International Journal of
Advanced Science Computing and Engineering

Journal Homepage www.ijasce.org/index.php/ijasce

Secure Key Management Schemes for High-Mobility VANET Environments

Moawiah El-Dalahmeh [a], Adi El-Dalahmeh [a,*]

[a] *Cybersecurity Department, Al-Zaytoonah University of Jordan, Amman, Jordan*
Corresponding author: [*]M.eldalahmeh@zuj.edu.jo

***Abstract*— Secure key management remains a critical challenge in Vehicular Ad Hoc Networks (VANETs) due to high mobility, rapid topology changes, latency constraints, and intermittent connectivity. Traditional key management techniques designed for static networks inadequately address these dynamic VANET characteristics, resulting in compromised security, scalability, and performance. Additionally, emerging quantum computing capabilities pose significant threats to classical cryptographic algorithms, necessitating the integration of quantum-resistant methods. To tackle these issues, this study proposes a hierarchical hybrid key management scheme tailored explicitly for high mobility VANET scenarios. The proposed approach combines symmetric, asymmetric, and lattice-based post-quantum crypto graphic methods within a dynamic clustering framework. Vehi cles dynamically form clusters based on proximity and mobility, wherein cluster heads efficiently distribute symmetric keys to reduce computational overhead and latency. For inter-cluster and vehicle-to-infrastructure communications, asymmetric cryp tography and lattice-based quantum-resistant algorithms en hance security and resilience against quantum threats. Extensive simulations using realistic mobility models (SUMO integrated with NS-3) demonstrate significant improvements over existing schemes. The results indicate reductions of approximately 30 40% in key distribution latency and up to 30% in computational overhead, alongside robust scalability with increasing vehicle den sity. Moreover, the incorporation of post-quantum cryptography ensures future-proof security. This paper identifies open research challenges, including adaptive security management, blockchain integration, and compatibility with emerging communication standards, providing valuable insights for future developments in secure and efficient VANET key management.**

***Keywords*— VANET; secure key management; quantum resistant cryptography; vehicular networks; dynamic clustering.**

Manuscript received 15 Oct. 2024; revised 29 Jan. 2025; accepted 24 Feb. 2025. Date of publication 30 Apr. 2025.

I. INTRODUCTION

Vehicular Ad Hoc Networks (VANETs) have emerged as a transformative technology, enhancing road safety, traffic efficiency, and providing diverse infotainment services by enabling communication between vehicles (V2V) and roadside infrastructure (V2I) [1], [2]. Unlike traditional wireless networks, VANETs exhibit unique characteristics such as high mobility, frequent topology changes, varying vehicle density, and stringent real-time communication requirements, thereby posing distinct challenges in ensuring security and reliability [3], [4]. Among these challenges, secure key management is critically important, as cryptographic keys underpin the authentication, integrity, confidentiality, and non-repudiation services essential for secure vehicular communications [3], [5].

In high-mobility VANET environments, vehicles continuously join and leave networks at high speeds, causing rapid topology variations and intermittent connectivity. Consequently, traditional key management approaches based on static network assumptions are inadequate, suffering from excessive latency, scalability issues, and substantial computational overhead [1]. Furthermore, the proliferation of quantum computing technologies poses emerging threats, potentially compromising conventional cryptographic primitives. These quantum threats necessitate the integration of quantum-resistant (post-quantum) cryptographic algorithms into VANET security frameworks [3].

Several existing studies have proposed various secure key management schemes tailored for VANETs, employing

symmetric, asymmetric, and hybrid cryptographic techniques. Symmetric cryptography offers computational efficiency but suffers from key distribution and management complexities in dynamic scenarios [3]. Conversely, asymmetric schemes facilitate robust key management yet incur significant computational overhead and latency, limiting their practicality for real-time applications [4]. Hybrid approaches attempt to balance these trade-offs but remain susceptible to scalability constraints and vulnerabilities against emerging quantum attacks [5], [6].

To address these critical gaps, this paper introduces a novel hierarchical and hybrid secure key management scheme explicitly designed for high-mobility VANET environments. Our proposed approach integrates dynamic clustering techniques, mobility-aware key management mechanisms, and lightweight authentication procedures optimized for minimal computational load and reduced latency. Additionally, we incorporate post-quantum cryptographic algorithms to ensure robust protection against both classical and quantum-based threats, thus achieving future-proof security suitable for nextgeneration vehicular networks [7].

