Grenze International Journal of Engineering and Technology, June Issue

A Review of Quantum Key Distribution Systems under Environmental Noise

Kumar Siddamallappa. U[1] and Shreedevi Prakash Gotur[2]
[1]Assistant Professor, DOS in Computer Science, Davangere University, Shivagangothri, Davangere-577007, Karnataka, India
Email: kumarkumarsm@gmail.com
[2]Research Scholar, DOS in Computer Science, Davangere University, Shivagangothri, Davangere-577007, Karnataka, India
Email: shreegotur@gmail.com

***Abstract*— Quantum Key Distribution (QKD) enables information-theoretically secure communication by exploiting quantum mechanics, making it a promising solution for next-generation network security. However, its practical deployment is hindered by environmental noise such as channel loss, background photons, atmospheric turbulence, and device imperfections, which degrade secret key rates and system reliability. This review analyzes the impact of noise on QKD systems across fiber, free-space, and hybrid communication channels, and compares the robustness of major protocols including discrete-variable (DV-QKD), continuous-variable (CV-QKD), entanglement-based, and one-sided device-independent (1SDI-QKD) schemes. It further surveys recent advancements in noise mitigation, including adaptive optimization, machine learning–based techniques, and improved optical architectures. Additionally, the integration of QKD into secure network infrastructures is discussed, focusing on key management and resilience against noise-assisted attacks. The study highlights current challenges and highlights future directions for developing scalable and noise-tolerant QKD systems.**

***Index Terms*— Quantum Key Distribution (QKD), Discrete-Variable QKD, Continuous-Variable QKD, One-Sided Device-Independent QKD, Environmental Noise, Network Security.**

I. INTRODUCTION

Quantum Key Distribution (QKD) offers theoretically secure communication with significant potential for broad adoption, but its practical implementation is challenged by environmental noise affecting key rates, prompting the development and evaluation of noise-modelling and mitigation strategies to ensure reliable real-world performance [1]. Quantum cryptography could well be the first application of quantum mechanics at the single-quantum level [2]. Quantum Key Distribution (QKD) offers theoretically secure communication with high potential for large-scale adoption, but its practical implementation is challenged by environmental noise affecting key rates, prompting the development and evaluation of noise-modelling and mitigation strategies to ensure reliable real-world performance [3]. Quantum Key Distribution (QKD) is a mature, commercially viable quantum communication technology that enables unconditionally secure key generation between authorized parties and is supported by practical security analyses across discrete-variable, continuous-variable, and distributed-phase-reference protocols [4].

Grenze ID: 01.GIJET.12.2.313_26

Quantum Key Distribution (QKD) enables two parties to share a secret cryptographic key whose security is guaranteed by quantum mechanics, positioning it as a promising foundation for next-generation network security. In conventional networks, key distribution typically relies on classical public key cryptography, which is vulnerable to quantum attacks and side channel exploitation; QKD provides an information theoretic alternative that can enhance long term security. However, moving QKD from controlled laboratory settings to real world deployments exposes it to environmental noise such as channel attenuation, background photons, atmospheric turbulence (in free space links), and device imperfections, which degrade secret key rates and may weaken security margins [5,6,7].

One-sided device-independent QKD (1SDI-QKD) provides a practical balance between security and implementation, but when realistic noise (amplitude damping, dephasing, depolarization) is considered, security depends on steering rather than entanglement and can be partially restored using optimized entanglement purification, defining practical limits for real-world quantum networks [8]. Machine learning–driven optimization of QKD protocols demonstrates that adaptive approaches significantly enhance efficiency, scalability, and eavesdropping detection under noisy conditions, outperforming entanglement-based and hybrid methods for secure real-world quantum communication [12].

A new optical architecture for CV-QKD based on the Faraday–Michelson interference optical architecture for continuous-variable quantum key distribution systems that mitigates polarization disturbances, enabling stable, robust, and high-rate (139 kbps over 70 km) secure key generation in real-world environments[21].

The main objective of this review is to analyze how QKD systems behave under environmental noise and how they can be integrated into secure network architectures. Specifically, we: Categorize major noise sources affecting QKD in fiber, free space, and wireless integrated links; Compare the noise robustness of DV-QKD, CV-QKD, entanglement based, and One Sided Device Independent like (1SDI-QKD) protocols; Survey adaptive and loss control based schemes that preserve secure key rates under noisy conditions; Discuss the role of QKD nodes in network security design, including key management, monitoring, and defence against noise assisted eavesdropping.

