UMYU Scientifica, Vol. 5 NO. 2, June 2026, Pp 408 – 419
https://doi.org/10.56919/usci.2652.037
ISSN: 2955 – 1145 (print); 2955 – 1153 (online)
A periodical of the Faculty of Natural and Applied Sciences, UMYU, Katsina

ORIGINAL RESEARCH ARTICLE

Securing Vehicular Ad-Hoc Networks Against Blackhole Attacks Using an Enhanced Trust Management Framework

Mukhtar Abubakar[1], Armaya'u Zango Umar[2] and Abubakar Aminu Mu'azu[3]
[1]Department of Computer Science, Federal College of Education, Katsina, Katsina State, Nigeria
[2]Department of Computer Science, Faculty of Natural and Applied Sciences, Umaru Musa Yar'adua University, Katsina, Katsina State, Nigeria
[3]Department of Software Engineering, College of Computing and Information Sciences, Al-Qalam University, Katsina, Katsina State, Nigeria

ABSTRACT
Vehicular Ad-Hoc Networks (VANETs) are essential for Intelligent Transportation Systems, enabling vehicle-to-vehicle and vehicle-to-infrastructure communication to improve road safety and traffic efficiency. However, VANETs are vulnerable to blackhole attacks, where malicious vehicles drop legitimate packets, disseminate false information, and provide misleading recommendations, thereby compromising network performance and trust. This study proposes an Enhanced Trust Management Framework (ETMF) that integrates neighbour monitoring, local and global trust evaluation, and collaborative decision-making between vehicles and Road Side Units (RSUs) to mitigate blackhole attacks. ETMF was implemented and evaluated using OMNeT++ 5.6.2, SUMO 1.8.0, and VEINS 5.2 in a realistic Abuja road network scenario comprising 50 vehicles, 5 RSUs, and 0–40 malicious nodes over a 600-second simulation period. The framework was compared with TEAM and FIDS-HMM using metrics such as end-to-end delay, anomaly detection ratio, convergence rate, event detection ratio, content delivery ratio, packet loss ratio, and computational overhead. Results showed that ETMF reduced end-to-end delay by up to 25%, improved anomaly detection by up to 8%, and increased detection rates by 2.06%–8.33% compared with FIDS-HMM under blackhole attack conditions. ETMF also achieved faster network convergence while maintaining acceptable computational overhead. These findings indicate that ETMF enhances trust management and blackhole attack mitigation in VANETs under realistic mobility conditions. Future work will focus on improving convergence behaviour and event detection performance in larger and more densely populated vehicular networks. Source code, simulation configurations, and parameter settings will be made publicly available upon publication.

ARTICLE HISTORY
Received March 16, 2026
Accepted June 29, 2026
Published June 30, 2026

KEYWORDS
Vehicular Ad-Hoc Networks (VANETs); Blackhole Attack; Trust Management; Intrusion Detection; Intelligent Transportation Systems

INTRODUCTION
VANETs play a pivotal role in Intelligent Transport Systems (ITS), enabling inter-vehicle communication to enhance road safety and traffic management (Mahrez et al., 2022; Raza et al., 2023). By allowing vehicles to exchange critical information, VANETs reduce the likelihood of accidents and improve traffic flow efficiency. However, VANETs face various security challenges due to their reliance on wireless communication and the potential for malicious entities to exploit this openness (Varma & Kumar, 2023). Blackhole attacks, wherein malicious vehicles disrupt communication by either dropping or fabricating messages, are particularly concerning (Ismail et al., 2023; Sultan et al., 2022). To counter these issues, trust management frameworks have been introduced, leveraging mechanisms to dynamically assess and counter malicious activity in VANETs (Aminu & Nura, 2025; Cheong et al., 2024; Ibrahim, 2022; Isiyaku et al., 2024; Muhammad & Umar, 2023; Ogbe & Abubakar, 2025)

Despite their advantages, VANET environments are highly vulnerable to a range of cooperative and deceptive attacks, including blackhole, greyhole, false-message injection, and reputation manipulation attacks. Among these, blackhole attacks are particularly damaging because malicious vehicles can selectively drop packets, falsify event information, or manipulate recommendation messages, leading to incorrect trust formation and degraded network reliability. These attacks are especially difficult to detect due to the highly dynamic topology and intermittent connectivity of vehicular networks.

Addressing these security challenges requires a robust trust management framework capable of dynamically identifying and mitigating malicious activities while

Correspondence: Mukhtar Abubakar. Department of Computer Science, Federal College of Education, Katsina, Katsina State, Nigeria. ✉ mukhtarabubakar59@gmail.com.
How to cite: Abubakar, M., Umar, A. Z., & Mu'azu, A. A. (2026). Securing Vehicular Ad-Hoc Networks Against Blackhole Attacks Using an Enhanced Trust Management Framework. *UMYU Scientifica*, 5(2), 408 – 419. https://doi.org/10.56919/usci.2652.037

adapting to the network's constantly changing conditions (Habbal et al., 2024). Although frameworks like the TEAM (Ahmad, Franqueira, et al., 2018) framework have shown potential by tackling Man in the Middle (MITM) attacks, their applicability to real-world VANET environments is limited, primarily due to a lack of realistic mobility models (Sarwatt et al., 2024). Similarly, recent models incorporating Fuzzy Logic-based Intrusion Detection Systems with Hidden Markov Models (FIDS-HMM) enhance blackhole attack detection but lack scalability and adaptability when managing complex VANET scenarios with high malicious node presence (A & Ravindran, 2024).

However, these existing frameworks exhibit several limitations. The TEAM framework primarily focuses on Man-in-the-Middle (MitM) attack detection and does not fully model blackhole-specific behaviours such as selective packet dropping and recommendation manipulation under realistic vehicular mobility. Similarly, FIDS-HMM improves detection using fuzzy logic and Hidden Markov Models but suffers from scalability issues and reduced adaptability in highly dynamic, large-scale VANET environments. In addition, both frameworks are limited in their integration with realistic mobility models, which reduces the accuracy of simulation-to-real-world generalization.

This study aims to address these limitations by developing an Enhanced Trust Management Framework (ETMF) that mitigates blackhole attacks through a novel approach combining localized and globalized trust assessments, utilizing dynamic thresholds, majority consensus, and collaborative evaluation with RSUs.

The main contributions of this study are summarized as follows:

- Development of an Enhanced Trust Management Framework (ETMF) that integrates local and global trust evaluation for improved blackhole attack detection.
- Introduction of a collaborative RSU–vehicle trust computation mechanism using majority consensus and dynamic trust thresholds.
- Implementation and validation using realistic mobility modelling in OMNeT++, SUMO, and VEINS within a real-world Abuja road network.
- Comprehensive performance evaluation against TEAM and FIDS-HMM using multiple QoS and security metrics, including delay, detection rate, convergence rate, and packet delivery performance.

Related Work

This study focuses specifically on blackhole attack scenarios in Vehicular Ad-Hoc Networks (VANETs). The threat model assumes the presence of malicious vehicles capable of dropping packets, injecting false event information, and manipulating recommendation messages. The objective is to evaluate trust degradation and mitigation strategies under these adversarial conditions.

