Enhancing vehicular ad hoc network security through a trust-based vehicular model for attack mitigation

Shilpa, Thiruvenkadam Prasanth
Department of Computer Science Engineering, REVA University, Bengaluru, India

Article Info

Article history:

Received Nov 28, 2025
Revised Dec 26, 2025
Accepted Jan 10, 2026

Keywords:

Attack prevention
Dynamic trust
IoV-PBFT
Security
Trust-based vehicular
Vehicular ad-hoc networks

ABSTRACT

In vehicular ad-hoc networks (VANETs), ensuring secure and reliable communication is essential due to the growing threat of cyber-attacks. As attacks can disrupt data transmission and compromise user privacy and network integrity, it is vital to develop robust security solutions. Hence, this work introduces a trust-based vehicular security (TVS) model, which leverages trust metrics to enhance VANET security. The main objective was to establish secure connections between vehicles and infrastructure nodes, effectively mitigating attacks while maintaining higher throughput. The methodology integrated a dynamic trust evaluation model to prevent malicious activities and ensure secure data transmission. The TVS model's performance was compared to an existing VANET model, showing improved results in terms of detection rate, misclassification rate, and throughput. The findings demonstrate an average misclassification rate of 22.75%, a detection rate of 14.77%, and a throughput of 11.45%, highlighting the superior effectiveness of the TVS model in attack-prone environments when compared with existing VANET models. The TVS model provides a promising security solution for VANETs, offering enhanced protection against denial-of-service (DoS) attacks and spoofing (cyber-attacks) with better accuracy and network performance. The novelty lies in the dynamic, multi-trust-based approach for secure communication in vehicular networks.

Corresponding Author:

Shilpa
Department of Computer Science Engineering, REVA University
Bengaluru, India
Email: shilpasadlapur@rediffmail.com

1. INTRODUCTION

Vehicular ad-hoc networks (VANETs) are specialized wireless networks designed for vehicles to communicate with each other and with roadside infrastructure, vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-everything (V2X) and other communication paradigms as presented in Figure 1 [1]. By utilizing dynamic topologies and short-range wireless technologies such as dedicated short-range communication (DSRC) and 5G, VANETs enable real-time communication for applications ranging from traffic management to safety alerts. These networks play a pivotal role in enhancing road safety, reducing traffic congestion, and improving overall transportation efficiency [1]. VANETs are characterized by high mobility, frequent topology changes, and the need for low-latency communication, making them a critical component of modern transportation systems [2]. Moreover, VANETs are intrinsically linked to the intelligent transportation system (ITS), a framework that leverages advanced technologies to create safer, more efficient, and sustainable transportation systems [3].

ITS integrates communication technologies, sensors, and data analytics to optimize traffic flow, improve safety, and reduce environmental impact [4]. VANETs form the backbone of ITS by providing real-time communication between vehicles and infrastructure, enabling applications like adaptive traffic lights, emergency vehicle prioritization, and collision avoidance systems. The synergy between VANETs and ITS facilitates smarter urban mobility and contributes to the development of connected and automated vehicle ecosystems [5]. Nevertheless, VANETs are integral to the broader internet of vehicles (IoV) framework, which connects vehicles to the internet and other devices, enabling a seamless flow of data and services [6]. IoV encompasses V2V, V2I, and V2X communication paradigms. V2V communication allows vehicles to exchange information about speed, location, and traffic conditions, enhancing safety, and traffic efficiency. V2I communication facilitates interaction with roadside units (RSUs) for traffic management and real-time updates. V2X extends this connectivity to pedestrians, cyclists, and other road users, creating a holistic ecosystem for connected mobility. These connectivity paradigms position VANETs as a cornerstone of modern transportation systems, enabling smarter, and more responsive traffic environments.

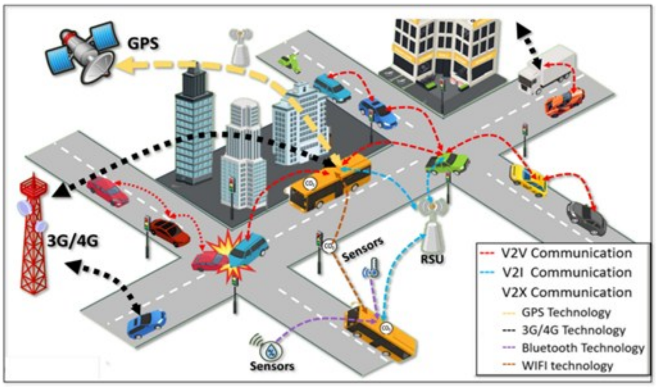

Figure 1. Advanced VANET environment (IoV) [1]

Despite their benefits, VANETs possess unique features that make them vulnerable to a wide range of attacks [7], [8]. High mobility and frequent topology changes increase the risk of unauthorized access and data breaches. The decentralized nature of VANETs can lead to challenges in maintaining secure communication. Additionally, open wireless communication channels are susceptible to eavesdropping, jamming, spoofing, and denial-of-service (DoS) attacks [9], [10]. The reliance on trust between nodes further complicates security, as malicious nodes can exploit trust-based interactions to disrupt the network or disseminate false information. Earlier approaches to securing VANETs relied heavily on traditional cryptographic methods [11], [12], including certificates [13], public key infrastructures (PKI) [14], and digital signatures [15]. These methods provided authentication and encryption to protect data from unauthorized access. However, they faced challenges in scalability, latency, and resource consumption, particularly in dynamic and high-mobility environments like VANETs. The need for frequent key exchanges and certificate revocations often introduced delays and computational overhead, which compromised the network's efficiency and responsiveness. Additionally, these methods struggled to detect and mitigate insider threats or compromised nodes, leaving networks vulnerable to attacks such as Sybil attacks and routing disruptions. To address these limitations, recent research has focused on trust-based security mechanisms for VANETs [16], [17].

