VANETGuard: A Scalable Lightweight Trust Management System for 5G-Enabled Smart Vehicular Networks

Reem Almaziad and Heba Kurdi *

Posted Date: 25 February 2026

doi: 10.20944/preprints202505.0242.v2

Keywords: VANETs; urban mobility; trust management; entropy-based detection; Bayesian inference; Distributed Ledger Technology; IOTA Tangle; vehicular security; intelligent transportation systems

 doi:10.20944/preprints202505.0242.v2

Article

VANETGuard: A Scalable Lightweight Trust Management System for 5G-Enabled Smart Vehicular Networks

Reem Almaziad [1] and Heba Kurdi [2,3,*]

[1] Cybersecurity, College of Computer and Information Sciences, King Saud University, Riyadh 11451, Saudi Arabia

[2] Computer Science Department, College of Computer and Information Sciences, King Saud University, Riyadh 11451, Saudi Arabia

[3] Mechanical Engineering Department, Massachusetts Institute of Technology; Cambridge, MA 02139, USA

* Correspondence: hkurdi@ksu.edu.sa

Abstract

Vehicular Ad Hoc Networks (VANETs) are essential to intelligent transportation systems (ITS), enabling secure, real-time communication among vehicles and infrastructure. However, their decentralized and dynamic nature makes them vulnerable to threats such as Sybil attacks, message forgery, replay attacks, and Denial-of-Service (DoS). This paper presents VANETGuard, a lightweight scalable trust management system that enhances security and scalability in 5G-enabled smart vehicular networks. The proposed system integrates entropy-based anomaly detection, Bayesian inference for adaptive trust scoring, and a lightweight distributed ledger for decentralized, tamper-resistant trust storage. Large-scale simulations under realistic traffic and attack conditions demonstrate that VANETGuard achieves 99.97% detection accuracy, significantly reduces false positives, and maintains low latency and computational overhead while supporting over 300 vehicles. These results highlight VANETGuard's potential to enable secure, efficient, and scalable trust mechanisms in next-generation ITS and urban mobility systems.

Keywords: VANETs; urban mobility; trust management; entropy-based detection; Bayesian inference; Distributed Ledger Technology; IOTA Tangle; vehicular security; intelligent transportation systems

1. Introduction

Vehicular Ad Hoc Networks (VANETs) are a foundational element of Intelligent Transportation Systems (ITS), enabling seamless Vehicle-to-Everything (V2X) communication to improve road safety, traffic efficiency, and overall driving experience [1–3]. However, their decentralized design and high mobility expose VANETs to numerous cyber threats, including Denial-of-Service (DoS) attacks, Sybil attacks, and message forgery [4–7], which can undermine data integrity and compromise traffic safety [2,4].

In response to these challenges, a variety of trust management frameworks have been proposed, including Reputation-Based [1,8–14], Entropy-Based [2,15–18], Bayesian Inference-Based [19–22], and Blockchain-Based solutions [6,14,23–28]. Each offers unique strengths but also critical limitations. Reputation models assess long-term behavioral consistency but often lack adaptability in dynamic environments [12]. Entropy-based systems detect anomalies through message pattern deviations but tend to yield high false positive rates [18]. Bayesian inference introduces adaptive, probabilistic reasoning for trust evaluation, enhancing resilience to misinformation and Sybil attacks [22]. Blockchain-based methods ensure tamper-resistant trust storage but suffer from high latency and computational overhead, limiting their suitability for time-sensitive vehicular applications [25,28].

 doi:10.20944/preprints202505.0242.v2

To overcome these shortcomings, we introduce VANETGuard, a lightweight Hybrid Trust Management System (HTMS) designed for the dynamic and latency-sensitive nature of 5G-enabled vehicular networks. The system combines four complementary components, each selected for its unique strengths: reputation-based assessment captures long-term behavioral consistency, providing a historical foundation for trust decisions; entropy-based anomaly detection rapidly identifies short-term irregularities in message patterns, improving early threat detection; Bayesian inference enables adaptive, probabilistic trust evaluation under uncertainty, enhancing resilience against evolving attack strategies; and a lightweight distributed ledger ensures decentralized, tamper-resistant trust storage with minimal computational overhead (implemented using the IOTA Tangle). These components are integrated within an edge computing framework to reduce communication latency and optimize real-time responsiveness. Together, this architecture delivers a scalable, secure, and efficient solution tailored to the demands of next-generation vehicular networks.

The proposed system is evaluated through extensive simulations under diverse vehicular conditions and realistic attack scenarios, including Sybil, DoS, DDoS, replay, and forgery attacks. These are modeled using both protocol-level and network-level adversary frameworks to assess system robustness. A custom dataset is developed to replicate real-world driving conditions in low-visibility highway environments, incorporating standard vehicular message formats and simulated hazard responses. The evaluation varies parameters such as vehicle density (20–400 vehicles), message transmission rates (1–10 Hz), speeds (30–90 km/h), and network delays (5–50 ms) to test system scalability and responsiveness. Key detection thresholds and reputation weightings are tuned to balance accuracy and responsiveness. System performance is assessed using metrics including detection accuracy, false positive rate, latency, and computational scalability. Results confirm that the proposed trust management system effectively detects malicious behavior while maintaining real-time responsiveness under dynamic and adversarial conditions.

The primary contributions of this paper include:

- A novel hybrid trust management architecture tailored for VANETs' dynamic conditions,
- Lightweight and decentralized trust storage using the IOTA Tangle,
- Adaptive trust evaluation using probabilistic and anomaly-based methods,
- Large-scale simulations evaluating detection accuracy, latency, and system scalability.

The remainder of this paper is organized as follows: Section 2 reviews related work; Section 3 details the proposed system design; Section 4 outlines the evaluation methodology; Section 5 presents experimental results and performance analysis; and Section 6 discusses future research directions and concluding remarks.

2. Literature Review

Effective trust management is essential for ensuring secure and reliable communication in VANETs, particularly given their decentralized, dynamic, and high-mobility nature. Over the past decade, a variety of trust management frameworks have been developed to detect malicious behavior and enhance vehicular communication security. These frameworks typically fall into five major categories: Reputation-Based, Entropy-Based, Bayesian Inference-Based, Blockchain-Based and Hybrid trust management systems. This section reviews key contributions in each of these categories, highlighting their strengths and limitations. The section concludes with a discussion of existing research gaps and the motivation for the proposed hybrid trust management framework.

2.1. Reputation-Based Trust Management Systems

Reputation-based models evaluate the trustworthiness of nodes by leveraging both direct and indirect feedback mechanisms. Raya et al. [1] introduced one of the earliest reputation systems, although it lacked capabilities for addressing Sybil and jamming attacks. Dahiya et al. [2] enhanced reputation-based trust management using NS-3 simulations, achieving a low error rate, yet their approach did not adequately handle high-mobility scenarios. Zhang et al. [3] incorporated machine

 doi:10.20944/preprints202505.0242.v2

learning into reputation systems, leading to improved detection accuracy but at the cost of increased computational complexity. Kumar et al. [4] emphasized secure data dissemination but encountered limitations in scalability. Mahmood et al. [5] proposed a distributed reputation model; however, latency in real-time scenarios remained problematic. Sheikh et al. [6] leveraged blockchain to enhance reputation integrity, mitigating tampering risks but introducing significant computational overhead. Feraudo et al. [7] presented the DIVA system, which integrates Decentralized Identifiers (DIDs) with the IOTA Tangle to provide secure and scalable V2V communication. Despite these advancements, reputation-based models continue to face challenges related to computational efficiency and adaptability in real-time threat environments.

