RESEARCH PAPER

A CARLA-Based Simulation Study of Quantum Key Distribution for Securing Vehicle-to-Infrastructure Communication

Shiksha Kumari, Dr. Mukta
Sushant University
Shiksha181991@gmail.com ,Mukta@sushantuniversity.edu.in

Abstract
Communication in VANETs (Vehicular Ad-Hoc Network) is crucial when the vehicle is moving. Since these communications take place wirelessly without a direct physical connection, they are vulnerable to attacks such as spoofing, eavesdropping and message tampering. To protect these communications, various classical cryptographic algorithms are in use so that security breach is minimised. However, the algorithms focus on the complexity of the mathematical solution of problems, and such problems can be vulnerable to advanced quantum computing attacks, which makes them less suitable for required long-term quantum-resilient security.
To address the challenges related with VANETs, this paper has introduced a new approach which is Quantum Key Distribution (QKD). In the proposed approach, QKD is used to securely establish the encryption key, while the actual messages are transmitted through the conventional classical communication system. In addition, Zero Trust verification is incorporated as an additional security layer, ensuring that communication entities are continuously verified before trusted communication is established. The paper implements and compares two security architectures in the CARLA 0.10.0 simulator: a classical RSA+ECC-based approach and a proposed QKD with Zero-Trust architecture using AES-256. Their communication latency and cryptographic processing time are evaluated to assess the suitability of QKD-based security for low-latency V2X communication.

Keywords: Quantum Key Distribution, BB84 protocol, Vehicle-to-Infrastructure communication, Intelligent Transportation Systems, zero-trust security, CARLA simulator, post-quantum readiness.

How to cite this article: Shiksha Kumari, Mukta. A CARLA-Based Simulation Study of Quantum Key Distribution for Securing Vehicle-to-Infrastructure Communication. Int J Drug Deliv Technol. 2026;16(79s):550-557. DOI: 10.25258/ijddt.16.79s.107

I. Introduction

Light exhibits both wave-like and particle-like behavior, known as wave–particle duality. In recent decades, researchers have explored the quantum properties of light and matter for emerging technologies such as quantum computing, quantum communication, quantum random number generation [1], and Quantum Key Distribution (QKD) [2]. In 1905, Albert Einstein proposed the quantum nature of light through the concept of photons. Light can be prepared and measured as quantum states, particularly at the single-photon level. Properties such as photon quantization, superposition, polarization, measurement disturbance, no-cloning, entanglement, and wave–particle duality form the basis of QKD. Classical cryptography relies on the difficulty on mathematics-based solutions, for example integer factorization and discrete logarithms etc., which are vulnerable to quantum computers. QKD establish a key by using the physical phenomenon of photon of light. That follows the quantum mechanics of physics which enable the detection of eavesdropping in communication and this cryptography mechanism is quantum resistant. This paper investigates the use of QKD-derived keys for securing Intelligent Transportation Systems (ITS), where AES-256 is employed to encrypt messages in VANETs. The proposed approach is evaluated against conventional RSA- and ECC-based architectures by comparing their cryptographic mechanisms and communication latency. The practical feasibility of QKD-based security in transportation has also been demonstrated by the UK Innovate-funded AirQKD project, which uses Free-Space Optical QKD through laser transmitter–receiver units installed on rooftops. The project successfully used the generated quantum keys to secure a real V2I communication route on the University of Warwick campus.

Installing QKD hardware at every roadside unit is both expensive and difficult, so before that investment is justified, it is worth answering a narrower software-level question first: how should V2I messages be sent

and received, and does Zero-Trust authentication meaningfully improve protection against spoofed messages? This paper reports on a simulation study built to explore exactly that question.

This paper presents a software-based simulation of QKD logic within the CARLA environment. Two security architectures are implemented and evaluated: the first combines QKD and Zero Trust verification with AES-256 encryption, while the second uses RSA and ECC with AES-256 encryption. The study compares both architectures in terms of key-generation latency and cryptographic performance to evaluate the suitability of QKD-based security for autonomous vehicle communication.