Recent studies have explored various trust management strategies to combat security issues in VANETs. Early frameworks, such as TEAM (Ahmad, Franqueira, et al., 2018), primarily focused on detecting Man-in-the-Middle (MitM) attacks and proposed extending research to blackhole attacks in future iterations. FIDS-HMM enhanced the detection framework by combining fuzzy logic with Hidden Markov Models to dynamically adapt to VANET conditions (A & Ravindran, 2024). FIDS-HMM integrates fuzzy logic to handle uncertain data and Hidden Markov Models (HMM) to model and predict attack patterns. While FIDS-HMM provides strong detection rates, its adaptability to highly dynamic mobility models and real-time performance in large-scale VANETs is still limited (Wlazlo et al., 2021).

More recently, Zhao et al. (2024) proposed a trust management model based on dynamic feedback and reputation scoring to improve the detection of malicious nodes in VANETs. This model adjusts trust scores in real-time based on the vehicle's past behavior, promoting a more adaptive and responsive trust evaluation system. However, like TEAM, this approach does not adequately address the full range of attacks, particularly blackhole attacks, which remain difficult to detect due to their stealthy nature in VANET environments. Similarly, Lone et al. (2024) introduced an adaptive trust-based approach to detect blackhole attacks in VANETs. This method uses vehicle collaboration, where neighboring vehicles monitor each other's behavior and share trust information to detect anomalies.

Abbasi et al. (2026) explored the use of machine learning techniques, including decision trees and neural networks, to enhance IDS performance in VANETs. Their approach demonstrated improved detection accuracy, particularly for complex attack scenarios like blackhole and Sybil attacks. While promising, this study acknowledged the challenge of real-time implementation, as machine learning models require significant computational resources and can be slow to adapt to rapidly changing network conditions. Moreover, such systems are typically data-hungry, requiring large amounts of historical data to train effective models, which may not always be available in VANETs.

Rashid et al. (2023) employed SUMO and OMNET++ to simulate realistic VANET environments and evaluated different trust management approaches for detecting blackhole attacks. While the study provided valuable insights into the effectiveness of various methods, it also highlighted the need for better scalability and real-time performance in larger networks. The simulation results suggested that combining trust management with intrusion detection would enhance the detection of blackhole attacks while maintaining network performance. Likewise, in another study, Al-Shareeda & Manickam, (2023) integrated dynamic trust evaluation with realistic mobility models using VEINS, a simulation framework

that combines SUMO and OMNET++ to simulate VANETs with more accurate vehicle movement patterns. Their results showed promising improvements in detecting blackhole attacks, but they also emphasized the challenge of balancing detection accuracy with the overhead of real-time trust management in large-scale environments.

Despite the progress made in VANET security, several challenges remain unresolved. The dynamic and highly mobile nature of VANETs makes it difficult to develop universal solutions for detecting and mitigating blackhole attacks. Trust management frameworks often fail to adapt quickly to changing network conditions, and traditional IDS models struggle to scale effectively in large, highly dynamic networks (ZLi et al., 2023). Moreover, many existing solutions lack integration with realistic mobility models, leading to discrepancies between simulation results and real-world performance (J. Li et al., 2021). There is a clear need for more adaptive, scalable solutions that can handle both the complexity of VANET environments and the dynamic behavior of malicious nodes.

Proposed Enhanced Trust Management Framework (ETMF)

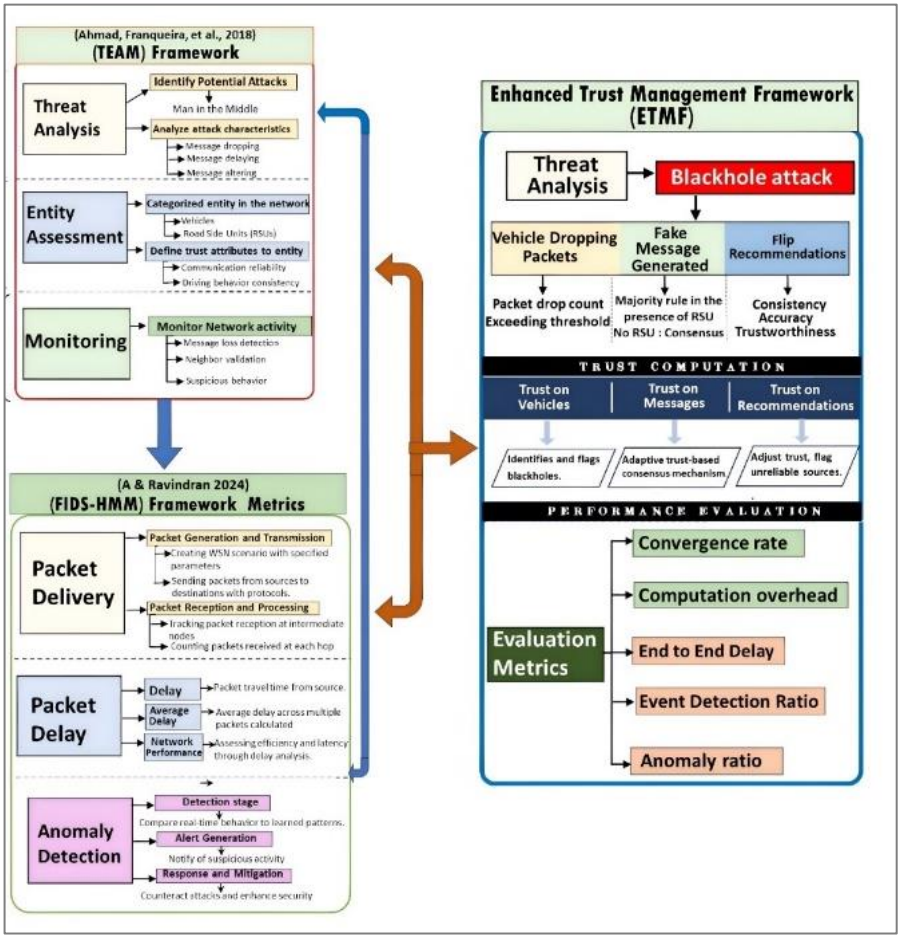

Figure 1: ETMF as hybridization and complementation of TEAM and FIDS-HMM

The proposed framework, ETMF, incorporates TEAM and FIDS-HMM as shown in Figure 1. Recall that Ahmad et al., (2018) proposed the Trust Evaluation and Management (TEAM) framework, in which its threat analysis component focused on Man-in-the-Middle (MitM) attacks (top left of Figure 1). The framework categorizes network entities into vehicles and RSUs; and defines trust attributes like reliability and driving consistency. Thus, in the framework, trust attributes of communication reliability for RSUs and driving behavior consistency for vehicles are initiated and assigned to corresponding entities. The trust attributes of the entities are updated by continuous monitoring of the network activities for anomalies (e.g., message loss or suspicious behavior). Although some of the behaviors of (MitM) overlap with those of a pure blackhole, TEAM threat analysis does not cover other specific malicious activities of a typical blackhole, such as generating and spreading fake messages in the network as well as flipping recommendations about its neighbors (report malicious entity as refutable and vice versa). Other equally important evaluation metrics, such as anomaly detection ratio was not considered.

