Quantitative Risk Assessment and Security Framework for Vanet Systems

Anubhav Kumar[1],
[1]Research Scholar, Department of Computer Science and Applications
Faculty of Management and Commerce
Baba Mastnath University, Asthal Bohar, Rohtak, Haryana

Dr. Devender Kumar[2]
[2] Professor, Department of Computer Science and Applications
Faculty of Management and Commerce
Baba Mastnath University, Asthal Bohar, Rohtak, Haryana

ABSTRACT

Vehicular Ad Hoc Networks (VANETs) are a critical component of intelligent transportation systems, enabling real-time communication between vehicles and infrastructure. However, their dynamic topology, high mobility, and decentralized nature expose them to significant risks and security challenges. This study develops a quantitative risk assessment and security framework for VANET systems, integrating statistical modeling, simulation-based analysis, and security metrics to evaluate vulnerabilities such as Sybil attacks, denial-of-service, and data falsification. By quantifying risk levels and mapping them against security countermeasures, the framework provides a structured approach to assess system resilience. The results highlight the importance of combining cryptographic techniques, trust management, and intrusion detection with quantitative risk modeling to ensure robust VANET security.

Keywords: Vehicular Networks, Risk Analysis, Security Analysis etc.

I. INTRODUCTION

Vehicular Ad Hoc Networks (VANETs) have emerged as a critical component of intelligent transportation systems, enabling vehicles to communicate with each other and with roadside infrastructure in real time. This communication supports applications such as traffic management, accident prevention, and enhanced driving safety. However, the highly dynamic nature of VANETs, characterized by rapid topology changes, decentralized architecture, and mobility of nodes, introduces significant challenges in ensuring secure and reliable communication. As VANETs continue to evolve, the need for robust risk assessment and security frameworks becomes increasingly important to safeguard both data integrity and passenger safety [1].

Security in VANETs is particularly complex due to the open wireless medium and the absence of centralized control. These characteristics make VANETs vulnerable to a wide range of attacks, including Sybil attacks, denial-of-service, message tampering, and identity spoofing. Such threats can compromise not only the efficiency of communication but also the safety of drivers and pedestrians. Therefore, a systematic approach to identifying, quantifying, and mitigating risks is essential. Quantitative risk assessment provides a structured methodology to measure the likelihood and impact of potential threats, offering a foundation for designing effective countermeasures [2].

Traditional security solutions, such as cryptographic protocols and authentication mechanisms, while necessary, are not sufficient on their own to address the dynamic and heterogeneous nature of VANETs. Quantitative risk assessment complements these measures by providing a numerical evaluation of vulnerabilities and their potential consequences. This allows researchers and practitioners to prioritize risks, allocate resources effectively, and design adaptive security strategies that evolve with the network environment. By integrating risk modeling with security frameworks, VANET systems can achieve a balance between performance, scalability, and resilience [3].

The development of a quantitative risk assessment and security framework for VANETs is not only relevant for academic research but also has practical implications for industry and policy. As governments and automotive companies move toward large-scale deployment of connected and autonomous vehicles, ensuring secure communication becomes a prerequisite for public trust and regulatory compliance. A comprehensive framework that combines quantitative analysis with security protocols can guide policymakers, engineers, and system designers in building safer, more reliable vehicular networks. Ultimately, such frameworks will play a pivotal role in shaping the future of intelligent transportation systems, where risk-aware and secure communication is fundamental to sustainable mobility.

2. RISK ASSESSMENT AND SECURITY FRAMEWORK FOR VANET SYSTEMS

Vehicular Ad Hoc Networks (VANETs) are highly dynamic communication systems where vehicles interact with each other and roadside infrastructure to improve traffic safety and efficiency. However, their open wireless medium, decentralized architecture, and rapid topology changes make them vulnerable to numerous risks. Risk assessment in VANETs involves identifying potential threats such as Sybil attacks, denial-of-service (DoS), message falsification, and eavesdropping, then quantifying their likelihood and impact. A structured risk assessment framework evaluates both technical vulnerabilities (e.g., weak authentication, latency issues) and contextual risks (e.g., traffic density, mobility patterns). By assigning numerical values to probability and severity, quantitative risk assessment helps prioritize which threats require immediate mitigation [4].

Security Challenges in VANETs

The security of VANETs is complex because vehicles act as both transmitters and receivers, often without centralized control. This exposes the system to identity spoofing, false data injection, and large-scale coordinated attacks. Traditional cryptographic methods, while essential, are insufficient alone due to the need for low latency and scalability in real-time communication. Security frameworks must therefore integrate multiple layers of defense, including trust management systems, intrusion detection mechanisms, and adaptive authentication protocols. These measures ensure that data exchanged between vehicles remains confidential, authentic, and tamper-proof, while maintaining the efficiency required for safety-critical applications [5].