The remainder of the paper is organized as follows. Section II reviews related work on QKD, on the AirQKD project specifically, and on classical RSA/ECC-based alternatives. Section III sets out the QKD and BB84 background needed to follow the rest of the paper. Section IV describes the CARLA-based simulation architecture. Section V describes the zero-trust check as implemented in the simulation. Section VI compares the proposed QKD+Zero-Trust architecture with classical RSA+ECC-combined architecture. Section VII discusses what CARLA can and cannot represent about a real FSO-QKD deployment. Section VIII discusses the results in the context of wider literature. Section IX outlines future work, and Section X concludes the paper.

II. Related Work

Hasan et al. [3] studied the security requirements and possible attacks in V2X system such as Eaves dropping, Spoofing, Replay Attack and Denial of Service [4]. Lonc et al. [5] describe a complete framework for C-ITS, explaining how a PKI should be structured and how a vehicle obtains a digital certificate and establishes trust before communicating; their work also touches on zero-trust principles within that framework. Bennett and Brassard's original BB84 paper [6] has described the full QKD working style. It covers all steps from basis selection to key generation from classical channel. In India ISRO, DRDO both have tested QKD. ISRO [7] establishes a video conferencing over a 300-meter using a resulting key of QKD. DRDO [8] has made significant progress in QKD from 2020 to 2026. Recently DRDO has reported progress toward military field deployment of scalable fiber-based QKD systems, moving the technology beyond laboratory demonstrations. QKD research is not limited to India; it is being actively pursued worldwide. In 2017, China demonstrated satellite-to-ground QKD over ~1,200 km [24]. Chinese and Austrian researchers demonstrated intercontinental QKD between China and Austria over 7600 km. All these demonstrations targeted fixed infrastructure rather than moving vehicles.

Fowler, Maple, and Epiphaniou [9] reported an important real-world project called AirQKD.In this project, QKD system has been built and tested using free space optical communication. The project included hardware capable of working with single photons, which are fundamental to QKD and it has also incorporated Angoka zero-trust authentication protocol (ZAP). This System was tested in a real Vehicle-to-Infrastructure (V2I) environment.

Most researcher has applied QKD in vehicular network is theoretical or simulation based. [10] has proposed a architecture where satellite is using to provide QKD-based secure communication between vehicles. [11] has proposed using quantum techniques to verify the identity of vehicles in a Vehicular Ad Hoc Network (VANET). Sandeep et al. [12] studied the performance of a hybrid communication system combining Radio Frequency (RF) and Free-Space Optical (FSO) communication to improve communication reliability. Xu et al. [13] has given the another perspective to use QKD. They have used QKD to protect communication in federated Learning. Yuan et al. [14] investigated QKD is working properly in 6G-V2X or not. In Moving System, there is one problem to establish a clear connection between sender and receiver. In most of the research QKD is promising but physical deployment is very difficult. This paper has proposed architecture where QKD can be used with AES and it will improve the communication reliability.

RSA and Elliptic Curve Cryptography (ECC) remain the incumbent alternatives against which any QKD-based proposal for V2I has to be compared. RSA's security rests on the difficulty of integer factorization [15], while ECC (and ECC-based schemes such as ECDSA) rest on the elliptic-curve discrete-logarithm problem, which is believed to require a smaller key size for an equivalent classical security level and is accordingly favored in several V2I performance-comparison studies [16]. Both are, in principle, vulnerable to Shor's algorithm on a sufficiently capable quantum computer, which is the long-term motivation for looking at QKD-derived keys as an alternative or a hybrid supplement to PKI. Several studies have explored the application of QKD and advanced authentication mechanisms in vehicular communication networks. Prateek et al. [17] proposed a QKD-based V2I authentication scheme to enhance security in vehicular communications. Similarly, Yang

et al. [18] developed a QKD-enabled Internet of Vehicles (IoV) architecture integrated with lattice-based authentication to strengthen security against emerging threats. In contrast, Yun et al. [19] proposed an optimized digital signature-based authentication scheme for VANETs, focusing on reducing authentication overhead and improving computational efficiency.

