal role in the future of transportation systems, as they enable diverse applications encompassing traffic safety, traffic management, and infotainment services [26]. These applications rely on the timely and dependable exchange of data between vehicles as well as between vehicles and roadside infrastructure. However, the open nature of VANETs and the lack of central authority make them vulnerable to various security threats (malicious attacks, spoofing, and eavesdropping), including insider and outsider attacks, which can compromise the reliability and security of data exchange [32, 33]. Trust-based routing protocols can provide a viable solution to enhance the security and reliability of data exchange in VANETs by enabling vehicles to selectively share data with trusted neighbors while filtering out untrustworthy ones. Trust-based routing is an emerging paradigm that has the potential to address security and privacy issues in VANETs by finding efficient routes for information dissemination [34]. Thus, the implementation of trust-based routing protocols is crucial for VANETs to achieve secure, reliable, and efficient communication. Hence, there is a growing interest in developing trust-based routing protocols for VANETs. However, there are still many challenges to be addressed, such as scalability, efficiency, and adaptability to different types of attacks [35, 36]. Therefore, further research is needed to design and evaluate efficient and effective trust-based routing protocols for VANETs that can meet the requirements of various applications and security scenarios.

3 Our scientific contribution

To remove the aforesaid limitations of secure routing in VANETs, we presents a ground-breaking contribution to the field of VANETs by proposing a novel approach to routing that utilizes graph-based topology and trust

metrics to enhance network reliability and security. The key innovation of the research work (GBTR) is the development and evaluation of a trust-enabled routing protocol that leverages both network topology and trust values to make routing decisions. The key scientific contributions are listed in bullet points as follows.

i. We proposes a novel trust model in VANETs that utilizes graph-based topology and various trust metrics (direct, indirect and contextual trust with a wonderful mobility factor) to enhance network reliability and security.
ii. Direct trust is obtained by incorporating frequency of successful communication, delay of communication, consistency of communication and punishment/reward parameter with mobility factor. The Indirect trust value is obtained using feedback trust value and link reliability with mobility factor.
iii. We develops and evaluates a trust-enabled routing protocol that considers robust trust values of vehicles in making routing decisions. The proposed routing protocol consists route discovery mechanism (RDM) and route maintenance mechanism (RMM). The RMM in GBTR involves two main components: route error detection and route error recovery. The route error recovery process involves two steps: local repair and global repair.
iv. GBTR incorporates a novel trust update algorithm (TrUp) with less reward and more penalty system to Encourages cooperation, Improves trustworthiness, Enhances fairness and Promotes stability. A reward and penalty system can enhance fairness in the network by ensuring that all nodes are treated equally. Nodes that engage in good behaviour receive rewards, while nodes that engage in malicious behaviour are penalized. A reward and penalty system can promote network stability by incentivizing nodes to maintain a consistent level of behaviour. This helps to reduce the likelihood of sudden changes in behaviour that can disrupt the network.
v. We perform extensive simulation experiments in the Veins simulator to demonstrate that the suggested protocol exhibits superior performance compared to traditional routing protocols in terms of PDR, DPR, E2E-D, normalized routing load and network throughput. These results have significant implications for the design of next-generation VANETs, as they suggest that trust-enabled routing could play a critical role in enhancing the overall performance and security of these networks.

By providing new insights into the role of trust in routing and proposing a practical solution for implementing trust-based routing in VANETs, this research makes a significant contribution to the broader literature on trust and security in VANETs. Overall, this study represents a major step forward in our understanding of how trust can be leveraged to enhance the reliability and security of VANETs, and sets the stage for future research in this exciting area.

4 Related work

VANETs are a form of Mobile Ad-hoc Networks (MANETs) that allow communication among vehicles and infrastructure to enable safety, entertainment, and traffic management applications. A key challenge in VANETs is reliable routing, which involves the selection of the most suitable path to forward messages to their destinations. Several approaches have been proposed to address this challenge, including graph-based routing, which considers the network topology as a graph and uses graph algorithms to find the optimal path [1–6]. However, traditional graph-based routing schemes suffer from the static nature of the network, which fails to account for the dynamic changes that occur in VANETs due to vehicle mobility and network dynamics. In this section, we discuss various existing routing algorithm for VANETs with their findings, advantage and limitations. Moreover, we find the motivation, design criteria and attacks in the VANET as shown in Fig. 2.

Eiza et al. [1] address the limitations of traditional graph-based routing schemes by considering the dynamic changes that occur in VANETs. Specifically, the suggested scheme consists of three main components: an evolving graph model, a reliable path selection algorithm, and a message forwarding mechanism. The evolving graph model dynamically updates the network topology based on the location and movement of vehicles. The reliable path selection algorithm selects the path with the lowest cost based on a combination of hop count and link quality. Finally, the message forwarding mechanism forwards messages along the selected path and dynamically adjusts the path based on changes in the network topology. The simulations on the Veins simulator were based on various performance metrics, including PDR, E2E-D, and throughput. The results showed that the proposed routing scheme outperforms traditional graph-based routing schemes and other state-of-the-art routing schemes in terms of PDR, E2E-D, and throughput. Specifically, the proposed scheme achieved a PDR of up to 97%, an E2E-D of less than 1 s, and a throughput of up to 15 Mbps. The scheme is also scalable, as it can handle large-scale networks with a high density of vehicles. The proposed routing scheme assumes the availability of accurate and up-to-date information on the location and movement of vehicles, which may not always be feasible in real-world scenarios. The scheme may also incur a high computational overhead due to the dynamic updates of the evolving graph model and the reliable path selection algorithm. Finally, the scheme may not perform well in scenarios with a high degree of congestion or interference.

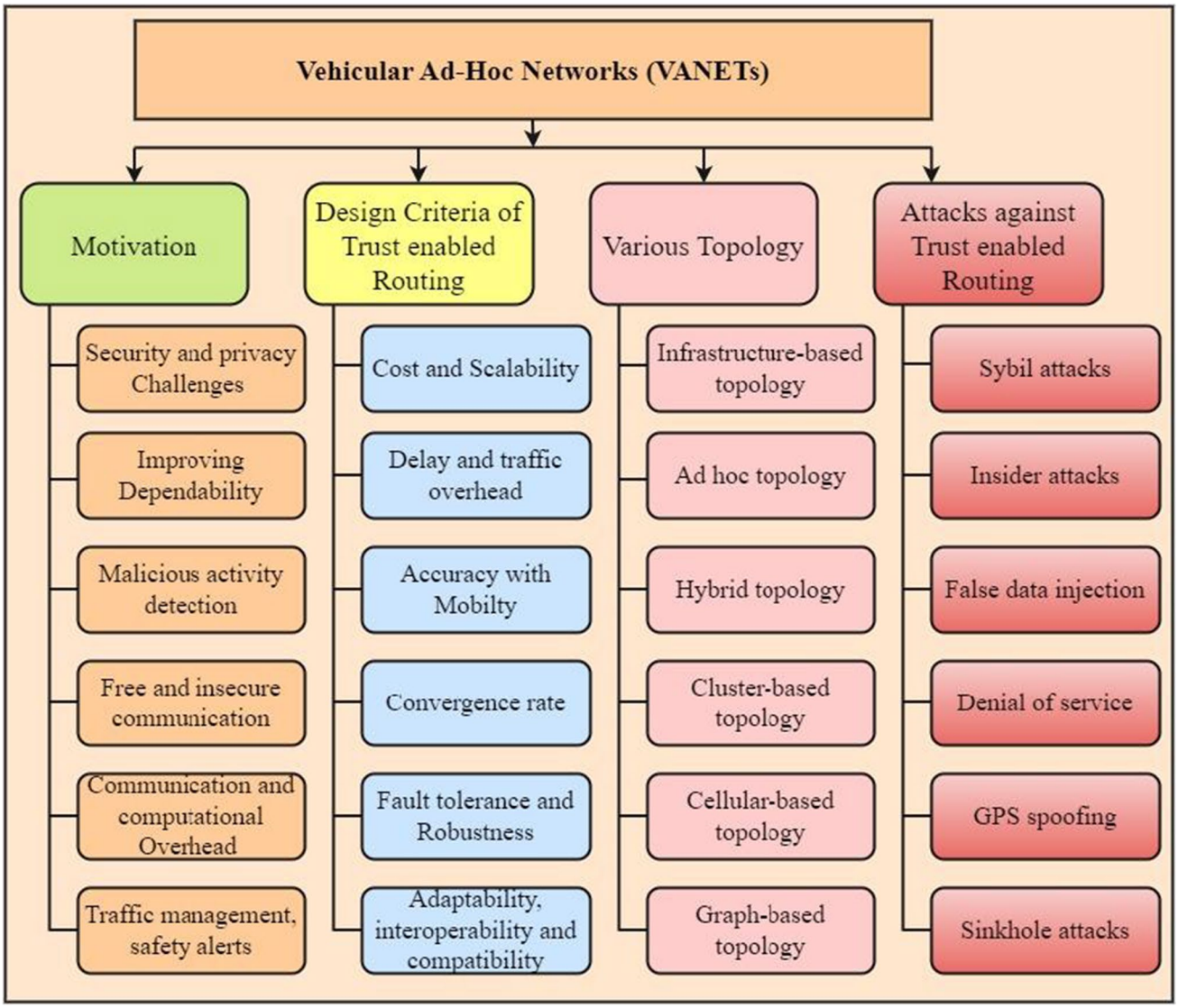

Fig. 2 Motivation, design criteria and attacks in the VANET

Kirtiga et al. [3] present a novel approach called "Reliable graph-based routing in VANET environment" aimed at optimizing the routing path for efficient packet delivery between source and destination nodes. The proposed scheme utilizes a graph-based model to represent the road network, where intersections are represented as nodes and the connecting roads as edges. Moreover, the scheme incorporates a reliability factor that takes into account real-time traffic conditions and wireless communication quality. By considering this reliability factor, the scheme selects the most dependable path for packet delivery, thereby enhancing the overall reliability of the routing mechanism. To assess the performance of the proposed scheme, the authors employed the widely used Veins simulator, specifically designed for VANETs. Through various simulation experiments involving different scenarios such as varying vehicle density and network size, the authors compared the proposed routing scheme with traditional protocols like AODV and DSR. The simulation results demonstrated the superior performance of the proposed scheme in terms of PDR, E2E-D, and throughput. Furthermore, the authors showcased the scheme's ability to maintain a high level of reliability across diverse traffic conditions and network sizes.