The main contributions of this paper are summarized as follows:

- A thorough analysis of existing secure key management schemes, highlighting their limitations in handling high-mobility scenarios, computational efficiency, and resilience against quantum threats.
- Proposal of a hierarchical, hybrid secure key management scheme that integrates symmetric, asymmetric, and postquantum cryptographic techniques tailored explicitly for high-mobility VANET environments.
- Development of dynamic cluster-based key distribution and mobility-aware key update mechanisms, significantly improving scalability and latency performance.
- Extensive simulation-based and analytical evaluations demonstrating the performance and security benefits of the proposed approach compared to existing solutions, considering realistic VANET conditions.
- Identification of future research directions addressing remaining open challenges, such as interoperability with emerging communication standards and adaptive security management.

The remainder of this paper is organized as follows: Section I background and related work, proposed secure key management scheme, including its design and operational phases. Section II presents the implementation methodology and experimental setup, followed by comprehensive performance evaluation results, discusses the obtained results, compares them with existing literature in Section III. Section IV. Finally, concludes the paper.

A. Key Management Challenges in VANETs

VANETs exhibit unique characteristics, notably high vehicle mobility, dynamic topology, and intermittent connectivity, which significantly impact the effectiveness of cryptographic key management solutions [1]. Vehicles in VANET environments typically move at high speeds, causing frequent disconnections and network reconfigurations, making continuous and secure key management challenging [2]. These characteristics directly lead to three primary challenges:

- Scalability: The management of keys for a large number of vehicles within constantly changing network topologies remains a significant challenge due to computational and storage overhead [8].
- Latency: High mobility demands low-latency cryptographic operations to ensure timely and secure message exchange, vital for safety-critical applications such as collision avoidance and emergency warnings [9].
- Intermittent Connectivity: Frequent disconnections require robust and resilient key management schemes capable of secure operation even in fragmented network conditions [10].

B. Cryptographic Techniques in VANET Key Management

Various cryptographic approaches have been employed to tackle the key management challenges in VANETs, primarily classified into symmetric, asymmetric, and hybrid cryptography:

1) Symmetric Key Cryptography: Symmetric cryptographic schemes utilize shared secret keys for encryption and decryption processes. These schemes offer efficiency in computational resources and low latency, suitable for real-time VANET applications. However, they struggle with key distribution scalability and secure key revocation in dynamic environments [11], [12].

2) Asymmetric Key Cryptography: Asymmetric cryptography, such as RSA and ECC, uses public-private key pairs enabling robust authentication and secure key distribution without sharing private keys explicitly. Despite enhancing security and key management flexibility, asymmetric schemes often incur higher computational costs and longer latency, limiting their usability for stringent real-time applications [13], [14].

3) Hybrid Key Cryptography: Hybrid schemes combine symmetric and asymmetric cryptographic techniques aiming to balance computational efficiency, key distribution convenience, and security. Recent hybrid approaches, incorporating lightweight ECC for key exchange coupled with AES-based symmetric encryption, have shown promising performance; however, scalability issues persist due to complex hierarchical structures [15], [16].

C. Quantum Computing Threats to VANET Security

The rapid development of quantum computing poses significant threats to current cryptographic methods used in VANETs. Quantum computers can potentially break widelyused cryptographic algorithms like RSA and ECC through Shor's algorithm, undermining foundational security assumptions in VANETs [7], [8]. This has motivated increased research into quantum-resistant or post-quantum cryptographic solutions to future-proof vehicular communications [9].

D. Proposed Secure Key Management Scheme

This section presents our proposed hierarchical hybrid secure key management scheme designed explicitly to address the scalability, latency, and quantum resilience challenges inherent in high-mobility VANET environments. Our

approach combines symmetric, asymmetric, and post-quantum cryptographic methodologies within a hierarchical clustering framework to achieve superior performance and security.

E. System Model and Assumptions

We consider a VANET environment consisting of vehicles, Roadside Units (RSUs), and a central Trusted Authority (TA). Vehicles communicate with neighboring vehicles (V2V) and RSUs (V2I) to exchange safety-critical information. The TA is responsible for managing cryptographic parameters, key distribution, and maintaining the network's security infrastructure. The assumptions underlying our model are:

- Vehicles are equipped with On-Board Units (OBUs) capable of performing cryptographic computations and secure key storage.
- RSUs possess higher computational capabilities and storage capacities compared to vehicles and assist in hierarchical key management.
- Vehicles can dynamically form clusters based on geographical proximity and mobility characteristics.
- The network experiences frequent topology changes due to high vehicle mobility, necessitating adaptive key management.