2.2. Entropy-Based Trust Management System

Entropy-based models detect trust anomalies by analyzing variations in network traffic behavior. Mejri and Ben-Othman [8] proposed the Packets Entropy method, which detects Denial-of-Service (DoS) attacks via IEEE 802.11p MAC layer manipulation. Ahmed and Tepe [9] developed a dynamic trust model that adjusts trust scores based on message dissemination patterns. Kumar and Mann [10] designed an entropy-based framework for mitigating DoS attacks, demonstrating high detection accuracy with minimal latency. Yin and Li [11] introduced an entropy-weighted trust model for real-time assessment. Nonetheless, entropy-based approaches often struggle with identifying long-term behavioral trends and are prone to high false positive rates.

2.3. Bayesian Inference-Based Trust Management Systems

Bayesian inference models manage uncertainty by employing probabilistic reasoning for trust assessment. Zhang et al. [12] proposed a TrustRank-based Bayesian framework that computes local and global trust values, incorporating social factors such as vehicle type and driver behavior. He et al. [17] introduced a Bayesian trust scheme tailored for cognitive radio-based VANETs, demonstrating effectiveness in identifying spectrum-based attackers. Fang et al. [18] utilized Bayesian networks to mitigate on-off attack strategies. Li et al. [19] combined Bayesian inference with game theory to enable secure content dissemination. Talal et al. [20] designed a decentralized Bayesian model that assigns low initial trust scores to discourage dishonest behavior. While Bayesian models offer robust uncertainty management, they require further optimization to scale efficiently in large, dynamic VANET environments.

2.4. Blockchain-Based Trust Management Systems

Blockchain-based trust management systems offer enhanced security and transparency by leveraging decentralized ledgers. Ahmed et al. [21] proposed a privacy-preserving authentication and trust model using blockchain infrastructure. Yang et al. [22] designed a blockchain-based reputation mechanism to evaluate message credibility. Lu et al. [23] developed BARS (Blockchain-based Anonymous Reputation System) to ensure certificate integrity. Zhao et al. [24] integrated machine learning techniques into blockchain-based trust management to improve malicious vehicle detection. Zhang et al. [25] employed deep learning alongside blockchain to classify untrustworthy vehicles. Kudva et al. [26] introduced a decentralized framework capable of blacklisting insider attackers. Liu et al. [27] incorporated Hidden Markov Models (HMMs) into blockchain-based systems to enhance detection of malicious behavior. Alhatrhi et al. [28] developed a biometric blockchain framework that achieved a 99.98% accuracy rate in trust classification, outperforming existing models. Although blockchain provides strong guarantees of security and privacy, its scalability and computational demands limit its practicality for real-time VANET applications.

2.5. Hybrid Trust Management Systems

Hybrid models integrate multiple trust evaluation mechanisms to enhance overall security performance. Zhang et al. [12] introduced AATMS, a system that combines Bayesian inference with

 doi:10.20944/preprints202505.0242.v2

TrustRank, although scalability remained a limitation. Xiang and Chen [13] proposed HTMS-V, which utilizes subjective logic to evaluate both direct and indirect trust. Liu et al. [14] developed HDRS, a model that dynamically adjusts reputation scores to counter collusion-based attacks. Mahmood et al. [15] combined long-term reputation data with real-time evaluations to improve scalability, though throughput analysis was insufficiently addressed. Mehra and Patidar [16] presented ART, an attack-resistant framework designed to withstand Sybil and false message injection attacks; however, it lacked validation under large-scale deployment conditions.

2.6. Research Gap and Motivation

Despite extensive research into trust management frameworks for VANETs, existing models often suffer from critical limitations in either scalability, computational efficiency, or adaptability to real-time, dynamic environments. Reputation-based systems lack resilience under high mobility; entropy-based models frequently produce false positives; Bayesian models require computational optimization; and blockchain approaches struggle with latency and scalability. While hybrid systems have attempted to combine strengths across methods, most lack decentralized, lightweight trust storage mechanisms and efficient real-time evaluation strategies. This highlights a clear need for a unified, scalable, and low-latency trust management system that leverages the complementary strengths of existing techniques. Addressing this gap, the proposed VANETGuard framework integrates Bayesian inference, entropy-based anomaly detection, and decentralized storage via the IOTA Tangle, augmented by edge computing, to deliver robust, efficient, and scalable trust management for next-generation VANETs.

3. System Design

This section presents the design and implementation of the proposed hybrid trust management system for VANETs. The system integrates Entropy-based anomaly detection, Bayesian inference-based reputation updating, and Distributed Ledger Technology (DLT) to ensure secure Vehicle-to-Everything (V2X) communication. The implementation is structured to detect malicious activities, dynamically update trust scores, and securely store reputation data in a decentralized and tamper-proof manner.

The proposed trust management architecture consists of six key components, as illustrated in Figure 1. These components interact to enable secure Vehicle-to-Everything (V2X) communication, protect against cyber threats, and ensure trust propagation in a decentralized manner.

- Edge Nodes: Act as local computing units that collect vehicle messages, authenticate them, and calculate reputation scores. These nodes use entropy-based anomaly detection and Bayesian inference to detect suspicious activity. If anomalies are found, Edge Nodes update the DLT node.
- Road-Side Units (RSUs): Positioned along the roads to relay messages, extend communication range, and validate the consistency of vehicle-reported information. RSUs collect environmental and traffic data to assist in message verification.
- Trusted Authority (TA): A centralized entity that manages vehicle identities. It assigns Decentralized Identifiers (DIDs), authenticates vehicles, and conducts periodic audits to ensure trust and compliance.
- Entropy System: Detects irregular message transmission patterns by monitoring message frequency and coherence. A high entropy value indicates potential attacks, such as DoS, Sybil, or replay attacks.
- Reputation System: Uses Bayesian inference to dynamically update vehicle reputation scores based on historical trust data and current behavior.
- DLT Node: Stores trust scores securely in the IOTA Tangle, ensuring tamper-proof and decentralized record-keeping. It prevents data manipulation and ensures secure retrieval of trust scores.

 doi:10.20944/preprints202505.0242.v2

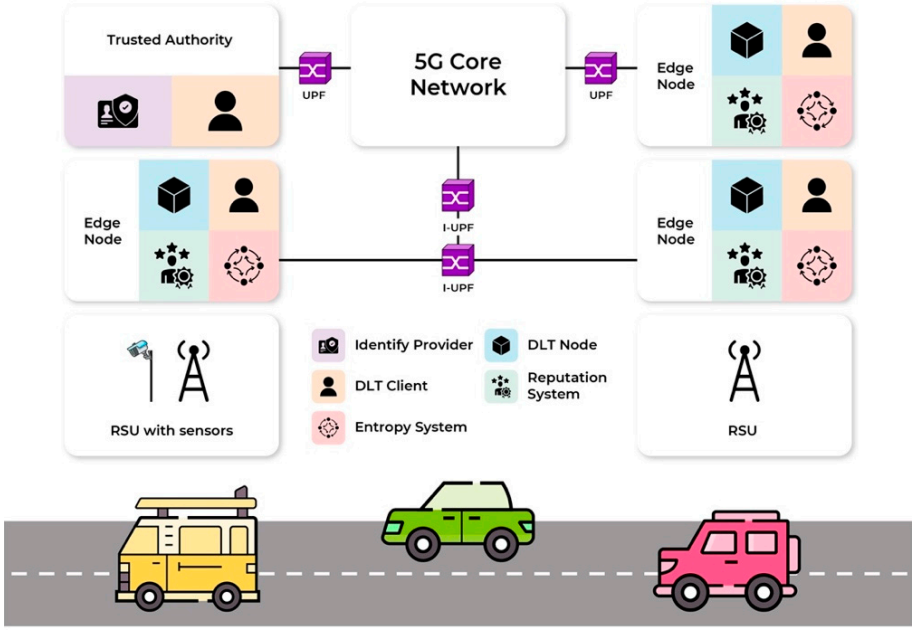

Figure 1. System overview.