Dietzel et al. [4] presents a methodology for detecting insider attacks in VANETs using graph-based metrics. According to authors, insider attacks are a major security threat in VANETs, and detecting them is crucial for ensuring the integrity and reliability of data dissemination protocols. Current proposals primarily concentrate on entity authorization through the establishment of a public key infrastructure. However, this approach fails to address insider attacks originating from authorized entities. As a result, it becomes

imperative to develop data-centric methods to complement entity-centric trust. One promising avenue involves leveraging redundant information dissemination for consistency checks, particularly in multihop scenarios. In this research paper, the authors introduce three graph-based metrics that gauge the redundancy of dissemination protocols. These metrics are applied to a baseline protocol, a geocast protocol, and an aggregation protocol, with extensive simulations conducted to evaluate their performance. The authors propose two metrics: the number of node-disjoint paths and the derived number of critical nodes. These metrics are computationally efficient, as they are related to the maximum flow problem in graph theory. The validity of these metrics is demonstrated through extensive simulations conducted under diverse network scenarios. The experimental results indicate that the Advanced Adaptive Geocast protocol exhibits favorable routing efficiency but lacks sufficient redundancy for ensuring data consistency mechanisms in most scenarios. Conversely, a simple aggregation protocol shows promising redundancy results.

Xia et al. [5] presents a novel approach "Towards a novel trust-based multicast routing for VANETs" by incorporating trust-based mechanisms. The authors recognize the importance of efficient and secure multicast communication in VANETs for various applications such as traffic management and safety services. The proposed approach focuses on the dependability of vehicles as opposed to traditional multicast routing protocols that only consider network topology and do not consider the reliability of the nodes. The trust metrics are calculated based on the vehicle's behavior and history, including its location, speed, and communication behavior. The authors introduced a trust model that calculates direct trust using Bayesian theory and indirect trust through credibility and activity evaluation. They utilize a fuzzy logic-based approach to calculate trust values for the vehicles, which are then used to select the most trustworthy intermediate nodes for message forwarding.They proposed a new protocol called MTAODV based on MAODV protocol to enhance routing efficiency and defend against multiple attacks. The protocol detects and eliminates malicious nodes during the process of route establishment and maintenance using trust values, resulting in trustworthy and proficient routes for data delivery. Simulation results demonstrated the effectiveness of the protocol in improving data packet transmission rates, although it caused a slight increase in E2E-D and control overhead.

Dhiman et al. [6] proposes a reliable and efficient routing mechanism for VANETs using a graph-based approach. The authors address the challenges of dynamic topology, intermittent connectivity, and high mobility in VANETs to develop an optimized and robust routing solution. The authors start by presenting an overview of the existing routing protocols used in VANETs, including AODV, DSR, and OLSR, and the associated limitations of these protocols in the context of VANETs. They then introduce their proposed graph-based routing protocol, which is based on a novel graph structure and utilizes multiple metrics to assess the performance of candidate routes. The proposed routing mechanism uses a weighted directed graph, where each node represents a vehicle in the network, and each edge represents the potential link between two vehicles. The authors employ multiple metrics, including link quality, distance, and direction of travel, to evaluate the quality of each link and select the most optimal route for data transmission. To evaluate the proposed routing protocol, the authors conduct a detailed simulation analysis that demonstrate the effectiveness of the proposed protocol in improving the PDR, reducing the E2E-D, and minimizing the routing overhead compared to existing routing protocols. The authors further conducted a sensitivity analysis to assess the resilience of the proposed routing protocol across diverse network conditions. The introduced routing protocol exhibits promising capabilities in tackling the inherent challenges posed by dynamic topology, intermittent connectivity, and high mobility in VANETs. By addressing these obstacles, the protocol holds significant potential in fostering the advancement of more dependable and efficient routing solutions for forthcoming VANET applications.

Husain et al. [7] proposed a "PSO optimized geocast routing in VANET" and introduces three geocast routing protocols, DREAMgeoOPT, LARgeoOPT, and ZRPgeoOPT, developed using particle swarm optimization (PSO) in VANET. The protocols were compared with existing protocols and showed improvements in PDR, throughput, E2E-D, and normalized routing load. The fitness function used in PSO reduced delays, routing loads, and dropped packets while increasing throughput and packet delivery ratio. The PSO approach resulted in a fast convergence and local maxima obtained in less time, contributing to the improved performance of the developed protocols.Although the PSO optimized geocast routing protocols show improvements in performance metrics, the limitations may include the reliance on particle swarm optimization, which might have certain convergence issues or limitations in scalability.

Kandali et al. [8] proposed a novel hybrid routing protocol called KMRP, which integrates a modified K-means clustering algorithm with the Maximum Stable Set Problem and Continuous Hopfield Network. The objective of KMRP is to enhance data transmission in high-density and high-mobility VANET environments. The protocol incorporates a link reliability model to form vehicle clusters and selects cluster heads based on parameters such as free buffer space, vehicle speed, and node degree. Extensive simulations were conducted to evaluate the performance of KMRP. The simulation results demonstrate the superiority of KMRP

over alternative schemes in various aspects. KMRP successfully mitigates traffic congestion and collisions, enhances throughput, reduces E2E-D, and improves PDR. These findings highlight the effectiveness and advantages of the proposed protocol in addressing the challenges associated with VANETs operating in dense and dynamic environments. KMRP guarantees cluster stability, avoiding redundant and repetitive data transmission. Although the hybrid routing protocol KMRP performs well in high-density and high-mobility VANET environments, but potential limitations could arise from the complexity and computational overhead associated with combining the modified K-Means algorithm, Maximum Stable Set Problem, and Continuous Hopfield Network. Furthermore, the performance improvements observed in simulation tests might not fully reflect real-world scenarios.

Diaa et al. [9] proposed "OPBRP-obstacle prediction based routing protocol in VANETs" for vehicle-to-RSU communication in VANETs. The protocol utilizes vehicle kinematics and mobility predictions to choose a reliable path and select intermediate nodes for higher PDR. The OPBRP outperforms existing routing protocols in terms of PDR, E2EDelay, and power consumption in simulation tests. The protocol predicts the road situation and radio obstacles to make forwarding and recovery decisions. Future work includes assessing the applicability of the protocol in traffic management systems, studying the use of UAVs for improved performance, and conducting field trials to validate simulation results. The OPBRP protocol achieves higher PDR, reduced E2EDelay, and improved power consumption, but limitations may include the accuracy of road situation and radio obstacle predictions, as well as potential challenges in effectively implementing and updating the prediction models in dynamic VANET environments. Further testing and validation under diverse real-world conditions would be beneficial to assess the practical limitations of these proposed methods.

Shokrollahi et al. [24] introduce TGRV (Trust-Based Geographic Routing Protocol for VANETs), which aims to mitigate the involvement of malicious vehicles in routing. TGRV routing protocol incorporates multiple factors, including direct trust, recommendation trust, distance, speed, and direction, to intelligently determine the next-hop for data transmission. A monitoring system enables vehicles to track the correct packet forwarding rate of the next-hop, updating their direct trust and retransmitting lost packets. Push-based notifications allow vehicles to share their observations of the next-hop, enabling neighbors to update their recommendation trust. The monitoring system employs distance prediction in a modified promiscuous mode for accurate packet forwarding rate estimation. Trust values decay over time to improve trust management accuracy. TGRV utilizes the trust of two-hop neighbors to select more trusted next-hops. Extensive simulations in OMNeT + + demonstrate that TGRV achieves a high packet delivery ratio (88.7%) and performs favorably against GPSR and PGRP protocols. Although TGRV exhibits increased E2E-D and average hop count, these trade-offs are acceptable given the absence of monitoring and retransmission in the other protocols. Cost and security analyses confirm the feasibility and resilience of TGRV, making it resistant to trust-based attacks while maintaining acceptable memory, communication, and computational overheads.

