International Research Journal of Education and Technology

Peer Reviewed Journal, ISSN 2581-7795

Entanglement-Based Communication Channels: A Study Towards Secure and Scalable Quantum Internet

Lalitha singupurapu[1]

[1]*Student, Dept of CSE-AI&ML, GMR Institute of Technology Rajam, India*

Abstract - *The strange and counterintuitive principles that define the quantum world, where particles can exist in several states at once and remain connected regardless of the distance between them, present a new foundation for secure communication. Classical communication systems depend on mathematical encryption methods that may eventually be broken by powerful computational technologies. In contrast, this study examines a transformative approach based on the physical laws of quantum mechanics. It focuses on entanglement-based communication channels, where the protection of information is guaranteed by nature rather than by complex algorithms. Through the use of quantum entanglement, two particles can remain linked in such a way that a change in one instantly affects the other, no matter how far apart they are. Any unauthorized attempt to intercept or observe the data disrupts the entangled state, exposing the presence of an intruder. This characteristic ensures a level of security that surpasses traditional cryptographic techniques. Unlike classical encryption, which depends on keys that can eventually be deciphered, entanglement-based systems reveal tampering the moment it occurs. This study represents a crucial step toward the realization of quantum communication networks capable of offering absolute data security. It also lays the groundwork for advancements in information transmission, network design, and the future integration of quantum technologies into global communication infrastructures.*

Key Words: **Quantum communication, Quantum cryptography Quantum Entanglement, Quantum key distribution (QKD), Quantum repeaters, Quantum security**

1.INTRODUCTION

Classical communication, which forms the foundation of today's digital world, relies on the transmission of data through mediums such as fiber-optic cables. Its security depends on complex mathematical encryption algorithms that can be vulnerable to attacks from advanced computational systems, particularly future quantum computers capable of breaking conventional codes. This growing risk has motivated the emergence of a transformative approach known as entanglement-based communication, which offers security guaranteed by the laws of quantum physics rather than computational strength. Entanglement-based communication operates on the principle of quantum entanglement, a phenomenon in which particles remain connected regardless of distance, allowing changes in one particle to instantly affect the other. This unique property ensures that any unauthorized attempt to intercept or observe the data disturbs the quantum state, immediately exposing the intrusion. Unlike classical encryption, which relies on complex mathematical problems, quantum communication makes security a fundamental aspect of physics itself. A secure and scalable quantum network requires components such as Quantum Key Distribution (QKD) and quantum repeaters. QKD protocols like BB84 and E91 use entanglement to securely exchange cryptographic keys that cannot be compromised, while quantum repeaters extend the communication range by re-establishing entanglement across long distances, overcoming signal loss and enabling global quantum connectivity. The primary application of entanglement-based communication lies in ensuring secure data transmission for sensitive domains such as Finance, Defense, and Government operations. Beyond security, it opens doors to distributed quantum computing, where interconnected quantum processors can collaborate to solve complex global

problems. Although maintaining entanglement over vast distances remains a technological challenge due to decoherence and environmental noise, global initiatives in quantum satellites and networks are rapidly advancing. Ultimately, this technology promises an unbreakable and intelligent Quantum Internet, redefining cybersecurity and transforming the future of digital communication.

2. LITERATURE REVIEW

This section presents a summary of previous research and developments related to quantum communication and entanglement-based systems. The existing literature provides a strong foundation for understanding how quantum mechanics can be used to enhance information security. Several studies have explored Quantum Key Distribution (QKD) protocols such as BB84 and E91, which utilize quantum states or entangled particles to securely exchange cryptographic keys. These works demonstrate the ability to detect any eavesdropping attempt due to the disturbance of the quantum state.

Recent advancements in quantum repeaters have addressed the challenge of long-distance communication by restoring entanglement between distant nodes. Research institutions and government projects in countries like India, China, the United States, and those in the European Union have contributed significantly to the creation of quantum networks and experimental QKD systems. Moreover, satellite-based QKD and fiber-based quantum communication systems have shown promising results, extending secure communication to hundreds of kilometers.