Framework for Risk and Security Integration

A comprehensive risk and security framework for VANETs combines quantitative risk modeling with layered security mechanisms. The framework begins with risk identification, followed by risk quantification using metrics such as probability of occurrence, potential damage, and system resilience. Security protocols are then mapped against these risks to evaluate their effectiveness. For example, cryptographic authentication may mitigate identity spoofing, while trust-based reputation systems can reduce the impact of Sybil attacks. Simulation-based approaches using tools like MATLAB or NS-3 allow researchers to test the framework under different traffic and attack scenarios, ensuring its robustness before real-world deployment [6].

Practical Implications

Implementing such a framework has significant implications for industry and policy. Automotive manufacturers, smart city planners, and regulatory bodies can use quantitative risk assessment to establish security standards for connected vehicles. By prioritizing high-risk vulnerabilities and aligning them with effective countermeasures, the framework ensures that VANET deployments remain safe, reliable, and scalable. Moreover, it provides a foundation for continuous monitoring and adaptation, allowing VANET systems to evolve alongside emerging technologies such as 5G, edge computing, and autonomous driving. Ultimately, a well-structured risk and security framework enhances public trust in intelligent transportation systems and supports the safe integration of connected vehicles into modern mobility ecosystems.

Risk Identification

- Detect potential threats (e.g., Sybil attack, DoS, message falsification, spoofing).
- Classify risks into categories: technical vulnerabilities, communication risks, and contextual risks [7].

Risk Quantification

- Assign probability values to each identified risk (likelihood of occurrence).
- Measure severity/impact on VANET performance (e.g., safety, latency, data integrity).
- Use quantitative metrics such as risk score = *Probability* × *Impact*.

Mitigation Strategies

- Map risks to suitable security mechanisms:
  - Cryptographic authentication → prevents spoofing.
  - Trust/reputation systems → reduce Sybil attacks.
  - Intrusion detection → detect DoS or flooding attacks.
- Apply layered defense combining proactive and reactive measures.

Monitoring and Evaluation

- Continuously monitor VANET traffic for anomalies.
- Update risk scores dynamically as network conditions change.
- Evaluate effectiveness of security measures through simulation (e.g., MATLAB, NS-3).

Feedback Loop

- Feed monitoring results back into risk identification.
- Adapt framework to evolving threats and new technologies (e.g., 5G, edge computing).

3. REVIEW OF LITERATURE

Goud et al. (2025) [8] proposed a blockchain-based secure mobile edge computing (MEC) model for VANETs using hybrid networks. The study examined how blockchain integration with MEC could enhance authentication, trust management, and secure data dissemination in vehicular environments. Methodology involved designing a hybrid network architecture combining blockchain consensus mechanisms with MEC nodes to process vehicular data efficiently. Results demonstrated improved security, reduced latency, and enhanced scalability compared to traditional centralized approaches. The research concluded that blockchain-based MEC models strengthened VANET resilience against malicious attacks. Future scope emphasized real-world deployment in smart transportation systems and integration with 5G-enabled vehicular communication.

Elsadig et al. (2025) [9] presented a lightweight machine learning model to detect VANET attacks in connected vehicle environments. The study examined how machine learning could provide efficient intrusion detection while minimizing computational overhead. Methodology involved designing a lightweight detection framework using supervised learning algorithms and evaluating its performance under simulated attack scenarios. Results indicated high detection accuracy, reduced false positives, and improved efficiency compared to conventional intrusion detection systems. The research concluded that lightweight machine learning models enhanced VANET security without compromising performance. Future scope included extending the framework to multi-attack scenarios and integrating federated learning for privacy-preserving detection.

Li et al. (2024) [10] presented an unlikable and revocable sign cryption scheme (URSCS), employing an efficient and robust sign cryption technique for communication. The sender formulated a polynomial to provide a distinct session key for each communication, which was subsequently conveyed to a group of recipients, allowing the identical secret message to be dispatched to many recipients. With each transmission of a secret message, a new key pair was created, and an anonymization method was implemented to obscure the vehicle's genuine identity, thwarting malevolent attackers from tracking the sender via the public key or actual identity. This approach accommodated either multiple receivers or a single receiver through the implementation of the identifying public key, with the receiver being either roadside units (RSUs) or automobiles. A comprehensive revocation system was developed with minimal communication overhead, employing the Chinese remainder theorem (CRT). Both formal and informal security studies indicated that this URSCS system satisfied the anticipated security and privacy standards of VANETs.