Naeem et al. [37] propose the Enhanced Cluster-Based Lifetime Protocol (ECBLTR) to enhance routing stability and average throughput in the network. The cluster heads (CH) are evaluated using a Sugeno model fuzzy inference system, considering parameters such as residual energy, local distance, node degree, concentration, and distance from the base station. The results indicate that the enhanced routing protocol, combined with an appropriate channel model, improves the link throughput of VANETs for a fixed network size. The findings demonstrate the effectiveness of the fuzzy system in selecting CHs, leading to a 10% increase in network lifetime. Furthermore, the performance evaluation highlights the impact of network size and routing protocols on metrics like packet delivery ratio, packet loss, average end-to-end delay, and transmission overhead. The research establishes the efficacy of the ECBLTR protocol in enhancing routing stability and overall network performance, emphasizing the importance of intelligent CH selection and efficient routing mechanisms. Luong et al. [38] present BADA (Black Hole Attack Detection Algorithm), a novel approach based on machine learning, to address the challenges of identifying malicious vehicles that attempt to evade detection in VANETs. BADA outperforms existing solutions by utilizing historical route request and response behavior of each vehicle, employing the k-Nearest Neighbors machine learning algorithm for identifying malicious vehicles. Additionally, a Black Hole Attack Detection Routing Protocol is proposed, integrating the BADA solution to enhance the security of an AODV-based protocol. The performance evaluation, conducted using the NS2 simulation system, demonstrates accurate detection of malicious nodes exceeding 99.0%, surpassing previously published algorithms. The research highlights the effectiveness of BADA in addressing the challenges associated with black hole attacks in VANETs and its superiority over existing detection algorithms. Xie et al. [39] introduce an approach that combines cluster-based routing protocols with pattern discovery methods to reduce latency in VANETs. The proposed method comprises four modules: primary data collection and analysis, primary data preparation and analysis, pattern extraction and vehicle route discovery,

and vehicle clustering and data/information transmission routing. Through simulations, it is demonstrated that the proposed method significantly improves the packet delivery rate, achieving an 88.56% delivery rate compared to previous methods. The approach leverages clustering and frequent pattern discovery to predict vehicle movement paths and employs a novel method for data transfer and information in VANETs by discovering vehicle trajectories, predicting future trajectories, and sending messages based on clustered vehicles. The contributions include utilizing decision tree classification, sequential pattern mining, vehicle clustering, and selecting the best cluster head for message transmission. However, the proposed method has limitations in storing the history of vehicle movement and producing accurate movement patterns, particularly in scenarios with fewer vehicles. The accuracy of path pattern prediction is lower in such scenarios, while the method proves more effective on busy roads with higher vehicle density. Monfared et al. [40] address location privacy and reliability concerns in VANet routing protocols and introduce DARVAN, a fully decentralized infrastructure offering anonymous and reliable routing. DARVAN utilizes a distributed database and collective consensus to minimize the exposure of critical data usually stored and processed in centralized units. The I2P protocol is modified to deploy DARVAN, enhancing routing reliability and resilience against various adversary activities in VANets. Notably, DARVAN presents an effective and efficient network-level approach to mitigate Sybil attacks. Extensive simulations conducted on NS3 demonstrate that DARVAN outperforms previous anonymous schemes proposed for VANet routing in terms of packet delivery ratio, overhead, delay, and reliability.

As a concluding remark, we can say that the existing literature [1–10, 24, 37–40] on trust-enabled routing for VANETs suggests that trust-enabled routing is a promising approach to improve the security and efficiency of VANETs. However, current trust-based routing protocols still face several limitations such as increased overhead [11], low scalability [12], vulnerability to new types of attacks [13], and the need for efficient and reliable trust models [14]. To address these limitations, a new trust-enabled routing protocol for VANETs should have efficient, lightweight, scalable and reliable trust models that can accurately evaluate direct and indirect trust values. It should also be resistant to new types of attacks and able to handle dynamic and complex network conditions. Additionally, the protocol should minimize overhead while ensuring fast and reliable route discovery and maintenance. The protocol should provide QoS guarantees such as high packet delivery ratio, low latency, and low packet loss rate as well as protect the privacy of users by preventing the disclosure of sensitive information to unauthorized parties. Moreover, the protocol should be designed to be compatible with existing VANET standards and protocols to ensure interoperability with other systems. Overall, a new trust-enabled routing protocol for VANETs should balance security and efficiency while meeting the additional requirements mentioned above to ensure reliable and trustworthy communication in vehicular networks.

5 Proposed model

This section presents a robust trust evaluation scheme and trust based routing scheme. Section 3.1 provides trust assessment scheme for VANETs and Section 3.2 discuss the proposed trust based routing scheme. Trust-based routing schemes play an important role in VANETs by enabling vehicles to make routing decisions based on the trustworthiness of other vehicles. These schemes use the concept of trust to evaluate the reliability and credibility of different nodes and make routing decisions based on this information. In a trust-based routing scheme, each vehicle in the network is assigned a trust score based on its past behavior and interactions with other vehicles. This score is then used to determine the vehicle's level of trustworthiness and reliability. When a vehicle needs to route a message to another vehicle, it can use this trust score to decide which vehicle to send the message to. Figure 3 shows the framework of proposed method along with graph based topology. Graph-based topology is a powerful approach for modelling and analysing VANETs, and it provides a flexible and scalable framework for developing efficient and effective routing algorithms. In a graph-based topology, each node represents a vehicle or infrastructure element, and the edges represent the connections or links between the nodes. This allows the topology to be easily visualized and analyzed, which is important for understanding the behavior of the network. Graph-based topology is also highly scalable, which is essential for VANETs, as the number of nodes in the network can vary widely depending on the location and time of day. Graphs can handle a large number of nodes and links without compromising the performance of the routing algorithms. While designing and implementing the proposed work, we assume that vehicles have limited energy resources, limited processing power and communication range, which requires the routing scheme to consider the communication range while selecting the next hop for forwarding packets. The network consists of homogeneous vehicles, meaning that all vehicles have similar hardware and communication capabilities. Moreover, we consider the localization system accurate as it affects the quality of the graph, which in turn impacts the routing performance. The initial trust value of each vehicle is 5 and maximum

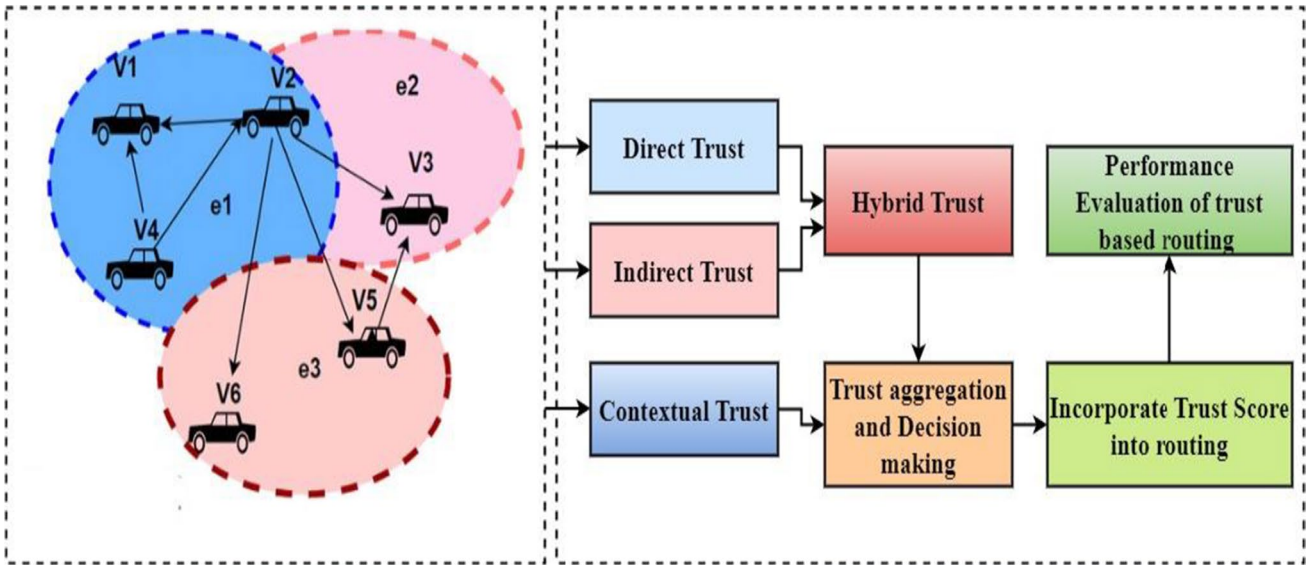

Fig. 3 Framework of proposed method

trust value is 10. The network operates in a decentralized manner without any central authority to govern or control its activities. The network may have a certain percentage (10% to 50%) of malicious nodes that try to disrupt the communication or attack other nodes. Moreover, we consider broadcast communication, in which source node sends the message to all the nodes within its transmission range. The destination node can then identify itself by responding to the message.

5.1 Trust assessment scheme

In the proposed trust assessment scheme, we consider direct trust, indirect trust and contextual trust. Direct trust is obtained by incorporating frequency of successful communication, delay of communication, consistency of communication and punishment/reward parameter with mobility factor.

The direct trust between two nodes j and j at time Δt can be computed using Eq. (1) as follows

$$D_{i,j}^{T}(\Delta t) = [\alpha + \beta L + \gamma D + \delta C + \omega P] * MF(i,j) \tag{1}$$

where α is the baseline trust score for the node, which can be set to a default value or adjusted based on the node's previous behaviour. It can help to establish trust between vehicles and maintaining the security and dependability of the VANET. Moreover, it is used to establish a starting point for evaluating the trustworthiness of each vehicle in the network. For example, the baseline trust score could be based on the vehicle's reputation, past behaviour, or other characteristics that are relevant to determining its trustworthiness. The trustworthiness of each vehicle could then be updated over time based on its interactions with other vehicles in the network. By using a baseline trust score, vehicles can make more informed decisions about which other vehicles to trust and which to avoid. This can help to prevent attacks and ensure the reliability and security of the VANET. In Eq. (1), the symbol β is the weight assigned to the frequency of successful communication (L) metric. γ is the weight assigned to the delay of communication (D) metric. δ is the weight assigned to the consistency of communication (C) metric. ω is the weight assigned to the punishment/reward parameter (P), which takes into account the node's previous behavior and adjusts its trust score accordingly. The value of L can be computed as the ratio of the number of successfully received packets (R) to the total number of transmitted packets (T) during a given time period:

$$L = \frac{(R + \rho R)}{(T + \rho T)} \tag{2}$$

where ρR and ρT are the reward and punishment parameters for L, respectively, which can be adjusted based on the node's previous behavior. For example, if the node successfully transmits and receives a packet, it could be rewarded by increasing the value of ρR, whereas if the node fails to transmit or receive a packet, it could be punished by increasing the value of ρT.

D (delay of communication) can be computed as the difference between the time when a packet was sent by the node (Ts) and the time when it was received by one of the node's immediate neighbors (Tr), averaged over all successful communication events:

$$D = \frac{1}{(R+\rho R)} * \sum_{1}^{R+\rho R} \left(Tr_i - Ts_i\right) \tag{3}$$

where ρR is the reward parameter for D, which can be adjusted based on the node's previous behavior. For example, if the node successfully transmits and receives packets with low delay, it could be rewarded by increasing the value of ρR.