Trust-based approaches evaluate the reliability and behavior of nodes to establish secure communication. These methods incorporate metrics such as direct trust, indirect trust, and historical trust to assess node authenticity. Trust-based models provide dynamic and adaptive security, enabling real-time identification of malicious nodes and fostering secure data exchange. They offer a more robust and flexible solution compared to traditional cryptographic approaches, as they adapt to the dynamic and distributed nature of VANETs. While trust-based approaches have significantly improved VANET security, existing models often lack comprehensive trust evaluation mechanisms that integrate multiple dimensions of trust. Furthermore, many models struggle to balance security with computational efficiency and scalability. Hence, this work proposes a trust-based vehicular security (TVS) model that addresses these challenges by integrating direct trust, indirect trust, recent trust, past trust, and anticipated future trust into a unified framework. The TVS model dynamically evaluates and updates trust values using weighted methods, ensuring robust security without compromising efficiency. By incorporating real-time position evaluation and dynamic state-changing mechanisms, the TVS model effectively identifies and mitigates malicious activities, providing a holistic solution to VANET security challenges. The contributions of the TVS model are presented as follows.

The TVS model integrates multiple dimensions of trust, including direct, indirect, recent, past, and future trust, for a robust and dynamic assessment of vehicle (node) reliability. Introduced a novel probabilistic state-changing mechanism to detect and mitigate attacks in real-time by analyzing changes in vehicle behavior, ensuring secure and efficient communication. Designed the TVS model to operate efficiently in large-scale, high-mobility VANET environments by optimizing resource utilization and reducing communication delays.

Demonstrated improved attack detection accuracy and reduced misclassification rates compared to existing approaches, ensuring robust protection against malicious activities. Evaluated the TVS model using real-world parameters and scenarios, highlighting its superior performance in throughput, latency, and attack prevention. By addressing the gaps in existing security frameworks, the TVS model establishes a new benchmark for securing VANETs, paving the way for safer and more efficient ITSs.

Further, the manuscript is organized in the following way: section 2 discusses the state-of-the-art advancements in trust management for VANETs, focusing on dynamic trust evaluation, cryptographic techniques, and blockchain-based solutions. Section 3 presents the TVS model. Section 4 discusses the results of the TVS model compared with existing approaches. Finally, section 5 presents the conclusion and future work.

2. LITERATURE SURVEY

VANETs have emerged as a critical component of ITS, enabling efficient communication and enhanced safety. However, the dynamic and decentralized nature of VANETs introduces significant security challenges, such as malicious node behavior, trust management, and attack prevention. Over the years, various trust-based and blockchain-integrated security mechanisms have been proposed to address these issues. This literature survey explores the state-of-the-art advancements in trust management for VANETs, focusing on dynamic trust evaluation, cryptographic techniques, and blockchain-based solutions.

Rehman *et al.* [18] presented a trust-based approach for IoV in VANET for the identification of malicious events and nodes. Their work was different from other works as they considered dynamic parameters and scenarios for building their model. Also, their framework was built based on a context-aware cognitive model with artificial intelligence for constantly learning the changes in the VANET environment. They evaluated their model in MATLAB, and the findings showed that their approach provided better IoV security in VANET in terms of trust levels and malicious node detection. Amari *et al.* [19] conducted a review on various trust approaches presented in recent years for VANET in various paradigms. Their review discussed different trust mechanisms, existing approaches presented in recent years, challenges faced by existing approaches and finally classified the existing approaches into different schemes, i.e., entity-based, data-based, hybrid, and technology-based. Finally concluded their work with future perspectives. Din *et al.* [20] presented contextual-aware cognitive-memory trust-management-system (CACMTM) for ITS. The CACMTM approach utilized game theory for modelling a trust-based approach, evaluating trust, updating trust and taking decisions on trust. Moreover, a cognitive-memory-based trust management approach was integrated into the model for learning past experiences and evolving the model's behavior for providing trust-based security. Their work employed a multi-dimensional trust approach for reducing failure of false-trust and a blockchain-security-based logging approach for providing transparency and security. The CACMTM had four stages, i.e., trust-evaluation, trust-decision, trust-update and trust-knowledge. Evaluation of CACMTM was done on the OMNet++ simulator, where real-world simulation parameters and evaluated in terms of detection accuracy, time, false-negative, and false-positive rate, where findings showed that CACMTM achieved 96.3% accuracy for identifying attacks.

Malik *et al.* [21] presented an approach for preventing grey-hole attacks (GHA) and ad-hoc on-demand distance-vector attacks (AODV) called as detection-prevention of grey-hole attacks (DPGHA) in VANETs. The DPGHA used dynamically changing threshold values for controlling and transmitting packets in VANET. The DPGHA was implemented using simulation of urban mobility (SUMO) and network simulator version 2 (NS-2) simulator, where DPGHA achieved 10.85, 3.85, 4.67, 2.3, and 6.58% better results for routing overhead, average end-to-end delay, packet-delivery rate, detection rate and throughput, respectively, when compared with the existing approach. Xie *et al.* [22] extended their previous work, which was based on IoV, where they provided security for RSUs using blockchain. They identified from their work that their previous work was vulnerable to attacks, hence proposed a blockchain-based elliptic-curve cryptography-based cross-trust approach for IoV. They used different physical-unclonable function (PUF) and biometric-based keys for resisting RSUs intrusion attacks. Findings showed that the presented approach provided better security. Ma *et al.* [23] provided an authentication blockchain trust-based approach for IoV.