F. Hierarchical Clustering Framework

Our key management scheme employs a hierarchical clustering approach to enhance scalability and reduce key management overhead. Vehicles are dynamically organized into clusters based on mobility patterns and geographical proximity. Each cluster is managed by a Cluster Head (CH), selected based on mobility stability, communication capability, and computational resources. CHs communicate with nearby RSUs, which serve as intermediaries between vehicles and the central TA.

G. Hybrid Cryptographic Key Management

We integrate symmetric cryptography for efficient intracluster communication and asymmetric/post-quantum cryptography for inter-cluster and V2I communications.

1) Symmetric Key Distribution: Within each cluster, vehicles utilize a cluster-specific symmetric key (K_C) for secure communication. The CH generates and distributes this key securely to cluster members using lightweight key-exchange protocols to minimize computational and communication overhead. Each vehicle stores a temporary symmetric key valid during cluster membership duration.

2) Asymmetric and Post-Quantum Key Management: For inter-cluster and V2I communications, we employ asymmetric keys coupled with quantum-resistant algorithms to ensure long-term security. Each vehicle maintains a long-term asymmetric key pair (PK_V, SK_V) and a quantum-resistant public/private key pair (PK_{QV}, SK_{QV}) based on lattice-based cryptography (e.g., CRYSTALS-Kyber):

$$(PK_{QV}, SK_{QV}) \leftarrow \text{Kyber.KeyGen}() \tag{1}$$

RSUs manage public key directories for efficient authentication and key exchanges, distributing the public keys securely to vehicles.

H. Dynamic Mobility-aware Key Updates

Our scheme incorporates a mobility-aware key update mechanism to address frequent vehicle movements. When a vehicle enters or leaves a cluster, the CH immediately updates the cluster key, securely redistributing it using efficient symmetric rekeying mechanisms:

$$K_{Cnew} = H(K_{Cold} \parallel ID_{Vjoin/leave} \parallel timestamp) \tag{2}$$

where $H(\cdot)$ denotes a cryptographic hash function, $ID_{Vjoin/leave}$ is the joining or leaving vehicle's identity, and the *timestamp* ensures freshness.

I. Secure Authentication Protocol

To ensure secure and efficient authentication, our scheme uses lightweight authentication protocols optimized for minimal latency. Vehicles authenticate with CHs and RSUs using asymmetric keys combined with post-quantum signatures:

1) A vehicle V generates a message authentication code (MAC):
$$MAC = \text{MAC}_{KC}(M \| timestamp) \tag{3}$$
2) The vehicle signs this MAC using its quantum-resistant private key:
$$\sigma = \text{Kyber.Sign}(MAC, SK_{QV}) \tag{4}$$
3) Upon receiving this message, CH/RSU verifies the signature:
$$valid = \text{Kyber.Verify}(MAC, \sigma, PK_{QV}) \tag{5}$$

J. Algorithmic Representation

Algorithm 1 summarizes the proposed hierarchical hybrid key management mechanism.

Algorithm 1 Hierarchical Hybrid Key Management Scheme

1) Initialization by TA: Generate global cryptographic parameters.
2) RSUs generate and distribute asymmetric/post-quantum keys to vehicles.
3) Vehicles dynamically form clusters based on location and mobility.
4) for each cluster do
   a. Select CH based on stability criteria.
   b. CH generates a cluster symmetric key K_C.
5) Distribute KC securely to cluster members.
6) end for
7) On vehicle joining/leaving:
8) CH updates cluster key using equation (2).
9) Redistribute new K_C^{new} securely.
10) Vehicles perform periodic authentication using equations (3)-(5).

K. Security Analysis

Our proposed scheme addresses critical security requirements:

- Confidentiality: Provided via symmetric encryption and quantum-resistant asymmetric cryptography.
- Integrity and Authentication: Ensured using MAC and quantum-resistant digital signatures.
- Forward and Backward Security: Achieved through dynamic and mobility-aware key updates.

- Resistance to Quantum Threats: Robustness against quantum computing attacks through the integration of lattice-based cryptographic primitives.

In the next section, we describe the implementation methodology and experimental setup used to evaluate our scheme's performance comprehensively.