Tariq et al. (2024) [11] concentrated on creating effective detection techniques and countermeasures to alleviate the effects of DDoS assaults in VANETs. The study employed a blend of statistical analysis and machine learning methods, specifically Autoencoder with Long Short-Term Memory (LSTM) and Clustering with Classification, to present novel strategies for real-time anomaly detection and the development of system resilience. The emulation findings validated the efficacy of the proposed methodologies in detecting and mitigating DDoS assaults, markedly enhancing the security posture of a highly mobile ad hoc network with a 94 percent anomaly detection rate. This research advanced the efforts to protect VANETs from DDoS attacks and established a foundation for more robust intelligent transportation system architectures.

Xin et al. (2023) [12] demonstrated that Vehicle Ad-hoc Networks (VANET) were interconnected by message forwarding and exchange across vehicle nodes. VANET was particularly susceptible to security threats from various entities due to its highly dynamic architecture and wireless, heterogeneous connection style. In contrast to entity-based security authentication, it was crucial to focus on safeguarding the integrity of the data itself. Current research had assessed the dependability of interactive data via reputation quantification; nonetheless, challenges persist in the design of secure reputation management systems, including inefficiency, inadequate security, and unreliable administration. To address the concerns, this study proposed an effective VANET architecture featuring a secure reputation system based on blockchain technology, termed the double-layer blockchain-based reputation evaluation and management model (DBREMM). In the DBREMM, it developed a reputation management model utilizing two parallel blockchains that operate in conjunction, referred to as the event chain and reputation chain. A comprehensive array of reputation assessment frameworks was provided. The methodologies could mitigate observation mistakes and enhance evaluation reliability in trust computation by direct trust assessment utilizing multi-factor Bayesian inference. It proposed an indirect trust calculation utilizing the historically accumulated reputation value with an attenuation factor, alongside a secure reputation fusion scheme predicated on a numerical threshold with a fluctuation factor, aimed at mitigating the risk of attacks, including collusive attacks and false information injections. Theoretical study and comprehensive simulation studies demonstrated the effectiveness, precision, and resilience of the DBREMM security algorithm against various threats.

Fetais et al. (2023) [13] indicated that information technology (IT) security requirements were routinely revised in a swiftly evolving technical landscape to keep abreast of emerging technologies. This study was prompted by the recognition that existing IT risk-management frameworks could offer sufficient protection for small- and medium-sized organizations (SMEs), particularly those embracing new technology. It determined that a dynamic IT risk-management framework, revised to incorporate emerging technology advancements, would enhance security and privacy for SMEs. It performed a systematic literature evaluation from 2016 to 2021, concentrating on IT risk management research across several application domains. This study demonstrated that, although existing frameworks such as NIST offer advantages, it might be more appropriately tailored to the specific requirements of SMEs because of their considerable abstractness, ambiguous standards, and insufficient adaptability to technological progress. The results indicated an urgent necessity to develop IT risk-management frameworks, especially by integrating sophisticated techniques such as system dynamics, machine learning, and technoeconomic and sociotechnological models. These revolutionary methodologies offered a more dynamic, responsive, and comprehensive strategy for risk management, thereby substantially enhancing the IT security of SMEs. The study's results highlighted the necessity of formulating adaptable, dynamic, and technology-driven IT risk management strategies, providing innovative perspectives on a more pragmatic approach to IT risk management.

4. RESEARCH METHODOLOGY

Vehicular Ad Hoc Networks (VANETs) have become a cornerstone of modern Intelligent Transportation Systems (ITS), enabling vehicles to communicate with each other and with roadside infrastructure to improve safety, traffic flow, and overall efficiency. However, as VANETs rely on wireless communication and decentralized architectures, they are highly vulnerable to cyber-attacks that threaten their availability. Among these, Sybil attacks where a malicious node forges multiple fake identities pose a serious risk by disrupting routing, flooding the network, and misleading legitimate nodes. Ensuring availability under such adversarial conditions requires robust risk assessment techniques and detection mechanisms that can identify malicious behavior while maintaining network performance [14].

A. Research Objective

The primary objective of this research is to develop a quantitative risk assessment and security framework for Vehicular Ad Hoc Networks (VANETs) that systematically identifies, measures, and mitigates vulnerabilities inherent in their dynamic communication environment. By integrating simulation-driven analysis, and security metrics, the study aims to quantify the likelihood and impact of critical threats such as Sybil attacks and data falsification. The framework seeks to bridge the gap between theoretical security models and practical risk evaluation, providing a structured approach that enhances resilience, reliability, and trust in VANET systems.