Initially, in their work, data was pre-processed and stored in edge for reducing response time and communication delay.

Further, smart contracts were utilized for authenticating data, and an optimal practical-byzantine fault-tolerant-consensus (PBFT) approach was presented for adding the authenticated data to the blockchain ledger. The security was verified using the automated validation of internet security protocols and applications (AVISPA) tool and the real-or-random oracle approach on the SUMO simulator. Findings showed that the approach reduced communication cost and reduced communication overhead. Han *et al.* [24] presented a novel trust incentive-based approach for VANET to provide security. Their approach evaluated the trust-based message using reputation evaluations and feedback functions. A penalty and reward were allocated to vehicles on the basis of game theory, which reduced the transference of false data and attacks. Moreover, a blockchain-based approach was presented for ensuring consistency in storage and the consensus approach. Evaluations were conducted on MATLAB considering real-time scenario parameters, where the presented approach reduced transference of false data, attacks, and improved the VANET environment. Bibi *et al.* [25] presented a trust-aware VANET architecture that was integrated with blockchain and information-centric networking for providing content-based security. Their approach utilized vehicle authentic data to ensure content integrity in VANET, thereby providing security. Evaluations of the approach were conducted in Jupyter, where the results were evaluated in terms of throughput, bandwidth usage, content delivery and network content usage. The approach showed better results when compared with existing approaches.

Existing approaches to enhancing security in VANETs face notable limitations as seen from the above study. Trust-based models like those proposed in [18], [20] often rely on predefined parameters or static frameworks, making them less adaptable to dynamic VANET environments. Contextual models and cognitive approaches, while innovative, may suffer from computational overhead and scalability issues in large-scale networks. Blockchain-integrated solutions, such as [22], [23], provide improved transparency and tamper-proofing but often incur high communication delays and resource consumption. Similarly, soft-computing approaches like [24]–[28] require extensive computational resources and may struggle to adapt to real-time changes. The TVS model overcomes these limitations by utilizing a comprehensive and adaptive trust evaluation mechanism that integrates multiple trust dimensions, including direct, indirect, recent, past, and anticipated future trust. By employing dynamic weight allocation, state-changing mechanisms, the TVS model ensures low computational overhead, high scalability, and robust attack detection [29], [30]. Its ability to dynamically converge transmitted information and identify malicious nodes in real-time addresses the gaps in previous models, providing a holistic and efficient solution for VANET security. In the next section, the TVS model is discussed in detail.

3. TRUST-BASED VEHICULAR SECURITY MODEL

This work introduces a TVS model aimed at enhancing security in VANETs. The TVS model leverages the concept of trust to establish secure connections between vehicles and nearby infrastructure. By utilizing trust as the basis for connection, the model ensures robust security measures and effectively mitigates potential attacks in VANETs. This novel approach integrates trust-based mechanisms with attack prevention to provide a comprehensive security solution. Consider a scenario where a moving vehicle, represented as a node, seeks to establish a connection with another vehicle or an infrastructure node in the VANET to exchange information, as presented in Figure 2. In such cases, it is crucial to achieve the highest possible level of security to ensure that unauthorized nodes cannot access the information or launch attacks. The TVS model addresses this need by prioritizing trust-based secure communication, thereby safeguarding data exchanges and preventing malicious activities within the network. In the TVS model, the process of establishing a connection begins with evaluating the trust level of the connecting node in relation to other nodes. The trust level in the TVS model is determined by considering multiple trust levels, including indirect trust, direct trust, past trust, recent trust, and anticipated future trust. This comprehensive evaluation ensures a robust and reliable trust assessment, enabling secure and trustworthy connections within the network. In the next section, the indirect trust and direct trust evaluation are discussed in detail.

Consider x as a vehicle (node) present in VANET, y as another vehicle node, u as the duration of the connecting node x connected with other nodes y and o. As the overall duration for exchanging information. From this, the security-based trust parameter can be established as $Sec_o^u(x,y)$, where $Sec_o^u(x,y)$ evaluates the overall trust level of x with y, which is evaluated using (1). In (1), γ denotes the difference between different trust levels to optimise the model dynamically and Sec_{rec} denotes trust level for a recently established connection. The main aim of Sec_{rec} provides validation-based security for connecting with a computing node, hence Sec_{rec} is denoted as (2).

$$Sec_o^u(x,y) = \gamma * Sec_{rec}(x,y) + (1-\gamma) * Sec_{o-1}^u(x,y) \tag{1}$$

$$Sec_{rec} = \begin{cases} 0, \; if\ connection\ is\ completly\ untrustable \\ 1, \quad if\ connection\ is\ completely\ trustable \\ \in (0,1), \quad otherwise \end{cases} \tag{2}$$

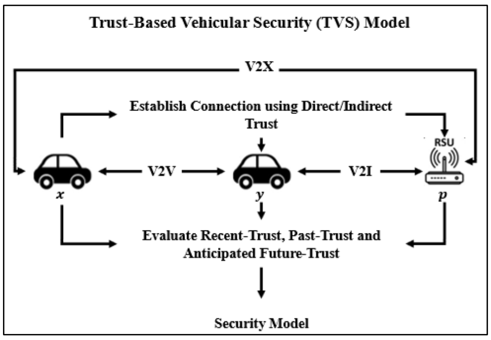
Trust-Based Vehicular Security (TVS) Model
V2X
Establish Connection using Direct/Indirect Trust
RSU
V2V
V2I
x
y
p
Evaluate Recent-Trust, Past-Trust and Anticipated Future-Trust
Security Model