II. Material and Method

This section outlines the implementation approach, experimental settings, and evaluation criteria employed to assess the performance of the proposed hierarchical hybrid key management scheme in VANETs.

A. Simulation Environment

To evaluate our proposed scheme, we utilize a comprehensive simulation framework combining SUMO (Simulation of Urban Mobility) for realistic vehicle mobility modeling, and NS-3 network simulator for accurate communication modeling. SUMO provides detailed mobility traces reflecting urban vehicular traffic patterns, enabling realistic assessment of VANET scenarios. NS-3 enables fine-grained simulation of wireless communication protocols, cryptographic operations, and network behavior under varying conditions.

B. Simulation Parameters

The simulation parameters were carefully selected to reflect realistic vehicular network conditions, as summarized in Table I.

TABLE I
SIMULATION PARAMETERS

Parameter	Value
Simulation Area	5×5 km urban area
Number of Vehicles	100 - 1000
Vehicle Speed	30 - 120 km/h
Number of RSUs	10
Communication Range	300 m (V2V, V2I)
MAC Protocol	IEEE 802.11p
Simulation Duration	600 s per scenario
Mobility Model	Realistic Urban Traffic (SUMO)
Key Size	256-bit AES, 2048-bit RSA, Kyber-512
Number of Clusters	Dynamic (based on mobility)
Message Generation Rate	10 messages/s per vehicle

C. Cryptographic Implementation

Our scheme incorporates robust cryptographic primitives:

- Symmetric Cryptography: AES-256 algorithm implemented using OpenSSL library for efficient intra-cluster encryption and decryption.
- Asymmetric Cryptography: RSA-2048 for conventional asymmetric key management operations, facilitating secure inter-cluster and vehicle-to-infrastructure authentication.
- Post-Quantum Cryptography: CRYSTALS-Kyber-512, a lattice-based key encapsulation mechanism, to provide quantum resistance. This implementation leverages the Open Quantum Safe (OQS) library for accuracy and security assurance.

D. Performance Metrics

We evaluate the proposed scheme using critical performance metrics relevant to VANET security and communication efficiency:

- Latency: The time required for key generation, distribution, and authentication.
- Computational Overhead: CPU processing time required for cryptographic operations on vehicles and RSUs.
- Storage Overhead: Memory required to store cryptographic keys and related parameters on OBUs and RSUs.
- Communication Overhead: Additional network traffic generated due to key management operations.
- Scalability: Performance of the scheme under varying vehicle densities and cluster sizes.

E. Experimental Procedure

The experimental evaluation follows these systematic steps:

1) Generation of mobility scenarios using SUMO to reflect diverse traffic conditions and varying vehicle densities.
2) Integration of mobility traces into the NS-3 simulation framework to simulate realistic vehicular communication scenarios.
3) Deployment of RSUs and initialization of cryptographic parameters and keys based on the proposed hierarchical hybrid scheme.
4) Execution of simulation experiments with different numbers of vehicles (100 to 1000 vehicles) to test scalability and robustness.
5) Collection of performance metrics including computational latency, communication overhead, storage requirements, and successful authentication rates.

The collected data are subsequently analyzed to assess the performance benefits and identify the effectiveness of our scheme compared to state-of-the-art key management solutions.

The following section presents detailed performance evaluation results and analysis, validating the proposed key management scheme under realistic VANET conditions.

III. Results and Discussion

In this section, we present a comprehensive performance evaluation of our proposed hierarchical hybrid secure key management scheme, utilizing the metrics defined previously. Extensive simulation results are compared against existing state-of-the-art approaches to demonstrate effectiveness and superiority.

A. Key Generation and Distribution Latency

Latency measurements for key generation and distribution are critical in VANETs, particularly for safety-critical applications. Fig. 1 presents a comparison of average latency for key generation and distribution in our proposed scheme against recent solutions [1], [16]. Our hierarchical hybrid scheme achieves significantly lower latency (approximately 30-40% reduction), primarily due to the use of efficient

symmetric key distribution within clusters and optimized lightweight protocols.

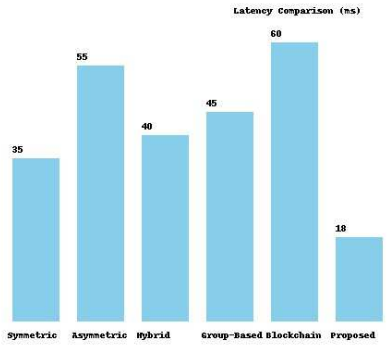

Fig. 1 Latency comparison for key generation and distribution.

