DOI: 10.15849/IJASCA.250730.12

Int. J. Advance Soft Compu. Appl, Vol. 17, No. 2, July 2025
Print ISSN: 2710-1274, Online ISSN: 2074-8523

Enhancing VANET Security with Lattice-Based Cryptography and Dynamic Pseudonym Updates

Adi El-Dalahmeh[1], and Mohammad Alia[1]

[1]Cybersecurity Department , Al-Zaytoonah University of Jordan , Amman ,Jordan
e-mail: a.eldalahmeh@zuj.edu.jo , and dr.m.alia@zuj.edu.jo

Abstract

Ensuring secure and efficient authentication in Vehicular Ad Hoc Networks (VANETs) is vital for real-time communication and network resilience. However, traditional authentication mechanisms, such as Elliptic Curve Cryptography (ECC) and Public Key Infrastructure (PKI), face significant challenges, including high computational overhead, complex certificate revocation, and vulnerability to quantum attacks. To overcome these limitations, we propose a lattice-based authentication protocol that integrates post-quantum cryptography (PQC), zero-knowledge proofs (ZKPs), and fog computing for secure Vehicle-to-Roadside (V2R) communication. Our protocol offers quantum resistance, decentralized authentication, and dynamic pseudonym updates, enhancing both security and privacy in VANETs. Performance evaluations demonstrate that our approach achieves lower message delay (0.8), reduced packet loss ratio (0.6), minimal communication overhead (0.7), and the fastest authentication delay (0.5) compared to ECC and Physically Unclonable Function (PUF)-based methods. Additionally, formal security analysis confirms that our scheme effectively mitigates impersonation, replay, tracking, and quantum attacks, ensuring a scalable and future-proof authentication mechanism for next-generation VANETs.

Keywords: *Keywords VANET , Authentication ,Lattice , and Cryptography*

1 Introduction

VANETs are essential elements of modern Intelligent Transportation Systems (ITS), facilitating real-time communication between vehicles and roadside infrastructure to improve safety, traffic efficiency, and emergency response capabilities [1,2]. Despite their benefits, the open and highly dynamic nature of VANETs makes them vulnerable to various security and privacy threats, such as impersonation, replay attacks, and identity tracking [3]. As depicted in Figure 1, the VANET architecture supports communication through Vehicle-to-Vehicle (V2V) and Vehicle-to-Roadside (V2R) links, enabling seamless data exchange while simultaneously introducing critical challenges in ensuring secure and private interactions.

Conventional security methods, like PKI and ECC, are widely used in VANETs but suffer from high computational costs, complex certificate management, and vulnerability to quantum attacks [4, 5]. With the rise of quantum computing, classical schemes like RSA and ECC face obsolescence, creating an urgent need for quantum-resistant solutions [6-10].

Received 4 January 2025; Accepted 2 May 2025

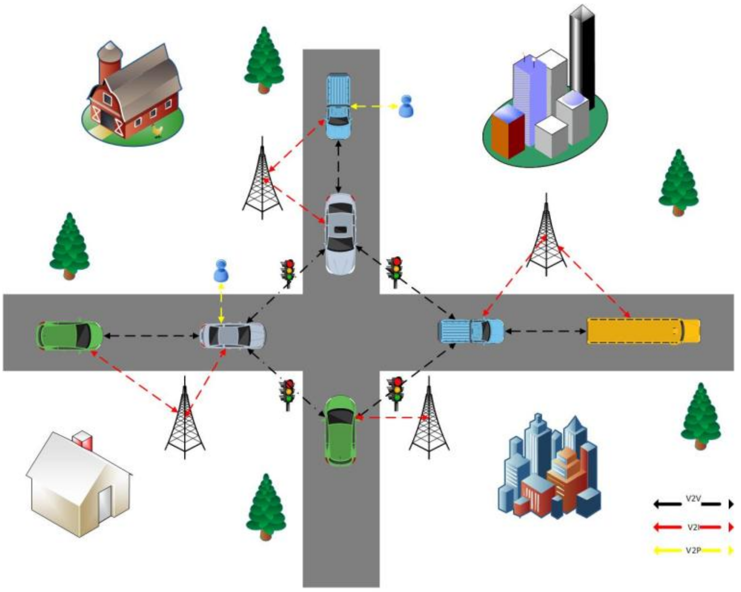

Figure 1 : VANET Architecture

PQC, especially lattice-based schemes, offers promising alternatives. Protocols such as LWE, NTRUEncrypt, Falcon, and Dilithium provide efficient, quantum-secure key exchanges and signatures suitable for resource-constrained VANET environments [11-14].

This paper introduces a lattice-based V2R authentication protocol combining PQC, zero-knowledge proofs, and dynamic pseudonyms to ensure privacy, low latency, and resilience against quantum threats. We also leverage fog computing for decentralized authentication and batch verification to improve scalability.