The interaction between subsystems is critical for ensuring trust propagation and real-time anomaly detection. The key interactions are:

- Message Exchange: Vehicles periodically transmit Cooperative Awareness Messages (CAMs) and Decentralized Environmental Notification Messages (DENMs), which RSUs and Edge Nodes intercept for validation.
- Integrity Verification: Upon receiving a message, an Edge Node verifies its authenticity using the vehicle's Decentralized Identifier (DID) issued by the Trusted Authority (TA).
- Reputation Evaluation: Messages are compared against RSU-collected sensor data to ensure accuracy and consistency.
- Anomaly Detection (Entropy-Based): The Entropy System analyzes message timing fluctuations. If entropy is above a threshold, the vehicle is flagged as suspicious.
- Trust Score Update (Bayesian Reputation System): Bayesian inference updates reputation scores dynamically, incorporating:
  - Historical interactions (long-term trust)
  - Real-time message consistency (short-term trust)
  - Entropy-based anomaly detection (behavior deviation)
- Tamper-Proof Storage on DLT: Updated trust scores are securely stored on the IOTA Tangle, ensuring decentralized reputation management.
- Reputation Query: Vehicles can request reputation scores from Edge Nodes, which fetch the latest verified scores from the DLT Node.

The hybrid trust management model integrates entropy-based anomaly detection with Bayesian inference for reputation updates. The trust score calculation follows these steps:

- Step 1: Initialize Parameters
  In this step, the algorithm defines essential parameters influencing its sensitivity to varying vehicle behaviours. The parameters include:
  - alfa (α): A weight assigned to the vehicle's previous reputation, representing its historical behaviour.

 doi:10.20944/preprints202505.0242.v2

- beta (β): A weight that measures the impact of the current message's consistency on the updated reputation score.
- gamma (γ): A weight that considers detected anomalies, particularly variations indicated by high entropy values.
- behaviour_variation_threshold: A predefined cut-off value used to distinguish between normal and abnormal vehicle behaviour based on entropy calculations.

- Step 2: Load Dataset
  The dataset containing information about vehicle messages is imported for subsequent analysis. This dataset includes critical fields such as vehicle identification numbers, message reception times, and geographic locations. It serves as the primary source of information for detecting behavioural anomalies.
- Step 3: Calculate Message Coherencies
  For each vehicle, the algorithm examines the time intervals between consecutive messages. The goal is to determine whether these intervals fall within an expected range. Time intervals that deviate significantly from this range are marked as inconsistent, which may signal an abnormality or potential attack. The coherency calculation assigns a binary value: 1 for consistent intervals and 0 for inconsistent intervals.
- Step 4: Calculate Entropy
  Using the message coherency values, the algorithm calculates Shannon entropy to quantify the degree of randomness or unpredictability in message timing. Higher entropy values indicate greater variability and suggest the possibility of irregular or suspicious vehicle behaviour.
- Step 5: Check for High Entropy
  The calculated entropy is compared against a predefined threshold. If the entropy exceeds this behaviour variation threshold, the vehicle is flagged for exhibiting abnormal behaviour. This flagging is represented by setting a variable, flag_dos, to True.
- Step 6: Calculate Evidence Probability
  At this stage, the algorithm updates the probability counts for good and bad behaviour based on observed evidence. Specifically:
  - If the entropy is high or message coherencies fail, the probability count for bad behaviour (P_bad) is incremented, indicating accumulating evidence of suspicious activity.
  - Conversely, if the messages are consistent and entropy is low, the probability count for good behaviour (P_good) increases, signalling evidence of normal operation.
- Step 7: Update Reputation Using Bayesian Formula

$$\left(r_{\{DID\}}\right)_t = \alpha \cdot \left(r_{\{DID\}}\right)_{\{t-1\}} + \beta \cdot \left(\left(r_{\{DID\}}\right)_{\{t-1\}} + repScore\right) + \gamma \cdot entropyScore \quad (1)$$

The algorithm employs a Bayesian updating approach to adjust each vehicle's reputation score. This method integrates three components:

- Historical reputation: The vehicle's previous reputation score $\left(r_{\{DID\}}\right)_{\{t-1\}}$.
- Current message integrity: The quality and consistency of the current message based on coherency checks $repScore$.
- Detected anomalies: Any inconsistencies or randomness detected in message timing (represented by the entropy score) $entropyScore$.

The Bayesian formula thus ensures a balanced assessment by incorporating past behavior, current evidence, and potential irregularities. This approach mitigates the risk of harsh penalties for minor anomalies, allowing for a more nuanced evaluation of vehicle trustworthiness. The flowchart of the algorithm is shown in Figure 2.

 doi:10.20944/preprints202505.0242.v2

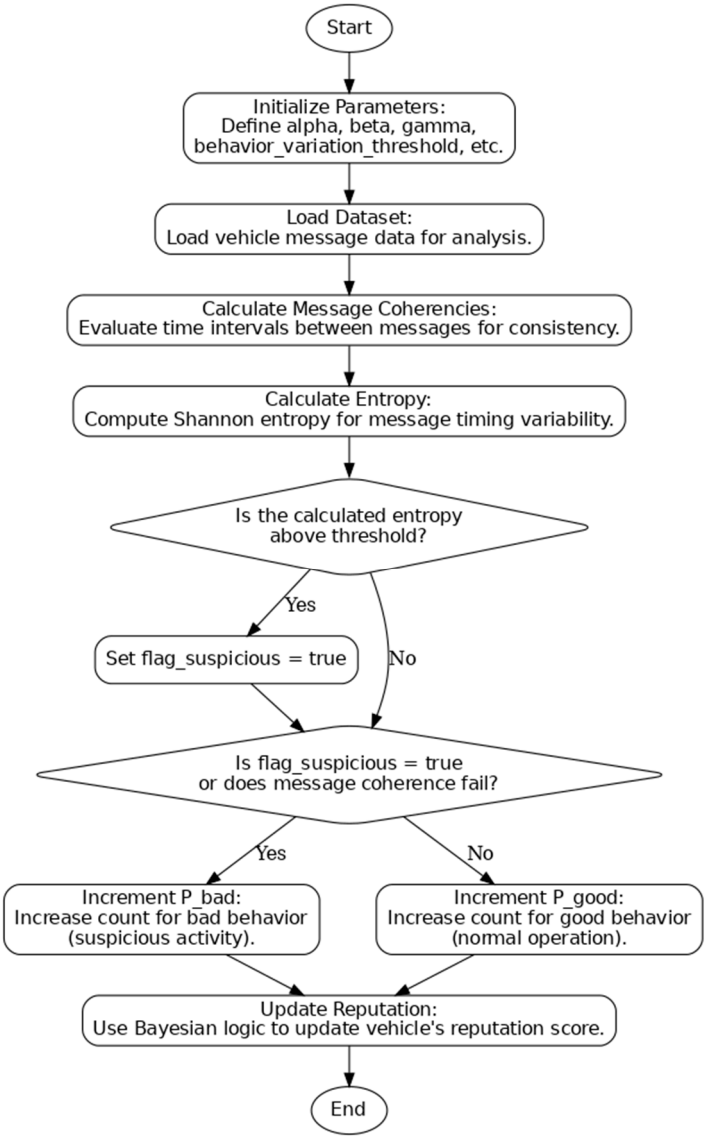

Figure 2. Flowchart of Entropy-Bayesian based Reputation Calculation Algorithm.

4. Evaluation Methodology

This section outlines the evaluation methodology of our VANETGuard. This setup ensures secure V2X communication by continuously monitoring vehicle behavior using an Entropy-Bayesian Reputation System. Reputation scores dynamically update based on message consistency and entropy analysis, while DLT enhances security by mitigating Sybil, DoS, and DDoS attacks through anomaly detection and authentication mechanisms. The proposed model ensures scalability and resilience for VANETs.