Similarly, recent work by (A & Ravindran, 2024) leverages a Fuzzy Logic-based Intrusion Detection System with Hidden Markov Models (FIDS-HMM) tailored for VANETs to detect and mitigate malicious activities (bottom-left of Figure1). However, the proposed technique will be difficult to scale in real-world settings and also lacks consideration of real traffic mobility models.

As shown in Figure 1, TEAM (top left of Figure 1) provides foundational components like threat analysis and

monitoring, which are extended in the proposed ETMF for enhanced threat detection and mitigation. Similarly, FIDS-HMM metrics are incorporated into ETMF for robust performance evaluation and anomaly detection.

Deployment Scenario and the attack model

The scenario in this paper simulates vehicle interactions with realistic mobility and multi-hop relaying. The network connectivity leverages the Dedicated Short-Range Communication (DSRC) framework for efficient message exchange. Thus, the ETMF framework assumes a deployment scenario where vehicles form a dynamic network.

The attack model was designed with black holes and innocent vehicles travelling together on a given route. On the route, events such as accidents will be generated at random locations and times**.** Vehicles closer to the event experience it first. As soon as the event is experienced by vehicles, they immediately adapt to the consequences of the event, such as a rapid deceleration and hard braking and start including parameters (the event and the changes in their driving behaviors) with this event in their multicast messages. Vehicles that are not close to the event will eventually observe it later as the network converges, as they will receive such information through messages.

For the attack, if there is an accident, malicious nodes keep dropping the message even though they have reacted to the event by acting appropriately. To appear genuine, malicious nodes will be dropping messages with a certain probability. The malicious node may also generate new fake messages and forward them to other vehicles. In addition, they provide wrong recommendations about other neighboring vehicles. For example, if the recommendation is represented as a binary value, the malicious nodes flip the value in order to badmouth honest vehicles. Algorithm 1 provides a succinct description of the attack model

Algorithm 1: Blackhole attack model

- *V*: Set of vehicles travelling on route
- *E*: Set of all possible event types (eg: accident, breakdown, construction).
- *L*: Set of all locations along the route
- *T*: Set of all possible time points during the simulation

Event Generation:

1. *Generate Event (t):* $E \times L \times T \rightarrow (e_{rand}, l_{rand}, t_{rand,})$ *where* $e \in E$, $l \in L$ *and* $t \in T$
2. *When a vehicle* $\boldsymbol{v}$ *encounters an event* $\boldsymbol{e} \in \boldsymbol{E}$ *at location* L_e *and time* t_e **,** *it adapts to the consequences of events by updating its driving behavior*

UpdateBehavior (l_e , e)

//The vehicles also creates a multicast message:

Multicast (e, l_e, t_e)

3. ReceiveEvent (e, v)

//Malicious Node Behavior

//Malicious nodes may drop messages with a certain probability p_d *to appear genuine:*

4. DropMessage (e, p_d)

6. *Generate fake messages* (e_{fake})

//Malicious nodes provide incorrect recommendations about neighboring vehicles:

1. FlipBinaryRecc (v)

Malicious nodes continue their behavior throughout the simulation, intermittently dropping messages, generating fake messages, and providing incorrect recommendations to neighboring vehicles.

In the above algorithm, line 1 indicates randomly generating an event, E, such as an accident at a location, l, and at time, t, along the route. Lines 1 through 4 indicate event handling by the vehicles for normal vehicle. On the other hand, the last part is the malicious behaviors by the malicious vehicles.

Trust Computation

Trust is computed using complementary approaches, i.e., global trust establishment and local trust establishment. Global trust establishment is accomplished via RSU, where vehicles in its vicinity share their opinions about the event with the available RSU. Local trust establishment between vehicles is also computed in the absence of an RSU, where information about an event, E, is received at vehicle V and is analyzed for its authenticity.

Trust on vehicle

Parameters

- *T*: Threshold (minimum number of consecutive packet drops to classify a node as a black hole).
- *M*: Monitoring interval (time duration for monitoring node behavior).
- *N*: Neighbor table (a data structure to maintain information about neighboring nodes).
- *S*: Suspicious nodes list (a list to keep track of nodes suspected of being blackholes)

//Initialization:

1. *Initialize neighbor table: N = {} (empty entries for each neighboring node).*
2. *Initialize node list: S = {} (empty).*

//Periodic Monitoring (While connected == true):

3. *for each node* i *in the network:*
4. *Foreach neighbor* j *of node* i
5. Initialize $D_{i,j}$ to 0
6. If j *is reachable, increment the drop count* D_{ij} *for that neighbor in the neighbor table*
7. If $D_{ij} \geq T$, *mark neighbor* j *as suspicious node*
8. If $D_{i,j} < T$, *reset* $D_{i,j}$ *to 0*
9. *After monitoring interval M check for suspicious node*
10. *If node has atleast one suspicious neighbour add the node to the suspicious neigbour list*
11. *Reset the drop count for all neighbors of the node*

//Blackhole Detection

12. Initialize TimerEvent with a random interval between 1 and 2 minutes
13. When TimerEvent expires:
14. *For each node* k *in the suspivious nodes list:*
15. *Send a series of test paacket to* k
16. *Let a* D_k *be the count of dropped packet in the series:*
17. *if* D_k *consistently exceeds T classify node* k *as blackhole*
18. Reset the TimerEvent

Trust on Message

In the presence of RSU, vehicles share their opinions about events with nearby RSUs, which perform majority rule to authorize trusted information and detect malicious vehicle disseminating fake messages. RSUs collect multicast messages from multiple vehicles in their vicinity, forming a pool of information about ongoing events. Using a majority rule algorithm, RSUs analyze the received messages to determine the most prevalent information about each event. This ensures that the information authorized by RSUs represents the consensus among vehicles in the area. RSUs prioritize information that is supported by the majority of vehicles, considering it more reliable and trustworthy. More specifically, the majority rule works as follows:

$D_{majority}\ (e,l) = Max(m)_{\in M\ (e,l)}$ ..... (1).

In equation (1), $e, l, m =$ *Count of occurrences of message m for event e, at location l;* $M_{majority}\ (e,l)$ *represents the majority message; M* is the set of all possible messages.

Based on the analysis of multicast messages using Equation (1), RSUs authorize certain information as trusted and accurate.

In the absence of RSUs, vehicles rely on peer-to-peer communication and consensus among neighboring vehicles to assess the reliability of received messages and recommendations. Vehicles analyze the messages they receive and compare them with the collective opinion or consensus of neighboring vehicles. In this paper, we use a weighted average, where each vehicle's opinion contributes to the overall consensus based on its perceived reliability or trustworthiness. That is, Let: $O_i =$ be the opinion of vehicle i; w_i be the weight assigned to vehicle's opinion, reflecting its reliability or

trustworthiness; n be the total number of vehicles participating in forming the consensus. Then the collective opinion O_c can be represented as the weighted average of individual opinions (Equation 2):

$$Oc = \frac{\sum_{i=1}^{n} wi.oi}{\sum_{i=1}^{n} wi} \quad (2)$$

If a received message contradicts the consensus among neighboring vehicles, it is deemed untrustworthy. Each vehicle assigns a reputation score to its neighboring vehicles based on the consistency and trustworthiness of their recommendations. Suspicious or inconsistent recommendations from a neighboring vehicle lead to a decrease in that vehicle's reputation score. Over time, vehicles adjust their trust levels and decision-making processes based on the reputation scores of neighboring vehicles, prioritizing recommendations from those with higher reputation scores.