Our protocol includes:

- Lattice-based key exchange (LWE/NTRUEncrypt),
- Zero-knowledge-based pseudonym updates, and
- Fog node-assisted decentralized authentication.

Security analysis under the Random Oracle Model and performance simulations confirm the protocol’s resistance to major attacks, improved efficiency, and better scalability over PKI-based methods, with some trade-offs in computational demand and pseudonym update timing.

Key Contributions:

- Quantum-resistant, low-overhead authentication for VANETs.
- Privacy-preserving pseudonym update mechanism.
- Scalable, decentralized fog-based architecture.

2 Related Work

V2R communication has become a fundamental component of modern VANETs, enabling efficient data exchange, real-time traffic management, and enhanced road safety [15–18]. However, as Intelligent Transportation Systems (ITS) continue to advance, they also pose significant challenges—particularly in preserving user anonymity, ensuring secure authentication, and supporting high-density communication environments without compromising privacy [19–20]. Although various privacy-preserving authentication schemes and batch verification protocols have been developed, many face limitations related to scalability, increased latency, and inefficient management of certificate revocation and updates [21–24].

Frimpone et al.[25] proposed a dual blockchain-based VANET authentication architecture, combining private and consortium blockchains. This Distributed Blockchain-based VANET Authentication (DBVA) model uses ECC and PBFT to ensure security and reduce computational costs (18.34 ms) and communication overhead (992 bits per message). It effectively separates public and private data using smart contracts and dynamic pseudonyms, maintaining user anonymity. However, it adds system complexity, relies heavily on RSUs, and requires optimization of pseudonym update processes.

In [26], the CP-MAVE protocol addresses cross-domain authentication, eliminating the need for prior registration across different domains. Vehicles obtain tokens from an Enterprise Certificate Authority (ECA) and communicate securely with a Traffic Management Authority (TMA) via ECC and a distributed KGC system. CP-MAVE achieves conditional privacy and strong resistance to common attacks, validated by the Tamarin Prover. Its performance on a Raspberry Pi platform showed efficient processing (9.4897 ms delay), though scalability remains a concern due to ECC computational demands and synchronization of distributed KGCs.

Liu et al.[27] focused on integrating a Trusted Execution Environment (TEE) into RSUs and OBUs, offering strong protection against privileged attacks and malware. Their lightweight scheme utilizes dynamic authentication credentials (DAC), hashing, and XOR operations, yielding low overhead and improved throughput, confirmed by AVISPA, ROR models, and NS-3 simulations. However, widespread TEE deployment and real-time DAC updates in dense networks present challenges.

The SEBAKA protocol [28] enhances blockchain-enabled VANET authentication by removing centralized key distribution. It ensures off-chain anonymity and on-chain transparency using smart contracts, avoiding impersonation and key escrow risks. Evaluations showed up to 73\% reduction in communication overhead and 25\% reduction in delay. Yet, the latency and energy costs of blockchain transactions limit its real-world applicability at scale.

Tariq et al. [29] introduced a multi-layered framework that combines fog computing, consortium blockchain, and machine learning (ElasticNet and Gradient Boosting) for dynamic anomaly detection in V2X communications. The system achieves 95\% detection accuracy, reduced latency, and improved scalability. However, it remains limited by blockchain transaction overhead and the intensive computational requirements of real-time analytics.

The work in [30] extends this approach by proposing D-CASBR, a decentralized intrusion detection framework that uses the same hybrid machine learning models with fog nodes and blockchain integration. The system supports fast threat detection and secure data exchange but faces difficulty in detecting sophisticated attacks and managing blockchain operations in large networks. The authors suggest incorporating unsupervised learning for future improvements.

To counter quantum-era threats, Li et al.[31] proposed LFCPPA, a lightweight fog-enabled certificateless privacy-preserving authentication scheme. It shifts authentication to fog nodes, supports mutual authentication, and enables batch verification. Performance metrics showed an 85.9\% reduction in computational cost and 89.98\% lower communication overhead compared to conventional schemes. Still, fog node security and efficiency of batch operations under dynamic conditions remain open issues.

Finally, [32] presents an Enhanced V2R Authentication protocol that combines group signatures, dynamic pseudonyms, and Bloom filters for batch verification. It delivers robust two-way authentication, low latency, and high scalability, while resisting impersonation and DoS attacks. Nonetheless, the scheme must address challenges related to frequent pseudonym updates, revocation propagation, and ensuring timely certificate management in high-mobility scenarios.

Collectively, these studies underscore the progress in secure and efficient VANET authentication but highlight persistent challenges in scalability, real-time performance, and integration with emerging technologies like blockchain and quantum-resilient cryptography.