4.1. Adversarial Models

This system aims to improve the safety and efficiency of vehicular communication by meeting a comprehensive set of established requirements. The security of vehicular communication networks depends heavily on the system's ability to withstand potential threats. We apply two key adversarial models to evaluate system resilience:

1. Dolev–Yao Model: This model provides a comprehensive framework for assessing how the system handles various attacks. It assumes that an attacker can intercept any message in the network, initiate communication with any participant, and even impersonate legitimate recipients. The following attacks are considered:

 doi:10.20944/preprints202505.0242.v2

- Eavesdropping Attack: An attacker gains unauthorised access to sensitive data, such as vehicle locations, personal information, or messages between vehicles and Road Side Units (RSUs), compromising communication confidentiality.
- Replay Attack: The attacker intercepts and retransmits previously recorded messages to deceive vehicles, disrupting traffic management, collision prevention, and cooperative driving systems.
- Forgery Attack: The attacker impersonates legitimate users or entities to forge messages, misleading other vehicles and potentially causing unsafe or unintended outcomes.
- Sybil Attack: The attacker creates multiple fake identities or vehicles to deceive network participants, disrupting routing protocols, manipulating traffic flow, and spreading false information [29].

2. Network Adversary Model: This model comprehensively analyses network traffic behaviour under real-world attack scenarios, such as DoS and DDoS, at the network level. It effectively simulates how the system handles high traffic loads and evaluates the resilience of the network infrastructure under stress. Key aspects include:
   - DoS Attack: The attacker overwhelms the network or specific nodes with excessive requests or messages, leading to resource exhaustion and reduced availability of communication services.
   - DDoS Attack: A more severe version where multiple sources coordinate to send high volumes of traffic to a target, exhausting bandwidth and processing power and crippling communication [30].

4.2. Simulation Setup and Dataset

The methodology adopted in this project was inspired by established approaches detailed in the literature review. Recent studies have validated the effectiveness of these techniques in meeting security requirements and resisting attacks. Using this simulation environment allowed for realistic and precise scenario modelling. Incorporating Entropy-Based algorithms alongside Bayesian inference enabled advanced anomaly detection and fair reputation scoring for vehicles. Together, these methods provided a thorough evaluation of the system's ability to detect and mitigate various attack models, ensuring strong performance and robust security against potential threats. The primary research question we sought to address in this study was: How effective (in terms of) performance metrics is a trust management system using Entropy-Based anomaly detection and Bayesian reputation updates in enhancing vehicular communication security against various attack vectors such as DoS, DDoS, forgery, Sybil, and replay attacks.

The hardware setup for this study consists of a MacBook Pro, which serves as the primary machine for simulations and analysis. It operates on macOS and is equipped with 512 GB of storage, 16 GB of RAM, and a processor speed of 3.5 GHz. This combination of hardware ensures efficient data processing, supporting high-performance vehicular network simulations while maintaining computational accuracy and security. The system's capability enables real-time simulation execution, data collection, and analysis, which are essential for evaluating the proposed hybrid trust management system in VANETs. .In addition to the hardware configuration, the study employs several specialized software tools designed for vehicular network simulation and analysis. The Veins Framework (Version 5.1) is used within OMNeT++, allowing the simulation of vehicular communications while integrating SUMO for realistic traffic modeling. The Artery Tool, an extension of Veins, is utilized to implement the ETSI ITS-G5 protocol stack, enabling Vehicle-to-Everything (V2X) communication. Furthermore, SUMO (Version 1.8.0) facilitates the creation of realistic road traffic scenarios that reflect real-world vehicular interactions. To ensure secure and decentralized reputation management, the study incorporates IOTA Distributed Ledger Technology (DLT), which securely stores vehicle reputation scores and prevents unauthorized modifications. The simulation framework is built on OMNeT++ (Version 5.6.2), a widely used network simulation platform that allows for extensive VANET modeling and evaluation. Additionally, Python (Version 3.9) is

 doi:10.20944/preprints202505.0242.v2

employed for scripting, data preprocessing, and analytical modeling, while Simu5G, a specialized simulation library, is integrated to model network behavior and 5G-based vehicular communication. The combination of these hardware and software tools provides a robust, scalable, and high-fidelity test environment, ensuring accurate validation of the proposed VANET trust management system.

Certain parameters remain fixed throughout the simulation to ensure consistency and fair comparisons. The entropy threshold is set to 0.5, which serves as a criterion to differentiate between normal and abnormal vehicle behavior while minimizing false alarms. The reputation weights are defined as (α, β, γ) = (0.4, 0.4, 0.2), where α (alfa) represents the weight assigned to historical behavior, β (beta) accounts for current message consistency, and γ (gamma) considers anomalies detected through entropy-based analysis. These values ensure that the system does not excessively penalize minor variations in vehicle behavior. Additionally, the message coherency time threshold is fixed at 1000 milliseconds (1 second), ensuring that messages are spaced out at reasonable intervals; messages sent too frequently or too infrequently could indicate irregular activity. To enhance the reliability of trust evaluation, the time window for CAM analysis is set to 5 seconds, meaning that only recent messages are used to update a vehicle's reputation score, preventing outdated data from influencing trust calculations.

These variables are adjusted across different scenarios to examine their impact on the system's effectiveness. The number of vehicles is varied between 20 to 400 analyze the system's scalability and performance under different traffic conditions. Different attack scenarios, including Denial-of-Service (DoS), Distributed Denial-of-Service (DDoS), Sybil, Replay, and Forgery attacks, are simulated to evaluate the system's robustness against diverse threats. The message transmission rate is tested at 1 Hz, 5 Hz, and 10 Hz to assess how frequently vehicles exchange information and its impact on entropy calculations. The system is also tested under different vehicle speeds (30 km/h, 60 km/h, and 90 km/h) to analyze message timing and coherency across urban, highway, and mixed driving conditions. Lastly, network delay is varied at 5 ms, 10 ms, and 50 ms to simulate different levels of network congestion and examine its influence on message propagation and anomaly detection.

The effectiveness of the trust management system is assessed using several performance metrics, which serve as dependent variables. These metrics help evaluate the system's capability to accurately detect malicious activities, minimize false alarms, and ensure scalability in real-world VANET environments. By analyzing these performance metrics across various simulation scenarios, the study provides a comprehensive evaluation of the proposed trust management system, ensuring its reliability, adaptability, and efficiency in mitigating security threats in VANET environments.

4.3. V2V Communications Dataset

After reviewing the available datasets and analysing their strengths and limitations, we developed a custom dataset to effectively evaluate our approach for detecting malicious messages. This dataset comprises ETSI-compliant messages exchanged during simulated road hazard scenarios. Following a methodology similar to that described in [29], we modelled dynamic VANET scenarios using the Artery tool [31] to illustrate a Decentralised Environmental Notification (DEN) use case. This approach allowed us to create realistic, scenario-based data that reflects the complexity of VANET communications under hazardous conditions. By simulating a variety of interactions and message exchanges, our dataset serves as a robust foundation for testing the system's ability to identify and respond to malicious behaviour, particularly in high-risk or emergency settings.

The scenario chosen simulated a low-visibility zone on the Jeddah-Makkah Highway as shown in Figure 3., known for instances of reduced visibility due to dust or fog, which can lead to sudden vehicle deceleration. This setting was the focal point, replicating situations where sudden incidents, such as emergency stops, increase the risk of collisions and trigger the broadcasting of Decentralised Environmental Notification Messages (DENMs). These DENMs provide critical information such as detection time, cause code, and event location. These messages are essential for identifying malicious behaviour. In addition, Cooperative Awareness Messages (CAMs) generated within the target area were collected to validate the accuracy of the DENMs in the DIVA [18] system by detecting

 doi:10.20944/preprints202505.0242.v2

inconsistencies in detection times and vehicle positions. To broaden the dataset's utility for testing purposes, we modified it to simulate various attacks, including DoS, DdoS, forgery, Sybil, and replay attacks [18].