C (consistency of communication) can be computed as the ratio of the number of time slots during which the node's immediate neighbors were available for communication (U) to the total number of time slots during the time period (N):

$$C = \frac{(U - \rho U)}{(N + \rho N)} \tag{4}$$

where ρU and ρN are the reward and punishment parameters for C, respectively, which can be adjusted based on the node's previous behavior. For example, if the node's immediate neighbors are consistently available for communication, it could be rewarded by decreasing the value of ρU, whereas if the node's immediate neighbors are frequently unavailable for communication, it could be punished by increasing the value of ρN.

$MF(i,j)is$ MobilityFactor (i,j) that represents the mobility of nodes i and j is used to improve the accuracy of the trust evaluation equation in VANETs.

$$MF(i,j) = e^{\frac{\mu * Distance(i,j)}{(Velocity(i)+Velocity(j))}} \tag{5}$$

where μ is a constant that adjusts the impact of distance on the mobility factor. Equation (5) uses an exponential function to weight the distance between nodes by their relative velocities. When nodes have similar velocities, the distance term has less impact on the mobility factor, and the factor approaches 1. Conversely, when nodes have vastly different velocities, the distance term has a greater impact, and the factor approaches 0.

The Indirect trust value is obtained using feedback trust value and link reliability with mobility factor as shown in Eq. (6). Link reliability is a crucial factor to consider when designing a trust model for VANETs. The dynamic and unpredictable nature of the communication links in VANETs makes it important to evaluate the quality of the links to ensure that the trust metrics used in the trust model are accurate and effective. A high link reliability can enhance the truthfulness of the trust model and improve the overall performance and security of the network, while a low link reliability can lead to incorrect trust evaluations and routing decisions.

$$I_{i,j}^{T}(\Delta t) = \left[w_1 * \frac{1}{n} * \sum_{1}^{n} D_{i,k}^{T}(\Delta t) * D_{k,j}^{T}(\Delta t) + w_2 * link\ reliability\right] * MF(i,j) \tag{6}$$

where w1, and w2 are weights assigned to each metric, which can be can be fine-tuned to achieve the desired balance and effectiveness in the trust evaluation process for the specific application. The symbol n represents the number of vehicles involved in indirect trust evaluation.

Contextual trust in VANETs refers to the consideration of contextual information in the trust calculation process. In other words, contextual trust takes into account the specific context in which the nodes in the network are operating, such as their location, time of day, weather conditions, traffic density, and other relevant factors. By integrating contextual information into the trust calculation process, contextual trust can significantly enhance the precision, dependability, and overall security of the VANET by refining the trust evaluation mechanism. By considering the specific context in which the nodes are operating, contextual trust can enable more effective detection and mitigation of attacks and enable more targeted security measures to be applied. Contextual trust(i,j) represents the contextual factor, which captures the specific context in which the nodes i and j are operating. This can be calculated using a context-aware algorithm that takes into account factors such as location, time of day, weather conditions, and traffic density. By incorporating the mobility factor and contextual factor into the trust evaluation equation, the projected approach can better capture the dynamics and specific context of the VANET, which can lead to more accurate and reliable trust evaluation results.

To calculate the contextual trust for a given node pair (i,j), following factors can be combined using a weighted sum approach:

$$\begin{aligned} C_{i,j}^{T}(\Delta t) =& w3 * Location\ Factor(i,j) \\ &+ w4 * Time\ Of\ Day\ Factor(i,j) + w5 \\ &* Weather\ Conditions\ Factor(i,j) \\ &+ w6 * Traffic\ Density\ Factor(i,j) \end{aligned} \tag{7}$$

where w3, w4, w5, and w6 are weight parameters that control the impact of each factor on the overall contextual factor. These weight parameters can be set based on the importance of each factor for the specific application. The location factor captures the geographic location of the nodes in the network. This can be calculated using GPS coordinates or by leveraging roadside units (RSUs) that provide location information. The location factor can be represented by a binary value indicating whether the nodes are in a high-traffic or low-traffic area. The time of day factor captures the time of day when the nodes are operating. This can be represented by a binary value indicating whether the nodes are operating during rush hour or off-peak hours. The weather conditions factor captures the weather conditions when the nodes are operating. This can be represented by a binary value

indicating whether the nodes are operating in clear weather or inclement weather. The traffic density factor captures the traffic density when the nodes are operating. This can be represented by a binary value indicating whether the nodes are operating in high-traffic or low-traffic areas.

The final trust score is computed using Eq. (8) as follows

$$F_{i,j}^{T}(\Delta t) = \frac{D_{i,j}^{T}(\Delta t) + I_{i,j}^{T}(\Delta t) + C_{i,j}^{T}(\Delta t)}{3} \tag{8}$$

The final trust value is an important metric in graph-based VANETs because it can be used to inform routing decisions. By leveraging the trustworthiness of nodes, the routing algorithm can effectively mitigate the effects of attacks and malicious behavior, while ensuring efficient and reliable message delivery. Additionally, the use of trust values in routing algorithms can help to enhance the overall quality of service for VANET applications, such as traffic management and collision avoidance. In the context of routing, nodes with higher trust values are typically considered more reliable and are given priority in the forwarding of messages. In the following subsection, we discuss the proposed Trust-Enabled Routing Algorithm in VANETs.

5.2 Trust-enabled routing algorithm in VANETs

In this subsection, we discuss the proposed Trust-Enabled Routing Algorithm (GBTR) in VANETs that incorporate route request/reply mechanism and route maintenance mechanism. The route request mechanism in trust-based energy-efficient routing aims to establish a path that maximizes both energy efficiency and security, by selecting trustworthy and efficient nodes for routing. This approach helps to minimize the energy consumption of the network, while ensuring that messages are delivered securely and reliably. In GBTR, the source node first evaluates the trustworthiness of its neighbouring nodes using proposed trust assessment scheme. The trust assessment scheme takes into account the factors such as direct trust, indirect trust, and contextual trust, and determines the nodes that are most trustworthy and efficient for routing. Once the trust evaluation is complete, the source node selects the most trustworthy node to act as the next hop in the route. The source node then sends a route request message to this node, which in turn evaluates the trustworthiness of its own neighbors and selects the next hop in the route. This process continues until the destination node is reached, at which point a route reply message is sent back to the source node, confirming the establishment of the secure and efficient path. The route reply message contains information about the most energy-efficient route to the destination vehicle, as well as the trustworthiness level of the vehicles along that route. The source vehicle then selects the route with the highest energy efficiency and trustworthiness level and begins sending the message to the destination vehicle along that route. The route maintenance mechanism (RMM) is responsible for maintaining the trustworthiness of the selected route over time. The goal of RMM is to detect and react to changes in the network that could affect the trustworthiness of the selected route and to select a new route if necessary. The RMM in GBTR involves two main components: route error detection and route error recovery. In route error detection, when a source vehicle is using a selected route to transmit data to the destination vehicle, it continuously monitors the trustworthiness level of the vehicles along the route. If the trustworthiness level of any vehicle along the route falls below a predefined threshold, the source vehicle assumes that there is an error in the route and begins the route error recovery process. The route error recovery process involves two steps: local repair and global repair. In the local repair step, the source vehicle first attempts to repair the route by selecting a new vehicle that is within its transmission range and has a higher trustworthiness level than the vehicle that caused the error. If such a vehicle is found, the source vehicle updates the route information and continues to transmit data along the repaired route. If the local repair step fails, the source vehicle initiates the global repair step, which involves broadcasting a new route request message to its neighbours. The new route request message contains updated information about the error that occurred and asks for suggestions for a new route to the destination vehicle. The neighbouring vehicles that receive the new route request message evaluate their trustworthiness level and respond with a route reply message containing information about the most energy-efficient and trustworthy route to the destination vehicle. The source vehicle then selects the new route with the highest energy efficiency and trustworthiness level and begins sending the message to the destination vehicle along the new route. RMM ensures that the most trustworthy and energy-efficient route is always used to transmit data between vehicles in VANETs. The detailed steps of the proposed algorithm is given in algorithm 1 as below.

A trust update algorithm is a critical component of trust-based routing in VANET as it helps to enhance the security, reliability, and effectiveness of the VANETs, and make routing decisions based on real-time trust evaluation. The proposed trust update algorithm 2 update the trust value according to trust value, known and unknown status. We maintain two list namely trust _list and known list to keep the updated trust value and known status. According to the proposed trust update algorithm (TrUp) 2, if sender is known and its trust value is greater than equal to trust threshold then TrUp increases its value by reward 1 but if its trust value is less than trust threshold then TrUp provide more punishment by

Algorithm 1 Trust-Enabled Routing Algorithm (GBTR)

Input: Vehicle IDs,Current position and velocity of the vehicles, Trust values of vehicles, trust_list, Trust threshold (ø), Initial Trust Value, Transmission Range, Road Network Map
Output: Optimal And Reliable Route Information