The paper proceeds as follows. Section 2 surveys relevant literature on QKD under environmental noise and in network contexts. Section 3 presents a comparative analysis of QKD protocols and architectures under noise. Section 4 concludes the paper and outlines open problems for noise tolerant QKD deployment in network security.

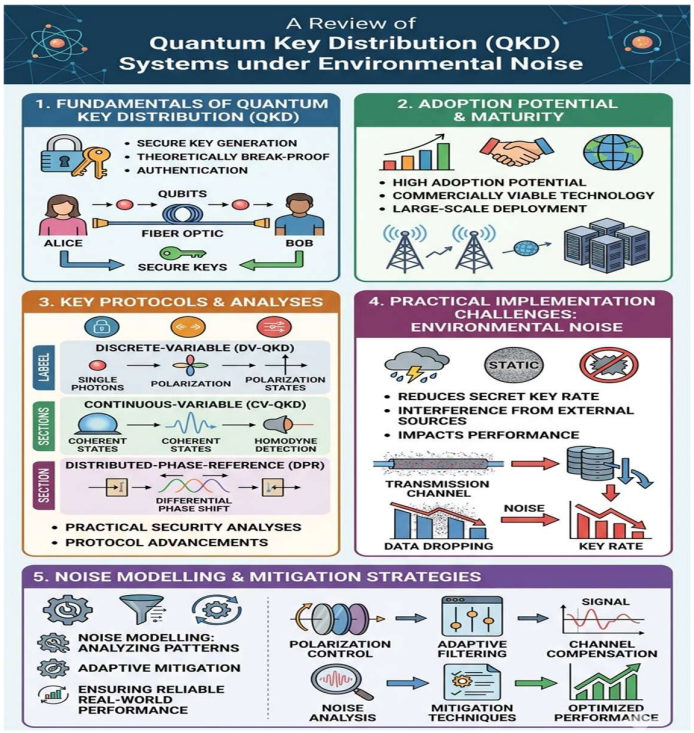

Fig 1

II. LITERATURE REVIEW

A. QKD Under Environmental Noise

Early theoretical work on QKD established fundamental limits imposed by loss and noise, showing that environmental disturbances can reduce or even eliminate the secret key rate if not properly handled. Recent studies demonstrate that Continuous Variable QKD (CV-QKD) can remain robust under moderate excess noise and background light, particularly when combined with efficient reconciliation and finite key analysis. Other investigations focus on Discrete Variable QKD (DV-QKD) designs, such as One Sided Device Independent QKD (1SDI-QKD), which are explicitly tailored to operate under realistic noise and imperfect devices [19,20,21,24,25]. Environmental noise is a major challenge in the practical deployment of Quantum Key Distribution (QKD) systems, as it increases the Quantum Bit Error Rate (QBER) and reduces key generation efficiency. Saiyed (2025) highlighted that channel disturbances, photon loss, and detector imperfections adversely affect QKD performance, emphasizing the need for optimized protocols and error-correction mechanisms to maintain secure communication [28]. Similarly, Imran et al. (2024) identified environmental factors such as attenuation, dark counts, and atmospheric disturbances as key obstacles to reliable quantum communication, recommending advanced detection and privacy amplification techniques to mitigate their effects [29]. Furthermore, Zhang et al. (2025) emphasized that environmental noise remains a critical concern for large-scale and global QKD networks, including fiber-based and satellite-based systems, necessitating the adoption of advanced protocols such as decoy-state and twin-field QKD to ensure secure long-distance communication [30]. Collectively, these studies demonstrate that effective noise mitigation is essential for enhancing the security, reliability, and scalability of QKD systems in real-world environments [28,29,30].

Experimental work on free space CV-QKD has shown that high solar background and atmospheric turbulence severely degrade key rates, but that adaptive schemes and noise reducing configurations can recover usable keys even under challenging conditions. These studies highlight the requirement for protocols with security proofs explicitly account for fluctuations in channel transmittance and excess noise, rather than assuming idealized, static conditions.

B. Network Oriented QKD Deployments

Several works have explored the integration of QKD into metropolitan and backbone networks, where QKD nodes distribute keys between backbone sites and edge devices. In such architectures, environmental noise arises from fiber attenuation and free space links (e.g., satellite ground terminals or rooftop to rooftop free space channels), necessitating noise aware route selection and key refresh strategies. Recent surveys emphasize that QKD based key management services must be treated as part of a broader network security framework, including authentication, monitoring, and post quantum hybrid security layers.