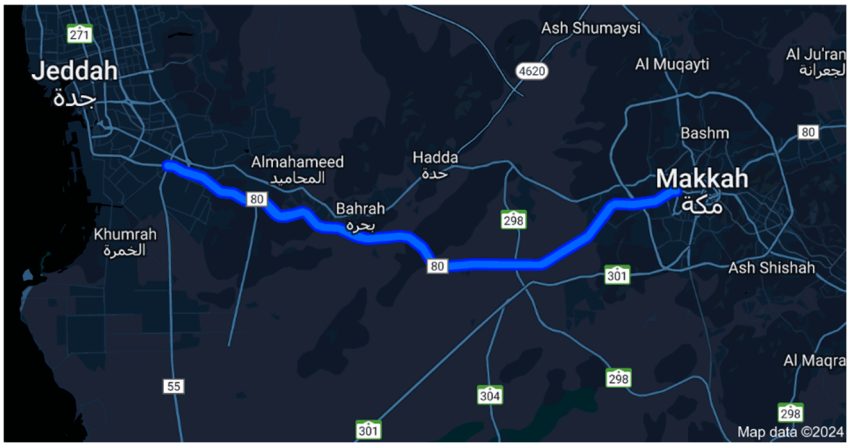

Figure 3. Simulated Highway.

5. Results & Discussions

The evaluation of the Entropy-Bayesian Trust Model involves analyzing the impact of three thresholding techniques: mode, median, and mean on system performance. These thresholding methods play a crucial role in adjusting the system's sensitivity to anomalous behaviors by dynamically balancing detection rates and reducing false classifications. The system was configured with parameter weights set at $\alpha = 0.4$, $\beta = 0.4$, and $\gamma = 0.2$, alongside a behavior variation threshold of 0.5. The results, presented in Table 1, highlight the effectiveness of each thresholding approach in terms of True Positive Rate (TPR), True Negative Rate (TNR), False Positive Rate (FPR), and False Negative Rate (FNR).

Mode-based thresholding achieved the highest TPR of 99.9%, indicating superior effectiveness in identifying malicious messages. However, this approach resulted in a lower TTNR of 79.80%, meaning that while it detected threats efficiently, it also had a higher tendency to misclassify benign messages as malicious, as reflected in the FPR of 20.20%. Median-based thresholding followed a similar trend, with a TPR of 99.95% and a slightly lower TNR of 79.60%, leading to an increased FPR of 20.40%. These results suggest that while mode and median thresholding methods exhibit strong detection capabilities, they introduce a higher likelihood of false alarms, potentially impacting network stability.

In contrast, mean-based thresholding demonstrated a more balanced approach, achieving the highest TNR of 100%. This indicates that the system accurately classified all non-malicious messages while maintaining a TPR of 99.91%. Additionally, mean thresholding resulted in the lowest FPR of 0%, ensuring minimal misclassification of benign nodes. However, the FNR was slightly higher at 0.2%, reflecting a minor trade-off in correctly identifying all malicious activities.

These findings illustrate that threshold selection significantly impacts detection performance. While mode-based thresholding prioritizes high TPR, it comes at the expense of an increased FPR. Conversely, mean-based thresholding ensures a lower misclassification rate and a perfect TNR, making it the optimal choice for minimizing unnecessary trust penalties on benign vehicles. By dynamically adjusting trust scores based on entropy fluctuations and Bayesian inference, the Entropy-Bayesian Trust Model effectively maintains robust detection accuracy across varying attack conditions. The selection of mean thresholding offers the most stable and reliable performance, ensuring a well-balanced trade-off between detection efficiency and classification accuracy in VANET security applications.

 doi:10.20944/preprints202505.0242.v2

Table 1. Threshold Study with 20% of malicious vehicles and 40 vehicles.

Threshold	$\alpha = 0.4, \beta = 0.4, \gamma = 0.2$	TPR (%)	TNR (%)	FPR (%)	FNR (%)
Mode	0.5	99.9	79.80	20.20	0.04
Median	0.5	99.95	79.60	20.40	0.08
Mean	0.5	99.91	100	0	0.2

5.1. Effect of Vehicle Count

The Entropy-Bayesian reputation model, configured with parameters $\alpha = 0.4$, $\beta = 0.4$, $\gamma = 0.2$, dynamically adjusts trust scores to enhance adaptability across different vehicular densities. The detection accuracy results, as summarized in Table 2, confirm the model's effectiveness in accurately identifying malicious behaviors while minimizing false classifications.

The TPR values indicate that the system maintains high detection performance, effectively identifying malicious activities even in high-density network scenarios. Similarly, the TNR confirms that benign vehicles are correctly classified, reducing false alarms and minimizing unnecessary penalties.

At a network density of 20 vehicles, the system achieves a detection accuracy of 99.99%, benefiting from a manageable message volume that facilitates efficient entropy calculations and stable Bayesian inference updates. The low network congestion ensures that message inconsistencies are promptly detected, leading to minimal FNR and FPR, thereby maintaining high trust evaluation accuracy.

As the number of vehicles increases to 40, detection accuracy slightly decreases to 99.98% due to the increased message traffic. The entropy-based detection system effectively adapts to the higher network load, but false positives show a minor rise as real-time message verification becomes more complex. To counteract this, the system dynamically adjusts trust scores, leveraging Bayesian inference to distinguish between genuine message inconsistencies and adversarial activities.

At 80 vehicles, network congestion becomes more noticeable, leading to delayed message transmissions and minor disruptions in entropy calculations. Consequently, detection accuracy further declines to 99.82%, as the increased message density slightly impacts trust evaluations. However, the Bayesian model stabilizes trust score fluctuations, preventing unjust reputation penalties and ensuring that malicious nodes are still accurately detected.

For 160 vehicles, detection accuracy drops to 99.1%, and at 320 vehicles, it further reduces to 98.95% as message collisions and processing delays introduce challenges in maintaining real-time consistency. Despite this, the system continues to adapt dynamically, ensuring reliable trust management and minimal false classifications.

At 400 vehicles, the highest network density tested, the system achieves 98.83% detection accuracy. While network congestion leads to higher message delays and slightly increased false positives, the Entropy-Bayesian model still ensures stable reputation management, effectively preventing malicious influence on VANET trust mechanisms.

These results confirm the scalability and robustness of the Entropy-Bayesian model, demonstrating its ability to maintain high detection accuracy across varying network densities. The integration of adaptive entropy calculations and Bayesian inference updates ensures that even in high-traffic scenarios, malicious vehicles are accurately detected while minimizing penalties on benign nodes. This makes it a viable and highly effective solution for trust management in VANET environments.

 doi:10.20944/preprints202505.0242.v2

Table 2. Performance metrics under Different Vehicle and Attack Densities.

Vehicles	Malicious (%)	TPR (%)	TNR (%)	Detection Accuracy (%)	FPR (%)	FNR (%)
20	5	99.98	100	99.99	0.0	0.13
	10	99.98	100	99.98	0.0	0.28
	20	99.93	100	99.94	0.3	0.55
	40	99.85	100	99.93	0.0	0.15
40	5	99.94	100	99.97	0.15	0.3
	10	99.94	100	99.97	0.4	0.7
	20	99.91	100	99.93	0.0	0.2
	40	99.85	99.95	99.9	0.25	0.5
80	5	99.64	99.95	99.80	0.5	0.9
	10	99.64	99.95	99.80	0.0	0.13
	20	99.57	99.85	99.71	0.1	0.28
	40	99.51	99.65	99.58	0.3	0.55
160	5	98.20	100.0	99.1	0.0	0.15
	10	97.74	99.92	98.83	0.15	0.3
	20	97.7	99.8	98.75	0.4	0.7
	40	97.4	99.6	98.5	0.0	0.2
320	5	97.0	100.0	98.5	0.25	0.5
	10	96.9	99.9	98.4	0.5	0.9
	20	97	99.75	98.4	0.0	0.13
	40	96.5	99.5	98.0	0.1	0.28
400	5	97.6	100.0	98.8	0.3	0.55
	10	96.75	99.85	98.3	0.0	0.15
	20	96.5	99.7	98.1	0.15	0.3
	40	96.4	99.4	97.9	0.4	0.7

5.2. Effect of Malicious Percentage

To assess the system's detection consistency, extensive evaluations were conducted with varying malicious vehicle percentages set at 5%, 10%, 20%, and 40%. These specific percentages were chosen to align with DIVA [18], allowing for a direct and fair comparison of performance. The results, summarized in Table 2, demonstrate the system's ability to maintain high detection accuracy across different attack scenarios and vehicle densities.