III. Preliminaries: Quantum Key Distribution and the BB84 Protocol

Quantum Key Distribution (QKD) provides a mechanism for securely distributing a secret key between two legitimate parties without revealing the key to an unauthorized third party. Unlike conventional cryptographic techniques, whose security primarily relies on the computational difficulty of mathematical problems, QKD derives its security from the fundamental principles of quantum mechanics. Several QKD protocols have been proposed, including BB84, E91, B92, and the Six-State protocol. Although these protocols use different mechanisms, their primary objective is to establish a shared secret key while detecting any attempt by an eavesdropper to interfere with the quantum communication. In this paper, the BB84 protocol is used because of its relatively simple implementation and suitability for the simulated sender–receiver communication model. In BB84, the communicating parties independently and randomly select measurement bases to encode and measure quantum states. After transmission, they publicly compare the selected bases without revealing the corresponding bit values and retain only the measurements obtained using compatible bases. Any unauthorized attempt to observe or disturb the transmitted quantum states can introduce detectable errors in the resulting measurements, thereby enabling the communicating parties to identify potential eavesdropping.

A. AES-256

The Advanced Encryption Standard (AES) [20] is a AES (Advanced Encryption Standard) is a symmetric-key encryption algorithm that uses the same secret key for encryption and decryption. It operates on 128-bit data blocks with key sizes of 128, 192, or 256 bits. In this work, AES-256-GCM is used because of its strong security and ability to provide both confidentiality and data integrity. GCM generates an authentication tag that enables the receiver to detect unauthorized modification or tampering of transmitted data. AES-256-GCM is used in both architectures to ensure that the performance comparison primarily reflects differences in key establishment and identity-verification mechanisms, rather than the underlying encryption algorithm

B. The BB84 Protocol and Photon Polarization

BB84 [21] encodes each key bit onto the polarization state of a single photon. Photons are transverse electromagnetic waves, and polarization describes the plane in which the associated electric field oscillates; BB84 uses linear polarization, typically expressed as one of two conjugate "bases" for example, a rectilinear basis with polarizer angles at 0° and 90°, and a diagonal basis at 45° and 135°.

To generate a key, the sender chooses a random bit and a random basis for each photon and sends the corresponding polarization state to the receiver. The receiver does not know in advance which basis the sender used for a given photon, so each incoming photon is measured in a randomly chosen basis of the receiver's own. After the transmission is complete, the sender and receiver publicly compare, over the classical channel, which basis they used for each photon — but not the bit value itself. Photons for which the bases happened to match are kept; those for which the bases differed are discarded, since a measurement in the wrong basis gives a result uncorrelated with the bit the sender sent. This basis-reconciliation step is usually called "sifting," and the surviving, basis-matched bits form the raw shared key.

Figure 1 illustrates this procedure for fifteen transmitted photons. Guessing incorrectly disturbs the quantum state and introduces errors into the shared key. By comparing a small, randomly chosen portion of their keys, the sender and receiver can detect these errors and determine whether eavesdropping has likely occurred. QKD therefore does not prevent interception outright, but it does make interception detectable.

Polarizer Used by Sender															
Polarizer	⤢	↕	⤡	⤢	↔	⤢	↕	↔	↕	⤢	↕	↕	↔	⤢	⤡
Bit Value	1	1	0	1	0	1	1	0	1	1	1	1	0	1	0
Polarizer used by Reciever															
Polarizer	↕	↔	↔	↕	↔	↔	↕	↕	↔	↕	↕	⤡	↔	↕	⤡
Bit Value	1	0	0	1	0	0	1	1	0	1	1	0	0	1	0
Key	X	X	X	X	0	X	1	X	X	X	1	X	0	X	0

Fig. 1. Illustrative BB84 basis-reconciliation ("sifting") example.

These field demonstrations, discussed in Section II, remain fixed-infrastructure deployments; extending QKD to a link where one or both endpoints are moving vehicles is the harder problem that motivates both the

AirQKD project's FSO-QKD work [9] and the software-level simulation reported in this paper.

IV. Proposed CARLA-Based V2I Simulation Architecture

Maintaining a continuous optical line of sight (LOS) between two moving vehicles is challenging. Therefore, a QKD-generated key is established at the initial stage of communication and used to encrypt the vehicle's messages before transmission to the RSU. The RSU then securely communicates the received information to the other vehicle. We follow the same architectural choice in the simulation described here: each vehicle establishes a session with the nearest Roadside Unit (RSU) rather than directly with other vehicles, and communication between neighboring RSUs (infrastructure-to-infrastructure, I2I) is treated as the more tractable case, since fixed infrastructure does not have the mobility or line-of-sight problems that moving vehicles do. The simulation is implemented in CARLA 0.10.0. Two vehicle actors are spawned manually: one under manual control and one under CARLA's built-in autopilot, so that the pairing can be driven into accident-prone scenarios (near-collisions, Rear Collision, Spontaneous vehicle, sudden braking, lane changes,) that exercise the V2I data path under realistic, if simulated, traffic conditions.