Figure 2. TVS model architecture

This means that when $Sec_{rec} = 0$, established connection among different vehicle and infrastructure pairs cannot be trusted and when $Sec_{rec} = 1$, established connection can be trusted. Moreover, in VANETs, a vehicle can connect to multiple nodes, i.e., V2I, V2V, and V2X, present in a smart city; hence, this work considers representing these nodes as p. In the TVS model, first direct-trust is determined among (x, y), (y, p), and (x, p). In the TVS model, the direct trust is represented as $\mathbb{D}_o^u(x,y)$, which is determined using (3).

$$\mathbb{D}_o^u(x,y) = Sec_o^u(x,y) \tag{3}$$

Using (3), the direct trust is determined for (x, y). Similarly, the direct-trust for (y, p) and (x, p) is established using (3). Further, similar to direct-trust, indirect trust is also determined among (x, y), (y, p), and (x, p), based on a previously established direct-trust. For determining previously established direct-trust, x initially connects with y and y connects with p, from which all nodes collect all the direct-trust values. For sending the collected values directly from (y, p) to x with security, y aggregates overall direct-trust information from p using (4).

$$\mathbb{G}_o^u(x,y) = \begin{cases} \frac{\sum_{p \in Z-\{x\}} \mathbb{F}_o^u(x,p) * \mathbb{D}_o^u(x,y)}{\sum_{p \in Z-\{x\}} \mathbb{F}_o^u(x,p)}, if\ |Z-\{x\}| > 0 \\ 0, if\ |Z-\{x\}| = 0 \end{cases} \tag{4}$$

In (4), $\mathbb{G}_o^u(x,y)$ represents overall direct-trust information gathered from p, $\mathbb{F}_o^u(x,p)$ represents authenticated security-based direct-trust among (x, p) nodes, and $Z = \mathbb{S}(y)$ represents that p was connected with y. Moreover, the TVS model uses weight-based method for dynamically allocating values, i.e., nodes having higher trust will have higher weights and nodes having lesser trust will have lesser weights. The $\mathbb{F}_o^u(x,y)$ in (4) is evaluated using (5). In (5), $\log\theta$ represents least-acceptable similarity parameter and $\mathbb{R}_o^u(x,y)$ represents a connection among (x,y). Using (5), $\mathbb{F}_o^u(x,p)$ is also evaluated.

$$\mathbb{F}_o^u(x,y) = \begin{cases} 1 - \frac{\log(Sec_o^u(x,y))}{\log\theta}, \; if\ \mathbb{R}_o^u(x,y) > \theta \\ 0, \; else \end{cases} \tag{5}$$

Further, the TVS model determines recent-trust using (3) and (4). In TVS model, the recent-trust is represented as $\mathbb{C}_o^u(x,y)$, which is determined using (6). In (6), δ it is a direct-trust weight variable, which is dynamically optimized based on x and y connection/interaction for u duration as defined in (7).

$$\mathbb{C}_o^u(x,y) = \delta * \mathbb{D}_o^u(x,y) + (1-\delta) * \mathbb{G}_o^u(x,y) \tag{6}$$

$$\delta = \frac{\mathbb{T}^u(x,y)}{\mathbb{T}^u(x,y) + \overline{\mathbb{T}}^u(x,y)} \tag{7}$$

In (7), $\mathbb{T}^u(x, y)$ denotes total interactions vehicle x has established with vehicle y for u time and $\vec{\mathbb{T}}^u(x, y)$ denotes average interaction-time that vehicular infrastructure p had interacted with vehicle y. The $\vec{\mathbb{T}}^u(x, y)$ is evaluated mathematically using (8). As duration u changes, the recent-trust determined changes to past-trust, which is represented as $\mathbb{Q}_o^u(x, y)$. The $\mathbb{Q}_o^u(x, y)$ is determined using (3) and (6) as presented in (9).

$$\vec{\mathbb{T}}^u(x, y) = \frac{\sum_{p \in Z-\{x\}} \mathbb{F}_o^u(x,p) * \mathbb{T}^u(p,y)}{|Z-\{x\}|} \tag{8}$$

$$\mathbb{Q}_o^u(x, y) = \frac{\varphi * \mathbb{D}_{o-1}^u(x,y) + \mathbb{C}_{o-1}^u(x,y)}{2} \tag{9}$$

In (9), $\varphi(0 \leq \varphi \leq 1)$ it is an incentive variable that automatically changes to 0, if direct-trust is $\mathbb{D}_0^0(x, y)$. From past-trust, no attacks can be induced to any of the nodes, i.e., x, y, and p. This is because, based on past trust, only the x can connect/interact with y or p. Moreover, the recent-trust changes to the past-trust only when y or p has connected/interacted with x in the TVS model, the model uses an anticipated future trust to provide better security. In the TVS model, the anticipated future trust is represented as $F_o^u(x, y)$, which is determined using (10). In (10), α it is a dynamically changing variable that can be changed according to the deviating variable. ω, i.e., the network size, but in the TVS model α has been set to 0. The ω has multiple possibilities, which are represented using (11).