At 5% malicious presence, the system achieves 99.99% detection accuracy for a network density of 20 vehicles. The manageable message volume allows for efficient entropy calculations, ensuring that inconsistencies in message transmissions are detected with minimal errors. As the number of vehicles increases to 40 and 80, detection accuracy slightly decreases to 99.98% and 99.82%, respectively. This minor reduction is due to increased network traffic, which slightly raises false positive rates, but the Bayesian reputation model dynamically compensates for these variations.

At 10% malicious presence, the system maintains 99.98% accuracy for 20 vehicles. With higher adversarial activity, the complexity of message verification increases, leading to a slightly higher false classification rate. However, Bayesian inference ensures that detection remains robust. As vehicle count increases to 40 and 80, detection accuracy declines slightly to 99.97% and 99.79%, respectively, demonstrating the impact of network congestion and malicious interference.

At 20% malicious presence, the system continues to perform strongly, maintaining 99.94% accuracy for 20 vehicles. The increased density of adversarial messages introduces a higher risk of misclassification, reflected in a small rise in false positive and false negative rates. As the network scales up to 40 and 80 vehicles, detection accuracy drops slightly to 99.96% and 99.71%, respectively.

 doi:10.20944/preprints202505.0242.v2

With 160 vehicles, detection accuracy decreases to 98.75%, as higher network congestion and processing delays slightly impact real-time verification.

At 40% malicious presence, the system retains 99.93% accuracy for 20 vehicles. As vehicle count increases to 40 and 80, detection accuracy drops slightly to 99.9% and 99.58%, respectively. At 160 vehicles, accuracy further decreases to 98.5%, and at 400 vehicles, the lowest tested density, the system still achieves 97.9% accuracy. This trend aligns with real-world expectations, where higher malicious activity introduces more uncertainty and detection complexity.

However, the system significantly outperforms DIVA [18], which experiences an accuracy drop to 89% under similar conditions. By maintaining detection accuracy above 97.9% even at 40% malicious presence, our results confirm the robustness of the Entropy-Bayesian reputation model. The system successfully adapts to different network densities and adversarial conditions, significantly outperforming existing solutions like DIVA [18].

Through the integration of entropy-based anomaly detection and Bayesian inference, our approach ensures high resilience, low misclassification rates, and superior adaptability to evolving threats in VANET environments.

5.3. System Robustness Against Attack Models

The Entropy-Bayesian reputation model demonstrates robust security mechanisms against major VANET attack models, including DoS), DDoS, Sybil, Replay, and Forgery attacks.

- DoS and DDoS Resistance: Entropy-based detection identifies message flooding attacks in real-time, ensuring that DoS attackers cannot manipulate vehicle communications. Unlike DIVA [18], which lacks strong DoS detection, our system flags anomalous frequency spikes and adjusts entropy thresholds dynamically.
- Sybil Attack Mitigation: The system ensures unique trust scores per vehicle, preventing identity spoofing. If multiple messages from a single entity exceed entropy variation limits, the system flags them as suspicious, reducing the risk of Sybil-based disruptions.
- Replay Attack Prevention: Timestamp-based message validation ensures that replayed messages are not treated as legitimate communications. The Bayesian update mechanism penalizes vehicles that repeatedly transmit outdated information, effectively neutralizing replay attacks.
- Forgery Attack Detection: The combination of entropy variations and Bayesian consistency checks enables the system to detect falsified messages, ensuring that only genuine, consistent data contributes to reputation scores.

5.4. Computational Efficiency and Scalability

The computational efficiency and scalability are critical performance dimensions for real-time trust management systems operating in large-scale VANET environments. In high-density vehicular networks, the ability to evaluate trust swiftly and accurately, without overwhelming processing resources, is essential to ensure timely and reliable communication.

The proposed model, VANETGuard, demonstrates robust computational performance, supported by the following observations:

- Real-Time Entropy Evaluation: The system employs lightweight Shannon entropy calculations to analyze message timing and behavioral variance. These calculations are computationally inexpensive, enabling continuous anomaly detection even in dense network conditions with hundreds of participating vehicles.
- Optimized Bayesian Inference: Bayesian trust score updates are selectively triggered based on entropy thresholds and behavioral deviations. This design significantly reduces the number of redundant trust updates, thus minimizing computational overhead while maintaining accurate reputation tracking.

 doi:10.20944/preprints202505.0242.v2

- Low-Latency Detection Performance: Empirical results from simulation show that the end-to-end latency for trust evaluation, including entropy scoring and Bayesian inference, consistently remains under 1.5 seconds, even in scenarios with up to 400 vehicles and 40% malicious participation. This latency is well within the operational thresholds required for real-time vehicular decision-making, such as message forwarding, event reaction, or route selection.

Collectively, these features confirm that the proposed model is both computationally efficient and highly scalable, making it suitable for deployment in real-world VANET applications with dynamic and large-scale topologies. The combination of adaptive inference and selective evaluation ensures that the trust system can maintain performance without compromising accuracy or responsiveness under heavy load.

5.5. Benchmarking with Existing Trust Management Models

To comprehensively evaluate the effectiveness of our proposed system, VANETGuard, we conducted a benchmark comparison against several established trust management models in VANETs, including DIVA [18], AATMS [12], HTMS-V [13], ART [16], and HDRS [14]. These models were selected due to their representative designs across various trust computation paradigms—ranging from static thresholding and cloud-based Bayesian systems to subjective logic, reputation dynamics, and hybrid scoring mechanisms. Notably, the comparison with DIVA is of particular significance, as VANETGuard builds directly upon DIVA's core structure. We adopted the same simulation setup and evaluation dataset described in DIVA to ensure consistency and fairness in performance comparison. Furthermore, our system retains DIVA's IOTA-based reputation storage but enhances the underlying algorithm by integrating real-time entropy-based detection, adaptive trust scoring, and Bayesian inference. This results in a system that is both operationally similar and significantly more robust in dynamic vehicular environments.

The evaluation focused on multiple performance indicators, including detection accuracy, false classification rates, adaptability under high-malicious settings, execution latency, and DDoS resilience. In terms of detection accuracy, VANETGuard demonstrates a marked improvement, achieving 99.925%, compared to 99.9% in DIVA, 98.5% in AATMS, 97.2% in HTMS-V, 96.8% in ART, and >97% in HDRS [14]. This enhancement is largely attributed to the integration of entropy-based anomaly detection and Bayesian reasoning, which allows VANETGuard to dynamically adapt trust scores based on message consistency and observed behavioral patterns. The True Positive Rate (TPR) of 99.85% and the False Negative Rate (FNR) of only 0.15% further support the system's ability to reliably detect malicious behavior with minimal oversight. In contrast, AATMS, HTMS-V, ART, and even HDRS [14] exhibit higher FNR values, ranging from approximately 2% to 5% under certain attack thresholds, indicating a greater susceptibility to undetected adversarial behavior when malicious density increases beyond the system's adaptive threshold.

A critical component of trust systems in VANETs is their performance under adversarial conditions. When 50% of network participants are malicious, VANETGuard maintains approximately 98% detection accuracy. This stands in contrast to the performance degradation observed in DIVA and others. DIVA's reliance on static thresholding, particularly mode-based decision rules, results in an increased likelihood of false evaluations in complex attack scenarios, such as collusion or Sybil attacks. Similarly, HTMS-V and ART, although incorporating logic-based and heuristic approaches, exhibit accuracy drops to approximately 90% and 88%, respectively. AATMS performs moderately better (~94%) but is hindered by its dependence on cloud-synchronized trust updates, which introduces latency and reduces responsiveness. HDRS [14], by contrast, maintains near-perfect detection when the malicious presence is under 40%, but its performance begins to decline once adversarial density exceeds that threshold—an expected limitation due to reputation convergence lag during high-malice states.