Trust on recommendation

In ETMF, each vehicle maintains a record of the recommendations it receives from neighboring vehicles over time. For each recommendation, the receiving vehicle evaluates its consistency, accuracy, and overall reliability.
Let:

- V = Set of vehicles in the VANET
- $R_{(v,t)}$: Reputation score of vehicle v at time t (numeric value)
- $T_{(v,w,t)}$: Trust level of vehicle v at vehicle w at time t (value between 0 and 1)
- $M_{(v,w,t)}$: Message sent by vehicle v to vehicle w at time t
- α: Weighting factor for reputation score ($0 \leq \alpha \leq 1$)

When vehicle v receives a message M (w, v, t) from neighbor w and the message aligns with previous recommendations and expectations: $R_{(w,t+1)} = R_{(w,t)} + \Delta$ (positive increment). If, however, the message is suspicious or contradicts previous information: $R_{(w,t+1)} = R_{(w,t)} - \Delta$ (negative decrement). In both cases, Δ represents the magnitude of reputation score adjustment based on message consistency.

Consequently, a vehicle *v* updates its trust in neighbor *w* based on reputation score:

- $T_{(v,w,t+1)} = \alpha * R_{(w,t+1)} + (1-\alpha) * T_{(v,w,t)}$

The trust level considers both the current reputation score (α) and past trust assessments (1-α).

Simulation Environment

In this study, the Vehicles in Network Simulation (VEINS) and Simulation of Urban MObility (SUMO) were used. Veins is an open-source framework built on top of the **O**bjective Modular Network Testbed in (OMNeT++ Community, 2025). Veins supports modelling wireless communication between vehicles (V2V) and between vehicles and infrastructure (V2I). OMNET++ offers various modules, including those for the application layer, DSRC, and physical layer, ensuring realistic network behavior. (German Aerospace Center [DLR], 2024) is an open-source software toolkit designed to create simulations of traffic flow in urban environments. Facilitating communication between OMNET++ and SUMO (Ching et al., 2020), is a small patch called Traffic Control Interface (TraCI). This real-time interaction allows the two simulators to function seamlessly. The specific parameters used are shown in Table 1.

Table 1: Simulation Parameters

	Parameter	Value
Simulation Framework	Network Simulator	OMNET++ 5.6.2
	Traffic Simulator	SUMO 1.8.0
	V2X Simulator	VEINS 5.2
Simulation details	No. of Vehicles	50
	No. of RSUs	5
	Number of Malicious Nodes	Multiple of 5 from 0 to 40
	Simulation Time	600 sec
	Fake Message Start time	Random
	False Recommendation	Random
	Communication Range	250 m
	Vehicle Maximum Speed	40.9 km/h
Protocols	MAC Protocol	IEEE 802.11p
	Network Protocol	IEEE 1609.4 (WAVE)
	Radio Propagation Model	Simple Path Loss
	Data Size	1024 bits
	Header Size	256 bits

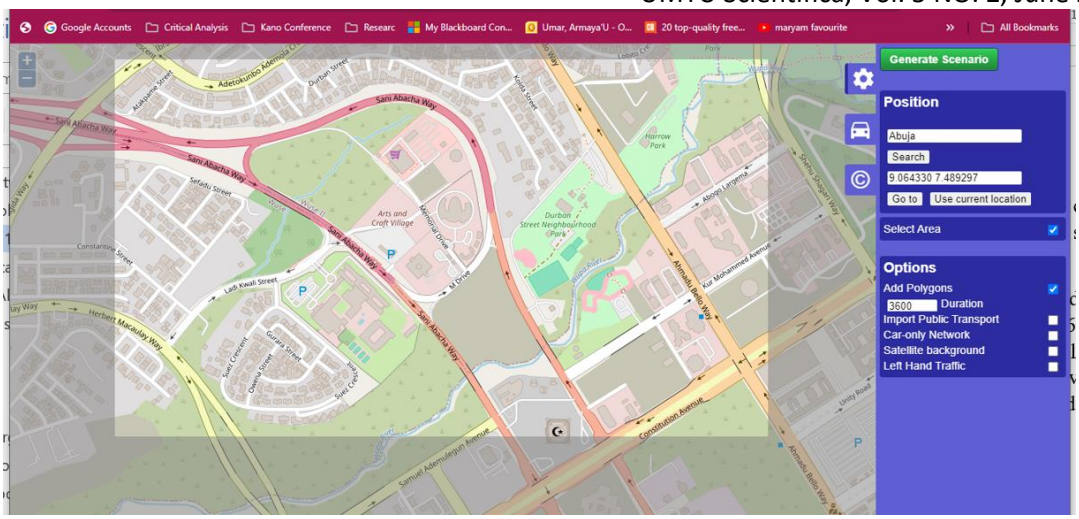

Figure 2: Selected area in Abuja, Nigeria

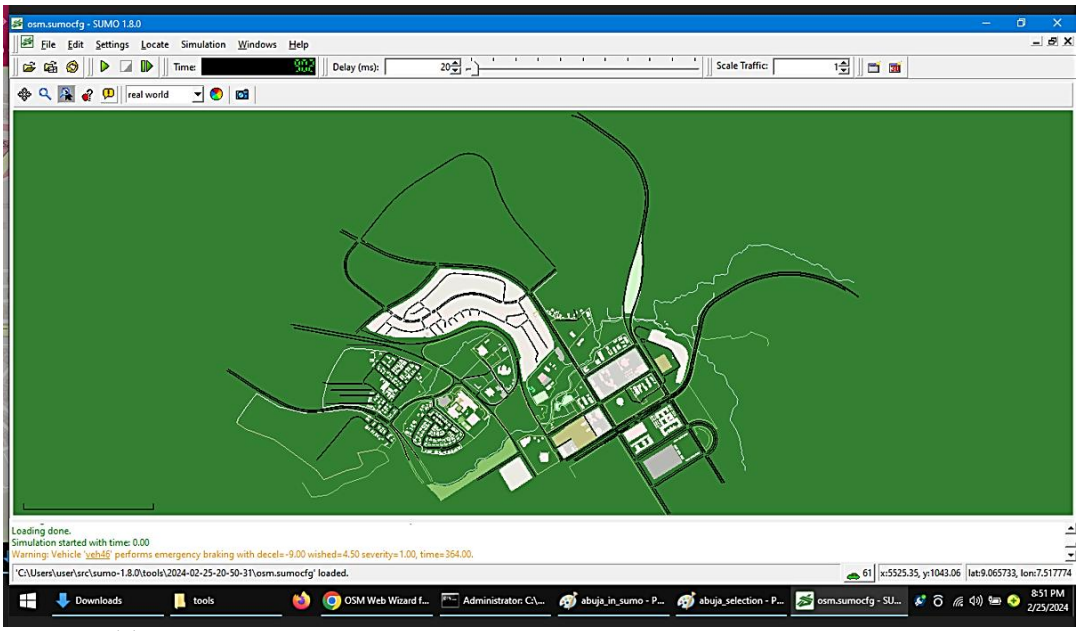

Figure 3: Traffic data of Abuja imported into SUMO

In this study, as shown in Figure 2, a traffic scenario in Abuja, Nigeria, was captured using SUMO software. The chosen location for the simulation has coordinates of latitude 9.064330 and longitude 7.489297. The data captured was made possible with (OpenStreetMap contributors, 2025) integration with SUMO.
The obtained geographic data was imported into SUMO (see Figure 3) to create a digital representation of the road network, including lanes, intersections, and traffic lights. The traffic flow data was used to define vehicle types, routes, and turning movements within the network.

