Simulation Based Evaluation of Cryptographic techniques, Traffic Optimisation using VANETs

Dr.Sowmya K.S., Shreyas D.K., Somanath Mikali, Vishesh P. Gowda
B.M.S. College of Engineering, Bangalore, India
shreyasdk.is22@bmsce.ac.in

Abstract - **This paper presents a simulation-based framework for secure and real-time vehicular communication using Post-Quantum Cryptography (PQC) and RSU-assisted edge computing. Designed for urban VANETs, the model integrates PQC algorithms like Kyber and Dilithium to ensure quantum-resilient V2V and V2I communication. A Python-based benchmarking module evaluates cryptographic performance, feeding results into a network simulator (NS-3 or OMNeT++) coupled with SUMO for realistic mobility modeling. Roadside Units (RSUs) act as hybrid relays and edge processors, supporting congestion alerts, signal broadcasting, and localized message routing. The framework provides for comparative evaluation of classical and PQC methods, providing insight into the feasibility and impact of quantum-safe encryption in vehicular environments.**

Index Terms - Quantum Cryptography, RSU, Secure V2X Communication, SUMO, VANET.

INTRODUCTION

The evolution of Intelligent Transportation Systems (ITS) has led to widespread adoption of Vehicular Ad Hoc Networks (VANETs), where vehicles and infrastructure nodes collaborate for traffic safety, routing, and urban mobility. However, with increasing connectivity there comes the pressing need for secure, real-time communication particularly since quantum computing threatens traditional cryptographic schemes like RSA and ECC.

This project explores a simulation-based approach to secure vehicular communication using Post-Quantum Cryptography (PQC) in conjunction with RSU-assisted edge computing. The goal is to assess the feasibility of integrating quantum-resistant encryption algorithms into VANET architectures, with a particular focus on communication reliability and real-time responsiveness.

As part of the initial development,there is successful establishment of inter-vehicle communication using encrypted message exchange and integrated SUMO with TraCI for mobility simulation. The simulation is modeled around B.M.S. College of Engineering area, using real road dimensions to create a geographically accurate test environment. Vehicles follow realistic movement patterns and exchange messages in response to mobility dynamics and signal information.

To simulate encryption-related delays and bandwidth overheads introduced by PQC algorithms such as Kyber and Dilithium, a Python-based benchmarking module is under development using libraries such as liboqs-python and pqcrypto to evaluate cryptographic performance metrics. This module is designed to measure key parameters such as encryption latency, key and ciphertext sizes, and computational load. These results will later be integrated into the communication simulation environment to reflect real cryptographic performance under network load.

LITERATURE SURVEY

Vehicular Ad Hoc Networks (VANETs) have emerged as a foundational technology in intelligent transportation systems (ITS), enabling real-time vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. As vehicles become increasingly autonomous and interconnected, ensuring secure, efficient, and resilient communication has become paramount. The literature reveals a strong focus on cryptographic solutions to protect VANET communication. Al-Mutiri et al. [1] demonstrated a four-stage authentication scheme combining challenge–response mechanisms, digital signatures, timestamping, and encryption, achieving a 97% authentication accuracy and 100% specificity in blocking unsafe communications. Raya and Hubaux [2] proposed a pseudonym-based PKI system using short-term certificates and certificate revocation lists (CRLs) to counter Sybil and replay attacks without significantly affecting latency. More recently, Kandali et al. [3] incorporated artificial neural networks (ANNs) into AODV routing to detect black hole attacks with 98.97% accuracy, enhancing both security and routing efficiency.

The integration of blockchain into trust management has also gained traction. Kchaou et al. [4] introduced a distributed trust model leveraging fuzzy logic and miner-based validation within VANET clusters. This approach allowed vehicles to assess message credibility and behavioral integrity, effectively identifying and isolating malicious nodes. Parallel developments in cryptographic agility have seen the rise of hybrid and post-quantum schemes. For instance, a study on performance analysis of cryptographic methods suggested a hybrid ECC–Blowfish scheme as optimal for balancing speed, key size, and attack resistance [9], while a partially hybrid post-quantum protocol combining ECDSA with lattice-based cryptography was shown to add just 0.39 ms of delay while reducing redundant transmissions by 90% [11].