Each vehicle periodically reports its location, speed, acceleration, and collision-related state to a simulated RSU node. And once a QKD is established then the same key is used in AES-256 CGM encryption mechanism. The system uses the BB84 QKD protocol at the logical level, rather than simulating the physical behavior of photons, weather effects, or optical receiver hardware. Once a packet is available, every incoming V2I message is first authenticated using a Zero-Trust mechanism: if the sender cannot prove its identity, or is identified as a spoofed device, the message is rejected immediately regardless of its content.

Figure 2 shows the resulting architecture: each vehicle's telemetry is treated as the payload that would, in a physical deployment, be encrypted under a QKD-derived session key before transmission; the RSU applies a zero-trust credential check before accepting an incoming message, and a separate, deliberately compromised on-board-unit (OBU) actor is used to inject spoofed messages so that the check's effect can be observed. The physical FSO-QKD system developed under the Innovate UK AirQKD project [9] demonstrates the practical feasibility of QKD at the hardware level while also highlighting the challenges associated with establishing and maintaining a reliable optical line-of-sight (LoS) link. To address this limitation, the proposed approach establishes a shared QKD-derived key in advance and uses it to secure multiple subsequent messages, rather than generating a new key for every individual transmission. Telemetry data are transmitted periodically and stored on a centralized server, while accident-related data are transmitted immediately upon detection and permanently recorded on the blockchain. In addition, cryptographic hashes of periodic telemetry records are tamper evidence. Once the corresponding verification information has been securely anchored on the blockchain, older routine telemetry data can be periodically removed from the centralized server, thereby reducing storage requirements while preserving their integrity-verification capability.

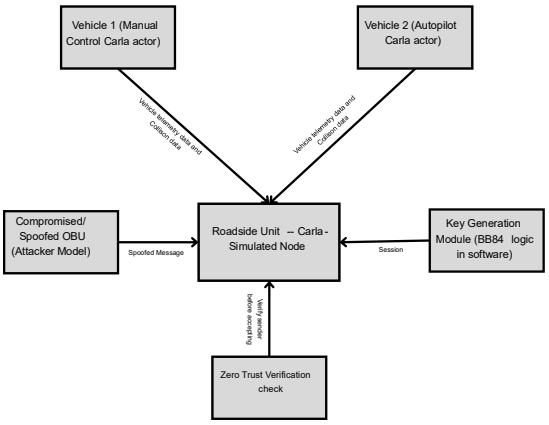

Fig. 2. Conceptual architecture of the CARLA simulated V2I setup

This single-key-generation and controlled key-reuse strategy reduces the frequency with which fresh key material must be generated and minimizes the computational and communication overhead associated with establishing a new key for every message. Consequently, the proposed approach improves the practicality of QKD-based security for vehicular communications by reducing the dependence on continuous optical LoS availability and addressing an important operational limitation highlighted by the AirQKD project. Figure 3 illustrates the proposed architecture, from QKD-based shared-key generation to the secure transmission of V2X messages with zero-trust verification. We represent QKD key derivation at the logical level described in Section III, including random basis selection, transmission, and sifting, rather than modelling the transport of individual photons through a simulated optical channel. This approach enables the evaluation of V2I message handling and zero-trust security logic independently of the physical QKD hardware layer. It also reduces simulation complexity while preserving the essential

key-establishment.