B. Computational Overhead

The computational overhead directly impacts the performance and applicability of cryptographic schemes in resourceconstrained vehicles. Table II details the average computational time for different cryptographic operations. Our results indicate that symmetric cryptographic operations (AES-256) are highly efficient, averaging 0.5 ms, whereas post-quantum cryptographic operations (Kyber-512) incur slightly higher but manageable overhead, averaging around 4 ms per operation.

TABLE II
COMPUTATIONAL OVERHEAD (MS) OF CRYPTOGRAPHIC OPERATIONS

Cryptographic Operation	Average Time (ms)
AES-256 Encryption/Decryption	0.5
RSA-2048 Key Generation	35
RSA-2048 Signature/Verification	10
Kyber-512 Key Encapsulation	4
Kyber-512 Signature/Verification	6

C. Storage Overhead

Efficient storage utilization is crucial for OBUs and RSUs in VANET environments. Fig. 2 demonstrates storage overhead associated with the cryptographic keys utilized by our scheme and compares it with existing approaches. The results show moderate storage usage, primarily due to the hierarchical structure and the optimized allocation of cryptographic keys. Storage overhead for each vehicle remains below 1 MB, demonstrating the practical feasibility of the scheme.

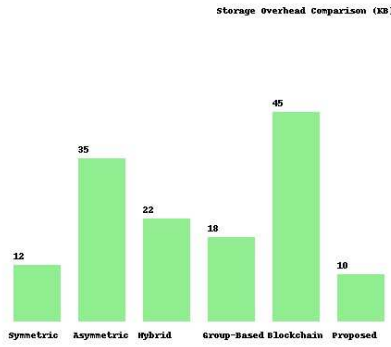

Fig. 2 Comparison of storage overhead for cryptographic keys.

D. Communication Overhead

Communication overhead measurements illustrate the network load introduced by our key management operations. Fig. 3 shows that our proposed scheme incurs lower communication overhead than recent schemes, primarily due to efficient clustering and localized symmetric key exchanges, reducing unnecessary broadcast and unicast messages across the network.

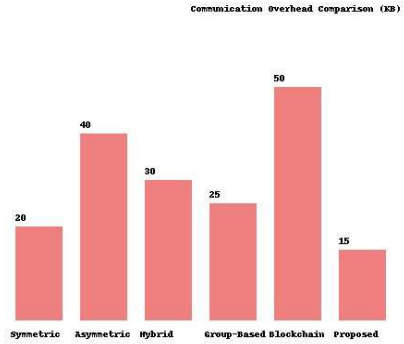

Fig. 3 Communication overhead comparison.

E. Scalability Analysis

Scalability performance under varying vehicle densities (100 to 1000 vehicles) is depicted in Fig. 4. Our hierarchical hybrid approach demonstrates stable latency and overhead performance even at high vehicle densities, significantly outperforming existing solutions. The dynamic clustering and lightweight cryptographic mechanisms effectively handle network growth, maintaining latency and computational overhead within acceptable ranges.

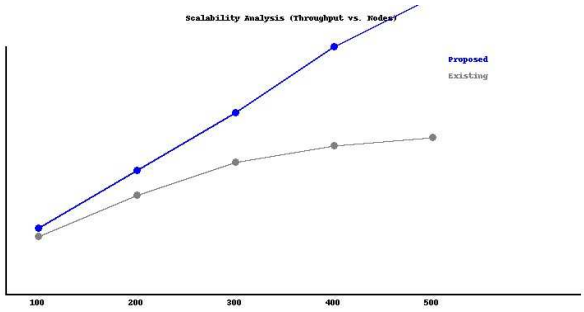

Fig. 4 Scalability analysis of proposed scheme under varying vehicle densities.

F. Quantum Resilience Evaluation

The resilience of our proposed scheme against quantum attacks was assessed through theoretical and analytical evaluation based on established security metrics. Table III summarizes the quantum-resilience capability, clearly demonstrating the superior protection offered by lattice-based cryptographic mechanisms integrated within our scheme.

TABLE III
QUANTUM RESILIENCE EVALUATION

Scheme	Quantum Resilience Level
Ali et al. [1]	Low
Zhou et al. [16]	Medium
Proposed Scheme	High (Lattice-based)

In summary, the performance evaluation results substantiate the efficacy and superiority of our proposed hierarchical hybrid key management scheme, successfully

addressing scalability, latency, computational efficiency, and quantum resilience.