Evaluation Metrics

To assess VANET performance in the presence of attackers, we adopted evaluation criteria specifically tailored to detect and mitigate blackhole attacks within VANET (Dhanaraj et al., 2022). These criteria include:

i. **End-to-End Delay (E2ED):** End-to-end delay quantifies the time it takes for packets generated by legitimate nodes to be transmitted to neighboring nodes. E2ED is determined by calculating the difference between the packet delivery time (PD) and the packet transmission time (TT), expressed as follows: Delay = PD –TT.

ii. **Convergence Rate:** This metric measures how quickly the system reaches a consensus or stabilizes after a disruptive event, indicating the system's responsiveness and adaptability. Convergence can be defined as follows: ∀vj ∈ MG, ∃a path from v1 to vj in the graph G = (V, E). Where v1 is the source vehicle, and vj represents each vehicle in the multicast group MG. This condition states that for each vehicle vj in the multicast group, there exists a path in the graph G from the source vehicle v1 to vj.

iii. **Event Detection Ratio:** Event Detection Ratio (EDP) refers to the percentage of events successfully detected by the system. A higher EDP indicates better effectiveness in identifying relevant events.

iv. **Content Delivery Ratio (CDR):** quantifies the effectiveness of message delivery in VANETs. It measures the proportion of messages successfully

received by legitimate vehicles compared to the total expected messages within the network.

Let MD denote the number of delivered messages, and MPRE denote the number of messages expected to be received within the network. Then, the CDR is determined by the formula: CDR=MD/ MREMR

v. **Packet Loss Ratio (PLR):** PLR is a vital metric used to assess the impact of blackhole nodes on message delivery within VANETs. It quantifies the proportion of messages lost due to blackhole attacks out of the total number of messages transmitted. Here's how PLR is calculated:

Let MT denote the total number of messages transmitted, out of which ML messages are lost. Then, the PLR is determined by the formula: PLR=MTML

12. Computation overhead

Computation overhead is a crucial consideration in blackhole detection and mitigation in VANET.

RESULTS AND DISCUSSION

End-to-End Delay

The ETMF (Figure 4) achieved up to a 25% reduction in end-to-end delay compared to FIDS-HMM. This improvement reflects the framework's ability to rapidly detect and isolate blackhole nodes, minimizing message rerouting and transmission delays.

The reduction in end-to-end delay is primarily due to ETMF's early isolation of blackhole nodes at the local trust layer, which prevents repeated route discovery and packet retransmission. Unlike FIDS-HMM, which relies on delayed probabilistic classification, ETMF uses real-time neighbour behaviour analysis combined with RSU verification, allowing faster routing decisions and reduced packet rerouting overhead.

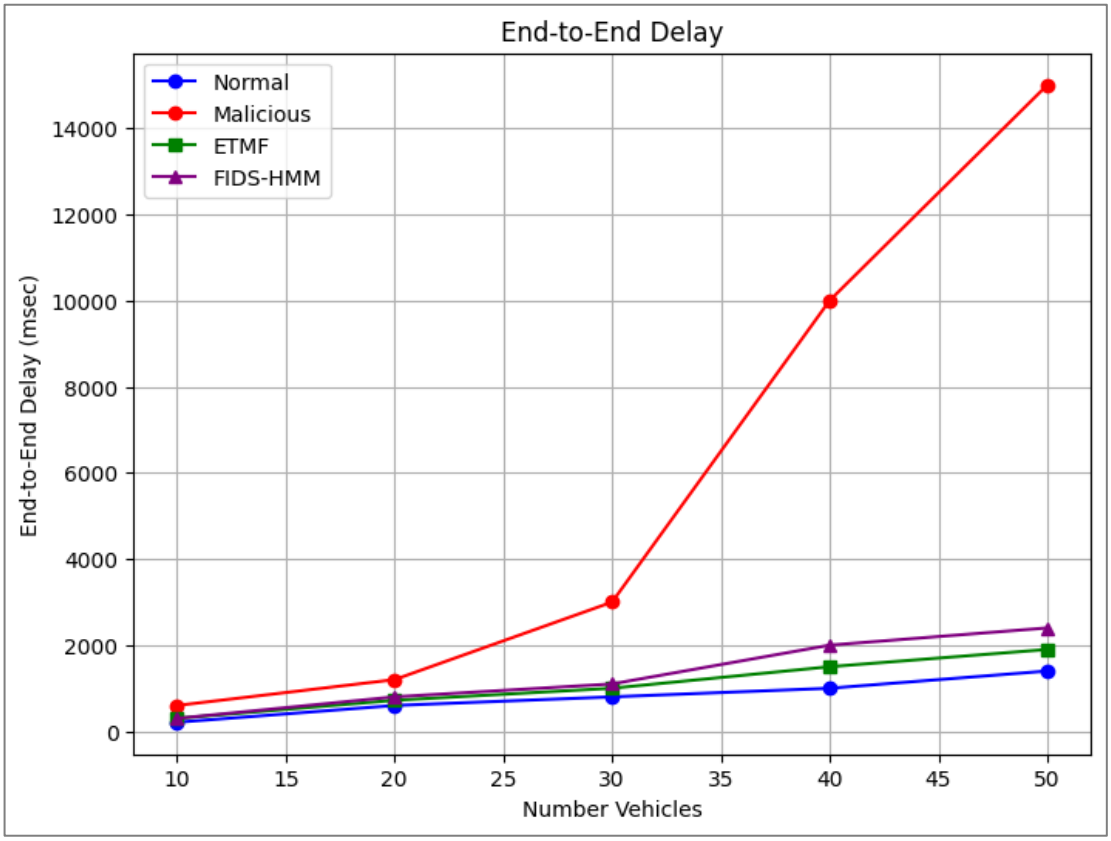

Figure 4: End-to-end delay: ETMF against TEAM and normal network

Anomaly Detection Ratio

ETMF demonstrated superior anomaly detection rates (Figure 5), outperforming FIDS-HMM by 8% under varying attack conditions. This improvement is attributed to ETMF's dynamic threshold adjustments, which enhance its sensitivity to blackhole behaviors (Ravula et al., 2024).