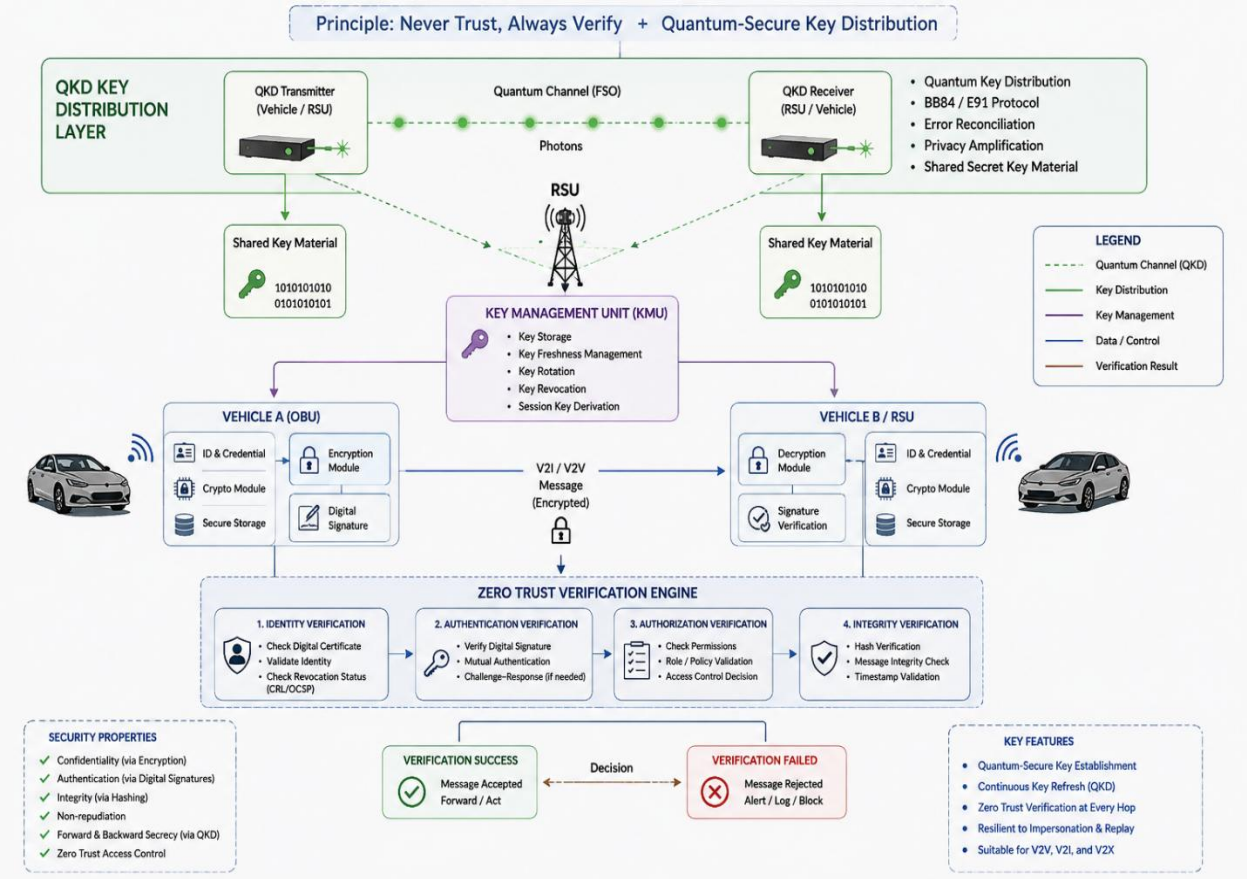

Fig. 3. Zero-trust verification with QKD architecture for V2V/V2I communication.

V. Zero-Trust Verification

The Zero-Trust principle [22] requires every communicating entity and request to be explicitly verified rather than assuming that a message is legitimate simply because it arrives through a trusted communication channel. In the physical AirQKD project [9], the Angoka Zero-Trust Authentication Protocol (ZAP) applied this principle to secure vehicular communications. In this work, the same principle is incorporated into the CARLA-based simulation. Before an incoming message is processed by a receiving vehicle or Roadside Unit (RSU), the claimed identity of the sender is verified. Even when an injected message conforms to the expected message structure, field format, and communication protocol, it is subjected to additional security checks. The Zero-Trust mechanism verifies who sent the message, whether the sender is authenticated and authorized, and whether the message is valid and sufficiently fresh. To evaluate this mechanism, a spoofed message was injected into the VANET communication through an OBU actor in the simulation. The receiving RSU performed the Zero-Trust verification and identified the message as unauthorized or spoofed, after which the message was rejected. This demonstrates that incorporating Zero-Trust verification provides an additional security layer for protecting VANET communication against spoofed or unauthorized messages. And It is a security decision process consisting of authentication, authorization, message-integrity, freshness, and policy checks. To achieve this, a trusted registry is created in an SQLite database before the simulation begins. The registry maintains essential information for each participating entity, including Driver ID, device type, status, role, and authorized permissions. During the simulation, the RSU uses this registry to perform Zero-Trust verification of incoming messages by validating the sender's identity, status, assigned role, and authorization for the requested operation. Only messages that satisfy the defined security policies are accepted and processed by the RSU.