Step 1 : Deploy the vehicles on the Road Network Map
Step 2: Check trustworthiness status of source vehicle (node) using Eq. (8) and append the trust value to the trust_list=[]
Step 3: If source is not trusted then
Return: "error: source not trusted"
End if
Step 4: Identify the number of neighbour vehicles (say m) of source vehicle (say s) at time Δt
Step 5: If m is empty then
Return " Error: no neighbours found"
Step 6: Else if source and destination have direct communication link & trust value (destination) ≥ ø
Send message directly to destination
Return " Success: message sent directly"
Step 7: Else for each neighbour in m do
Compute $F_{s,m}^{T}(\Delta t)$ using Eq. (8)
identify good vehicles and add the malicious vehicles into a blacklist
update the trust value in trust_list using trust update algorithm 2
End If
End If
Step 8: If no neighbour in m is trusted i.e. $F_{s,m}^{T}(\Delta t) < ø$ for all values of m
Return " Error: no trusted neighbours found"
Else
Next_hop = max (trust score of trusted neighbour) && min (distance from destination)
Step 9 : Apply Route request mechanism using step 10
Step 10: Source vehicle send the route request message (RREQ) to the next_hop vehicle
Step 11 : Repeat step 6 to step 10 until RREQ message reached at the destination
Step 12 : Apply Route reply mechanism
If a vehicle has a valid route to the destination, it sends an RREP message back to the source vehicle, containing the route information using the reverse path taken by the RREQ message.
Step 13 : Apply Route maintenance mechanism using step 14 to step 20
Step 14: source continuously monitor the vehicles participated in the current routing process
Step 15: if $F_{s,m}^{T}(\Delta t) < ø$ then
Step 16: Apply route recovery process (Local repair and global repair)
Step 17:If($F_{s,m}^{T}(\Delta t) \geq ø$ and transmission range ≤ range) // local repair process
Select this new vehicle as a next_hop and update the new route
Else
Broadcast RREQ message to neighbours // Global repair
Step 18: Neighbours evaluate the trust level of sender node
Step 19: If sender is trustworthy then
Neighbours will provide better route to the sender
Step 20: If the message has been broadcasted for a predefined number of times then
Terminate the search and repeat the steps until the destination is reached
End If
End If
End If
Step 21 : The source vehicle select updated route for data transmission

Algorithm 2 Trust Update Algorithm (TrUp)

Input: Old Trust Value, Trust Threshold (ø), trust_list, known list, black list

Output: Updated trust values, Alert message

Step 1: If sender is known vehicle and $(F_{s,m}^{T}(\Delta t) \geq ø$ then
update trust value = old trust value + 1
Step 2: Else if sender is known vehicle and $(F_{s,m}^{T}(\Delta t) < ø)$ then
update trust value = old trust value – 1.5
Step 3: Else if sender is unknown vehicle and $(F_{s,m}^{T}(\Delta t) \geq ø$ then
Add it to then known list and assign default trust value
Step 4: Else if sender is unknown vehicle and $(F_{s,m}^{T}(\Delta t) < ø$ then
Add it to the black list and discard its message
Broadcast the ID of malicious vehicles to the neighbours
End If
End If
End If
End If

decreasing its value by 1.5. A reward and penalty system is a valuable addition to the trust update algorithm in proposed routing algorithm. By encouraging good behavior, discouraging malicious behavior, and promoting fairness and stability in the network, a reward and penalty system can help to improve the trustworthiness and security of the network. Furthermore, if sender is unknown and trusted then TrUp adds it to then known list and assign default trust value. Moreover, if sender is unknown and untrusted then TrUp adds it to then black list and discard its message as well as broadcast its ID to the neighbours. Blacklist and known list are important components of the trust update algorithm in trust-based routing for VANETs. They help to improve security, promote fairness, and reduce congestion on the network, while providing a mechanism for real-time trust evaluation and reducing false positives.

Updating trust metrics in real-world scenarios can be done through periodic updates using a logical time window. Periodic updates involve regularly recalculating the trust metrics based on the latest observations and feedback. Periodic updates allow for regular and systematic re-evaluation of trust metrics over specific time intervals. This approach can provide a more comprehensive and balanced assessment of trustworthiness by considering a sufficient amount of recent data. It ensures that trust values are updated consistently and allows for the detection of long-term patterns or changes in behavior. Periodic updates can be beneficial in scenarios where stability and overall behavior trends are essential. By calculating and updating trust metrics in real-world scenarios using the proposed scheme, VANETs can enhance the reliability, security, and performance of communication by effectively evaluating the trustworthiness of nodes and making informed routing decisions.

6 Simulation and results

In this section, we discuss the simulation setting and results obtained after experiments on Veins (3.0) simulator [41]. Veins is an open-source, event-driven simulator for vehicular networks that is based on the popular network simulator OMNeT++. It is designed to simulate the communication between vehicles and roadside infrastructure in VANETs and is widely used in research and development of VANETs. Veins allows users to create and simulate realistic vehicular network scenarios, including the behaviour of vehicles, road infrastructure, and wireless communication channels. It includes a variety of mobility models, including the SUMO (Simulation of Urban MObility) traffic simulator, which simulates vehicle movement on road networks. In addition to the mobility models, Veins also includes various communication models, such as IEEE 802.11p and 3G/4G LTE, which allow users to simulate different communication technologies and protocols in vehicular networks. The simulator also includes support for different routing protocols, such as AODV, DSR, and GPSR [42].

For the experimental work, we have used 12th Gen Intel® Core™ i5-1235U, Windows 11withIntel® Iris® Xe Graphics, 32GBDDR4 RAM(3200 MHz), 512 GBSSD. In the proposed work, the number of vehicles can vary from 10 to 200, with vehicle speed ranging from 20 to 120 kmph. The mobility model used is SUMO, and the road length is set to 5 km. The vehicle size is set to 5 m, and the packet size is 1024 bytes. The simulation time is set to 200 s, and the maximum transmission range is 300 m. The MAC protocol used is IEEE802.11p, with a range of trust value between 0 to 10 and a trust threshold of 5. The weights assignment strategy is equal weights, with a queue size of 60 packets. The topology

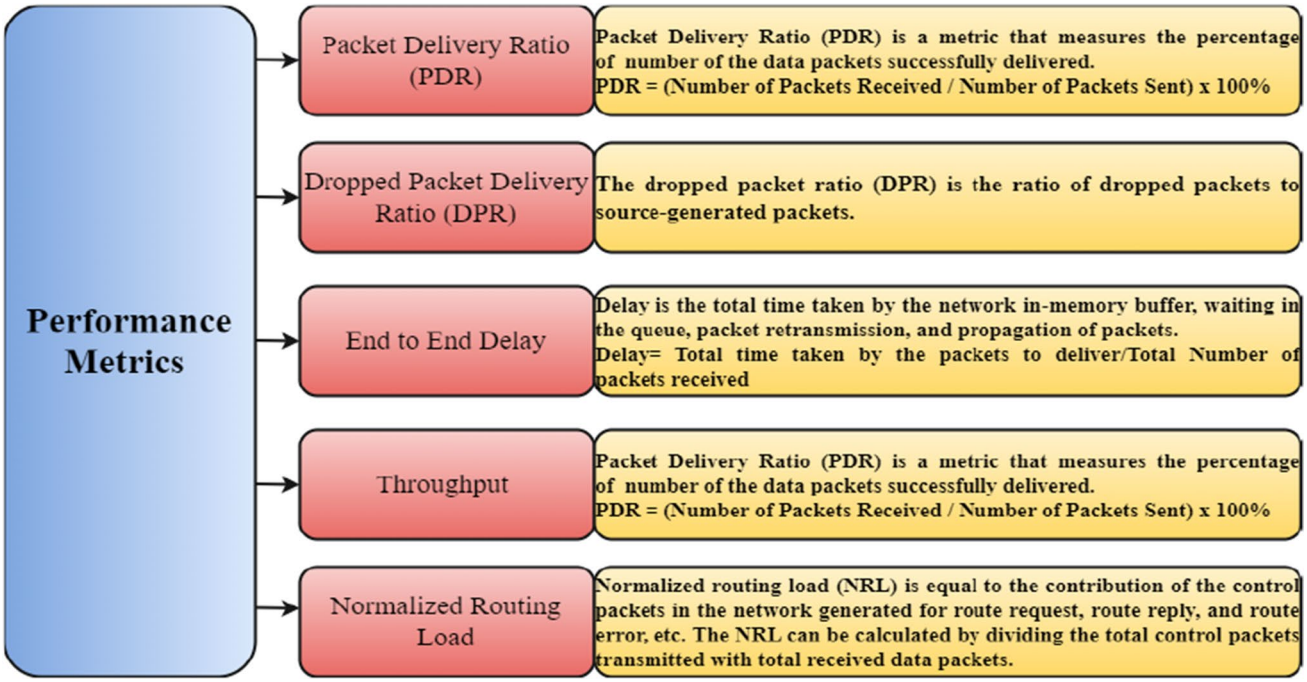

Fig. 4 Performance metrics

is graph-based, and the channel type is wireless. The data sending rate is 2 Mbps, and the values of ρR and ρT are set to 0.5. The values of ρU and ρN are also set to 0.5, while the value of μ ranges from 0.5 to 1. These settings can be modified based on the specific requirements of the VANET simulation to be carried out. Figure 4 illustrates the performance metrics that were utilized in this research study, including their respective formulas for computation (Table 2).

Figure 5 shows the impact of vehicle density on packet delivery ratio (PDR). It shows that as the number of vehicles are increasing, the PDR of proposed GBTR is increasing and higher than LARgeoOPT [7], KMRP [8], and OPBRP [9]. Moreover, in the proposed GBTR, the PDR is consistently increasing but in other schemes, PDR value is fluctuating as the number of vehicles are increasing. Furthermore, with vehicle density as 100, the PDR of proposed GBTR, LARgeoOPT [7], KMRP [8], and OPBRP [9] are 94%, 90%, 92% and 28% respectively. Based on the PDR values and assuming that higher PDR is better, GBTR has the highest PDR among the four algorithms, followed by KMRP, LARgeoOPT, and OPBRP. The percentage improvement of GBTR over LARgeoOPT, KMRP, and OPBRP were found to be 4.44%, 2.17%, and 235.71% respectively. Therefore, GBTR has a significant improvement in PDR compared to LARgeoOPT, KMRP, and OPBRP, with the highest improvement seen over OPBRP. The main reason behind this remarkable performance is robust trust model that provide accurate trust value for efficient routing. The proposed trust model eliminate the malicious nodes from the dense network and avoids redundant as well as repetitive data transmission to improve packet delivery ratio.