Latency is another critical factor in VANET deployment. While DIVA achieves microsecond-level latency through its lightweight IOTA trust propagation, it lacks dynamic evaluation, limiting its adaptability. VANETGuard introduces slightly higher latency (in milliseconds) due to real-time

 doi:10.20944/preprints202505.0242.v2

trust recalibration through entropy and Bayesian inference. Compared to AATMS, which incurs seconds-level delays due to its dependence on cloud infrastructure, and HTMS-V and ART, which utilize less flexible local models, VANETGuard strikes a meaningful balance between speed and adaptability. HDRS [14], which incorporates adaptive reputation update intervals, performs competitively in latency as well—introducing only negligible communication overhead, with minor beacon-size expansions (~4 bytes) and dynamic adjustments tuned to vehicle density and message rates.

A distinct advantage of VANETGuard is its resilience to DDoS attacks. Unlike DIVA, which does not account for such threats, VANETGuard continuously monitors entropy variations in message patterns to detect anomalous traffic surges. This enables timely mitigation of flooding attempts, preserving communication integrity even under large-scale attacks. While AATMS includes basic filtering mechanisms and ART uses simple anomaly thresholds, neither implements adaptive entropy-based mitigation. HDRS [14], while highly effective at filtering collusion, intelligent, and false data attacks, does not specifically address DDoS resilience, limiting its protection against bandwidth-targeted message floods.

Finally, in terms of trust update mechanisms, VANETGuard offers the most comprehensive solution. While DIVA, AATMS, HTMS-V, and ART update trust scores through periodic or event-driven rules, VANETGuard utilizes an adaptive model combining entropy scores, Bayesian probability updates, and real-time behavioral assessments. HDRS [14] adopts a similar hybrid strategy, using a dynamic update interval and analytic hierarchy process (AHP) to determine the optimal timing for trust recalibration. However, VANETGuard further improves on this by integrating IOTA's distributed ledger with entropy-responsive updates, minimizing false penalties and accelerating detection of emerging malicious actors. By using the same foundational architecture as DIVA but layering advanced inference and learning capabilities, VANETGuard ensures compatibility while delivering significant improvements in accuracy, adaptability, and defense robustness in highly dynamic and adversarial VANET environments.

Table 3. Performance Metrics Comparison Between VANETGuard, DIVA [18], AATMS [12], HTMS-V [13] ,ART [16] and HDRS [14].

Metric	VANETGuard	DIVA [18] (Mode Threshold)	AATMS [12]	HTMS-V [13]	ART [16]	HDRS [14]
Detection Accuracy (%)	99.925	99.9	~98.5 (derived from TPR/TNR)	>95 under most attacks	96.8 (estimated from robustness section)	>97% across conditions (dynamic)
TPR (%)	99.85	99.8	≥97.8 (at 20–30% collusion)	96%+ (for malicious node identification)	~95.9 (collusion scenarios)	100% (≤40% malicious); drops after
TNR (%)	100.0	100.0	~99 (stable across conditions)	>95–97%	97.6	High; contextually adaptive

 doi:10.20944/preprints202505.0242.v2

FPR (%)	0.0	0.0	1.0% or less (verified)	<4%, even under hybrid attacks	~2.4	Low, adaptive to context
FNR (%)	0.15	0.2	~2.2% (drops at high collusion)	<4–5%, drops when malicious rate >40%	~4.1%	Slight rise >40% malicious, stays low
Performance in High Malicious (50%)	Maintains ~98%	Drops significantly	Drops moderately (~94%)	Moderate drop (~90%)	Severe drop (~88%)	Can't detect all at 50%, but stable below
Execution Latency	ms (Bayesian + IOTA)	µs (Tangle)	Seconds (cloud sync + Bayesian)	Milliseconds (local-only)	Milliseconds (lightweight)	ms range, dynamic interval
DDoS Mitigation	Effective (entropy analysis)	Not addressed	Limited (weighted filtering)	Not explicitly addressed	Basic thresholds	Effective (entropy + reliability filters)
Trust Update Mechanism	Entropy + Bayesian + DLT	DLT only	TrustRank + Forgetting + Feedback filters	Subjective logic + indirect decay	History + weighted scoring	Hybrid V2V/RSU + Reliability eval + AHP weights

6. Conclusions

This study introduced VANETGuard, a scalable and adaptive trust management system designed for vehicular ad hoc networks (VANETs). By integrating entropy-based anomaly detection, Bayesian inference, and distributed ledger technologies, the system addresses critical challenges in trust evaluation, including detection accuracy, real-time adaptability, and resilience under adversarial conditions.

Comprehensive simulation results across varying network densities (20 to 400 vehicles) and malicious participation rates (5% to 40%) confirm the robustness and scalability of VANETGuard. The system consistently achieved detection accuracy exceeding 99.9% in low to moderate-density networks, and maintained competitive accuracy (≥97.9%) even in high-density environments with up to 40% malicious nodes. True Positive Rates remained above 96.4%, and True Negative Rates consistently approached 100%, validating the system's reliability in correctly classifying vehicle behavior. Furthermore, False Positive and False Negative Rates were kept exceptionally low across all scenarios, highlighting the system's capability to minimize misclassifications while preserving communication integrity.

Despite these promising results, several avenues for future research remain. First, adaptive threshold tuning is necessary to better accommodate region-specific traffic dynamics, especially in

 doi:10.20944/preprints202505.0242.v2

heterogeneous urban deployments. This could be achieved through localized learning or reinforcement-based adjustments. Second, although VANETGuard is effective against common attack vectors such as Sybil and flooding, future research should explore more sophisticated threat models, including on-off (gray hole) attacks and coordinated adversarial behavior. Enhancing temporal and graph-based anomaly detection can improve robustness in these contexts.

Additionally, optimization for resource-constrained edge nodes remains an important consideration, particularly as real-world deployments demand lightweight models with minimal computational and energy overhead. Integrating privacy-preserving trust evaluation mechanisms, such as differential privacy or secure multi-party computation, can further align the system with modern data protection standards. Finally, large-scale real-world testing and ledger optimization are needed to validate system performance under live network conditions and ensure the scalability of IOTA-based reputation storage under high-frequency update loads.

In summary, VANETGuard presents a strong foundation for real-time, resilient trust management in VANETs. With continued enhancements in adaptability, efficiency, and privacy, it holds significant promise for deployment in next-generation intelligent transportation systems.

Author Contributions: Conceptualization, Heba Kurdi; Data curation, Reem Almaziad; Formal analysis, Reem Almaziad; Investigation, Reem Almaziad; Methodology, Reem Almaziad; Project administration, Reem Almaziad; Resources, Reem Almaziad; Software, Reem Almaziad; Supervision, Heba Kurdi; Validation, Reem Almaziad and Heba Kurdi; Visualization, Reem Almaziad; Writing – original draft, Reem Almaziad; Writing – review & editing, Reem Almaziad and Heba Kurdi. All authors have read and agreed to the published version of the manuscript.

Funding: This research project was supported by the Researchers Supporting Project number (RSP2025R204), King Saud University, Riyadh, Saudi Arabia.

Data Availability Statement: The data supporting the reported results are available upon request.