Disaster management and emergency communication are critical domains where VANETs can prevent fatalities. Hassan et al. [5] proposed a hybrid RF/VLC protocol that maintained 95% connectivity under simulated Road Side Units(RSU) failure scenarios, reduced end-to-end delay by 70%, and increased packet delivery by 23% compared to RF-only systems. Similarly, Kaur et al. [6] merged VANETs with IoT and machine learning for real-time accident detection, achieving 95% accuracy and dynamic rerouting for emergency vehicles. Jan et al. [7] evaluated multiple routing protocols (AODV, OLSR, DSDV, DSR) under disaster-like conditions using SUMO–NS3 integration, concluding that OLSR suits urban scenarios with high packet delivery ratios, while AODV and DSDV are more adaptable in dynamic, infrastructure-compromised environments.

Addressing urban congestion, Noori and Valkama [8] introduced a dynamic travel time computation system using IEEE 802.11p, with SUMO–OMNeT++ simulations on real urban maps. Their approach reduced travel times by up to 60% and decreased fuel consumption by 48%. Advances in adaptive traffic signal control, such as using YOLOv8 and VGG16 for emergency vehicle detection [12], have enabled smart intersections with green light prioritization and dynamic signal timing, significantly improving flow and safety.

On the privacy front, identity-based cryptography (IBC) continues to be explored for simplifying authentication while maintaining security. A comparative analysis [13] found that while bilinear pairing offers strong security, elliptic curve cryptography (ECC) provides a more lightweight and efficient alternative. Complementing this, PUF and secret-sharing-based message authentication protocols [14] have been introduced to eliminate dependency on CRLs, reduce computational load, and enhance physical attack resistance. Additionally, the rise of machine learning-based intrusion detection has led to frameworks like sFlow–Kafka–Spark pipelines with Random Forest classifiers [15], achieving high detection accuracy with minimal network impact. In federated learning applications for VANETs, privacy-preserving aggregation using zero-knowledge proofs and continuous authentication [16] has shown to outperform conventional schemes in training speed, security, and resilience against malicious clients.

This comprehensive review illustrates the multi-disciplinary progress in VANET research—spanning cryptographic robustness, decentralized trust, adaptive traffic control, and AI-driven threat detection—while highlighting the role of simulation frameworks (e.g., SUMO, NS3, OMNET++) in validating these approaches under realistic conditions. The convergence of lightweight security, post-quantum readiness, and intelligent control systems signals the path forward for robust, scalable, and secure VANET deployments.

PROPOSED MODEL

In this project, we introduce a simulation-based framework that integrates Post-Quantum Cryptography (PQC) and RSU-assisted edge computing to enhance security, scalability, and responsiveness in Vehicular Ad Hoc Networks (VANETs). This model is designed to address multiple critical challenges specifically those related to quantum-resilient communication, efficient data dissemination, and intelligent traffic management in urban smart transportation systems. As quantum computing advances, legacy cryptographic methods such as RSA and ECC are becoming increasingly vulnerable. Our framework aims to future-proof VANETs by embedding quantum-resistant algorithms within a simulated, real-world urban setting around the B.M.S. College of Engineering, Bangalore.

The simulated environment; models realistic vehicular mobility and communication patterns using synchronized tools like NS-3, TraCI and SUMO. Roadside Units (RSUs) are deployed at strategic intersections where they serve as both communication relays and localized edge computing nodes. Vehicles in the system are capable of securely exchanging traffic-related messages such as congestion alerts, signal state notifications, and emergency broadcasts that are encrypted using PQC protocols recommended by NIST like Kyber and Dilithium.

I. Objectives for Design

The model is designed with four objectives that drive the system architecture and simulation strategy:

- **Cryptographic Security**: One of the primary goals is to evaluate and implement post-quantum cryptographic algorithms that can secure both vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications. By leveraging recommended techniques such as Kyber (Key Encapsulation Mechanism) for key exchange and Dilithium (a digital signature scheme), the system ensures message integrity and confidentiality even in the face of emerging quantum threats.
- **RSU-Assisted Communication**: RSUs are not only static communication relays but also function as intelligent edge processors. They play role of offloading communication tasks, filter messages based on priority (e.g., emergency vs. normal traffic data), and ensure real-time responsiveness by reducing reliance on centralized infrastructure.
- **Performance Benchmarking**: To ensure practicality and gain deeper insights, the model includes a performance comparison between legacy cryptographic techniques (RSA, ECC) and PQC algorithms in terms of encryption latency, key sizes, and packet delivery performance and other parameters. NS-3 could be used to simulate and evaluate the impact of each scheme under realistic network load. The resulting analysis helps to identify how post-quantum encryption methods may affect message propagation, node processing time, and bandwidth consumption in a future-proof vehicular network and can lead to insights for subsequent research and development efforts.