$$F_o^u(x, y) = \begin{cases} 0, if\ neither\ \mathbb{Q}\ or\ \mathbb{C}\ is\ available \\ \alpha\mathbb{C}_o^u(x, y) + (1-\alpha)\mathbb{D}_o^u(x, y)\ if\ either\ \mathbb{Q}\ or\ \mathbb{C}\ is\ available \end{cases} \tag{10}$$

$$\alpha = \begin{cases} \alpha + 0.1,\ if\ \mathbb{C}_o^u(x, y) - \mathbb{L}_o^u(x, y) > \omega, \\ \alpha - 0.1,\ if\ \mathbb{C}_o^u(x, y) - \mathbb{L}_o^u(x, y) < -\omega, \\ \alpha, \quad if\ -\omega < \mathbb{C}_o^u(x, y) - \mathbb{L}_o^u(x, y) < \omega. \end{cases} \tag{11}$$

By using (11), the α can be altered using ω. Also, by making ω a vehicle can change its past established trust to the latest established trust. Moreover, it is important that. ω should not be set very less as malicious vehicles use this parameter for changing their behavior, i.e., they may change from malicious to non-malicious vehicle (i.e., can affect recent-trust and past-trust), hence leading to an attack on the vehicle x. Hence, in the TVS model ω has been set very less to reduce any kind of attacks. Further, if any attack happens in VANET, for identification and prevention, the TVS model presents a security parameter represented as $\mathcal{F}_o^u(x, y)$. This security parameter uses (9) and (10) for providing security from attacks. The $\mathcal{F}_o^u(x, y)$ it is evaluated using (12).

$$\mathcal{F}_o^u(x, y) = \mathbb{Q}_o^u(x, y) * F_o^u(x, y) \tag{12}$$

By utilizing (12), there is less change in different trust values, which thereby reduces the risk of the attack. If any attack occurs, the attacking node will have very less values through which the TVS model identifies whether an attack has occurred. Using this security model, the TVS model provides better throughput for information transmission, better attack detection and lesser attack misclassification, which has been discussed in the results and discussion section in detail. The complete working process of the proposed TVS model is given in Algorithm 1.

```
Algorithm 1. TVS method
Step 1. Start.
Step 2. Create an IOV network with a set of vehicles V and RSU R, gateway server E and malicious nodes M.
Step 3. Deploy the IoV network and start the simulation.
Step 4. The RSUs compute the different trust metrics of different vehicles.
Step 5. The vehicle communicates to the vehicle/RSUs with best trust metrics using (12) /////. Note the trust metrics >0.5 to 1 are secured.
Step 6. The communication is till all the vehicle completes their task execution.
Step 7. Stop.
```

4. RESULTS AND DISCUSSION

The evaluation of the TVS model was conducted using a standard IoV attack dataset obtained from the Canadian Institute of Cybersecurity (CIC) [26]. For consistency, the simulation parameters used in the IoV-PBFT approach [23] were adopted in this study. Moreover, to compare the performance of the TVS model with the IoV-PBFT approach, both models were implemented using the NS3-based SIMITS simulator implemented using C# [27], [28]. Various scenarios were tested by varying the attack percentages to 10, 20, 30, and 40%, providing a comprehensive analysis of the model's effectiveness under different attack conditions. The evaluations were conducted in terms of throughput, misclassification and detection rate [29], [30]. The misclassification rate results for the IoV-PBFT and TVS models under varying attack percentages (10, 20, 30, and 40%) indicate the TVS model's superior ability to minimize false classifications, as presented in Figure 3. At an attack rate of 10%, the IoV-PBFT model exhibited a 35% misclassification rate, whereas the TVS model achieved a lower rate of 28%, demonstrating its better accuracy in distinguishing between malicious and legitimate nodes. As the attack percentage increased to 20%, both models showed higher misclassification rates, with IoV-PBFT at 50% and TVS at 36%. At 30%, the IoV-PBFT model maintained its misclassification rate at 50%, while the TVS model rose slightly to 42%, yet still outperformed IoV-PBFT. At the highest attack rate of 40%, IoV-PBFT showed a 37% misclassification rate, while the TVS model achieved a significantly lower rate of 27%. The average misclassification rate analysis, i.e., 22.75% reveals that the TVS model consistently maintained lower misclassification rates across different attack intensities. This suggests that the TVS model not only provides more accurate attack detection but also minimizes false attacks, making it a more reliable approach for ensuring VANET security. The significant reduction of misclassification aids the model in significantly reducing communication overhead.