The review also highlights ongoing challenges such as photon loss, decoherence, and the need for high-efficiency quantum detectors. These issues must be addressed to build scalable and practical quantum communication networks. Overall, previous studies establish the groundwork for implementing secure, large-scale entanglement-based communication systems and support the growing potential for a global quantum internet.

Table -1: Achievements in quantum communication

Year	Technique	Achievement (What Happened)	Performance Metrics	Location
2025	Entangled QKD	"Unhackable" Secret Key Sent 1+ km through the AIR	Key Rate: ≈240 bits/second (Secure) Error Rate (QBER): <7%	India (IIT Delhi & DRDO)
2022-2024	QKD Network	First Quantum Network Between Major Cities	Length: ≈100 km of fiber-optic cable. Goal: Establish long-term secure links.	India (Vindhyachal to Prayagraj)
2024	QKD Integration	Companies Start Selling Quantum-Safe Network Gear	Metric: Commercial Availability (moved from lab to market). Goal: Offer ≈1–10 kbits/sec keys commercially.	Global
2022	Entanglement	Kept Two "Linked" Atoms Entangled over 33 km	Fidelity: Maintained a high-quality "link" (entanglement fidelity). Goal: Proof-of-Concept for the Quantum Internet.	Europe/Global Research

3. METHODOLOGY

Quantum entanglement forms the foundation of secure communication in quantum networks by creating an unbreakable correlation between two distant parties commonly referred to as Alice (sender) and Bob (receiver). In this system, pairs of entangled particles, often photons or qubits, are generated such that the state of one particle instantaneously defines the state of the other, regardless of the distance separating them. This distinctive feature is employed to establish a secure quantum channel for data transmission.

During the communication process, quantum information is encoded within these entangled particles to facilitate the generation of encryption keys using Quantum Key Distribution (QKD) protocols such as BB84 and E91. These protocols exploit the fundamental randomness and measurement sensitivity of quantum mechanics, guaranteeing that the shared keys between Alice and Bob remain unique, unpredictable, and resistant to unauthorized access. Any interception attempt by an eavesdropper, commonly referred to as Eve, inevitably disturbs the quantum state due to the Heisenberg Uncertainty Principle. This disturbance provides an immediate indication of intrusion, allowing Alice and Bob to detect tampering and ensure data authenticity.

To overcome the limitation of distance in quantum transmission, quantum repeaters are employed. These devices use quantum memory and entanglement swapping to extend communication links without compromising quantum coherence. Through this mechanism, long-distance quantum networks can be achieved, connecting multiple nodes

in a secure and efficient manner. Furthermore, the quantum communication channel is continuously monitored for noise, decoherence, and other environmental interferences that could degrade signal integrity. Advanced quantum error correction and privacy amplification techniques are applied to enhance data reliability and ensure secure key distribution across the network.

By integrating entanglement, QKD protocols, and quantum repeater technologies, this methodology achieves a level of security that surpasses traditional cryptographic methods. The system is especially applicable in highly sensitive areas such as defense communications, financial transactions, government data exchange, and healthcare systems, where privacy and integrity are paramount. Ultimately, quantum entanglement revolutionizes secure communication by combining the principles of quantum physics with cryptographic security ensuring that any unauthorized attempt to breach the system becomes fundamentally detectable and preventable.