- **Traffic Flow Optimization**: The system integrates traffic signal data and mobility simulation using SUMO and TraCI, to support intelligent routing decisions. Vehicles can adapt routes dynamically based on live congestion and information broadcast by RSUs, thereby improving traffic efficiency and reducing idle time.

II. System Architecture

The system architecture is comprised of 3 intertwined layers whose functions mirror the real-world VANET deployments.

- **Vehicle nodes**: Every vehicle is considered to be a mobile network node that can send, receive and process the messages. All outgoing messages, including signal timing updates, routing suggestions, and critical alerts, are encrypted using PQC algorithms. Vehicles manage cryptographic keys locally and establish secure links with RSUs for authentication and data communication. Messages are prioritised by metadata tagging which allow emergency messages to be considered urgently.
- **Roadside Units(RSU):** RSUs are deployed at junctions and along the road at specific intervals and facilitate communication between vehicles (V2V) and between vehicles and traffic infrastructure (V2I). By relaying encrypted packets, RSUs help overcome the limited transmission range of individual vehicles. RSUs also share information about signals RSUs periodically with nearby vehicles. This enables smoother traffic flow, and the avoidance of congested intersections.
- **Simulated Central Control:** A simulated control mechanism is included for global traffic monitoring. It aggregates data from RSUs to provide system-wide insights. In future iterations, this layer could integrate machine learning-based signal optimization strategies like reinforcement learning for traffic signal control.

III. Post-Quantum Cryptography Integration

To assess the computational and bandwidth impact of Post-Quantum Cryptography (PQC) within vehicular networks, a dedicated benchmarking module will be developed using Python. Leveraging libraries such as liboqs-python and pqcrypto, the module evaluates key performance indicators associated with quantum-resistant cryptographic algorithms such as encryption and decryption latency, key and ciphertext sizes and overhead per transaction that quantify the real-world performance implications of integrating PQC into vehicular communication protocols.

The model is to be designed to interface with either NS-3 or OMNeT++, both of which are well-established tools for simulating VANET environments. Provision of modular input ensures that encryption-related delays, message sizes, and processing overheads can be easily integrated regardless of the simulation software.

The model proposes to use Kyber as the primary Key Encapsulation Mechanism (KEM) for secure key exchange, while Dilithium serves as the post-quantum digital signature scheme. Both algorithms are part of the NIST-recommended suite of PQC standards. By incorporating these schemes into the simulation environment, we can enable a performance comparison between classical cryptographic approaches and next-generation quantum-resistant methods[17].

IV. RSU-Driven Traffic Simulation

To mimic realistic traffic simulation, we employ SUMO to generate a mobility map that replicates the road network around B.M.S. College of Engineering. Vehicle mobility traces are imported using the TraCI interface, ensuring synchronized and time-accurate simulation of communication and movement.

RSUs disseminate real-time traffic signal states to vehicles as well as relaying congestion alerts to approaching vehicles and route packets based on the message priority that is tagged to the metadata. This allows for high-fidelity simulation of urban vehicular dynamics.

CONCLUSION

This work presents a foundational framework for simulating secure and intelligent vehicular communication using Post-Quantum Cryptography (PQC) and RSU-assisted edge computing. With a focus on real world traffic modelling it showcases successful creation of encrypted vehicle-to-vehicle communication and integrated SUMO with TraCI to simulate mobility in a geographically accurate map of locality. These initial steps validate the feasibility of incorporating secure communication protocols into VANET environments under real-world constraints.

The ongoing development includes a Python-based cryptographic benchmarking module, which will provide performance metrics such as encryption latency and overhead for quantum-resistant schemes like Kyber and Dilithium. These parameters will be integrated into the network simulation layer to emulate the real-world impact of PQC on communication efficiency. The system is designed to be modular and compatible with either NS-3 or OMNeT++ for future extensions. Future work would include implementing PQC-enabled communication, enhancing RSU functionality to include localized edge processing, and conducting a comprehensive performance comparison between classical and post-quantum cryptographic methods. This research contributes towards the design of resilient and scalable VANET systems that are prepared to meet the security challenges of the quantum computing era.

REFERENCES

[1] Al-Mutiri, R., Al-Rodhaan, M., & Tian, Y. (2022). Improving vehicular authentication in VANET using. *International Journal of Communication Networks and Information Security (IJCNIS)*, *10*(1). https://doi.org/10.17762/ijcnis.v10i1.3124.

[2] Raya, Maxim, and Jean-Pierre Hubaux. "Securing Vehicular Ad Hoc Networks." *Journal of Computer Security*, vol. 15, no. 1, 2007, pp. 39–68.