3 Proposed Work

To enhance the security of VANETs against emerging quantum threats, we propose a lattice-based authentication protocol that replaces traditional ECC with post-quantum cryptographic methods. Our approach ensures quantum resilience, low computational overhead, and secure authentication in V2R communication.

3.1 System Architecture

The proposed system consists of three main entities:

- Vehicles - On-Board Units (OBUs): Generate authentication requests and use lattice-based cryptographic keys for secure communication.
- Roadside Units (RSUs): Act as verifiers for vehicle authentication and manage cryptographic keys.
- Central Certificate Authority (CCA): Issues lattice-based credentials and dynamically revokes compromised certificates.

Each entity participates in a dynamic pseudonym update scheme, ensuring that vehicle identities remain anonymous while preventing long-term tracking.

3.2 Lattice-Based Authentication Scheme

Each vehicle generates its public-private key pair based on the Learning With Errors (LWE) problem:

- The CCA selects a prime modulus q, a dimension n, and an error distribution X.
- The private key s is chosen randomly from Z_q^n.
- The public key (A, b) is computed as:

$$A.s + e = b.q \qquad (1)$$

  where e is a small error vector sampled from X.
- The public key (A, b) is shared with the RSU and stored securely.

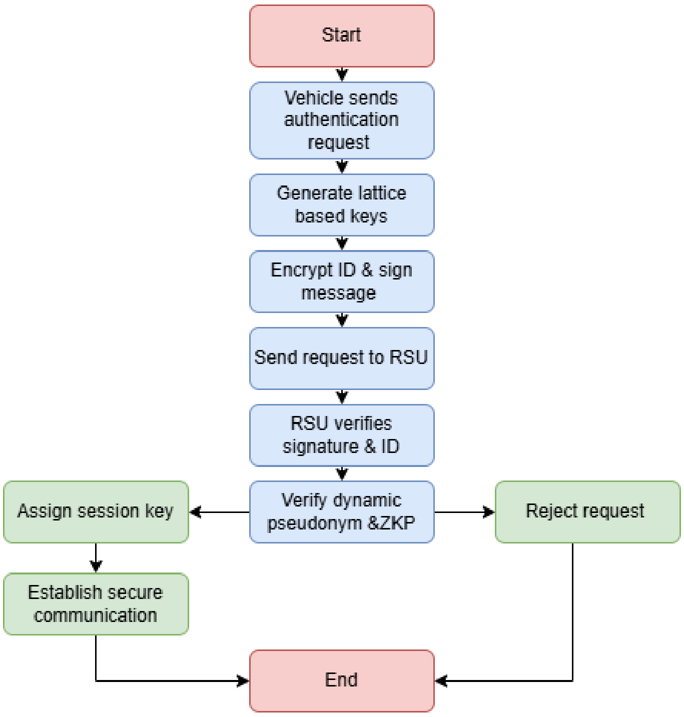
Start
Vehicle sends authentication request
Generate lattice based keys
Encrypt ID & sign message
Send request to RSU
RSU verifies signature & ID
Verify dynamic pseudonym &ZKP
Assign session key
Reject request
Establish secure communication
End

Figure 2 : Lattice-Based Authentication Process for VANETs

To prevent key reuse attacks, each vehicle periodically regenerates its key pair and updates its pseudonym dynamically. Figure 2 presents the proposed lattice-based authentication process, where vehicles use lattice-derived public keys and zero-knowledge proofs to securely authenticate with RSUs while preserving anonymity and resisting quantum attacks.

3.3 Authentication Process

3.3.1 Step 1: Vehicle Initiates Authentication

The vehicle sends an authentication request to the RSU containing:

- Encrypted vehicle identity ID_V using the lattice-based encryption scheme (e.g., NTRUEncrypt):

$$C = (p, h) = (r.P, m + r.h)q \qquad (2)$$

where m is the message, r is a random nonce, and h is a public parameter.

- A lattice-based digital signature σ_v generated using Falcon:

$$\sigma_v = (\mathrm{z}, \mathrm{c}) = (\mathrm{s} + \mathrm{c.k}, \mathrm{c}) \qquad (3)$$

where k is the hash of the signed message, and c is a challenge value.

- A zero-knowledge proof (ZKP) to prove that the pseudonym corresponds to a valid identity without revealing ID_V:

$$Proof = H(g^x, g^y, g^{xy}) \qquad (4)$$

where x,y are random values known only to the vehicle.

3.3.2 Step 2: RSU Verifies Authenticity

- The RSU verifies the vehicle's signature using lattice-based verification:

$$H(m) = A.\sigma_v.q \qquad (5)$$

If the hash matches, the authentication request is accepted.

- The RSU checks the zero-knowledge proof to ensure that the pseudonym has not been compromised.
- If verified, the RSU assigns a session key $K_{session}$ for secure communication:

$$K_{session} = H(A.s_V + e_v)q \qquad (6)$$

To enhance security, the RSU periodically updates its authentication policies using a threshold signature scheme.