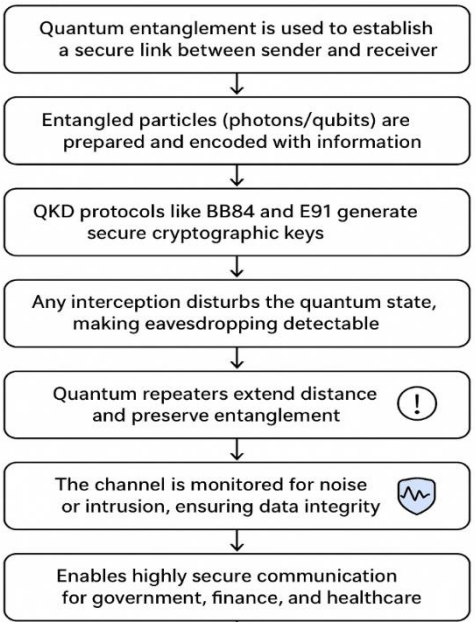

Fig-3.0.1: Flowchart of Entanglement based communication

3.1 Quantum Key Distribution (QKD)

Quantum Key Distribution (QKD) is a quantum communication method that allows two users, commonly known as Alice and Bob, to share a secure encryption key by transmitting information through quantum states of photons. In this process, Alice encodes binary data onto photons using different polarization orientations such as horizontal, vertical, or diagonal and sends them to Bob through a quantum channel like an optical fiber or free-space link. Bob then measures the incoming photons using randomly chosen bases, and only the results obtained with matching bases are kept to form the raw key.

If a third party, often called Eve, attempts to intercept or measure the photons, the act of observation disturbs their quantum states. This disturbance can be detected immediately, ensuring that any intrusion attempt is exposed. This feature makes QKD fundamentally secure, as it relies on the unchangeable laws of quantum physics rather than computational assumptions.

After the transmission, Alice and Bob use a classical communication channel to carry out a process called key reconciliation, where they compare a portion of their data to identify and remove errors. They also perform privacy amplification to eliminate any partial information that might have leaked to an eavesdropper. The result is a shared,
identical, and secret key that can be used for secure data encryption.

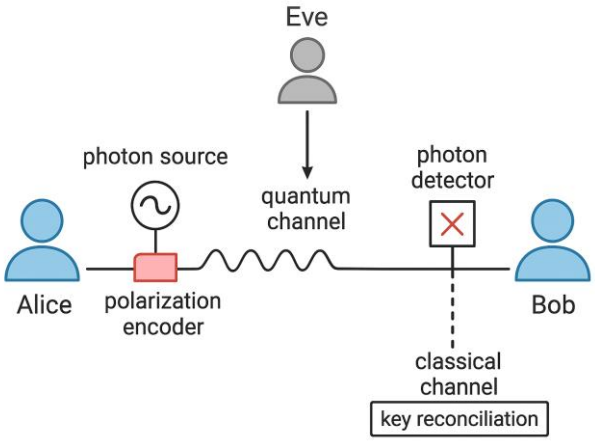

Fig-3.1.1: Architecture of QKD

Protocols such as BB84 and E91 are commonly used for QKD, each employing different quantum principles to enhance security. Modern implementations of QKD have proven successful over optical fiber networks, free-space communication links, and satellite-based systems. This technology forms the foundation of future quantum communication networks, enabling unbreakable data security and ensuring trustworthy information exchange.