Table 2 List of simulation parameters

Parameter name	Value
Simulation Area	3400 m *3400 m
Number of Vehicles	[10–200]
Vehicle Speed Ranges	(20–120) kmph
Mobility Model	SUMO traffic simulator
Road Length	5 km
Vehicle Size	5
Packet Size	1024 Bytes
Simulation Time	200 s
Maximum Transmission Range	300 m
Mac Protocol	IEEE802.11p
Range of Trust Value	[0 to 10]
Trust Threshold (ø) and initial trust value	5
Weights Assignment Strategy	Equal weights
Queue Size (In Packets)	60
Topology	Graph based
Channel Type	Wireless
Communication	Broadcast
Data Sending Rate	2 Mbps
ρR and ρT	0.5
ρU and ρN	0.5
μ	[0.5 to 1]

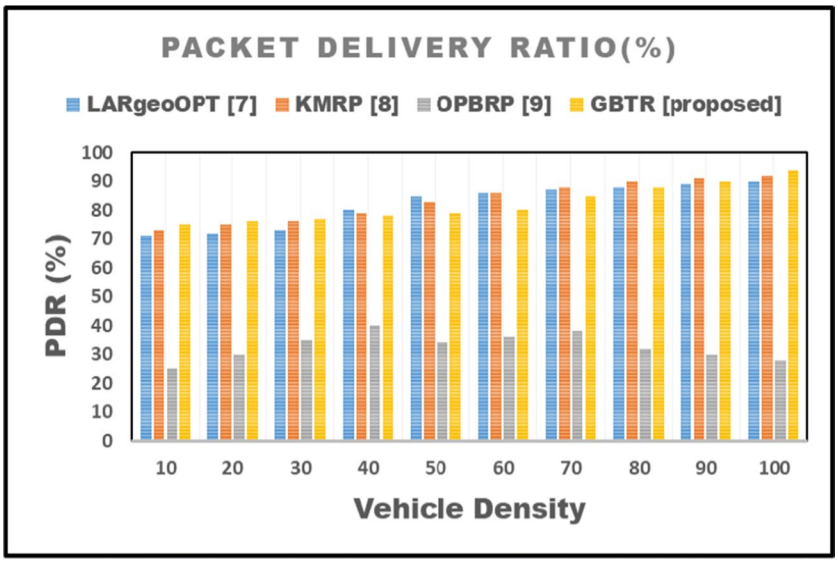

Fig. 5 Packet delivery ratio vs. vehicle density

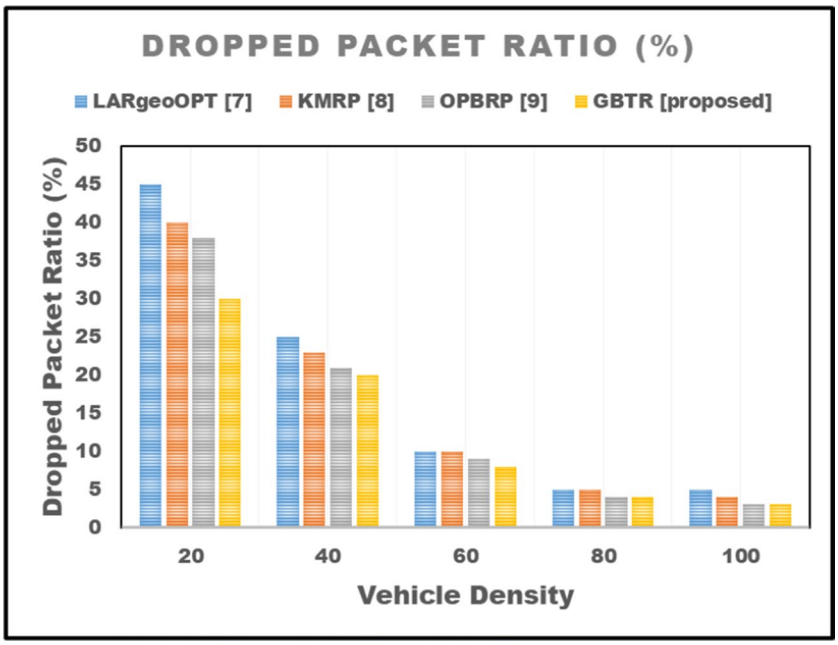

Fig. 6 Dropped packet delivery ratio vs. vehicle density

Figure 6 shows the comparative analysis of dropped packet ratio (DPR) of proposed GBTR, LARgeoOPT [7], KMRP [8], and OPBRP [9]. It is observed that as the vehicle density is increasing, the DPR (%) is decreasing since more vehicles are generating packets and sharing the channel so packets are dropping due to congestion. However, DPR (%) in GBTR is least than LARgeoOPT [7], KMRP [8], and OPBRP [9]. With vehicle density as 100, the DPR of proposed GBTR, LARgeoOPT [7], KMRP [8], and OPBRP [9] are 3%, 5%, 4% and 3% respectively. It shows that GBTR outperforms the other schemes for dropped packet ratio in this scenario, with a percentage improvement of between 25 to 40% over the other schemes. Moreover, With vehicle density as 80, the DPR of proposed GBTR, LARgeoOPT [7], KMRP [8], and OPBRP [9] are 4%, 5%, 5% and 5% respectively. Furthermore, it is observed that GBTR scheme has the lowest dropped packet ratio for all scenarios, followed by OPBRP, KMRP, and LARgeoOPT.

Figure 7 shows the impact of vehicle density on end-to-end delay (E2E-D) for recommended GBTR, LARgeoOPT [7], KMRP [8], and OPBRP [9]. It is observed that end-to-end delay for GBTR is less than LARgeoOPT [7], KMRP [8], and OPBRP [9] in all scenarios of vehicle density since GBTR employs a lightweight trust model in fast routing algorithm that select reliable route with less link failure. During indirect trust evaluation, we consider link reliability factor to reduce

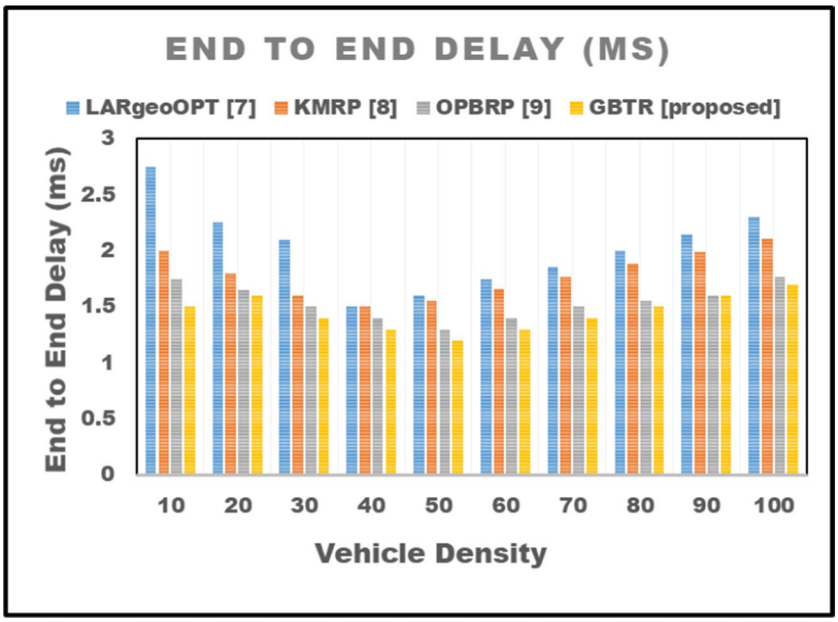

Fig. 7 End to end delay vs. vehicle density

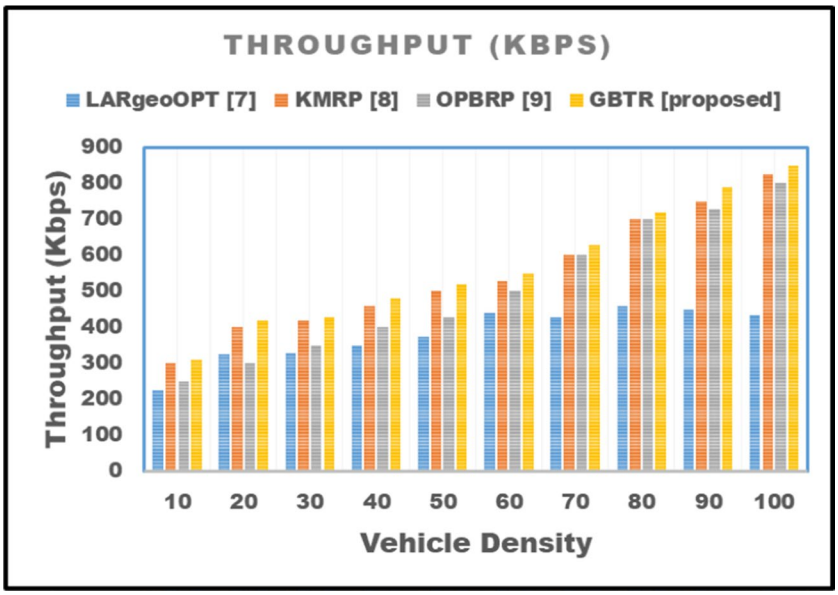

Fig. 8 Throughput vs. vehicle density

link failure probability. With vehicle density as 100, the E2E-D of proposed GBTR, LARgeoOPT [7], KMRP [8], and OPBRP [9] are 1.7 ms, 2.3 ms, 2.11 ms, and 1.77 ms, respectively. It shows that GBTR outperforms the other schemes for E2E-D in this scenario, with a percentage improvement of between 3.95% to 26.09% over the other schemes. Moreover, With the vehicle density as 90, the E2E-D of proposed GBTR, LARgeoOPT [7], KMRP [8], and OPBRP [9] are 1.6 ms, 2.15 ms, 1.99 ms, and 1.6 ms, respectively. Furthermore, it is observed that GBTR scheme has the lowest E2E-D for all scenarios, followed by OPBRP, KMRP, and LARgeoOPT. Our developed protocol suggest that messages can be transmitted in less time compared to the protocol in [7–9].