VI. Comparison of the Proposed Architecture with an RSA+ECC Combined Architecture

To evaluate the security-latency trade-off in V2I communication, two candidate architectures were implemented for encrypting and authenticating telemetry messages sent from the vehicle to the roadside unit (RSU). Several architectures have been proposed in the existing literature for securing vehicular communication networks. Most studies primarily rely on RSA, ECC, or hybrid RSA–ECC architectures for authentication and secure communication. However, the existing literature does not provide a dedicated and systematic comparison of encryption time or key-setup time for these architectures under a common simulation environment. Therefore, based on an analysis of multiple existing studies, this research considers two representative architectures: (i) a classical cryptography-based architecture using RSA–ECC and (ii) a QKD-based architecture incorporating Zero-Trust verification. Both architectures are implemented and evaluated in the CARLA simulator to provide a comparative analysis of key setup, authentication, encryption, and communication latency under vehicular scenarios. The first architecture, referred to as QKD with Zero trust, uses a symmetric encryption key derived from a quantum key distribution (QKD) channel. Rather than generating a brand-new key for every single message which would be impractical given the limited key-generation rate of real QKD hardware, the key is refreshed periodically, after a fixed number of messages. Each message is then encrypted using AES-256 in Galois/Counter Mode (GCM), which provides both confidentiality and message integrity in a single operation; no separate authentication step is needed, since the GCM authentication tag serves that purpose. Alongside encryption, every message is subjected to a zero-trust identity check, meaning the sender's identity and trust status are re-verified each time. In practice, most of these checks are served quickly from a local cache, with occasional full re-verification against policy. The second architecture, referred to as RSA and ECC, represents a conventional public-key infrastructure (PKI) approach. It uses Elliptic Curve Diffie–Hellman (ECDH) key agreement [21] to establish a temporary session key between the vehicle and the RSU, which is then used with the same AES-256-GCM cipher as the first architecture. This design choice was deliberate: by keeping the underlying encryption algorithm identical across both architectures, the comparison isolates the effect of the key-establishment and identity-verification mechanism rather than simply comparing different ciphers. In addition to encryption, this architecture attaches an RSA-2048 digital signature [22] to every message, using the PSS padding scheme. This signature step exists because a shared symmetric key alone cannot prove, to a third party, who actually sent a message a property known as non-repudiation, which is a standard requirement in PKI-based systems. Identity is verified through a certificate check, which confirms the sender's certificate is valid and has not been revoked; unlike the zero-trust model, this check relies on a long-lived certificate and does not re-evaluate the sender's live trust status on every message. By holding the encryption algorithm constant between the two architectures, the comparison presented in this work reflects the cost of how identity and key material are established and verified, rather than differences in the encryption cipher itself.

Table 1 Latency Breakdown by Path Step

Path Step	QKD+ZT Mean (ms)	RSA+ECC Mean (ms)
Encryption / Key Setup	0.352	2.689
Identity Check (Zero-Trust / Cert)	1.183	1.065
Sent to RSU	2.922	2.872

Table 2 shows the end-to-end latency of sending a telemetry message from the vehicle to the RSU under the two architectures, measured on the same 104 real messages captured during a live CARLA simulation. The QKD + Zero-Trust architecture achieved a lower mean latency than the RSA + ECC combined architecture, a reduction of approximately 33%. This trend held for the median as well. The QKD + Zero-Trust architecture also showed lower variability, with a standard deviation of 1.420 ms compared to 2.725 ms for RSA + ECC combined, and a lower worst-case latency (9.637 ms versus 14.024 ms). This latency advantage is consistent with the architectural difference between the two schemes: AES-256-GCM's built-in authentication tag allows the QKD with Zero-Trust architecture to achieve confidentiality and integrity in a single pass, whereas the RSA + ECC architecture additionally requires an RSA-2048 digital signature over every message to provide non-repudiation, which is a comparatively expensive operation and the likely source of both its higher mean latency and greater variance.