International Research Journal of Education and Technology

Peer Reviewed Journal, ISSN 2581-7795

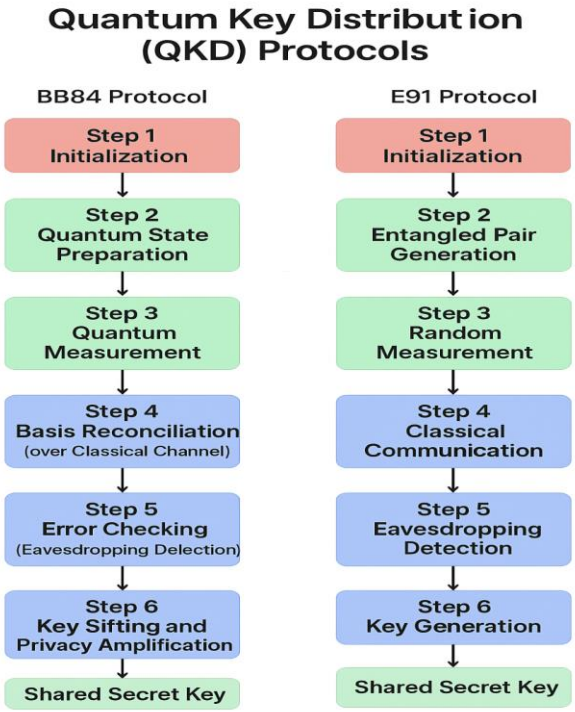

Fig-3.1.2: Flowchart of QKD

3.2 Entangled Quantum Key Distribution (E-QKD)

Entangled Quantum Key Distribution (E-QKD) enables secure key exchange using pairs of entangled photons shared between two parties, Alice and Bob. When one photon of the pair is measured, the state of the other is instantly determined, ensuring strong quantum correlation even across long distances. Any interception attempt by an eavesdropper (Eve) disturbs this entanglement, allowing both parties to immediately detect unauthorized access.

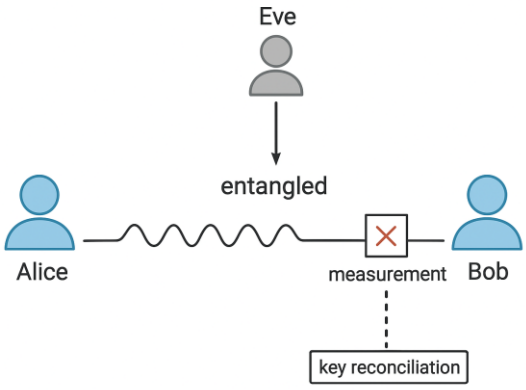

Fig-3.2.1: Architecture of E-QKD

During the process, Alice and Bob perform synchronized measurements on their respective photons using randomly chosen measurement bases. The correlated outcomes are then compared over a classical communication channel to identify and correct any discrepancies through key reconciliation and privacy amplification techniques. The final output is a shared, identical secret key that is completely secure against interception or cloning.

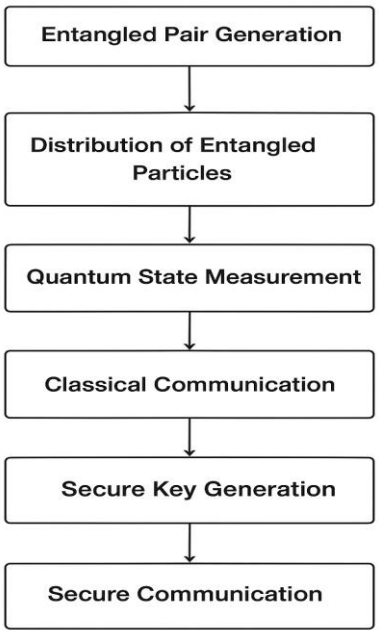

Fig-3.2.2: Flowchart of E-QKD

E-QKD also benefits from the use of quantum repeaters and entanglement swapping, which extend communication distances and minimize signal degradation, making it suitable for large-scale quantum networks. Additionally, its resistance to both computational and physical attacks makes it ideal for high-security applications such as Defense communication, Financial transactions, and Healthcare data protection. By combining the principles of Quantum mechanics with advanced Cryptographic methods, E-QKD represents a major step toward realizing the quantum internet and unbreakable communication systems.

3.3 Quantum Repeater

Quantum repeaters are essential components in quantum communication systems that extend transmission distances while maintaining the accuracy of quantum information. In traditional quantum communication, direct transmission of entangled photons over long distances is hindered by photon loss, decoherence, and signal weakening in optical fibers or free-space links. Quantum repeaters address these challenges by dividing the total communication path into smaller sections, maintaining strong entanglement across each segment.

In this process, local entanglement is first created between intermediate nodes, such as between point A and Repeater I, and between Repeater II and point B. Once local entanglement is established, a process called entanglement swapping is performed at the repeater nodes. This technique connects the smaller entangled links into one continuous long-distance entangled connection between A and B, allowing quantum information to be transmitted securely over large distances without loss of fidelity.