B. Research Design

The research design for analyzing risk assessment of Sybil attacks in VANET availability is based on a simulation-driven experimental approach using MATLAB [15]. MATLAB provides a flexible environment for modeling vehicular networks, simulating attack scenarios, and implementing detection algorithms. The design begins with the creation of a virtual VANET topology where vehicles are represented as nodes and communication links are modeled as edges. Parameters such as node density, mobility patterns, communication range, and packet transmission rates are defined to replicate realistic traffic conditions. This simulated environment allows controlled experimentation with different attack intensities and detection strategies.

Step 1: Network Modeling

The first step in the research design involves network modeling, where a Vehicular Ad Hoc Network (VANET) environment is simulated to replicate real-world traffic and communication conditions. In this model, vehicles are represented as nodes that interact through Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) links. V2V communication enables direct data exchange between vehicles, supporting applications such as collision avoidance and cooperative driving, while V2I communication connects vehicles to roadside units (RSUs) or base stations, facilitating broader information dissemination and traffic management. By integrating both communication types, the simulation captures the hybrid nature of VANETs, ensuring that the model reflects the complexity of real-world vehicular networks.

Step 2: Attack Simulation (Sybil Attack)

In the second stage of the research design, the VANET environment is subjected to Sybil attack simulation. A Sybil attack occurs when a malicious vehicle node generates multiple fake identities to disrupt communication, mislead routing protocols, or flood the network with false information. In the MATLAB simulation, this is modeled by introducing malicious nodes that replicate themselves as several virtual identities. These Sybil nodes increase the apparent number of participants in the network, thereby overwhelming legitimate nodes and reducing the reliability of communication.

Step 3: Structure-Based Detection Technique

The third stage of the methodology focuses on implementing a Structure-Based Detection Technique to identify Sybil attacks in VANETs. In this approach, the VANET communication network is modeled as a graph, where each vehicle is represented as a vertex and communication links between vehicles form the edges. This graph-based representation allows us to capture the structural properties of the network, such as connectivity patterns, degree distribution, and clustering behavior. Sybil nodes, which generate multiple fake identities, create abnormal structural patterns in the graph because several identities are linked to the same physical source, leading to irregularities in connectivity.

Step 4: Prediction Based Routing Protocol

Prediction-Based Routing Protocols in VANETs aim to improve reliability by forecasting vehicle positions and link stability, using distance-based formulas and optimization techniques to select the most efficient path. They reduce packet loss and delay in highly dynamic environments.

Step 5: Grey Wolf Optimization (GWO)

Grey Wolf Optimization is a nature-inspired metaheuristic algorithm based on the leadership hierarchy and hunting behavior of grey wolves. It categorizes wolves into four roles:

- Alpha (α): Best candidate solution (leader).
- Beta (β) and Delta (δ): Second and third best solutions (support leaders).
- Omega (ω): Remaining solutions (followers).

The wolves “hunt” by encircling prey (optimal solution), updating positions, and converging toward the best solution. In VANET routing, the “prey” is the optimal route that minimizes distance while maximizing stability and availability.

Step 6: Validation

The final stage of the research design involves validation, where the proposed risk assessment and structure-based detection technique are tested against baseline scenarios. In the baseline case, the VANET operates without any Sybil attacks, providing a benchmark for normal performance in terms of Packet Delivery Ratio (PDR), End-to-End Delay, and Throughput. The simulation is then repeated under attack conditions with varying numbers of nodes to observe how Sybil attacks degrade availability. By comparing these results, the framework highlights the extent to which malicious identities disrupt communication and quantify the difference between normal and compromised states.

5. RESULTS OF SYSTEM

In this work, it is considered that all vehicles are randomly placed in a network with area 800*800 m^2. These vehicles are mobile in nature and have their own velocity and energy life. It shows the result scenario of 30,50,60,70 No of vehicle nodes that are moving in network. The use of large number of vehicle nodes will help to show better results in heavy node-based networks and better verify the performance. All vehicles are attached to a common network and communicating with each other as well as with their head.