Standards bodies such as the ITU-T have begun to define security requirements for QKD nodes and their integration into telecommunication networks, specifying resilience criteria and operational constraints for QKD enabled infrastructures. These efforts underscore the significance of understanding how environmental noise impacts not only the quantum layer but also higher layer security protocols and network management [1,2,3,4,5].

Network-oriented Quantum Key Distribution (QKD) has emerged as a promising solution for securing future communication networks. The International Telecommunication Union (ITU, 2024) established security requirements for QKD-based services, emphasizing secure architectures, key management, and interoperability for practical network deployment [11]. Lin et al. (2014) proposed an efficient QKD scheme capable of mitigating collective noise without reducing transmission efficiency, thereby improving network reliability [17]. Zhang et al. (2025) highlighted the importance of noise-reduction techniques for enhancing the performance and scalability of QKD networks operating over fiber and free-space channels [14]. Furthermore, Imran et al. (2024) identified QKD as a key technology for securing future 5G/6G, cloud, and IoT networks while addressing challenges related to scalability and network integration [29]. Collectively, these studies demonstrate that secure, scalable, and noise-resilient architectures are essential for successful network-oriented QKD deployments.

C. Noise Mitigation and Adaptive Techniques

To combat environmental noise, researchers have proposed loss control based QKD schemes that dynamically adjust channel properties or trusted node strategies to maintain non-zero secret key rates. Other approaches include noise reducing QKD protocols that exploit bounds on device imperfections and channel noise to relax assumptions on the hardware while still guaranteeing security. Adaptive modulation schemes—where the modulation variance, repetition rate, or post selection thresholds are tuned in real time based on channel estimation—have been shown to improve the robustness of CV-QKD[19,20,21,24,25] under fluctuating noise.

Emerging work also explores machine learning assisted noise classification and channel monitoring, using the error rate of quantum bits (QBER) and other measurements to distinguish between natural noise and potential eavesdropping activity. These techniques align closely with network security paradigms (e.g., intrusion detection and anomaly monitoring), suggesting that QKD systems should be designed as intelligent, security aware components of larger networks.

III. Comparative Analysis

A. QKD Protocol Families Under Noise

The following table provides a high level comparative view of major QKD protocol families under environmental noise [15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30]:

TABLE I. COMPARISON OF QKD PROTOCOL FAMILIES UNDER ENVIRONMENTAL NOISE

Protocol family	Noise sensitivity	Typical QBER threshold	Noise-robustness mechanism	Best-fit network scenario
BB84-type DV-QKD	Sensitive to high loss and background	~11% (standard)	Error correction, privacy amplification	Point-to-point fiber links
Entanglement-based QKD	Moderate detector-noise sensitivity	Depends on setup	Bell/steering-based security tests	Backbone/inter-node links
CV-QKD	Tolerant to moderate excess noise	Varies with modulation	Gaussian modulation, reconciliation	Free-space, short-haul links
1SDI-QKD/ device-independent-like	Designed for noisy devices/channel	Varies by noise type	Steering-based security, noise-tolerant bounds	Heterogeneous QKD nodes

In general, higher environmental noise lowers secret key rate and effective transmission range, but some protocols (e.g., 1SDI-QKD and certain CV-QKD variants) trade device assumptions for improved noise tolerance. For network security, this implies that protocol selection should be guided by the expected noise profile at each link and the trust assumptions on the involved nodes.

B. Architectures and Network Topologies

Fiber only QKD networks are primarily affected by attenuation, bend induced loss, and temperature dependent fluctuations, where as free space and satellite integrated links introduce additional challenges from atmospheric turbulence and background light noise. In hybrid architectures that combine fiber and free space segments, the most susceptible component of the route often dictates the overall key rate and availability, necessitating careful noise characterization and fallback strategies.

From a network security perspective, backbone edge QKD architectures allow central QKD nodes to distribute keys to edge devices, supporting secure key management services for applications such as 5G/6G backhaul, IoT, and data-center interconnects. In such models, environmental noise impacts not only individual links but also overall stability and reliability of key distribution services, requiring redundancy and monitoring mechanisms similar to those in classical security infrastructures.