Acknowledgments: This research project was supported by the Researchers Supporting Project number (RSP2025R204), King Saud University, Riyadh, Saudi Arabia.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

VANETs	Vehicular Ad Hoc Networks
V2V	Vehicle-to-Vehicle
V2I	Vehicle-to-Infrastructure
HTMS	Hybrid Trust Management System
DLT	Distributed Ledger Technology
DoS	Denial-of-Service
DDoS	Distributed Denial-of-Service
TPR	True Positive Rate
FPR	False Positive Rate
ITS	Intelligent Transportation Systems
V2X	Vehicle-to-Everything
IRS	Intelligent Reputation System
TA	Trusted Authority
DIDs	Decentralized Identifiers
RSUs	Road-Side Units
CAMs	Cooperative Awareness Messages
DENMs	Decentralized Environmental Notification Messages
FNR	False Negative Rate
TNR	True Negative Rate
IOTA	A type of Distributed Ledger Technology (DLT)

 doi:10.20944/preprints202505.0242.v2

ML	Machine Learning
5G	Fifth Generation Mobile Network
OMNeT++	Objective Modular Network Testbed in C++
SUMO	Simulation of Urban MObility
Simu5G	5G Network Simulation Tool
ETS-G5	European Telecommunications Standards Institute Intelligent Transport Systems G5
DIVA	Decentralized Identification-Based Vehicular Authentication
MDPI	Multidisciplinary Digital Publishing Institute
DOAJ	Directory of Open Access Journals
TLA	Three Letter Acronym
LD	Linear Dichroism

References

1. M. Raya and J.-P. Hubaux, “Securing vehicular ad hoc networks,” Journal of Computer Security, vol. 15, no. 1, pp. 39–68, 2007, doi: 10.3233/JCS-2007-15103.
2. T. Thakur et al., “TrustMod: A Trust Management Module for NS-3 Simulator,” arXiv:2207.09945, 2022.
3. A. Saad et al., “MESMERIC: A machine learning-based trust management mechanism for surrounding cars in intelligent connected vehicles,” Sensors, 2024. [VERIFY volume/article/DOI].
4. N. Gupta et al., “Authentication-Based Secure Data Dissemination Protocol and Framework for 5G-Enabled VANET,” Future Internet, vol. 12, no. 4, art. 63, 2020, doi: 10.3390/fi12040063.
5. N. Fan and C. Q. Wu, “On trust models for communication security in vehicular ad-hoc networks,” Ad Hoc Networks, vol. 90, art. 101740, 2019, doi: 10.1016/j.adhoc.2018.08.010.
6. B. Hou et al., “VANET Secure Reputation Evaluation & Management Model Based on Double-Layer Blockchain,” Applied Sciences, vol. 13, no. 9, art. 5733, 2023, doi: 10.3390/app13095733.
7. A. Feraudo et al., “DIVA: A DID-based reputation system for secure transmission in VANETs,” Computer Networks, 2024. [VERIFY: article number + DOI].
8. M. N. Mejri, “Entropy as a new metric for denial of service attack detection in vehicular ad-hoc networks,” 2014, doi: 10.1145/2641798.2641800. [VERIFY venue/proceedings].
9. S. A. Soleymani et al., “Trust management in vehicular ad hoc network: a systematic review,” EURASIP Journal on Wireless Communications and Networking, 2015, doi: 10.1186/s13638-015-0353-y.
10. T. Nandy et al., “A review of security attacks and intrusion detection in the vehicular ad hoc network,” Alexandria Engineering Journal, 2024. [VERIFY volume/pages/DOI].
11. H. Che et al., “On trust management in vehicular ad hoc networks,” Frontiers in the Internet of Things, 2022, doi: 10.3389/friot.2022.995233.
12. J. Zhang et al., “AATMS: An anti-attack trust management scheme in VANET,” IEEE Access, vol. 8, pp. 21077–21090, 2020, doi: 10.1109/ACCESS.2020.2966747.
13. L. Wang et al., “VANETs group message secure forwarding with trust and mobility evaluation,” 2024. [VERIFY venue/DOI].
14. X. Liu et al., “HDRS: A Hybrid Reputation System With Dynamic Update Interval for Detecting Malicious Vehicles in VANETs,” IEEE Transactions on Intelligent Transportation Systems, 2022. [VERIFY vol/issue/pages/DOI].
15. R. Mühlbauer et al., “A Feasible Trust System for Vehicular Ad Hoc Networks,” Future Internet, vol. 7, no. 3, art. 37, 2018. [VERIFY year].
16. W. Li and H. Song, “ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks,” IEEE Transactions on Intelligent Transportation Systems, vol. 17, no. 4, pp. 960–969, 2016.
17. X. Li, J. Liu, X. Li, and W. Sun, “RGTE: A Reputation-Based Global Trust Establishment in VANETs,” Proc. IEEE INCoS, 2013, doi: 10.1109/INCOS.2013.91.
18. W. Fang et al., “BTDS: Bayesian-based trust decision scheme for intelligent connected vehicles in VANETs,” Transactions on Emerging Telecommunications Technologies, 2020, doi: 10.1002/ett.3879.
19. F. G. Mármol and G. M. Pérez, “TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks,” Journal of Network and Computer Applications, vol. 35, no. 3, pp. 934–941, 2012. [VERIFY DOI].

 doi:10.20944/preprints202505.0242.v2

20. Z. H. Dong et al., "TMEC: Trust Management based on Evidence Combination on Vehicular Ad Hoc Networks," IEEE Access, vol. 7, pp. 148913–148922, 2019, doi: 10.1109/ACCESS.2018.2876153.
21. F. Ahmad et al., "Notrino: A novel hybrid trust management scheme for Internet-of-Vehicles," IEEE Transactions on Vehicular Technology, vol. 70, pp. 9244–9257, 2021, doi: 10.1109/TVT.2021.3049189.
22. X. Sun et al., "A trust model for edge-driven VANETs using fuzzy logic," IEEE Transactions on Intelligent Transportation Systems, 2023, doi: 10.1109/TITS.2023.3305342.
23. Z. Lu et al., "BARS: A Blockchain-based Anonymous Reputation System for Trust Management in VANETs," arXiv:1807.06159, 2018.
24. A. Kudva et al., "A scalable blockchain based trust management in VANET routing protocol," Journal of Parallel and Distributed Computing, vol. 152, pp. 144–156, 2021, doi: 10.1016/j.jpdc.2021.02.024.
25. W. Ahmed et al., "Privacy-preserving blockchain-based authentication and trust management in VANETs," IET Networks, 2022, doi: 10.1049/ntw2.12036.
26. R. Su, Y. Jin, and Y. Song, "Assessing Trustworthiness of V2X Messages: A Cooperative Trust Model Against CAM- and CPM-Based Ghost Vehicles in IoV," 2024, doi: 10.5220/0012605200003702. [VERIFY venue].
27. B. Luo et al., "AIT: An AI-enabled Trust Management System for Vehicular Networks Using Blockchain Technology," IEEE Internet of Things Journal, vol. 8, no. 5, pp. 3157–3169, 2021, doi: 10.1109/JIOT.2020.3044296.
28. N. B. Sapuan et al., "Biometric blockchain-based multifactor privacy-preserving authentication scheme for VANETs," Journal of Information Technology and Applications (JITA), 2021. [VERIFY indexing/DOI].
29. B. Mokhtar and M. Azab, "Survey on Security Issues in Vehicular Ad Hoc Networks," Alexandria Engineering Journal, vol. 54, no. 4, pp. 1115–1126, Dec. 2015, doi: 10.1016/j.aej.2015.07.011.
30. H. Setia, A. Chhabra, S. K. Singh, S. Kumar, S. Sharma, V. Arya, B. B. Gupta, and J. Wu, "Securing the road ahead: Machine learning-driven DDoS attack detection in VANET cloud environments," Cyber Security and Applications, vol. 2, art. 100037, 2024, doi: 10.1016/j.csa.2024.100037.
31. R. Riebl, H.-J. Günther, C. Facchi, and L. Wolf, "Artery: Extending Veins for VANET applications," in Proc. 2015 Int. Conf. Models and Technologies for Intelligent Transportation Systems (MT-ITS), Budapest, Hungary, Jun. 3–5, 2015, pp. 450–456, doi: 10.1109/MTITS.2015.7223293.