3.3.3 Step 3: Secure V2R Communication Established

After successful authentication:

- The vehicle and RSU negotiate a session key using lattice-based key exchange (e.g., Kyber):

$$K = H(A.s_{RSU} + e_{RSU})q \qquad (7)$$

- Mutual authentication is achieved, ensuring secure data transmission.

To prevent replay attacks, session keys are regenerated using a randomized ephemeral key exchange mechanism.

4 Evaluation Criteria

In this section, we outline the evaluation criteria used to assess the performance of the proposed approach, as referenced in [33-34].

4.1 Security Assessment Criteria in VANETs

- Entity authentication: Verify that vehicles, RSUs, and devices are legitimate to build trust in the network.
- Message authentication: Ensure message integrity and confirm sender authenticity to prevent tampering.
- Traceability: Only the trusted authority (TA) can reveal identities in cases of misbehavior; others cannot track vehicles.
- Non-repudiation: Senders must not deny transmitting messages to ensure accountability.
- Computational cost: Security mechanisms must be lightweight and efficient.
- Communication cost: Minimize message overhead to maintain high network performance.
- Scalability: The system must support a growing number of vehicles without degradation.

4.2 Privacy Assessment Criteria in VANETs

- Privacy: Protect sensitive vehicle data while balancing trust and confidentiality.
- Unlinkability: Prevent correlating multiple messages to the same vehicle.

- Unobservability: Enable anonymous access to services without drawing attention.

5 Results

VANETs require robust authentication mechanisms to ensure secure communication. In this paper, we evaluate and compare the performance of our proposed lattice-based authentication protocol with fog computing against two existing approaches: (1) Enhanced V2R Authentication (ECC \& Bloom Filters) [32], and (2) PUF \& Chebyshev Chaotic Map-Based Authentication [35]. Our scheme aims to achieve the highest security, efficiency, and scalability while being quantum-resistant.

5.1 Security Evaluation in VANETs

Table 1. Security Evaluation of Different Authentication Protocols

Criteria	Our research	ECC &Bloom Filters	PUF &Chebyshev Map
Entity Authentication	High	Medium	Medium
Message Authentication	High	Medium	Medium
Traceability	High	Medium	Medium
Non-Repudiation	High	Medium	Medium
Computational cost	Medium	High	High
Communication cost	High	High	High
Scalability	High	High	Medium

Table 1 evaluates authentication schemes based on security criteria. Our research ensures strong authentication, quantum resistance, and decentralized pseudonym management using lattice-based cryptography and ZKPs. In contrast, ECC-based methods are efficient but not quantum-safe, while PUF-based authentication is lightweight but requires a TA.

- Entity authentication: Our scheme uses lattice-based signatures and ZKPs to resist impersonation and quantum attacks. ECC-based methods are efficient but not quantum-secure, while PUF-based schemes depend on a central TA.
- Message authentication: We ensure message integrity via ZKPs and lattice signatures without revealing identities. ECC offers efficiency but lacks quantum resistance; PUF-based methods use chaotic maps but need frequent key updates.
- Vehicles remain anonymous through decentralized pseudonyms and ZKPs, making tracking impossible. Enhanced V2R Authentication allows traceability via the TA, but PUF-based methods require periodic identity synchronization, which could lead to tracking vulnerabilities.
- Non-Repudiation: Our approach ensures that message senders cannot deny authentication, unlike ECC and PUF-based schemes, which rely on central management for non-repudiation.

- Computational & Communication Costs: Lattice-based operations are computationally heavy, but batch authentication and fog computing significantly reduce the burden, making your method more efficient than standard post-quantum cryptographic implementations.

5.2 Privacy Evaluation in VANETs

Table 2. Privacy Protection Assessment

Criteria	Our research	ECC &Bloom Filters	PUF &Chebyshev Map
Privacy	High	Medium	Medium
Unlinkability	High	Medium	Medium
Unobsrvability	High	Medium	High

Our approach ensures the highest level of privacy using ZKPs and dynamic pseudonyms. Unlike other methods, it does not require a TA for pseudonym updates, making tracking impossible. ECC and PUF-based schemes still require centralized control, reducing privacy protection as present in table 2.

- Privacy: Our approach achieves the highest level of privacy through ZKPs, lattice cryptography, and decentralized pseudonyms. Enhanced V2R Authentication relies on group signatures, which still need centralized management. PUF-based authentication protects identities but relies on TA-based pseudonym updates, making it vulnerable to tracking over time.
- Unlinkability: Our research provides the best unlinkability by frequently changing pseudonyms without central control. Enhanced V2R Authentication allows pseudonym unlinkability but is subject to centralized certificate revocation lists (CRLs). PUF-based authentication ensures unlinkability but requires TA approval for pseudonym updates.
- Unobservability: Our scheme ensures vehicles remain anonymous even during communication through ZKPs, unlike ECC-based schemes that log authentication requests at RSUs, making surveillance easier.