C. Security Aware Noise Management

Under environmental noise, error correction and privacy amplification must be strengthened to maintain information-theoretic security, particularly in the presence of finite-key effects and fluctuating excess noise. Furthermore, an increased QBER can obscure potential eavesdropping activities, making noise monitoring and adaptive re-authentication critical elements of secure network design. Recent approaches integrate QKD-generated QBER traces with machine learning techniques to identify anomalies and classify noise sources, enabling prompt actions such as re-handshaking or key revocation.

These advancements align QKD with broader network security objectives, including zero-trust architectures and post-quantum hybrid frameworks, where QKD-derived keys enhance or support classical cryptographic mechanisms. Consequently, noise-resilient QKD systems should be considered essential components of secure network infrastructures rather than standalone cryptographic links.

IV. Conclusion

In conclusion, this review underscores that while Quantum Key Distribution (QKD) provides information-theoretic security; its real-world deployment is significantly influenced by environmental noise, which affects both key generation rates and security margins. The comparative analysis of DV-QKD, CV-QKD, entanglement-

based, and 1SDI-QKD protocols reveals differing levels of noise tolerance, indicating that no single approach is universally optimal for all communication scenarios. However, recent advances in noise modelling, adaptive protocol design, and machine learning–based optimization have notably enhanced the resilience, efficiency, and practicality of QKD systems under realistic conditions.

From a broader network perspective, the integration of QKD into secure communication infrastructures requires a holistic approach that combines robust physical-layer implementations with efficient key management, continuous monitoring, and adaptive security mechanisms. Noise-resilient architectures and intelligent control strategies position QKD as a vital component of next-generation network security, particularly within hybrid and zero-trust frameworks. Future research should emphasize scalable deployment, standardized evaluation under diverse noise environments, and the development of fully adaptive QKD systems capable of sustaining secure performance in dynamic real-world networks. This review paper challenge is to reduce secret key rate under noise and for future enhancement use Twin-Field QKD and high-dimensional QKD for reduced the secret key rate and QBER rate for secure communication.

REFERENCES

[1] Haoran Zhang1, Wei Li, Ruihua He, Yan Zhang, Feihu Xu and Weibo Gao.(2025). Noise-reducing quantum key distribution. Reports on Progress in Physics, 88 (2025) 016001 (24pp). https://doi.org/10.1088/1361-6633/ad9505.

[2] Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. Reviews of Modern Physics, 74(1), 145–195. https://doi.org/10.1103/RevModPhys.74.145.

[3] Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. In Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing (pp. 175–179). IEEE.

[4] Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., & Peev, M. (2009). The security of practical quantum key distribution. Reviews of Modern Physics, 81(3), 1301–1350. https://doi.org/10.1103/RevModPhys.81.1301

[5] Philipp Sohr , Sebastian Ecker, Lukas Bulla, Martin Bohmann, and Rupert Ursin. Noise-reducing quantum key distribution. (2024). Physical Review Applied, 22, 024059. https://doi.org/10.1103/PhysRevApplied.22.024059

[6] Xue-Tao Zheng, Qi-Fa Zhang, Jie Ling, Guang-Can Guo & Zheng-Fu. Han Free-space continuous-variable quantum key distribution under high background noise. (2025). npj Quantum Information, 11, 1009.

[7] Valeria Pastushenko, Aleksei Kodukhov, Artyom Shindin, Vladislav Zemlyanov, Markus Pflitsch & ValeriiVinokur. Loss control-based QKD with noisy devices. (2025). Scientific Reports, 15, 17662.

[8] Syed M. Arslan, Muhammad T. Rahim, Asad Ali, Hashir Kuniyil, Saif Al-Kuwari, Qatar Center for Quantum Computing, HBKU, Doha, Qatar Noise-resilient 1SDI-QKD for practical quantum networks. (2026). arXiv. https://arxiv.org/abs/2602.00916

[9] Bourgoin, J.-P., Jennewein, T., Higgins, B. L., Helou, B., Erven, C., Hübel, H., Kumar, B., Hudson, D., D'Souza, I., Girard, R., Laflamme, R., & Weihs, G. (2015). Free-space quantum key distribution to a moving receiver. Optics Express, 23(26), 33712–33721.