Convergence Rate and Detection Rate

ETMF achieved a convergence rate that outperformed FIDS-HMM, even with substantial malicious node presence (Figure 6). Detection rates varied between 2.06% and 8.33% above FIDS-HMM, underscoring ETMF's robustness in maintaining network integrity.

The improved convergence behaviour is attributed to RSU-assisted global trust aggregation, which consolidates local trust observations from multiple vehicles. This reduces inconsistent trust updates and accelerates stabilization of the network trust state, especially under varying malicious-node densities (Shokrollahi & Dehghan, 2025).

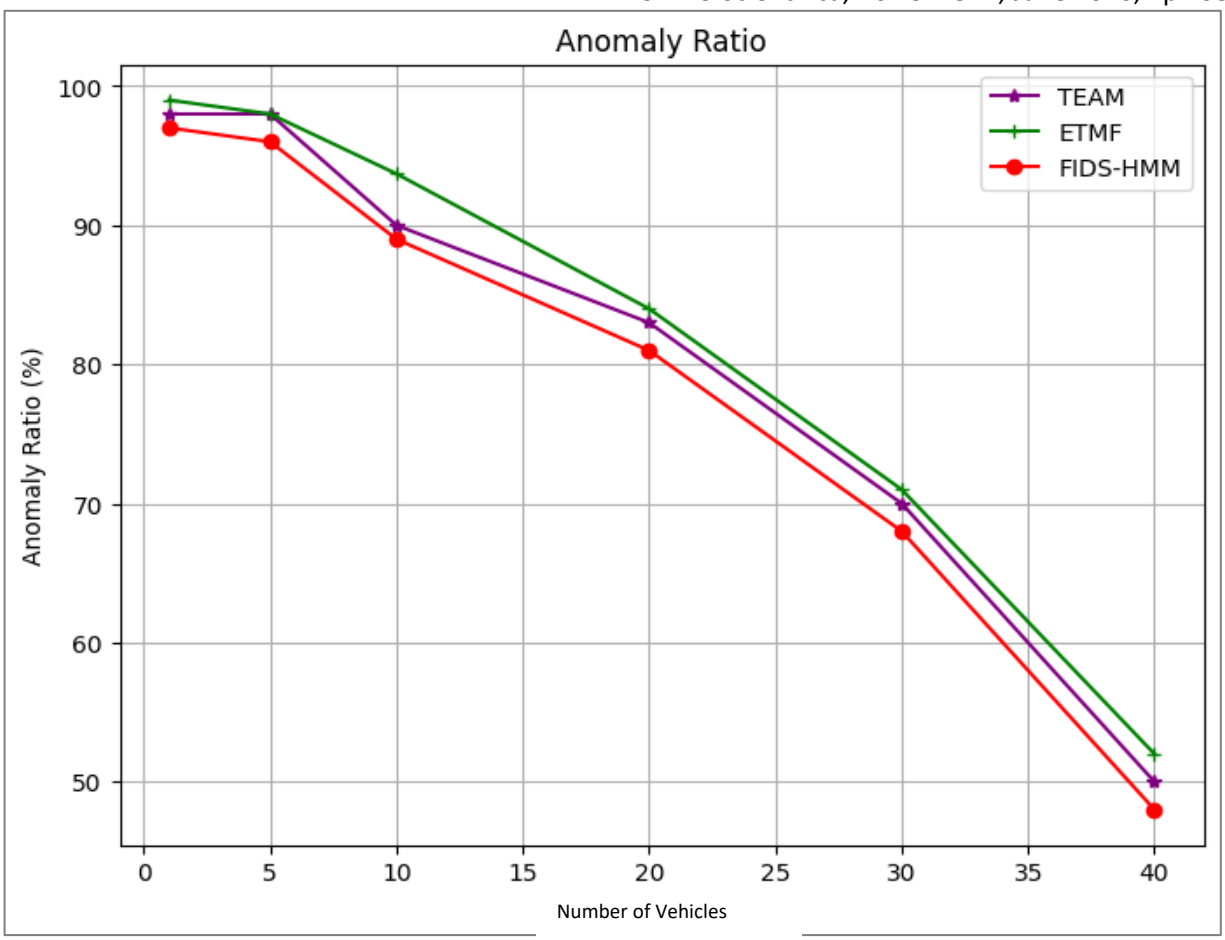

Figure 5: Anomaly Detection ratio

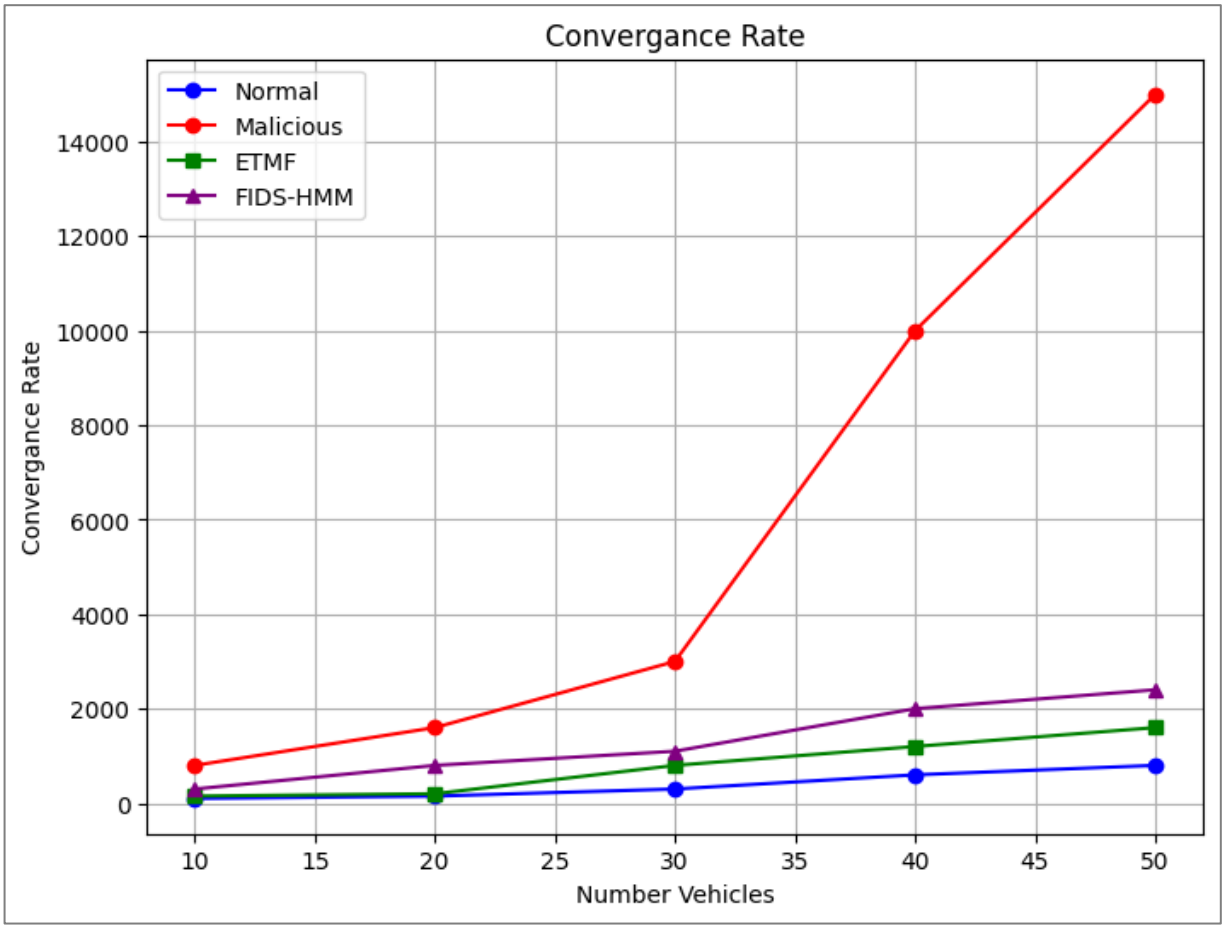

Figure 6: Convergence Rate: ETMF against normal network and network with malicious vehicles.