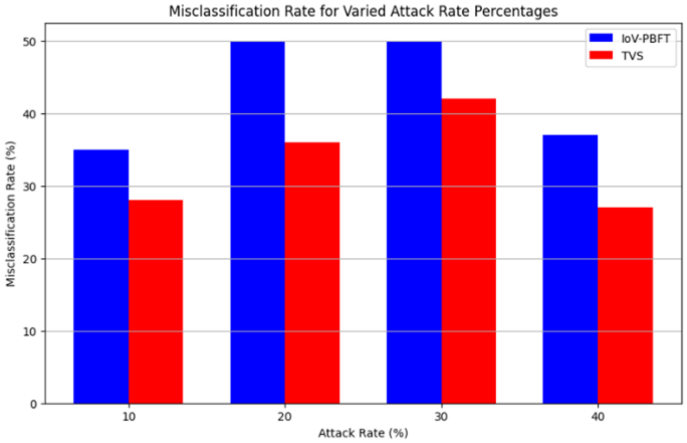

Figure 3. Misclassification rate vs varied attack rate

The detection rate results for the IoV-PBFT and TVS models across varying attack percentages (10, 20, 30, and 40%) highlight the superior performance of the TVS model in identifying malicious activities within VANETs, as presented in Figure 4. At 10% attack intensity, the IoV-PBFT model detected 65% of attacks, while the TVS model achieved a higher detection rate of 72%. As the attack rate increased to 20%, the detection rates for both models dropped, with IoV-PBFT detecting 50% of attacks and TVS detecting 64%. At 30%, the performance gap between the models began to widen, with IoV-PBFT maintaining a detection rate of 50%, whereas the TVS model dropped slightly to 58%. However, the TVS model still outperformed IoV-PBFT. At the highest attack intensity of 40%, the TVS model reached a detection rate of 73%, a notable improvement over the IoV-PBFT model's 63%. The average detection rate across the attack percentages, i.e., 14.77% indicated that the TVS model consistently outperformed the IoV-PBFT approach, with the TVS model showing higher resilience in detecting attacks under varying conditions. This demonstrates the effectiveness of the TVS model in providing robust security by accurately identifying malicious nodes, even under increasing attack intensities. The significant improvement in detection rate aids the model in significantly reducing communication delay.

The throughput results for the IoV-PBFT and TVS models across varying attack rates (10, 20, 30, and 40%) highlight the TVS model's superior performance in maintaining communication efficiency, as presented in Figure 5. At the lowest attack rate of 10%, the TVS model achieved a throughput of 0.525, which is slightly higher than IoV-PBFT's throughput of 0.481. This continued as the attack rate increased to 20%, with TVS showing a throughput of 0.3385, outperforming IoV-PBFT at 0.275. Even as the attack rate escalated to 30 and 40%, the TVS model consistently demonstrated better throughput. At 30%, TVS maintained a throughput of 0.2201, compared to 0.205 for IoV-PBFT, and at 40%, TVS achieved 0.1572, while IoV-PBFT dropped to 0.1386. The average throughput for the TVS model, i.e., 11.45% was consistently higher than the IoV-PBFT model across all attack rates, indicating that TVS effectively sustains communication performance even under attack conditions. This performance advantage suggests that the TVS model not only improves security but also ensures better network efficiency, making it a more robust solution for VANETs, particularly in environments where network traffic and security are critical concerns.

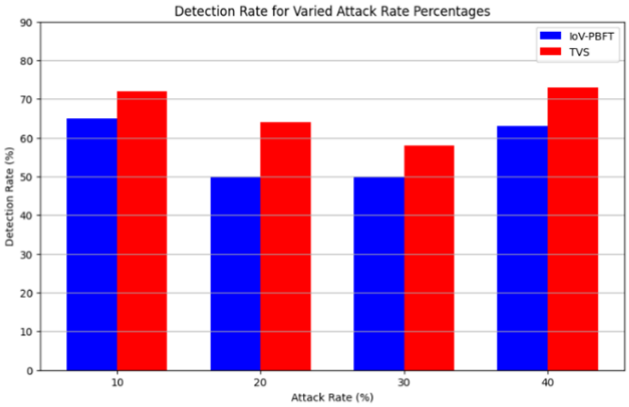

Figure 4. Detection rate vs varied attack rate

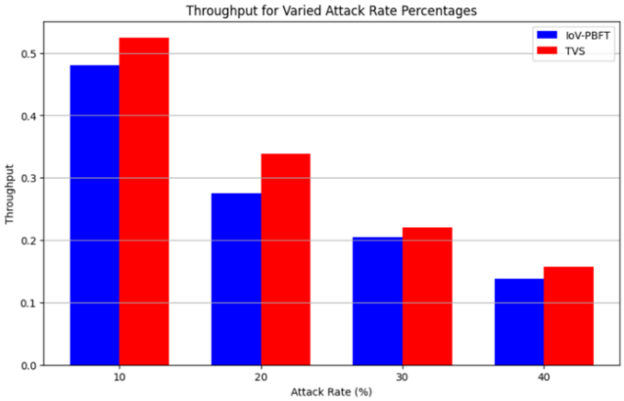

Figure 5. Throughput vs varied attack rate

5. CONCLUSION

In this work, a TVS model was proposed to enhance the security and communication efficiency of VANETs, particularly in the presence of various attacks. The introduction provided an overview of VANETs and their critical need for secure, reliable communication due to increasing security threats, highlighting the importance of trust mechanisms for attack prevention and secure data transmission. The literature survey outlined various existing approaches, including the IoV-PBFT model, and identified the need for a more effective solution that could offer better attack detection and network throughput. The methodology detailed the TVS model, which integrates direct-trust, indirect-trust, recent-trust, past-trust, and anticipated future-trust to ensure secure connections between vehicles and infrastructure nodes. By leveraging these trust levels, the TVS model enhances communication reliability and reduces the impact of malicious attacks in VANETs. The model's security approach involved advanced techniques like dynamic probability and state-changing methods to prevent attacks during information transmission. The results demonstrated that the TVS model outperformed the IoV-PBFT model in several metrics. The average misclassification rate was reduced to 22.75%, indicating better accuracy in identifying malicious nodes. The average detection rate across varying attack percentages was 14.77%, while the average throughput was 11.45%, showcasing the TVS model's ability to maintain network performance even under attack conditions. The findings showed better outcomes in comparison with the existing IoV-PBFT model. For future work, the TVS model can be expanded to consider more dynamic attack scenarios and evaluate its performance in real-world VANET environments. Additionally, enhancing the model with machine learning techniques for dynamic trust evaluation and considering the impact of mobility and large-scale networks could further improve its robustness and applicability.

ACKNOWLEDGMENTS

The authors would like to express their sincere gratitude to our advisor for his unwavering guidance, invaluable insights, and encouragement throughout the research process. We sincerely thank REVA University for granting us the opportunity to carry out this research. The encouragement and support provided by the University greatly contributed to this work.