Table 2 End-to-End Latency (Vehicle → RSU)

Architecture	Mean (ms)	Median (ms)	StDev (ms)	Min (ms)	Max (ms)
QKD + Zero-Trust	4.457	4.419	1.420	0.603	9.637
RSA + ECC combined	6.626	5.815	2.725	1.986	14.024

VII. Simulation Scope and Limitations

CARLA is a rigid-body vehicle and traffic simulator; It is good in to track the vehicle and for the traffic simulation and, but it has no built-in representation of the physical layer that a real FSO-QKD deployment depends on. A CARLA-based implementation of the kind described here cannot capture the laser signal travels through space and how much of its power remains available at the receiver as the distance increases. Carla is working irrespective of real Environment. In real scenario, Fog, rain, and atmospheric turbulence can interfere with the laser beam used in an FSO/QKD communication link, reducing its signal strength and sometimes making communication impossible. But it is not considerable in this simulation process. QKD demands transmitter must be pointed exactly towards Receiver. QKD is in software version it is not in physical way.

In this simulation, the integration of QKD, AES-256-GCM, and Zero-Trust verification demonstrates a strong security approach for VANET communications. However, the results do not imply that the proposed architecture provides 100% or absolute security against all possible attacks. The simulation primarily demonstrates its effectiveness against the specific threats and scenarios evaluated, while more sophisticated attacks, such as the compromise of a legitimately authenticated device, require further investigation. In this simulation, atmospheric pressure has been bypassed.

VIII. Discussion

The findings from Sections II–VII indicate that AirQKD and CARLA provide complementary approaches. AirQKD demonstrates the physical feasibility of QKD-secured, zero-trust V2I communication, while CARLA enables software-based evaluation of operational aspects such as key lifetime, key refresh, message handling, traffic conditions, and attacks without requiring a physical FSO-QKD system.

In the proposed architecture, QKD generates shared secret keys that seed AES-256-GCM rather than being used as a conventional one-time pad, which would require impractically large fresh keys for every message. Periodic key refresh improves practical deployment while retaining quantum-derived key generation and zero-trust identity verification. The proposed QKD+Zero-Trust architecture is compared with a conventional RSA+ECC-based VANET security architecture in terms of security, key generation, encryption, and communication overhead, as summarized in Table 3.

Table 3 Qualitative Comparison of Architectures

Property	QKD + Zero-Trust	RSA + ECC Combined
Key origin	Quantum-derived	Computationally hard math problem
Long-term (post-quantum) security	Information-Simulation Based	Vulnerable to Shor's algorithm
Per-message re-authentication	Yes (live trust check)	No (certificate valid until expiry)
Non-repudiation	Requires additional design	Built in (RSA signature)
Single point of failure	QKD link availability	Certificate Authority
Infrastructure required	Dedicated QKD hardware	Standard PKI

IX. Future Scope

The current work employs the BB84 protocol for quantum key generation. The framework could be extended by implementing and evaluating more advanced QKD protocols, such as Measurement-Device-Independent QKD (MDI-QKD) [25] and Twin-Field QKD (TF-QKD) [26], to improve resistance to device-level attacks and support longer-distance secure communication in V2I environments. A separate but related direction, noted in Section VIII, is to benchmark the classical architecture studied here against a post-quantum variant using NIST's ML-KEM/ML-DSA standards [20] rather than RSA/ECC, to see whether a purely software-based quantum-resistance strategy closes the gap with the QKD+Zero-Trust architecture on both latency and long-term security grounds.

A more significant next step is to replace the simulated QKD key-generation mechanism with an actual physical QKD system, which would allow the proposed security architecture to be evaluated under realistic communication and channel conditions rather than idealised ones. This would also make it possible to repeat the RSA/ECC comparison reported in Section VI using identical V2V and V2I scenarios but with genuine, hardware-generated keys, providing quantitative evidence on security, key-generation rate, message latency, and computational overhead under real-world conditions, and enabling a more realistic assessment of this approach's practical advantages and limitations.