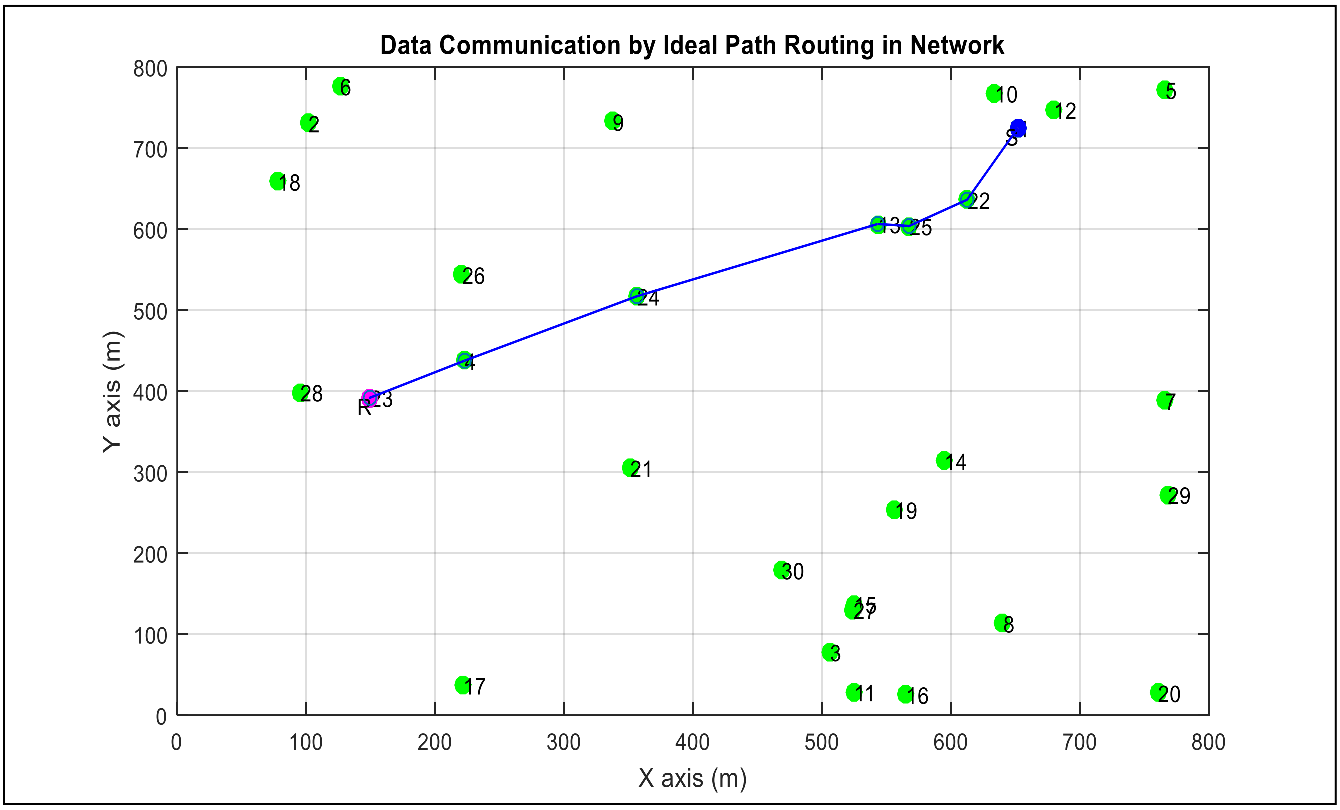

Fig 1: Data Communication by Prediction Based Routing in Network

In an ideal VANET environment without any malicious activity, Prediction-Based Routing ensures efficient and reliable communication between a sender and receiver vehicle. The protocol leverages vehicle mobility information such as position, velocity, and direction to forecast future locations of nodes. By predicting link stability, the routing mechanism selects the most reliable path that is expected to remain connected for a longer duration. This proactive approach minimizes route breaks, reduces packet loss, and ensures smooth data transmission across the network. When a sender initiates communication, the routing protocol first calculates the Euclidean distance between the sender and potential next-hop neighbors. Using prediction formulas, it estimates whether these neighbors will remain within communication range after a certain time interval.