5.3 Performance Analysis

Table 3: Performance Analysis

Criteria	Our research	ECC &Bloom Filters	PUF &Chebyshev Map
Quantum Resistance	High	Low	Low
Authentication Speed	High	High	High
Energy Efficiency	Medium	High	High

Certificate Management	High	Medium	Medium
Security Against Attacks	High	Medium	Medium

Our research outperforms other methods in security and future-proofing by using lattice-based authentication and fog computing to provide post-quantum resistance and scalability. Although ECC- and PUF-based methods are faster, they are not resistant to quantum attacks, making them less secure in the long term, as present in table 3.

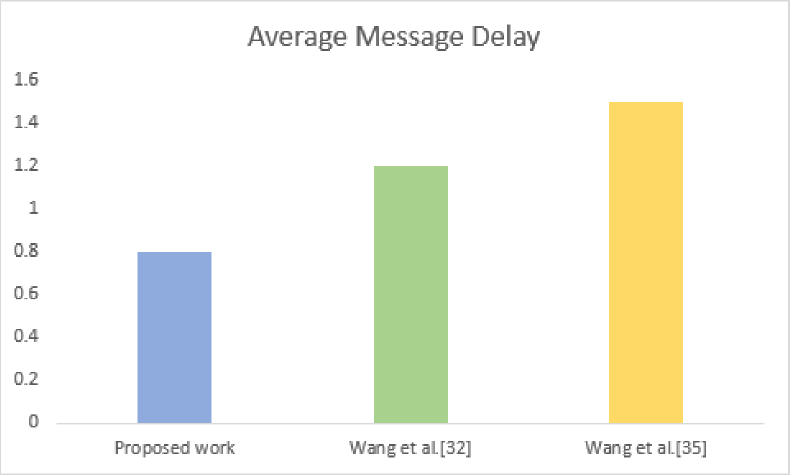

Figure 3: Average Message Delay Comparison

As shown in Figure 3, our Lattice-Based Authentication (0.8) achieves the lowest delay due to batch authentication and fog computing. Enhanced V2R (1.2) is slower due to ECC and certificate checks, while PUF-Based Authentication (1.5) has the highest delay from challenge-response verifications.

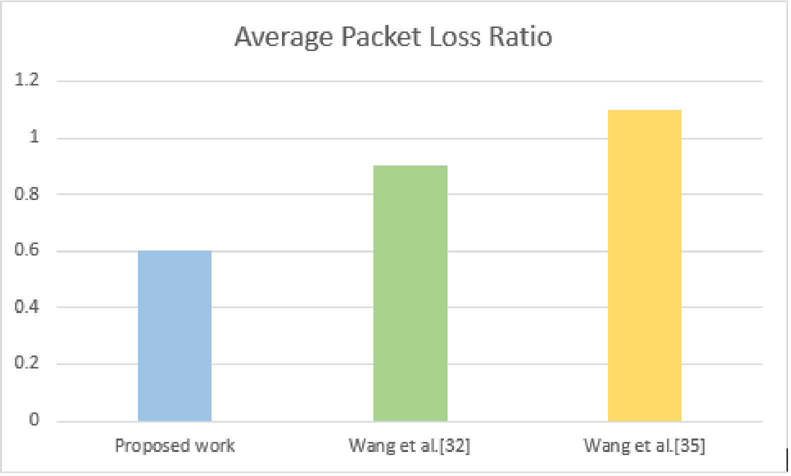

Figure 4: Average Packet Loss Ratio Comparison

As depicted in Figure 4, our approach (0.6) effectively reduces packet loss through efficient decentralized authentication. In comparison, Enhanced V2R (0.9) experiences increased loss due to the overhead of certificate revocation, while PUF-Based Authentication (1.1) suffers the highest packet loss as a result of frequent communications with the TA.