FUNDING INFORMATION

No funding is raised for this research.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Shilpa	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	
Thiruvenkadam Prasanth	✓	✓			✓	✓		✓	✓	✓	✓	✓		

C	: **C**onceptualization	I	: **I**nvestigation	Vi	: **Vi**sualization
M	: **M**ethodology	R	: **R**esources	Su	: **Su**pervision
So	: **So**ftware	D	: **D**ata Curation	P	: **P**roject administration
Va	: **Va**lidation	O	: Writing - **O**riginal Draft	Fu	: **Fu**nding acquisition
Fo	: **Fo**rmal analysis	E	: Writing - Review & **E**diting		

CONFLICT OF INTEREST STATEMENT

The author declares no conflict of interest.

DATA AVAILABILITY

No dataset is utilized in this research.

REFERENCES

[1] A. Dutta, L. M. S. Campoverde, M. Tropea, and F. De Rango, “A comprehensive review of recent developments in VANET for traffic, safety & remote monitoring applications,” *Journal of Network and Systems Management*, vol. 32, no. 4, Oct. 2024, doi: 10.1007/s10922-024-09853-5.

[2] J. Mahmood, Z. Duan, Y. Yang, Q. Wang, J. Nebhen, and M. N. M. Bhutta, “Security in vehicular ad hoc networks: challenges and countermeasures,” *Security and Communication Networks*, vol. 2021, pp. 1–20, Jun. 2021, doi: 10.1155/2021/9997771.

[3] M. A. Naeem, S. Chaudhary, and Y. Meng, “Road to efficiency: V2V enabled intelligent transportation system,” *Electronics*, vol. 13, no. 13, Jul. 2024, doi: 10.3390/electronics13132673.

[4] M. Elassy, M. Al-Hattab, M. Takruri, and S. Badawi, “Intelligent transportation systems for sustainable smart cities,” *Transportation Engineering*, vol. 16, Jun. 2024, doi: 10.1016/j.treng.2024.100252.

[5] S. M. Hosseinian, H. Mirzahossein, and R. Guzik, “Sustainable integration of autonomous vehicles into road networks: ecological and passenger comfort considerations,” *Sustainability*, vol. 16, no. 14, Jul. 2024, doi: 10.3390/su16146239.

[6] S. Kumar and J. Singh, “Internet of vehicles over VANETs: smart and secure communication using IoT,” *Scalable Computing: Practice and Experience*, vol. 21, no. 3, pp. 425–440, Aug. 2020, doi: 10.12694/scpe.v21i3.1741.

[7] E. Abdelkreem, S. Hussein, and A. Tammam, “Feature engineering impact on position falsification attacks detection in vehicular ad-hoc network,” *International Journal of Information Security*, vol. 23, no. 3, pp. 1939–1961, 2024, doi: 10.1007/s10207-024-00830-2.

[8] S. Khan, I. Sharma, M. Aslam, M. Z. Khan, and S. Khan, “Security challenges of location privacy in VANETs and state-of-the-art solutions: a survey,” *Future Internet*, vol. 13, no. 4, Apr. 2021, doi: 10.3390/fi13040096.

[9] T. Nandy, R. Md Noor, R. Kolandaisamy, M. Y. I. Idris, and S. Bhattacharyya, “A review of security attacks and intrusion detection in the vehicular networks,” *Journal of King Saud University - Computer and Information Sciences*, vol. 36, no. 2, 2024, doi: 10.1016/j.jksuci.2024.101945.

[10] K. V. Krishna and K. G. Reddy, “Classification of distributed denial of service attacks in VANET: a survey,” *Wireless Personal Communications*, vol. 132, no. 2, pp. 933–964, Sep. 2023, doi: 10.1007/s11277-023-10643-6.

[11] A. El-Dalahmeh, M. El-Dalahmeh, M. A. Razzaque, and J. Li, “Cryptographic methods for secured communication in SDN-based VANETs: a performance analysis,” *Security and Privacy*, vol. 7, no. 6, Nov. 2024, doi: 10.1002/spy2.446.

[12] W. Ali, S. Z. Ninoria, G. Khan, and K. K. Gola, “Robust cryptographic scheme for reliable data communication in VANET (RCSRC) using clustering approach,” *EURASIP Journal on Wireless Communications and Networking*, vol. 2024, no. 1, 2024, doi: 10.1186/s13638-024-02408-x.

[13] M. N. S. Perera, T. Nakamura, M. Hashimoto, H. Yokoyama, C.-M. Cheng, and K. Sakurai, “Certificate management scheme for VANETs using blockchain structure,” *Cryptography*, vol. 6, no. 2, Apr. 2022, doi: 10.3390/cryptography6020020.

[14] M. Gayathri and C. Gomathy, “Design of CSKAS-VANET model for stable clustering and authentication scheme using RBMA and signcryption,” *Frontiers in Computer Science*, vol. 6, May 2024, doi: 10.3389/fcomp.2024.1384515.

[15] D. Denny and K. P. Kumar, “Secure authenticated communication via digital signature and clear list in VANETs,” *ECS Transactions*, vol. 107, no. 1, pp. 20065–20071, Apr. 2022, doi: 10.1149/10701.20065ecst.

[16] B. Akwirry, N. Bessis, H. Malik, and S. McHale, "A multi-tier trust-based security mechanism for vehicular ad-hoc network communications," *Sensors*, vol. 22, no. 21, Oct. 2022, doi: 10.3390/s22218285.