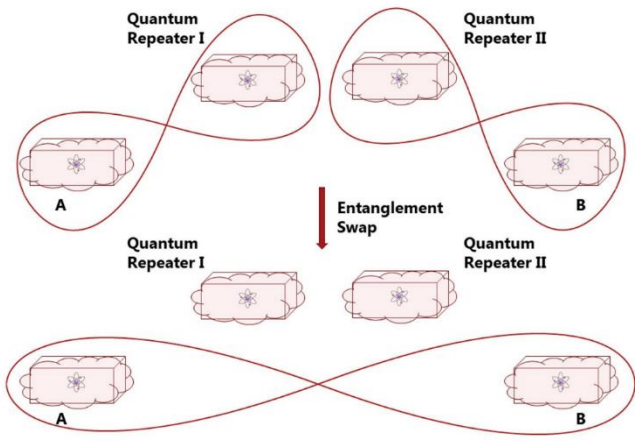

Fig-3.3.1: Flowchart of Quantum Repeaters

Quantum repeaters also include quantum memory systems that temporarily store quantum states until all segments are synchronized. This helps reduce data loss and ensures reliable communication. Additionally, error correction and purification methods are applied to eliminate noise or distortions during transmission.

By linking several repeaters together, large-scale quantum communication networks can be created that maintain stable entanglement across thousands of kilometers. These repeaters form the foundation of the quantum internet, connecting quantum computers, sensors, and communication devices globally. This advancement makes long-distance quantum communication both practical and highly secure, paving the way for a new
era of information transfer based on quantum technology.

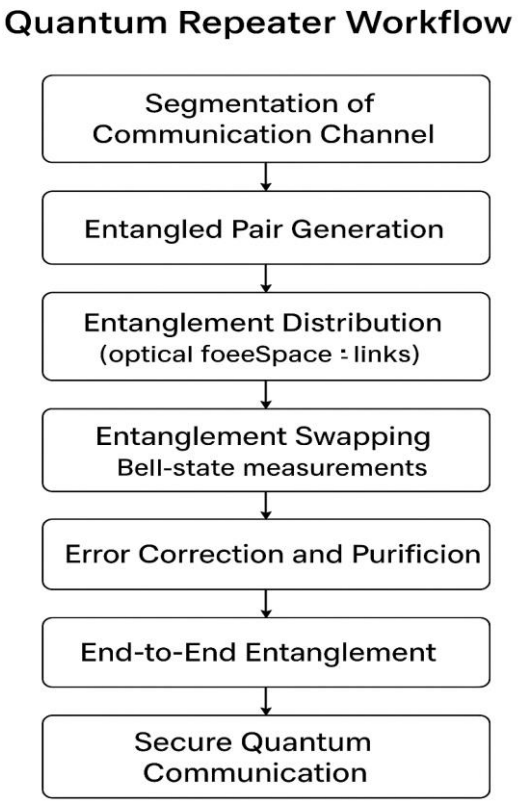

Fig-3.3.2: Flowchart of Quantum Repeaters

4. CONCLUSIONS

Entanglement-based communication marks a revolutionary step in developing highly secure and scalable communication networks. Grounded in the

core principles of quantum mechanics particularly quantum entanglement and Quantum Key Distribution (QKD) this method ensures security based on the laws of physics rather than computational difficulty. Protocols such as BB84 and E91 make any interception instantly detectable, as interference disturbs the quantum state itself, thereby guaranteeing tamper-evident communication. The inclusion of quantum repeaters further mitigates one of the main challenges in quantum communication signal degradation over long distances by maintaining entanglement integrity and facilitating the construction of large-scale quantum networks. The findings suggest that entanglement-based systems serve as the foundation for the emerging quantum internet, enabling unbreakable, high-fidelity, and scalable data transmission. Although current barriers include hardware costs, environmental instability, and classical quantum integration issues, ongoing research continues to reduce these limitations. Ultimately, entanglement-based communication promises to redefine the landscape of digital security, ensuring data privacy and authenticity through the immutable laws of quantum physics, and ushering in an era of truly secure global connectivity.