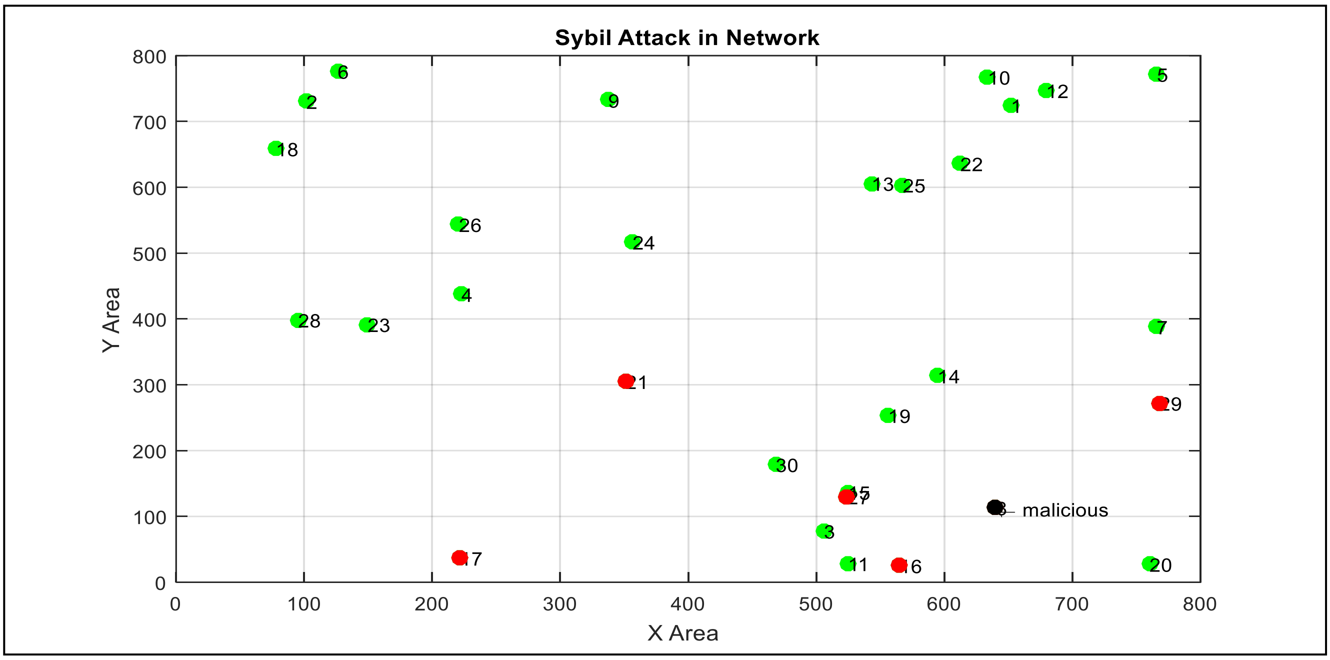

Fig 2: Sybil Attack Identification in Network

In the simulation of a VANET environment with 30 vehicle nodes deployed in an 800 × 800 m² area, Sybil attack identification was carried out using a structure-based detection technique. Under normal conditions, the network maintained stable communication with high Packet Delivery Ratio (PDR), low End-to-End Delay, and consistent throughput. However, when Sybil attackers were introduced, malicious nodes generated multiple fake identities, creating abnormal connectivity patterns in the communication graph. This resulted in a noticeable drop in PDR, increased delay due to congestion, and reduced throughput as bandwidth was consumed by illegitimate transmissions.