[10] Peev, M., Pacher, C., Alléaume, R., Barreiro, C., Bouda, J., Boxleitner, W., Debuisschert, T., Diamanti, E., Dianati, M., Dynes, J. F., Fasel, S., Fürst, M., Gautier, J.-D., Gay, O., Gisin, N., Grangier, P., Happe, A., Hasani, Y., Hentschel, M., … Zbinden, H. (2009). The SECOQC quantum key distribution network. New Journal of Physics, 11, 075001. https://doi.org/10.1088/1367-2630/11/7/075001

[11] International Telecommunication Union. (2024). Security requirements for the deployment of quantum key distribution-based services (ITU-T X.1713). ITU.

[12] Ajlouni, N., Almassri, A., & Atallah, R. R. (2025). Enhancing Quantum Key Distribution Efficiency and Security.

[13] Sharma, N., & Saxena, V. (2025). A comparative analysis of error correction techniques used for QKD protocols. Journal of Optics, 1-7.

[14] Zhang, H., Li, W., He, R., Zhang, Y., Xu, F., & Gao, W. (2025). Noise-reducing quantum key distribution. Reports on Progress in Physics, 88(1), 016001.

[15] Banerjee, S., & Panigrahi, P. K. (2025). Machine Learning assisted noise classification with Quantum Key Distribution protocols. arXiv preprint arXiv:2504.00718.

[16] Harraz, S., Wang, C., & Cong, S. (2024). Enhancing quantum key distribution performance in the presence of noise. International Journal of Theoretical Physics, 63(5), 119.

[17] Lin, S., Guo, G., Gao, F., & Liu, X. F. (2014). Quantum key distribution: defeating collective noise without reducing efficiency. Quantum Inf. Comput., 14(9-10), 845-856.

[18] Bhatia, A., Bitragunta, S., & Tiwari, K. (2025). Enhanced lightweight quantum key distribution protocol for improved efficiency and security. IEEE Open Journal of the Communications Society, 6, 926-943.

[19] Huang, D., Huang, P., Lin, D., & Zeng, G. (2016). Long-distance continuous-variable quantum key distribution by controlling excess noise. Scientific reports, 6(1), 19201.

[20] Zhang, C. X., Wu, D., Cui, P. W., Ma, J. C., Wang, Y., & An, J. M. (2023). Research progress in quantum key distribution. Chinese Physics B, 32(12), 124207.

[21] Zhao, H., Wang, T., Xu, Y., Li, L., Tan, Z., Tan, P., ... & Zeng, G. (2024). Continuous-variable quantum key distribution robust against environmental disturbances. Optics Express, 32(5), 7783-7799.
[22] Ain, N. U., Waqar, M., Bilal, A., Kim, A., Ali, H., Tariq, U. U., & Nadeem, M. S. (2025). A novel approach based on quantum key distribution using BB84 and E91 protocol for resilient encryption and eavesdropper detection. IEEE Access, 13, 32819-32833.
[23] Parihar, A. S. (2025). A secure communication in distributed system using quantum key distribution. The Journal of Supercomputing, 81(16), 1468.
[24] Motaharifar, M., Hasani, M., & Kaatuzian, H. (2025). A survey on continuous variable quantum key distribution for secure data transmission: Toward the future of secured quantum-networks. Quantum Information & Computation, 25(2025), 175-194.
[25] Li, Z., Zhang, Y. C., Xu, F., Peng, X., & Guo, H. (2014). Continuous-variable measurement-device-independent quantum key distribution. Physical Review A, 89(5), 052301.
[26] Li, X. H., Deng, F. G., & Zhou, H. Y. (2008). Efficient quantum key distribution over a collective noise channel. Physical Review A—Atomic, Molecular, and Optical Physics, 78(2), 022321.
[27] Tsai, C. W., Yang, C. W., Lin, J., Chang, Y. C., & Chang, R. S. (2021). Quantum key distribution networks: challenges and future research issues in security. Applied Sciences, 11(9), 3767.
[28] Saiyed, A. I. (2025). Optimizing quantum key distribution (QKD) protocols for secure communication in noisy quantum networks. Annals of Applied Sciences, 6(1).
[29] Imran, M., Altamimi, A. B., Khan, W., Hussain, S., & Alsaffar, M. (2024). Quantum cryptography for future networks security: A systematic review. IEEE Access, 12, 180048-180078.
[30] Zhang, H., Zhu, H., He, R., Zhang, Y., Ding, C., Hanzo, L., & Gao, W. (2025). Towards global quantum key distribution. Nature Reviews Electrical Engineering, 1-13.