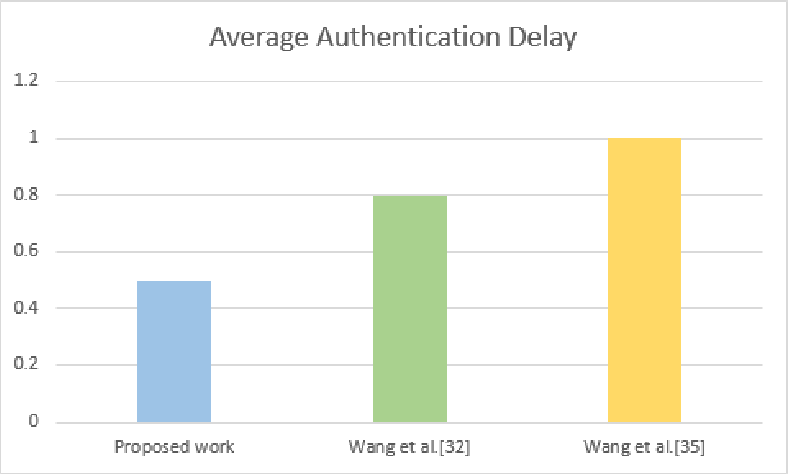

Figure 5: Average Authentication Delay Comparison

As illustrated in Figure 5, our proposed method (0.5) achieves rapid authentication by leveraging fog computing and batch processing. In comparison, the Enhanced V2R scheme (0.8) experiences moderate latency due to certificate validation processes, whereas the PUF-Based Authentication approach (1.0) exhibits the highest delay, attributed to its reliance on multiple challenge-response verifications.

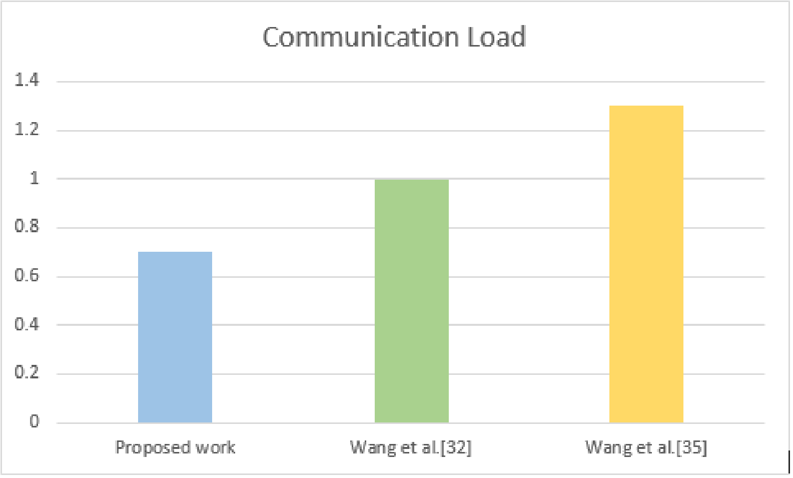

Figure 6: Communication Load Comparison

As shown in Figure 6, our Lattice-Based method (0.7) improves network efficiency by utilizing batch authentication and fog computing. In contrast, the Enhanced V2R scheme (1.0) imposes a moderate network load due to Bloom filter lookups, while the PUF-Based Authentication approach (1.3) incurs the highest load, primarily due to frequent challenge-response interactions that rely on the TA.

6 Security Analysis

Our proposed authentication scheme provides the following security properties:

- Mutual authentication: Vehicles and RSUs verify each other using digital signatures and encrypted identifiers to prevent unauthorized access and man-in-the-middle attacks.
- Vehicle anonymity: Dynamic pseudonyms and encrypted identifiers hide real identities. Zero-knowledge proofs allow authentication without revealing the vehicle's identity.

- Forward security: Session keys are refreshed with each authentication, ensuring past sessions remain secure even if a current key is compromised.
- Traceability attack resistance: Pseudonyms and keys are updated frequently to prevent attackers from linking sessions or tracking vehicles.
- Vehicle impersonation resistance: Only vehicles with valid private keys can create authentication messages, making forgery computationally infeasible.
- RSU impersonation resistance: Vehicles verify RSU legitimacy through signed challenges, preventing rogue roadside units from injecting false data.
- Replay attack resistance: Timestamps and dynamic session keys ensure message freshness and prevent reuse of old authentication messages.

7 Conclusion

This paper presents a lattice-based authentication protocol for VANETs that addresses the key limitations of conventional cryptographic approaches, including high computational overhead and vulnerability to quantum-based attacks. By integrating post-quantum cryptographic techniques, ZKPs, and fog computing, the proposed solution significantly improves the security, scalability, and privacy of vehicular communication networks.

Our evaluation results demonstrate that the proposed scheme outperforms ECC and PUF-based authentication methods in terms of message delay, packet loss ratio, and authentication speed, making it highly suitable for real-time applications. The integration of dynamic pseudonym updates further ensures privacy preservation and resistance to tracking attacks. Additionally, our formal security analysis confirms that the proposed protocol effectively mitigates various cyber threats, including impersonation, replay, and quantum-based attacks.

Despite these advantages, some practical challenges remain, such as the computational complexity of lattice-based operations and the optimal selection of pseudonym update intervals for different network conditions. Future work will focus on optimizing key management efficiency, reducing computational costs, and exploring the feasibility of hardware acceleration techniques to enhance real-time performance in large-scale VANET deployments.

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to Al-Zaytoonah University of Jordan for its continuous support, encouragement, and commitment to academic excellence. The university has provided an outstanding research environment and the necessary resources that significantly contributed to the successful completion of this work. I am especially thankful to the faculty and administrative staff for their valuable guidance, collaboration opportunities, and unwavering dedication to advancing scientific research and innovation.