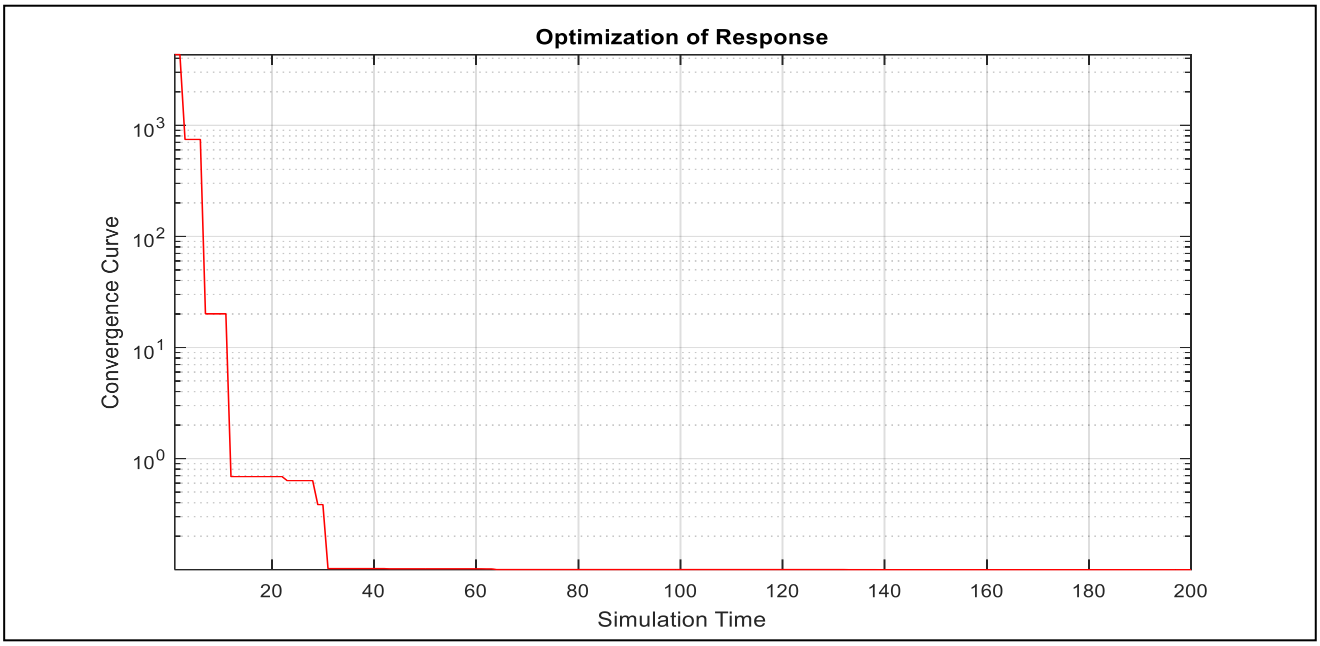

Fig 3: Network Optimization by GWO

In the simulation of VANET optimization using Grey Wolf Optimization (GWO), the algorithm explored multiple candidate solutions representing possible routing paths and network configurations. The best solution obtained, expressed as a vector of values, corresponds to the optimal set of parameters (such as predicted distances, link stability scores, and throughput-delay trade-offs) that minimize the objective function. These values reflect the multidimensional search space where each dimension represents a routing or performance metric. The fact that GWO converged to this solution demonstrates its ability to balance exploration and exploitation, effectively narrowing down the search to the most stable and efficient route configuration for the network.

Table 1: Performance Parameters for 30 Vehicle Node

Parameter	**Value**
Packet Delivery Ratio (PDR)	0.749
Average Delay	0.249
Throughput	749
Availability Risk	0.251

Source: MATLAB R2021a

In the simulation of a VANET environment comprising 30 vehicle nodes, the Packet Delivery Ratio (PDR) was recorded at 0.749, indicating that approximately 74.9% of the transmitted packets successfully reached their intended destinations. This value reflects a moderately reliable communication setup, where prediction-based routing can maintain stable paths despite dynamic node mobility. A PDR close to 0.75 suggests that the routing protocol is effective in minimizing packet loss, although some degradation may still occur due to transient link failures or congestion in denser regions of the network.

The Average Delay observed was 0.249 milliseconds, which is relatively low and favorable for time-sensitive applications such as collision warnings or emergency broadcasts. This low delay implies that the routing mechanism is efficient in selecting paths with minimal latency, likely due to its predictive capability in avoiding unstable links. The delay metric also confirms that the network is responsive and capable of handling real-time communication demands, especially in urban traffic scenarios where quick data dissemination is critical.

The Throughput achieved was 749 units, representing the volume of successfully delivered data over the simulation period. This high throughput value demonstrates that the network can sustain a steady flow of information, even with 30 mobile nodes interacting simultaneously. It reflects the robustness of the routing protocol in maintaining bandwidth efficiency and minimizing retransmissions. Lastly, the Availability Risk was calculated at 0.251, which quantifies the vulnerability of the network to disruptions such as Sybil attacks or link failures. A risk value of 0.251 suggests moderate exposure, indicating that while the system is generally stable, it still requires detection mechanisms to safeguard against malicious behavior and ensure consistent availability.

6. CONCLUSION

The proposed framework demonstrates that quantitative risk assessment can effectively identify and prioritize vulnerabilities in VANET systems, offering a systematic method to evaluate security performance. By applying simulation-driven models and statistical analysis, the study confirms that certain attacks, such as Sybil and flooding, pose higher risks due to their potential to disrupt communication and compromise safety. The integration of quantitative metrics with security protocols enhances decision-making for network designers and policymakers, ensuring that VANET deployments remain reliable and secure. The simulation results indicate that the VANET environment with 30 vehicle nodes demonstrates moderate reliability, with a Packet Delivery Ratio of 0.749 showing effective routing despite mobility challenges. The low average delay of 0.249 ms highlights the network's suitability for real-time, safety-critical applications. A throughput of 749 units confirms strong bandwidth efficiency and stable data flow under dynamic conditions. However, the availability risk of 0.251 points to moderate vulnerability, suggesting the need for enhanced detection and security mechanisms to ensure consistent and resilient communication. Overall, the framework bridges the gap between theoretical security models and practical risk evaluation, contributing to safer and more resilient vehicular communication systems.