5. REFERENCES

[1] Gattupalli, K., Gollavilli, V. S. B. H., Nagarajan, H., Alagarsundaram, P., Sitaraman, S. R., & Pushpakumar, R. "Quantum Internet for Healthcare: Securing Patient Data with QKD and Entanglement-Based Communication" Vol. 07, Issue 08, pp. 43–55, August 2025.

[2] F. H. Panahi, "Energy-efficient decoherence-aware entanglement generation for Quantum Internet of Things," IEEE Internet of Things Journal, pp.18, 2025, doi:10.1109/JIOT.2025.3593026.

[3] A. Zaballos, A. Mallorquí, and J. Navarro, "Quantum-assisted trustworthiness for the Quantum Internet," Engineering Department, La Salle Campus Barcelona, Universitat Ramon Llull, pp. 1–15, 2025.

[4] Abane, A., Cubeddu, M., Mai, V. S., & Battou, A. "Entanglement Routing in Quantum Networks: A Comprehensive Survey," pp. 39, 2025.

[5] Hosseinnezhad, A. & Sabri, H. (2025). "Secure quantum relay networks using distributed entanglement without classical authentication," Department of Physics, University of Tabriz, Iran, 1–14.

[6] X. Liu, R. Xue, H. Wang, H. Li, X. Feng, F. Liu, K. Cui, Z. Wang, L. You, Y. Huang, and W. Zhang, "Fully connected entanglement-based quantum communication network without trusted node," [Journal/Conference Name if available], 2025.

[7] Y.-R. Fan, Y. Luo, K. Guo, J.-P. Wu, H. Zeng, G.-W. Deng, Y. Wang, H.-Z. Song, Z. Wang, L.-X. You, G.-C. Guo, and Q. Zhou, "Quantum entanglement network enabled by a state-multiplexing quantum light source," Light: Science & Applications, vol. 14, no. 189, 2025. doi:10.1038/s41377-025-01805-1.

[8] Gattupalli, K., Gollavilli, V. S. B. H., Nagarajan, H., Alagarsundaram, P., Sitaraman, S. R., & Pushpakumar, R. "Quantum Internet for Healthcare: Securing Patient Data with QKD and Entanglement-Based Communication" Vol. 07, Issue 08, pp. 43–55, August 2024.

[9] H. Dutta and A. K. Bhuyan, "Quantum Communication: From Fundamentals to Recent Trends, Challenges and Open Problems," pp. 1–30, 2024.

[10] Z.-Z. Sun, Y.-B. Cheng, Y.-C. Liu, D. Ruan, D. Pan, and G.-L. Long, "Message-oriented entanglement distribution network," IEEE Internet of Things Journal, vol. 11, no. 21, pp. 1–12, Nov. 2024.

[11] H. Hu, H. Lun, Z. Deng, J. Tang, J. Li, Y. Cao, Y. Wang, Y. Liu, D. Wu, H. Yu, X. Wang, J. Wei, and L. Shi, "High-fidelity entanglement routing in quantum networks," Results in Physics, vol. 60, p. 107682, 2024.

[12] Z. Li, K. Xue, J. Li, L. Chen, R. Li, Z. Wang, N. Yu, D. S. L. Wei, Q. Sun, and J. Lu, "Entanglement-assisted quantum networks: Mechanics, enabling technologies, challenges, and research directions," IEEE Communications Surveys & Tutorials, vol. 25, no. 4, pp. 2133–2189, Fourth Quarter 2023.

[13] T. Guha, S. Roy, and G. Chiribella, "Quantum networks boosted by entanglement with a control system," Physical Review Research, vol. 5, no. 3, p. 033214, Sep. 2023.

[14] H. Dwivedi, "Quantum entanglement: Defining future of information communication," IOSR Journal of Applied Physics (IOSR-JAP), vol. 13, no. 6, pp. 82–84, Nov.–Dec. 2021.

[15] A. Singh, K. Dev, H. Siljak, H. D. Joshi, and M. Magarini, "Quantum Internet Applications, functionalities, enabling technologies, challenges, and research directions," IEEE Communications Surveys & Tutorials, vol. 23, no. 4, pp. 2218–2247, Fourth Quarter 2021.