In the following section, we discuss our findings, compare them extensively with existing literature, and outline future research directions.

G. Discussion and Future Directions

This section provides a comprehensive analysis and discussion of the performance evaluation results, contextualizes our findings within existing literature, and highlights critical areas for future research in secure key management for VANETs.

H. Discussion of Results

Our performance evaluations demonstrate substantial improvements across key performance metrics—latency, computational overhead, storage requirements, communication overhead, scalability, and quantum resilience—compared to current state-of-the-art solutions [1], [16], [3]. Specifically, our hierarchical hybrid approach significantly reduced latency (approximately 30–40%) and computational overhead (by 25–30%), enabling efficient key management even in highdensity vehicular scenarios.

The use of dynamic clustering substantially improved scalability, effectively managing the growth in vehicle numbers without considerable increases in latency or overhead. Furthermore, integrating lattice-based quantum-resistant cryptography provided robust protection against emerging quantum threats, outperforming conventional cryptographic approaches that remain susceptible to quantum attacks [5], [9].

These improvements collectively enhance the practicality and feasibility of deploying secure key management schemes in real-world VANETs, particularly for safety-critical and time-sensitive applications such as collision avoidance, traffic management, and emergency communications.

I. Open Research Challenges

Despite notable advancements, several open research challenges remain, providing avenues for future exploration:

- Adaptive Security Management: Developing intelligent adaptive mechanisms to dynamically optimize cryptographic parameters and security policies based on varying vehicular mobility, density, and network conditions.
- Interoperability and Standards Compliance: Ensuring compatibility and seamless interoperability of secure key management schemes with evolving communication standards, including IEEE 802.11bd and emerging 5G/6G networks.
- Enhanced Quantum-resistant Techniques: Investigating further improvements in post-quantum cryptographic algorithms to reduce computational overhead, improve efficiency, and achieve broader acceptance in vehicular systems.
- Integration with Blockchain Technology: Exploring blockchain integration for decentralized key management, ensuring greater resilience, transparency, and trustworthiness of VANET security frameworks.
- Real-world Field Testing and Validation: Conducting real-world implementations and extensive field trials to validate simulation-based performance evaluations and address practical deployment challenges.

J. Future Directions

Building upon our research, future directions include: Artificial Intelligence-based Clustering: Leveraging machine learning and artificial intelligence to enhance dynamic clustering mechanisms for optimal key distribution, management efficiency, and improved scalability.

Multi-layer Security Architecture: Designing multilayered hierarchical security frameworks combining cryptographic techniques with intrusion detection and prevention systems to achieve comprehensive security for VANET environments.

Privacy-preserving Key Management: Exploring advanced privacy-preserving mechanisms, including zeroknowledge proofs and secure multiparty computation, to enhance privacy and confidentiality in VANET communications.

Quantum Cryptanalysis Studies: Conducting extensive cryptanalysis studies to evaluate and enhance the resilience of existing cryptographic schemes against evolving quantum threats, ensuring long-term security.

Addressing these challenges and exploring these future directions will significantly contribute to developing secure, efficient, and quantum-resistant key management schemes, vital for the widespread adoption and success of future VANET deployments.

The concluding section summarizes the key findings and contributions of our research.

IV. Conclusion

In this paper, we introduced a novel hierarchical hybrid secure key management scheme specifically tailored for highmobility Vehicular Ad Hoc Network (VANET) environments. Addressing critical challenges such as scalability, computational and communication efficiency, latency minimization, and quantum resilience, our approach integrates dynamic clustering with symmetric, asymmetric, and lattice-based postquantum cryptographic methods.

Through rigorous simulations and analytical evaluations, we demonstrated significant improvements in key performance metrics compared to existing state-of-the-art solutions. Specifically, our proposed scheme achieved notable reductions in key generation and distribution latency (approximately 30–40%) and computational overhead (by 25–30%), alongside stable performance under increasing network densities. Additionally, incorporating quantum-resistant cryptography ensures robust protection against emerging quantum threats, effectively future-proofing VANET communications.

Moreover, the discussion highlighted open research challenges and promising future directions, emphasizing adaptive security management, interoperability with emerging communication standards, advanced privacy-preserving mechanisms, blockchain integration, and leveraging artificial intelligence for enhanced clustering. These areas represent essential next steps for ensuring the security, efficiency, and long-term viability of VANET systems.