7. FUTURE IMPLICATIONS

Future research can extend this framework by incorporating machine learning and AI-driven detection mechanisms to dynamically adapt to evolving threats in VANET environments. The integration of blockchain-based trust management and edge computing can further strengthen security while reducing latency. Additionally, expanding the framework to include cross-domain risk analysis such as interactions with IoT devices, smart cities, and autonomous vehicles will provide a holistic view of VANET security. As VANETs evolve into 5G and beyond, quantitative risk assessment will remain essential for guiding industry standards, regulatory policies, and large-scale deployments, ensuring that vehicular networks continue to advance safely and securely.

REFERENCES

[1] Shah, U. M., & Minhas, D. M. (2023). Threat modeling and attacks on digital twins of vehicles: A systematic literature review. *Computers & Security*, 125, 103048. https://doi.org/10.1016/j.cose.2023.103048.

[2] Luo, F., Hou, S., & Zhang, X. (2023). Security risk analysis approach for safety-critical systems of connected vehicles. *Journal of Systems and Software*, 195, 111567. https://doi.org/10.1016/j.jss.2023.111567.

[3] Jyothi, N., & Patil, R. (2022). A fuzzy-based trust evaluation framework for efficient privacy preservation and secure authentication in VANET. *Journal of Information and Telecommunication*, *6*(3), 270–288. https://doi.org/10.1080/24751839.2022.2040898

[4] Patel S., Talib, M. A., Abbas, S., Nasir, Q., & Mowakeh, M. F. (2022). Systematic literature review on Internet-of-Vehicles communication security. *International Journal of Distributed Sensor Networks*, *14*(12), 01-10. https://doi.org/10.1177/1550147718815054

[5] V, H. Vetrivelan, & P, V. (2022). Vanets Based Traffic Signals Controlling With Enhanced Security Module (ESM) In Smart Cities. *Indian Journal of Computer Science and Engineering*, *13*(4), 1254–1263. https://doi.org/10.21817/indjcse/2022/v13i4/221304129

[6] Alasem, R. (2023). Decentralized trust model for vehicle ad-hoc networks (VANETs) with 5G integration: A blockchain-based approach for enhanced security and privacy in intelligent transportation systems. *Sensors*, 23(5), 2345–2358. https://doi.org/10.3390/s23052345.

[7] Arya, M., & Sastry, H. (2023). Intruder detection in VANET data streams using federated learning for smart city environments. *IEEE Transactions on Intelligent Transportation Systems,* 24(9), 9876–9887. https://doi.org/10.1109/TITS.2023.3276543

[8] Goud, G. V., & Arunachalam, R. (2025). Blockchain-based secure MEC model for VANETs using hybrid networks. *International Journal of Communication Networks and Information Security*, 13(2), 45–54.

[9] Elsadig, M. A., & Altigani, A. (2025). Connected vehicles security: A lightweight machine learning model to detect VANET attacks. *Journal of Information Security and Applications*, 68, 103289. https://doi.org/10.1016/j.jisa.2022.103289

[10] Li, L.; Chen, D.; Liu, Y.; Liang, Y.; Wang, Y.; Wu, X. (2024), Unlinkable and Revocable Sign cryption Scheme for VANETs. *Electronics*, *13*, 3164. https://doi.org/10.3390/ electronics13163164.

[11] Tariq, U. (2024), Optimized Feature Selection for DDoS Attack Recognition and Mitigation in SD-VANETs. *World Electrical Vehicular Journal*, *15*, 395. https://doi.org/10.3390/ wevj15090395

[12] Hou, B., Xin, Y., Zhu, H., Yang, Y., & Yang, J. (2023). VANET Secure Reputation Evaluation & Management Model Based on Double Layer Blockchain. *Applied Sciences*, *13*(9), 5733. https://doi.org/10.3390/app13095733

[13] Al-Dosari, K., & Fetais, N. (2023). Risk-Management Framework and Information-Security Systems for Small and Medium Enterprises (SMEs): A Meta-Analysis Approach. *Electronics*, *12*(17), 3629. https://doi.org/10.3390/electronics12173629

[14] Rajesh Kanna R., (2023), Risk identification and traffic prediction based on AI Technologies in VANET, *Journal of Survey in Fisheries Sciences*, pp. 4084-4089.

[15] Sánchez-García, I. D., Mejía, J., & Gilabert, T. S. F. (2023). Cybersecurity Risk Assessment: A Systematic Mapping Review, Proposal, and Validation. *Applied Sciences*, *13*(1), 395. https://doi.org/10.3390/app13010395.