[3] Kandali, Khalid, Lamyae Bennis, Omar El Bannay, and Hamid Bennis. "An Intelligent Machine Learning Based Routing Scheme for VANET." *IEEE Access*, vol. 10, 2022, pp. 1–1.

[4] Kchaou, Amira, et al. "Toward a Distributed Trust Management scheme for VANET." *ACM International Conference on Availability, Reliability and Security (ARES)*, August 27-30, 2018, Hamburg, Germany, pp. 1-6.

[5] Hassan, Noha, Xavier Fernando, and Isaac Woungang. “An Emergency Message Routing Protocol for Improved Congestion Management in Hybrid RF/VLC VANETs.” *Telecom*, vol. 5, no. 1, 2024, pp. 21–47.

[6] Kaur, Manjinder, Jyoteesh Malhotra, and Pankaj Deep Kaur. “A VANET-IoT Based Accident Detection and Management System for the Emergency Rescue Services in a Smart City.” *2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, 2020, pp. 964–968.

[7] Jan, Maria, et al. “VANET Routing Protocols: Implementation and Analysis Using NS3 and SUMO.” *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 10, no. 3, 2021, pp. 1914–1919.

[8] Noori, H., and M. Valkama. “Impact of VANET Based V2V/V2I Communication Using IEEE 802.11p on Reducing Traveling Time in Realistic Large Scale Urban Area.” *Proceedings of ICCVE 2013*, 2013.

[9] Alimohammadi, M., and A. A. Pouyan. “Performance Analysis of Cryptography Methods for Secure Message Exchanging in VANET.” *International Journal of Scientific & Engineering Research*, vol. 5, no. 2, Feb. 2014, pp. 911–918.

[10] Gayathri M and Gomathy C (2024) Design of CSKAS-VANET model for stable clustering and authentication scheme using RBMA and signcryption. Front. Comput. Sci. 6:1384515. doi: 10.3389/fcomp.2024.1384515.

[11] Twardokus, Geoff, et al. “When Cryptography Needs a Hand: Practical Post-Quantum Authentication for V2V Communications.” *Network and Distributed System Security (NDSS) Symposium*, 2024.

[12] G., D. S., G., G. A., and L. D. "Next-Generation Traffic Control: Adaptive Timer and Emergency Vehicle Priority in Intelligent Traffic Management." *2024 International Conference on E-mobility, Power Control and Smart Systems (ICEMPS)*, Thiruvananthapuram, India, 2024, pp. 1-6. DOI: 10.1109/ICEMPS60684.2024.10559373.

[13] Al-Shareeda, M. A., et al. “Security and Privacy Schemes in Vehicular Ad-Hoc Network With Identity-Based Cryptography Approach: A Survey.” *IEEE Access*, vol. 9, 2021, pp. 121522–121531.

[14] Othman, W., M. Fuyou, K. Xue, and A. Hawbani. “Physically Secure Lightweight and Privacy-Preserving Message Authentication Protocol for VANET in Smart City.” *IEEE Transactions on Vehicular Technology*, vol. 70, no. 12, 2021, pp. 12902–12917.

[15] Zang, M., and Y. Yan. “Machine Learning-Based Intrusion Detection System for Big Data Analytics in VANET.” *2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring)*, Helsinki, Finland, 2021, pp. 1-5. DOI: 10.1109/VTC2021-Spring51267.2021.9448878.

[16] Feng, X., X. Wang, H. Liu, H. Yang, and L. Wang. “A Privacy-Preserving Aggregation Scheme With Continuous Authentication for Federated Learning in VANETs.” *IEEE Transactions on Vehicular Technology*, vol. 73, no. 7, July 2024, pp. 9465–9477.

[17] Demir, Elif Dicle, Buse Bilgin, and Mehmet Cengiz Onbaşlı. "Performance Analysis and Industry Deployment of Post-Quantum Cryptography Algorithms." *arXiv preprint* arXiv:2503.12952v2 [cs.CR], 31 Mar. 2025.

AUTHOR INFORMATION

[1] **Dr. Sowmya K.S.**, Assistant Professor, Department of Information Science and Engineering, B.M.S. College of Engineering.

[2] **Shreyas D.K.**, U.G. Student, Department of Information Science and Engineering, B.M.S. College of Engineering.

[3] **Somanath Mikali**, U.G. Student, Department of Information Science and Engineering, B.M.S. College of Engineering.

[4] **Vishesh P. Gowda**, U.G. Student, Department of Information Science and Engineering, B.M.S. College of Engineering.