Figures 8 and 9 shows the impact of vehicle density and velocity on throughput for recommended GBTR, LARgeoOPT [7], KMRP [8], and OPBRP [9]. It is observed that throughput for GBTR is higher than LARgeoOPT [7], KMRP [8], and OPBRP [9] in all scenarios of vehicle density and velocity since GBTR employs a competent trust model in an efficient routing algorithm that reduce delay and improve PDR. In Fig. 8, throughput of GBTR is increasing with the rise in vehicle density. However, if we increase the velocity of vehicles, the value of throughput is decreases for all the schemes due to dynamic nature of VANET and link failure probability. Even the throughput of all schemes are decreasing with the rise in velocity,

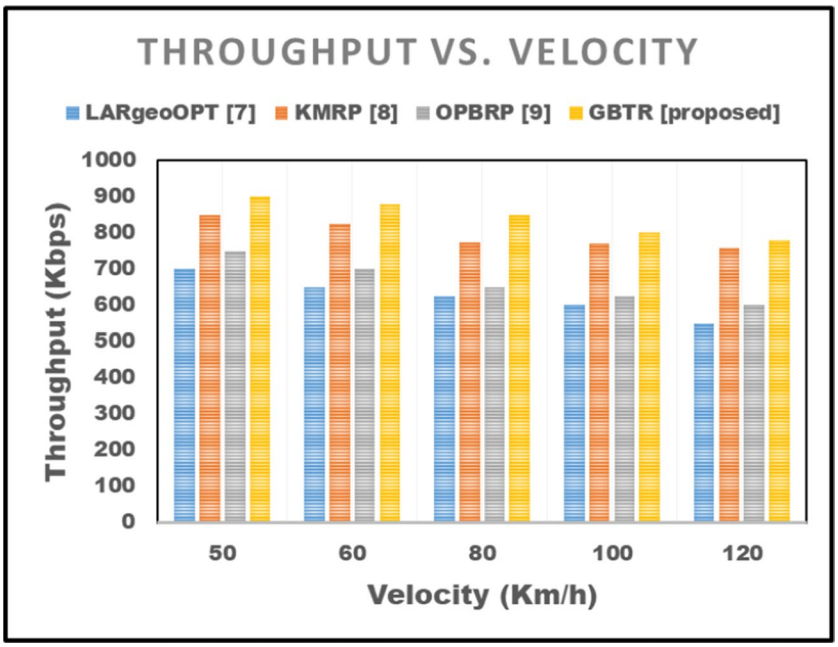

Fig. 9 Throughput vs. velocity

still the proposed scheme achieves better throughput than LARgeoOPT [7], KMRP [8], and OPBRP [9] due to incorporation of link reliability factor during indirect trust evaluation. Moreover, the proposed scheme (GBTR) achieves good PDR, less delay for better throughput. With the vehicle velocity as 80 km/h, the throughput of proposed GBTR, LARgeoOPT [7], KMRP [8], and OPBRP [9] are 850 kbps, 624kbps, 775 kbps, and 650 kbps, respectively. Moreover, With the vehicle velocity as 100 km/h, the throughput of proposed GBTR, LARgeoOPT [7], KMRP [8], and OPBRP [9] are 800 kbps, 600kbps, 770 kbps, and 624 kbps, respectively. Furthermore, With the vehicle velocity as 120 km/h, the throughput of proposed GBTR, LARgeoOPT [7], KMRP [8], and OPBRP [9] are 780 kbps, 550kbps, 760 kbps, and 600 kbps, respectively. In this case, GBTR outperforms LARgeoOPT [7], KMRP [8], and OPBRP [9] by 41.82%, 2.63%, and 30%, respectively.

Figure 10 shows the impact of vehicle density on normalized routing load (NRL). It is observed that as the number of vehicles are increasing, NRL is increasing in all schemes

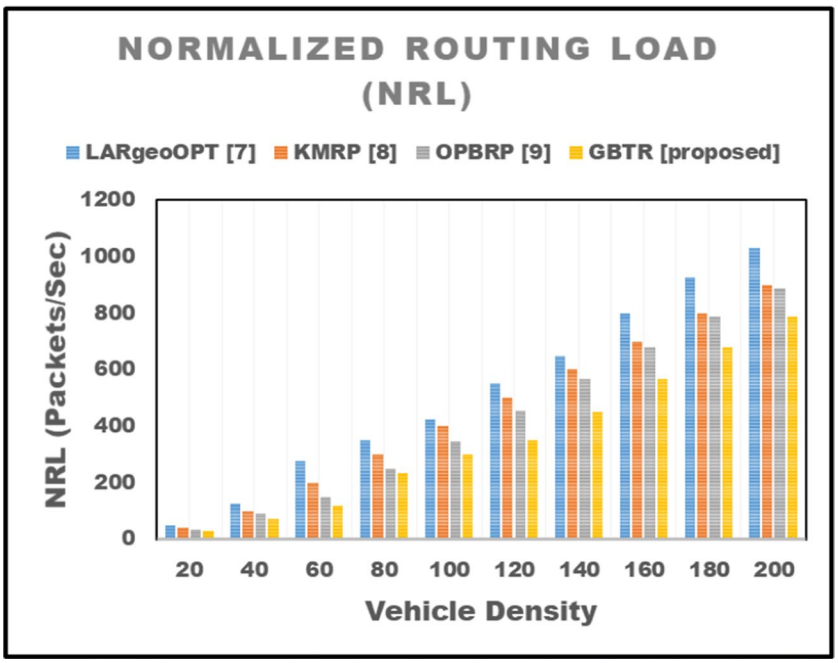

Fig. 10 NRL vs. vehicle density

since wireless channel is shared by more number of vehicles. However, the value of NRL in proposed scheme is less than LARgeoOPT [7], KMRP [8], and OPBRP [9] in all cases. In existing routing protocols, all vehicles in the network are considered equal, and any vehicle can participate in routing packets. This can lead to increased routing load as packets are forwarded through the network, even if some vehicles may not be trustworthy or reliable. GBTR addresses this issue by using a trust-based approach to routing where each vehicle in the network is assigned a trust score based on its past behavior and interactions with other vehicles. The trust scores are then used to to make routing decisions, only forwarding packets through the most trustworthy and reliable routes. By reducing the number of vehicles involved in routing packets and only using the most trustworthy connections, GBTR is able to reduce network routing load. This results in improved network efficiency and can also reduce the potential for malicious attacks or data tampering, as only trusted vehicles are involved in the routing process. With vehicle density as 100, the NRL of proposed GBTR, LARgeoOPT [7], KMRP [8], and OPBRP [9] are 300 packest/sec, 425 packest/sec, 400 packest/sec, and 345 packest/sec, respectively. Moreover, with vehicle density as 200, the NRL of proposed GBTR, LARgeoOPT [7], KMRP [8], and OPBRP [9] are 789 packest/sec, 1030 packest/sec, 900 packest/sec, and 890 packest/sec, respectively. In this worst case, we can see that GBTR performs significantly better than LARgeoOPT [7], KMRP [8], and OPBRP [9], with a percentage improvement of 23.30%, 12.33% and 11.35%, respectively.

7 Conclusion and future work

VANETs are wireless networks where vehicles communicate with each other and roadside infrastructure, face security vulnerabilities due to their dynamic nature and absence of centralized infrastructure. Trust-based routing is crucial in VANETs because it can enhance the security, reliability, and efficiency of communication between vehicles. In this paper, we propose a Graph-Based Trust-Enabled Routing (GBTR) in VANETs that utilizes direct trust, indirect trust, and contextual trust to assess the trustworthiness of nodes. Direct trust considers factors like successful communication frequency, consistency, delay, and a mobility factor. Indirect trust incorporates feedback trust value, link reliability, and the mobility factor. Contextual trust integrates location, time of day, weather conditions, and traffic density for each node pair. The final trust score is used in routing algorithm to find the reliable route without loss of sensitive information. The routing algorithm uses request/reply mechanism and route maintenance mechanism to ensure a reliable route for data transmission in the VANET. Moreover, a trust update algorithm is also employed to improve the efficiency of GBTR in terms of security, reliability, and robustness. The proposed scheme (GBTR) is simulated using Veins (3.0) simulator and results are obtained in terms of packet delivery ratio (PDR%), dropped packet ratio (DPR%), end-to-end delay (ms),throughput (Kbps) and normalized routing load (packets/sec). The experimental outcome proves that the proposed scheme (GBTR) resolves the limitations of existing schemes by ensuring the reliability and security of VANETs.

Future research directions involve addressing limitations of the proposed routing scheme. This includes developing more efficient algorithms for updating the evolving graph model and reliable path selection. Improving accuracy and reliability of vehicle location and movement information through sensor fusion and machine learning techniques is another area of investigation. Additionally, exploring techniques to handle routing limitations in highly congested or interfered scenarios is crucial for future research.

Author Contribution Intyaz Alam: Writing – original draft, Methodology.

Manisha manjul: Writing – original draft, Methodology, Software, Validation, Visualization.

Vinay Pathak: Conceptualization, Formal analysis, Investigation.

Vajenti Mala: Conceptualization, Writing – review & editing, Methodology.

Anuj Mangal: Conceptualization, Writing, Formal analysis, Investigation Editing.

Data Availability The datasets generated and/or analyzed during the current study are available from the corresponding author on reasonable request.

Declarations

We declare that this manuscript is original, has not been published before, and is not currently being considered for publication elsewhere. As a corresponding author, I confirm that the manuscript has been read and approved for submission by all the named authors.