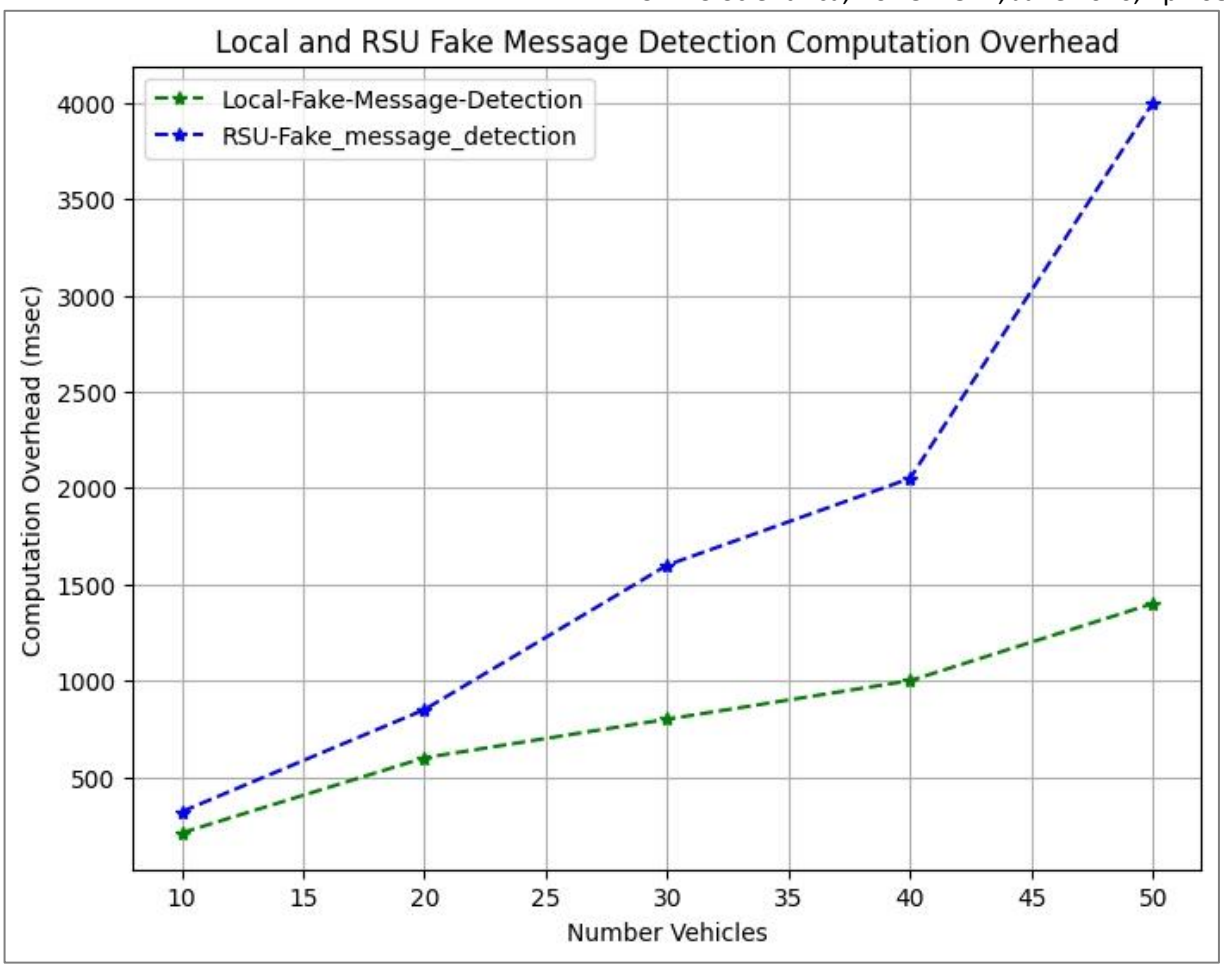

Figure 7: Local and RSU Fake Message Detection

The ETMF framework introduces moderate computational overhead due to dual-layer trust evaluation (Figure 7). Local trust computation operates with O(n) complexity per node, where n is the number of neighbouring vehicles. RSU-based aggregation introduces additional O(k) complexity, where k represents vehicles under RSU coverage. However, selective trust updates reduce unnecessary computations, ensuring scalability compared to FIDS-HMM.

Computation Overhead

The results demonstrated that the ETMF significantly outperforms the existing FIDS-HMM framework in various aspects. Compared with recent VANET trust-based intrusion detection models such as Zhao et al. (2024) and Rashid et al. (2023), ETMF demonstrates improved balance between detection accuracy and computational efficiency. While some models achieve similar detection rates, they often suffer from scalability limitations under high node mobility. However, ETMF performance may degrade under conditions of high collusion among malicious nodes or sparse RSU deployment, where global trust validation becomes less effective.

Specifically, the ETMF exhibited a 25% reduction in end-to-end delay, an 8% improvement in anomaly detection, and a higher detection rate (ranging from 2.06% to 8.33%) across different conditions. Furthermore, the ETMF exhibited scalable performance, converging faster than FIDS-HMM even in the presence of significant malicious activity, while maintaining computational efficiency.

The evaluation of ETMF is based on simulation using OMNeT++, SUMO, and VEINS, which may not fully represent real-world wireless channel variability. The study focuses exclusively on blackhole attacks and does not consider composite or hybrid attack scenarios such as Sybil–blackhole combinations. In addition, statistical validation using repeated simulation runs and confidence intervals was not performed. Finally, ablation analysis of individual ETMF components was not included and is identified as future work.

CONCLUSION AND FUTURE WORK

The Enhanced Trust Management Framework (ETMF) presents a robust solution to mitigating blackhole attacks in VANETs. By incorporating advanced trust computation, dynamic threshold adjustments, and collaboration between RSUs and vehicles, the ETMF enhances the security and reliability of VANETs in real-time. The framework's ability to scale effectively, detect attacks swiftly, and maintain manageable computational overhead positions it as a promising approach for future VANET security solutions.

This novel approach also offers a significant advancement over existing trust management frameworks for VANETs by improving detection accuracy, and reducing end-to-end

delay. By leveraging a hybrid approach combining local and global trust evaluations, ETMF remains adaptable and scalable, even as the number of malicious nodes increases.