[17] A. Hbaieb, S. Ayed, and L. Chaari, "A survey of trust management in the internet of vehicles," *Computer Networks*, vol. 203, Feb. 2022, doi: 10.1016/j.comnet.2021.108558.

[18] A. Rehman *et al.*, "CTMF: context-aware trust management framework for internet of vehicles," *IEEE Access*, vol. 10, pp. 73685–73701, 2022, doi: 10.1109/ACCESS.2022.3189349.

[19] H. Amari, Z. A. El Houda, L. Khoukhi, and L. H. Belguith, "Trust management in vehicular ad-hoc networks: extensive survey," *IEEE Access*, vol. 11, pp. 47659–47680, 2023, doi: 10.1109/ACCESS.2023.3268991.

[20] I. U. Din, K. A. Awan, and A. Almogren, "Secure and privacy-preserving trust management system for trustworthy communications in intelligent transportation systems," *IEEE Access*, vol. 11, pp. 65407–65417, 2023, doi: 10.1109/ACCESS.2023.3290911.

[21] A. Malik, M. Z. Khan, S. M. Qaisar, M. Faisal, and G. Mehmood, "An efficient approach for the detection and prevention of gray-hole attacks in VANETs," *IEEE Access*, vol. 11, pp. 46691–46706, 2023, doi: 10.1109/ACCESS.2023.3274650.

[22] Q. Xie, Z. Sun, Q. Xie, and Z. Ding, "A cross-trusted authority authentication protocol for internet of vehicles based on blockchain," *IEEE Access*, vol. 11, pp. 97840–97851, 2023, doi: 10.1109/ACCESS.2023.3308601.

[23] Z. Ma *et al.*, "A blockchain-based secure distributed authentication scheme for internet of vehicles," *IEEE Access*, vol. 12, pp. 81471–81482, 2024, doi: 10.1109/ACCESS.2024.3409361.

[24] H. Han, M. Zhang, Z. Xu, X. Dong, and Z. Wang, "Decentralized trust management and incentive mechanisms for secure information sharing in VANET," *IEEE Access*, vol. 12, pp. 124414–124427, 2024, doi: 10.1109/ACCESS.2024.3453368.

[25] A. Bibi *et al.*, "TR-block: a trustable content delivery approach in VANET through blockchain," *IEEE Access*, vol. 12, pp. 60863–60875, 2024, doi: 10.1109/ACCESS.2024.3386461.

[26] E. C. P. Neto, H. Taslimasa, S. Dadkhah, S. Iqbal, P. Xiong, T. Rahmanb, and A. A. Ghorbani, "CIC IoV dataset 2024," *Canadian Institute for Cybersecurity*. [Online]. Available: https://www.unb.ca/cic/datasets/iov-dataset-2024.html

[27] N. Ababneh and J. N. Al-Karaki, "On the lifetime analytics of iot networks," in *2020 International Conference on Communication and Signal Processing (ICCSP)*, Chennai, India: IEEE, Jul. 2020, pp. 1086–1090. doi: 10.1109/ICCSP48568.2020.9182272.

[28] N. Gadde, B. Jakkali, R. B. H. Siddamallaih, and G. Gowrishankar, "Quality of experience aware network selection model for service provisioning in heterogeneous network," *International Journal of Electrical and Computer Engineering*, vol. 12, no. 2, pp. 1839–1848, Apr. 2022, doi: 10.11591/ijece.v12i2.pp1839-1848.

[29] K. N. Tripathi, S. C. Sharma, and A. M. Yadav, "Analysis of various trust based security algoithm for the vehicular ad-hoc network," in *2018 International Conference on Recent Innovations in Electrical, Electronics & Communication Engineering (ICRIEECE)*, Bhubaneswar, India: IEEE, Jul. 2018, pp. 1546–1551, doi: 10.1109/ICRIEECE44171.2018.9009288.

[30] C. Scott, M. S. Khan, B. Bajracharya, and A. Paraniothi, "Trust-based security for decentralized clustering in IoV," in *2024 International Conference on Smart Applications, Communications and Networking (SmartNets)*, Harrisonburg, USA: IEEE, May 2024, pp. 1–4, doi: 10.1109/SmartNets61466.2024.10577675.

BIOGRAPHIES OF AUTHORS

Shilpa received B.E. in Computer Science and Engineering in 2006 and M.Tech. in Computer Science and Engineering in 2019, both from Visvesvaraya Technological University, Belgaum, Karnataka. She has been working as senior scale lecturer at Government Polytechnic Immadihalli, Bangalore, Karnataka, since 2010, and a research scholar at the School of Computer Science and Engineering, REVA University, Bangalore since 2022. With an industry background, she has worked from 2006 to 2010 on telecom domain-based projects, including fraud detection and prevention at Torry Harris business solutions and a mastercard project at INTEC Billing Solutions. Her research interests focus on autonomous vehicles and data security, exploring advanced solutions to improve safety and data privacy. She can be contacted at email: shilpasadlapur@rediffmail.com.

Dr. Thiruvenkadam Prasanth is received the Ph.D. degree in the Department of Information and Communication Engineering from the Anna University, Chennai, India in 2020 and he also received the M.Tech. degree in the Department of Information Technology from the SRM University, Chennai, India in 2011. Currently, he is working as an associate professor in the Department of Computer Science and Engineering at Reva University, Bangalore. His research interest includes big data analytics, machine learning, and social network analysis. He has published many papers in the area of big data analytics, machine learning, and data science. He can be contacted at email: dr.tprasanth@gmail.com.