X. Conclusion

This paper has made the case for using Quantum Key Distribution to secure Vehicle-to-Infrastructure communication, summarized the BB84 protocol that

underlies QKD key generation, and described a CARLA-based simulation (CARLA 0.10.0) that represents the logical behavior of a QKD-keyed, zero-trust V2I link: two vehicles, one manually driven and one under autopilot, exchanging state information with a simulated roadside unit, with a zero-trust credential check used to reject messages from a simulated compromised device. The proposed architecture provides a quantum-resilient security framework for V2V and V2I communication by combining QKD-based key generation, AES-256-GCM encryption, and Zero-Trust verification. The use of QKD provides a quantum-resistant foundation for key establishment, while AES-256-GCM provides both confidentiality and message integrity in a single, efficient operation without the impractical key-generation demands of a true per-message one-time pad. The integration of Zero-Trust verification adds a further layer of security by continuously verifying communicating entities before accepting their messages, rather than trusting a device indefinitely once it has authenticated. The results summarized in Section VI indicate that the proposed architecture achieves lower simulated message-processing latency than the RSA- and ECC-based classical cryptographic mechanisms considered in this study, primarily because AES-256-GCM's built-in authentication removes the need for the separate digital-signature step that the classical architecture requires for non-repudiation. Overall, the proposed approach demonstrates the potential of combining QKD-derived keys, efficient authenticated encryption, and Zero-Trust verification to provide practical, quantum-resilient security for future V2V and V2I communication systems.

References

[1] M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," Rev. Mod. Phys., vol. 89, 015004, 2017.

[2] J. P. Dowling and G. J. Milburn, "Quantum technology: The second quantum revolution," Philos. Trans. R. Soc. Lond. Ser. A Math. Phys. Eng. Sci., vol. 361, pp. 1655–1674, 2003.

[3] M. Hasan, S. Mohan, T. Shimizu, and H. Lu, "Securing Vehicle-to-Everything (V2X) Communication Platforms," IEEE Trans. Intell. Veh., vol. 5, pp. 693–713, 2020.

[4] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: A survey," Vehicular Communications, vol. 7, pp. 7–20, 2017.

[5] B. Lonc, F. Haidar, and D. Filatov, "Cooperative ITS Security Standards: Implementation, assessment and next challenges," in Proc. Virtual ITS European Congress, Lisbon, Portugal, 2020.

[6] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in Proc. IEEE Int. Conf. Computers, Systems & Signal Processing, Bangalore, India, 1984, pp. 175–179.

[7] Indian Space Research Organisation, "ISRO makes breakthrough demonstration of free-space Quantum Key Distribution over 300 metres," ISRO press release, Ahmedabad, India, 2021.

[8] Press Information Bureau, Government of India, "DRDO and IIT Delhi scientists demonstrate Quantum Key Distribution between two cities 100 kilometres apart," Ministry of Defence press release, Feb. 2022.

[9] D. S. Fowler, C. Maple, and G. Epiphaniou, "A Practical Implementation of Quantum-Derived Keys for Secure Vehicle-to-Infrastructure Communications," Vehicles, vol. 5, no. 4, pp. 1586–1604, 2023.

[10] M. Q. Vu, N. T. Dang, and A. T. Pham, "HAP-Aided Relaying Satellite FSO/QKD Systems for Secure Vehicular Networks," in Proc. 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), Kuala Lumpur, Malaysia, 2019.

[11] Z. Chen, K. Zhou, and Q. Liao, "Quantum identity authentication scheme of vehicular ad-hoc networks," Int. J. Theor. Phys., vol. 58, pp. 40–57, 2019.

[12] V. Sandeep, D. S. Gurjar, S. Yadav, P. Pattanayak, and Y. Jiang, "On the Performance Analysis of V2N Mixed RF and Hybrid FSO/RF Communication System," IEEE Photonics J., vol. 14, no. 6, pp. 1–14, Dec. 2022.

[13] Q. Xu, L. Zhao, Z. Su, D. Fang, and R. Li, "Secure Federated Learning in Quantum Autonomous Vehicular Networks," IEEE Netw., pp. 1–8, 2023.

[14] H. Yuan, D. S. Fowler, C. Maple, and G. Epiphaniou, "Analysis of outage performance in a 6G-V2X communications system utilising free-space optical quantum key distribution," IET Quantum Commun., 2023.

[15] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Commun. ACM, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[20] A.M.Abdullah,"Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data" 2017.

[21] M. SujayKumar Reddy and B. Chandra Mohan, "Comprehensive Analysis of BB84, A Quantum Key Distribution Protocol," *arXiv preprint arXiv:2312.05609*, 2023.

[22] J. Vinod, "Zero Trust Security Research paper," Dec. 10, 2025, doi: 10.13140/RG.2.2.17771.20001.