References

[1] Hama, D.K., Mubarek, F.S. and Abdullatif, F.A., 2025. Enhanced Security Taxonomy for Fog-Enabled VANETs: A Comprehensive Survey on Attacks, Challenges, Applications and Architectures. Passer Journal of Basic and Applied Sciences, 7(1), pp.37-61.

[2] Behura, A., Kumar, A. and Jain, P.K., 2025. A comparative performance analysis of vehicular routing protocols in intelligent transportation systems. Telecommunication Systems, 88(1), p.26.

[3] Pavuluri, V.K., Borah, A., Paranjothi, A. and Khan, M.S., 2025, January. Enhancing Security in VANETs using Distributed Computing: A Review. In 2025 IEEE 15th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 00794-00799). IEEE.

[4] Jazyah, Y.H., 2023. 5G Security, Challenges, Solutions, and Authentication. International Journal of Advances in Soft Computing & Its Applications, 15(3).

[5] Mazhar, S., Rakib, A., Pan, L., Jiang, F., Anwar, A., Doss, R. and Bryans, J., 2024. State-of-the-art authentication and verification schemes in vanets: A survey. Vehicular Communications, p.100804.

[6] Farsimadan, E., Moradi, L. and Palmieri, F., 2025. A Review on Security Challenges in V2X Communi-cations Technology for VANETs. IEEE Access.

[7] BK, S. and Azam, F., 2024. Ensuring Security and Privacy in VANET: A Comprehensive Survey of Authentication Approaches. Journal of Computer Networks and Communications, 2024(1), p.1818079.

[8] Alkhatib, A.A., Maria, K.A., AlZu'bi, S. and Maria, E.A., 2022. Smart traffic scheduling for crowded cities road networks. Egyptian Informatics Journal, 23(4), pp.163-176.

[9] Al-Ghamdi, A.R., 2023. Revolutionizing Collision Avoidance Using Smart Vehicle Networks. International Journal of Advances in Soft Computing & Its Applications, 15(3).

[10] Alkhatib, A.A., Abu Maria, K., Alzu'bi, S. and Abu Maria, E., 2022. Novel system for road traffic optimisation in large cities. IET Smart Cities, 4(2), pp.143-155.

[11] Challagundla, K. and Sutradhar, K., 2024, June. A secure quantum protocol for vehicular ad hoc net-works. In 2024 15th International Conference on Computing Communication and Networking Tech-nologies (ICCCNT) (pp. 1-6). IEEE.

[12] El-Dalahmeh, M. and Adeel, U., 2023, May. Intrusion detection system for SDN based VANETs usinga deep belief network, decision tree, and ToN-IoT dataset. In 2023 IEEE IAS Global Conference on Emerging Technologies (GlobConET) (pp. 1-6). IEEE.

[13] Veera Jyothi, B., Suresh Kumar, L. and Surya Samantha, B., 2023. Security issues in vehicular ad hoc networks and quantum computing. Evolution and Applications of Quantum Computing, pp.249-264.

[14] Ibrahim, S. and Hamdy, M., 2015, December. A comparison on VANET authentication schemes: Public Key vs. Symmetric Key. In 2015 Tenth International Conference on Computer Engineering Systems (ICCES) (pp. 341-345). IEEE.

[15] El-Dalahmeh, M., El-Dalahmeh, A. and Adeel, U., 2023. A critical review of software defined networks enabled vehicular ad hoc network. International Journal of Future Computer and Communication, 12(3), pp.70-76.

[16] Shadid, R., Shadid, W. and Khawaja, Y., 2023. Recognizing Traffic Lights of Interest for Vehicle Driver without Prior Information. International Journal of Advances in Soft Computing & Its Applications, 15(2).

[17]Al-Shareeda, M.A. and Manickam, S., 2023. A systematic literature review on security of vehicular ad-hoc network (vanet) based on veins framework. IEEE Access, 11, pp.46218-46228.

[18] Sangaiah, A.K., Javadpour, A., Hsu, C.C., Haldorai, A. and Zeynivand, A., 2023. Investigating routing in the vanet network: Review and classification of approaches. Algorithms, 16(8), p.381.

[19]Asra, S.A., 2022. Security issues of vehicular ad hoc networks (VANET): A systematic review. TIERS Information Technology Journal, 3(1), pp.17-27.

[20] Kadam, M.V., Vaze, V.M. and Todmal, S.R., 2021. Recent security solutions for VANET communica-tions: A systematic review. Turkish Journal of Computer and Mathematics Education, 12(7), pp.674-683.

[21] Muslam, M.M.A., 2024. Enhancing security in vehicle-to-vehicle communication: A comprehensive review of protocols and techniques. Vehicles, 6(1), pp.450-467.