Conflict of Interest The authors declare that they have no competing interests.

References

1. Eiza MH, Ni Q (2013) An evolving graph-based reliable routing scheme for VANETs. IEEE Trans Veh Technol 62(4):1493–1504
2. Wahid I, Ikram AA, Ahmad M, Ali S, Ali A (2018) State of the art routing protocols in VANETs: A review. Proc Comput Sci 130:689–694
3. Kirtiga R, GnanaPrakasi OS, Kavipriya D, Anita R, Varalakshmi P (2014) Reliable graph based routing in VANET environment. In: 2014 international conference on recent trends in information technology. IEEE, pp 1–6
4. Dietzel S, Petit J, Heijenk G, Kargl F (2012) Graph-based metrics for insider attack detection in VANET multihop data dissemination protocols. IEEE Trans Veh Technol 62(4):1505–1518
5. Xia H, Zhang S-s, Li B-x, Li L, Cheng X-g (2018) Towards a novel trust-based multicast routing for VANETs. Security and Communication Networks 2018

6. Dhiman M, Jadhav MV (2015) Reliable graph-based routing in vanet environment. In: 2015 international conference on computation of power, energy, information and communication (ICCPEIC). IEEE, pp 0235–0238
7. Husain A, Singh SP, Sharma SC (2020) PSO optimized geocast routing in VANET. Wirel Pers Commun 115:2269–2288
8. Kandali K, Bennis L, Bennis H (2021) A new hybrid routing protocol using a modified K-means clustering algorithm and continuous hopfield network for VANET. IEEE Access 9:47169–47183
9. Diaa MK, Mohamed IS, Hassan MA (2023) OPBRP-obstacle prediction based routing protocol in VANETs. Ain Shams Eng J 14(7):101989
10. Mahdi HF, Abood MS, Hamdi MM (2021) Performance evaluation for vehicular ad-hoc networks based routing protocols. Bull Electr Eng Inf 10(2):1080–1091
11. Belamri F, Boulfekhar S, Aissani D (2021) A survey on QoS routing protocols in vehicular Ad Hoc network (VANET). Telecommun Syst 78(1):117–153
12. Talin J, Rajesh RS, ArunMozhiSelvi SS (2018) A survey on topology and geography based routing protocols in vanets. Int J Appl Eng Res 13(20):14813–14822
13. Hosmani S, Mathpati B (2017) Survey on cluster based routing protocol in VANET. In: 2017 international conference on electrical, electronics, communication, computer, and optimization techniques (ICEECCOT). IEEE, pp 1–6
14. Chen Y-S, Lin Y-W, Pan C-Y (2011) DIR: diagonal-intersection-based routing protocol for vehicular ad hoc networks. Telecommun Syst 46:299–316
15. Abdalla AM, Salamah SH (2022) Performance comparison between delay-tolerant and non-delay-tolerant position-based routing protocols in VANETs. Int J Commun Netw Syst Sci 15(1):1–14
16. Bengag A, Bengag A, Elboukhari M (2020) Routing protocols for VANETs: a taxonomy, evaluation and analysis. Adv Sci Technol Eng Syst J 5(1):77–85
17. Elira B, Keerthana KP, Balaji K (2021) Clustering scheme and destination aware context based routing protocol for VANET. Int J Intell Netw 2:148–155
18. Satyajeet D, Deshmukh AR, Dorle SS (2016) Heterogeneous approaches for cluster based routing protocol in vehicular ad hoc network (vanet). Int J Comput Appl 134(12):1–8
19. Oche M, Tambuwal AB, Chemebe C, Md Noor R, Distefano S (2020) VANETs QoS-based routing protocols based on multi-constrained ability to support ITS infotainment services.". Wirel Netw 26:1685–1715
20. Hamdi MM, Al-Dosary OAR, Alrawi OAS, Mustafa AS, Abood MS, Noori MS (2021) An overview of challenges for data dissemination and routing protocols in VANETs. In: 2021 3rd international congress on human-computer interaction, optimization and robotic applications (HORA). IEEE, pp 1–6
21. Sehrawat P, Chawla M (2023) Interpretation and investigations of topology based routing protocols applied in dynamic system of VANET. Wireless Pers Commun 128(3):2259–2285
22. Shrivastava PK, Vishwamitra LK (2021) Comparative analysis of proactive and reactive routing protocols in VANET environment. Meas Sens 16:100051
23. Shafi S, Ratnam DV (2022) A trust based energy and mobility aware routing protocol to improve infotainment services in VANETs. Peer Peer Netw Appl 1–16
24. Shokrollahi S, Dehghan M (2023) TGRV: A trust-based geographic routing protocol for VANETs. Ad Hoc Netw 140:103062
25. Kudva S, Badsha S, Sengupta S, La H, Khalil I, Atiquzzaman M (2021) A scalable blockchain based trust management in VANET routing protocol. J Parallel Distrib Comput 152:144–156
26. Kaur G, Kakkar D (2022) Hybrid optimization enabled trust-based secure routing with deep learning-based attack detection in VANET. Ad Hoc Netw 136:102961
27. Khan T, Singh K, Hasan MH, Khaleel Ahmad G, Reddy T, Mohan S, Ahmadian A (2021) ETERS: A comprehensive energy aware trust-based efficient routing scheme for adversarial WSNs. Futur Gener Comput Syst 125:921–943
28. Khan T, Singh K, Manjul M, Ahmad MN, Zain AM, Ahmadian A (2022) A Temperature-Aware Trusted Routing Scheme for Sensor Networks: Security Approach. Comput Electr Eng 98:107735
29. Khan T, Singh K (2021) TASRP: a trust aware secure routing protocol for wireless sensor networks. Int J Innovative Comput Appl 12(2–3):108–122
30. Khan T, Singh K, Abdel-Basset M, Long HV, Singh SP, Manjul M (2019) A novel and comprehensive trust estimation clustering based approach for large scale wireless sensor networks. Ieee Access 7:58221–58240
31. Kumar A, Singh K, Khan T, Ahmadian A, MdSaad MH, Manjul M (2021) ETAS: an efficient trust assessment scheme for BANs. IEEE Access 9:83214–83233
32. Kchaou A, Abassi R, El Fatmi SG (2021) Towards the performance evaluation of a trust based routing protocol for VANET. In: Advanced information networking and applications: proceedings of the 35th international conference on advanced information networking and applications (AINA-2021), vol 1 35. Springer International Publishing, pp 113–124
33. Gayathri M, Gomathy C (2022) An overview of security services and trust-based authentication schemes in VANET. Micro-Electron Telecommun Eng: Proc 5th ICMETE 2021:193–205
34. Fatemidokht H, Rafsanjani MK, Gupta BB, Hsu C-H (2021) Efficient and secure routing protocol based on artificial intelligence algorithms with UAV-assisted for vehicular ad hoc networks in intelligent transportation systems. IEEE Trans Intell Transp Syst 22(7):4757–4769
35. Velayudhan NC, Anitha A, Madanan M (2022) An optimisation driven deep residual network for sybil attack detection with reputation and trust-based misbehaviour detection in VANET. J Exp Theor Artif Intell 1–24
36. Gupta M, Gera P, Mishra B (2022) Direct Trust-Based GPSR Protocol (DT-GPSR) in VANET. In: Inventive Communication and Computational Technologies: Proceedings of ICICCT 2022. Springer Nature Singapore, Singapore, pp. 41–57
37. Naeem A, Rizwan M, Alsubai S, Ahmad Almadhor Md, Akhtaruzzaman SI, Rahman H (2023) Enhanced clustering based routing protocol in vehicular ad-hoc networks. IET Electric Syst Transp 13(1):e12069
38. Luong NT, Hoang D (2023) BAPRP: a machine learning approach to blackhole attacks prevention routing protocol in vehicular Ad Hoc networks. Int J Inf Secur 1–20.
39. Xie X, Navaei YD, Einy S (2023) A clustering-based routing protocol using path pattern discovery method to minimize delay in VANET. Wirel Commun Mob Comput
40. Monfared SK, Shokrollahi S (2023) DARVAN: A fully decentralized anonymous and reliable routing for VANets. Comput Netw 223:109561
41. Speiran J, Shakshuki EM (2022) Understanding the effect of physical parameters on packet loss in Veins VANET simulator. Proc Comput Sci 201:359–367
42. Sommer C, Eckhoff D, Brummer A, Buse DS, Hagenauer F, Joerer S, Segata M (2019) Veins: The open source vehicular network simulation framework. Recent Adv Netw Simul: OMNeT++ Environ Ecosyst 215–252

Authors and Affiliations

Intyaz Alam[1] · Manisha Manjul[2] · Vinay Pathak[3] · Vajenti Mala[4] · Anuj Mangal[5] · Hardeo Kumar Thakur[6] · Deepak Kumar Sharma[7]

✉ Intyaz Alam
intyazcsejnu@gmail.com

✉ Hardeo Kumar Thakur
hardeokumar@gmail.com

Manisha Manjul
manisha.manjul@dseu.ac.in

Vinay Pathak
vinaypathak85@gmail.com

Vajenti Mala
er.vajenti@gmail.com

Anuj Mangal
anuj.mangal@gla.ac.in

Deepak Kumar Sharma
dk.sharma1982@yahoo.com

1 School of Computer and Systems Sciences, JNU, New Delhi, India

2 Computer Science and Application at G.B. Pant DSEU Okhla-I Campus, New Delhi, India

3 Computer Science and Engineering, IIIT, Sonipat, India

4 Department of Computer Engineering & Applications, GLA University, Mathura, UP, India

5 Computer Science and Engineering, Galgotias University, UP, India

6 Bennett University, Greater Noida, India

7 Department of Information Technology, Indira Gandhi Delhi Technical University for Women, Delhi, India