Further research is needed to optimize the framework's convergence time and improve detection ratios, particularly as the network scale and number of malicious vehicles increase.

Also to focus on optimizing ETMF's convergence time and enhancing event detection ratios, especially for high-density networks with increased malicious vehicle activity. These improvements are crucial for further enhancing VANET security and ensuring real-time applicability in increasingly complex vehicular networks. Future work will focus on extending ETMF to multi-attack scenarios, performing ablation analysis, and incorporating statistical validation for stronger experimental robustness.

REFERENCE

A, B., & Ravindran, S. (2024). Intelligent fuzzy logic based intrusion detection system for effective detection of black hole attack in WSN. *Peer-to-Peer Networking and Applications*, (0123456789). [Crossref]

Abbasi, M., Al-Momani, L., Al-Khatib, O., & Elkhouly, A. (2026). Intrusion Detection in VANETs: A Comparative Study of Machine Learning and Deep Learning Models. *Lecture Notes in Networks and Systems*. [Crossref]

Ahmad, F., Adnane, A., Franqueira, V. N. L., Kurugollu, F., & Liu, L. (2018). Man-in-the-middle attacks in vehicular ad-Hoc networks: Evaluating the impact of attackers' strategies. *Sensors (Switzerland)*, *18*(11), 1–19. [Crossref]

Ahmad, F., Franqueira, V. N. L., & Adnane, A. (2018). TEAM: A Trust Evaluation and Management Framework in Context-Enabled Vehicular Ad-Hoc Networks. *IEEE Access*, *6*(3), 28643–28660. [Crossref]

Al-Shareeda, M. A., & Manickam, S. (2023). A Systematic Literature Review on Security of Vehicular Ad-Hoc Network (VANET) Based on VEINS Framework. *IEEE Access*. [Crossref]

Aminu, A. A., & Nura, A. (2025). Improved Fast Mobile IPv6 Scheme with Optimized Distributed Signaling Utilizing Media Independent Handover and Efficient Link Layer Triggers. *UMYU Scientifica*, *4*(2), 396–404. [Crossref]

Cheong, C., Song, Y., Cao, Y., Zhang, Y., Cai, B., & Ni, Q. (2024). Multidimensional Trust Evidence Fusion and Path-Backtracking Mechanism for Trust Management in VANETs. *IEEE Internet of Things Journal*. [Crossref]

Ching, B., Amoozadeh, M., Chuah, C. N., Zhang, H. M., & Ghosal, D. (2020). Enabling performance and security simulation studies of intelligent traffic signal light control with VENTOS-HIL. *Vehicular Communications*. [Crossref]

Dhanaraj, R. K., Islam, S. H., & Rajasekar, V. (2022). A cryptographic paradigm to detect and mitigate blackhole attack in VANET environments. *Wireless Networks*. [Crossref]

Habbal, A., Ali, M. K., & Abuzaraida, M. A. (2024). Artificial Intelligence Trust, Risk and Security Management (AI TRiSM): Frameworks, applications, challenges and future research directions. In *Expert Systems with Applications*. [Crossref]

Ibrahim, Y. (2022). Sampling of thermodynamic systems with neural network surrogates. *UMYU Scientifica*, *1*(1), 336–341. [Crossref]

Isiyaku, H., Aliyu, M. S., & Muaazu, A. A. (2024). Early Address Detection: A Soft Vertical Handover Approach in Proxy Mobile IPv6. *UMYU Scientifica*, *3*(4), 36–45. [Crossref]

Ismail, S., Dawoud, D. W., & Reza, H. (2023). Securing Wireless Sensor Networks Using Machine Learning and Blockchain: A Review. In *Future Internet*. [Crossref]

Li, J., Rombaut, E., & Vanhaverbeke, L. (2021). A systematic review of agent-based models for autonomous vehicles in urban mobility and logistics: Possibilities for integrated simulation models. *Computers, Environment and Urban Systems*. [Crossref]

Li, Z., Fang, W., Zhu, C., Gao, Z., & Zhang, W. (2023). AI-Enabled Trust in Distributed Networks. *IEEE Access*. [Crossref]

Lone, F., Verma, H. K., & Sharma, K. P. (2024). A systematic study on the challenges, characteristics and security issues in vehicular networks. *International Journal of Pervasive Computing and Communications*. [Crossref]

Mahrez, Z., Sabir, E., Badidi, E., Saad, W., & Sadik, M. (2022). Smart Urban Mobility: When Mobility Systems Meet Smart Data. *IEEE Transactions on Intelligent Transportation Systems*. [Crossref]

Muhammad, M. Y., & Umar, D. M. (2023). Resource Limitations for Wireless Sensor Networks to Establish a Comprehensive Security System in the 5G Network. *UMYU Scientifica*, *2*(2), 44–52. [Crossref]

Ogbe, S. M., & Abubakar, A. A. (2025). An Efficient Neural Architecture Search Algorithm for AutoEncoder Optimization - A Systematic Literature Review. *UMYU Scientifica*, *4*(3), 9–18. [Crossref]

Rashid, K., Saeed, Y., Ali, A., Jamil, F., Alkanhel, R., & Muthanna, A. (2023). An Adaptive Real-Time Malicious Node Detection Framework Using Machine Learning in Vehicular Ad-Hoc Networks (VANETs). *Sensors*. [Crossref]

Ravula, P. K., Uppalapati, S., & Karri, G. R. (2024). An early detection and prevention of wormhole attack using dynamic threshold value in VANET. *International Journal of Vehicle Information and Communication Systems*. [Crossref]

Raza, A., Iqbal, Z., & Aadil, F. (2023). UAV-assisted ubiquitous communication architecture for urban VANET environment. *Journal of Supercomputing*. [Crossref]

Sarwatt, D. S., Lin, Y., Ding, J., Sun, Y., & Ning, H. (2024). Metaverse for Intelligent Transportation Systems

(ITS): A Comprehensive Review of Technologies, Applications, Implications, Challenges and Future Directions. *IEEE Transactions on Intelligent Transportation Systems*. [Crossref]

Shokrollahi, S., & Dehghan, M. (2025). CTVAN: a cooperation-based RSU-assisted trust management model for reliable communication in VANETs. *Cluster Computing*. [Crossref]

Sultan, S., Javaid, Q., Malik, A. J., Al-Turjman, F., & Attique, M. (2022). Collaborative-trust approach toward malicious node detection in vehicular ad hoc networks. *Environment, Development and Sustainability*. [Crossref]

Varma, I. M., & Kumar, N. (2023). A comprehensive survey on SDN and blockchain-based secure vehicular networks. In *Vehicular Communications*. [Crossref]

Wlazlo, P., Sahu, A., Mao, Z., Huang, H., Goulart, A., Davis, K., & Zonouz, S. (2021). Man-in-the-middle attacks and defence in a power system cyber-physical testbed. *IET Cyber-Physical Systems: Theory and Applications*. [Crossref]

Zhao, J., Huang, F., Liao, L., & Zhang, Q. (2024). Blockchain-Based Trust Management Model for Vehicular Ad Hoc Networks. *IEEE Internet of Things Journal*. [Crossref]