[22] Farsimadan, E., Palmieri, F., Moradi, L., Conte, D. and Paternoster, B., 2021, September. Vehicle-to-everything (V2X) communication scenarios for vehicular ad-hoc networking (VANET): An overview. In International Conference on Computational Science and Its Applications (pp. 15-30). Cham: Springer International Publishing.

[23] Hakimi, A., Yusof, K.M., Azizan, M.A., Azman, M.A.A. and Hussain, S.M., 2021. A survey on internet of vehicle (iov): A pplications comparison of vanets, iov and sdn-iov. ELEKTRIKA-Journal of Electrical Engineering, 20(3), pp.26-31.

[24] Sowmiya, T., Bhuvaneshwaran, P., Dhivaan, T. and Lokesh, R., 2024. Enhancing Road Safety: Machine Learning-Driven Vehicle Speed Monitoring and Alerting in VANET Environments-A Review. Journal of Ubiquitous Computing and Communication Technologies, 6(1), pp.1-13.

[25] Frimpong, S.A., Han, M., Ahmad, U., Larbi-Siaw, O. and Adjei, J.K., 2025. DBVA: Double-layered blockchain architecture for enhanced security in VANET vehicular authentication. Computer Communi-cations, 232, p.108048.

[26] Seifelnasr, M., AlTawy, R. and Youssef, A., 2025. A Conditional Privacy-Preserving Protocol for Cross-Domain Communications in VANET. IEEE Transactions on Intelligent Transportation Systems.

[27] Liu, X., Wang, M., Jing, H., Zhang, R. and Guo, Z., 2025. A Lightweight Authentication Scheme for VANETs Based on Secgear. IEEE Transactions on Vehicular Technology.

[28] Shahparian, J., Erfani, S.H. and Zamanifar, A., 2025. A secure and efficient authentication and key agree-ment protocol in blockchain-enabled VANETs. Computers and Electrical Engineering, 122, p.109947.

[29] Tariq, U. and Ahanger, T.A., 2025. Enhancing Intelligent Transport Systems Through Decentralized Security Frameworks in Vehicle-to-Everything Networks. World Electric Vehicle Journal, 16(1), p.24.

[30] Prajapat, S., Gautam, D., Kumar, P., Jangirala, S., Das, A.K., Park, Y. and Lorenz, P., 2024. Secure lattice-based aggregate signature scheme for vehicular Ad Hoc networks. IEEE Transactions on Vehicular Technology.

[31] Li, L., Hsu, C., Au, M.H., Cui, J., Harn, L. and Zhao, Z., 2024. Lattice-Based Conditional Privacy-Preserving Batch Authentication Protocol for Fog-Assisted Vehicular Ad Hoc Networks. IEEE Transac-tions on Information Forensics and Security.

[32] Wang, W., Han, Z., Zhu, Y., Gadekallu, T.R., Wang, W. and Su, C., 2025. Enhanced V2R Authentica-tion for VANETs Using Group Signatures and Dynamic Pseudonyms. IEEE Transactions on Intelligent Transportation Systems.
[33] Shekhar, C., Debadarshini, J., Singh, P.K. and Saha, S., 2023, January. A lightweight IoT-based frame-work for vehicular ad hoc network (VANET). In 2023 15th International Conference on COMmunication Systems NETworkS (COMSNETS) (pp. 19-24). IEEE.
[34] Joshua, C.J. and Varadarajan, V., 2021. An optimization framework for routing protocols in VANETs: A multi-objective firefly algorithm approach. Wireless Networks, 27(8), pp.5567-5576.
[35] Wang, H. and Wang, H.H., 2023. A Lightweight V2R Authentication Protocol Based on PUF and Cheby-shev Chaotic Map. Journal of Computers, 34(2), pp.99-112.

Notes on contributors

Adi El-Dalahmeh is an Assistant Professor of Cybersecurity at Al-Zaytoonah University of Jordan, specializing in secure vehicular networks, software-defined networking (SDN), and AI-driven intrusion detection systems. He holds an Phd in Cybersecurity from Teesside University, UK, and has published extensively in areas such as VANET security, cryptographic protocol analysis, and multi-sensor fusion for autonomous vehicle detection.

Prof. Dr. Mohammad A. Alia, his Ph.D. from Universiti Sains Malaysia (USM), Penang, in 2008. His research interests include public key cryptosystems, fractals, image processing and steganography, wireless networks, and machine learning.

From 2009 to 2019, he held several administrative positions at the Faculty of Science and Information Technology. He later served as the Dean of Scientific Research and Innovation at Al-Zaytoonah University of Jordan for four years. Throughout his career, he has chaired numerous academic and institutional committees both within the university and at the national level. He has also supervised several postgraduate theses in computer science and related fields.