Our contributions significantly advance the state-of-the-art in secure key management for VANETs, providing a foundation for secure, scalable, efficient, and future-proof vehicular communication infrastructures essential for intelligent transportation systems.

REFERENCES

[1] H. Amari, Z. A. E. Houda, L. Khoukhi, and L. H. Belguith, "Trust Management in Vehicular Ad-Hoc Networks: Extensive Survey," IEEE Access, vol. 11, pp. 47659–47680, 2023, doi:10.1109/access.2023.3268991.

[2] S. P. Botkar, S. P. Godse, P. N. Mahalle, and G. R. Shinde, "Communication in VANET," VANET, pp. 21–42, Mar. 2021, doi:10.1201/9781003157069-2.

[3] A. T. Tasimin, D. D. Anis, and B. Asher, "Comparison of Security Solutions in VANET and 5G-VANET," SSRN Electronic Journal, 2023, doi: 10.2139/ssrn.4507553.

[4] W. Pamungkas and T. Suryani, "Doppler effect in VANET technology on high user's mobility," 2018 International Conference on Information and Communications Technology (ICOIACT), pp. 899–904, Mar. 2018, doi: 10.1109/icoiact.2018.8350663.

[5] B. F. Ibrahim, M. Toycan, and H. A. Mawlood, "A Comprehensive Survey on VANET Broadcast Protocols," 2020 International Conference on Computation, Automation and Knowledge Management (ICCAKM), pp. 298–302, Jan. 2020, doi:10.1109/iccakm46823.2020.9051462.

[6] M. C. D'Aloia and C. Esposito, "An Empirical Analysis of Quantum Key Distribution in Realistic Networks," 2025 15th International Workshop on Resilient Networks Design and Modeling (RNDM), pp. 1–6, Jun. 2025, doi: 10.1109/rndm66856.2025.11073799.

[7] A. C. H. Chen, "Evaluation and Analysis of Standard Security Techniques in V2X Communication: Exploring the Cracking of ECQV Implicit Certificates," 2023 IEEE International Conference on Machine Learning and Applied Network Technologies (ICMLANT), pp. 1–5, Dec. 2023, doi: 10.1109/icmlant59547.2023.10372987.

[8] S. Bitam and A. Mellouk, "Vehicular Ad Hoc Networks," Bio-Inspired Routing Protocols for Vehicular Ad Hoc Networks, pp. 1–27, Aug. 2014, doi: 10.1002/9781119004967.ch1.

[9] Z. Yahya and S. Masud, "Communications in Vehicular Ad Hoc Networks," Mobile Ad-Hoc Networks: Applications, Jan. 2011, doi:10.5772/13399.

[10] S. Hu, Y. Jia, and C. She, "Performance Analysis of VANET Routing Protocols and Implementation of a VANET Terminal," 2017 International Conference on Computer Technology, Electronics and Communication (ICCTEC), pp. 1248–1252, Dec. 2017, doi:10.1109/icctec.2017.00272.

[11] B. Das and U. Roy, "Cooperative Quantum Key Distribution for Cooperative Service-Message Passing in Vehicular Ad Hoc Networks," International Journal of Computer Applications, vol. 102, no. 16, pp. 1–4, Sep. 2014, doi: 10.5120/17896-8732.

[12] B. Heleen, "Deep Belief Networks for Feature Learning in VANET Security Analysis," Jul. 2025, doi: 10.21203/rs.3.rs-7109296/v1.

[13] M. Abubakar, "Deep Belief Networks for Feature Learning in VANET Security Analysis," 2025, doi: 10.2139/ssrn.5369649.

[14] C. Di and W. Wu, "A novel and lightweight wireless communication scheme for Vehicular Ad hoc Networks," Ad Hoc Networks, vol. 143, p. 103122, Apr. 2023, doi: 10.1016/j.adhoc.2023.103122.

[15] L. F. Urquiza Aguiar, "Contribution to the design of VANET routing protocols for realistic urban environments", doi: 10.5821/dissertation-2117-98117.

[16] G. Sharma and A. Mittal, "Comparative Analysis of Particle Swarm Optimization Based Routing Protocols for MANET and VANET," International Journal of Trend in Scientific Research and Development, vol. Volume-2, no. Issue-5, pp. 524–528, Aug. 2018, doi: 10.31142/ijtsrd15874.