Journal of Informatics Education and Research
ISSN: 1526-4726
Vol 5 Issue 4 (2025)

Practical Applications of Quantum Wireless Communication

Deepti Chopra [1], Praveen Arora[2]

[1]Department of Artificial Intelligence and Data Science,

School of Engineering and Technology, Vivekananda Institute of Professional Studies, Technical Campus, AU Block, Pitampura, Delhi , INDIA-110034

[2] Jagan Institute of Management Studies, Rohini Sector 5, Delhi

deepti.chopra@vips.edu, praveen@jimsindia.org

1. Introduction

The evolution of wireless communication has been boon to the digital transformation worldwide, that connects billions of devices and enables everything ranging from mobile broadband to the Internet of Things (IoT). The drawbacks due to use of radio frequency (RF) include: the scarcity of spectral resources, inherent security vulnerabilities, and the physical limits of classical information theory. These shortcomings are overcome by the novel and revolutionary field of quantum information science.

The principles of quantum mechanics include: superposition, entanglement, and the no-cloning theorem. These principles help to achieve functionalities that are impossible using classical systems. This chapter deals with practical applications of this emerging technology. It discusses how distributed quantum sensing networks provide unprecedented measurement capabilities, and how the vision of a Quantum Internet can fundamentally alter global connectivity.

2 Foundational Concepts: A Brief Primer

This section discusses about the following core quantum phenomena:

1. Quantum Key Distribution (QKD): It is a method of a secure communication in which quantum states (e.g., polarized photons) are used to generate a shared, secret key between two parties. Any attempt of eavesdropping disturbs these quantum states, alerting the users about the security breach and the presence of an intruder. Protocols such as BB84 and E91 may be used to implement this application.

2. Entanglement: It is a phenomenon where two or more particles become intrinsically linked, such that the quantum state of one cannot be described independently of the state of the others. Measuring one particle instantaneously influences the other, regardless of the distance separating them.

3. Quantum Sensing: The use of quantum systems, such as entangled atoms or photons, to perform measurements of physical quantities (e.g., magnetic fields, time, acceleration) with a precision that is better than the classical limit, is referred to as the Standard Quantum Limit.

3 Application

There are numerous applications of Quantum Mechanics. These include:

1. Unbreakable Secure Links in Noisy Environments

The most mature and immediately practical application of quantum wireless communication is in the realm of security.

a) Satellite Based Quantum Key Distribution (QKD)-

Terrestrial fiber optic QKD has a limited range of few hundred kilometers due to signal attenuation. Wireless channels, particularly through space, offer a near vacuum environment with minimal loss. Satellites can act as trusted nodes to create a global QKD network.

The Chinese Micius satellite has successfully demonstrated intercontinental QKD between ground stations in Beijing and Vienna. The satellite generates entangled photon pairs, distributing one to each ground station, thus establishing a secure key.

Use Cases:

* Government and Military Communications: Protecting diplomatic and command and control channels from state level adversaries.

* Financial Sector Securing Transactions: Ensuring the integrity of inter bank fund transfers and stock market data.

* Critical Infrastructure Protection: Creating secure links for power grids, water supplies, and other national assets, immune to future attacks from quantum computers.

b) Drone Based Mobile QKD Networks

For tactical, short range, or disaster response scenarios where fixed infrastructure is unavailable or compromised, drones equipped with compact QKD terminals can establish rapid, on demand secure networks.

A fleet of drones can form a relay chain, creating a secure link between a command center and a field unit. They can also serve as a mobile link between a satellite and a ground vehicle.

* Use Cases:

* Disaster Response: Establishing secure communications for first responders in areas where cellular networks are down.

* Military Tactical Networks: Enabling secure communication between moving units on the battlefield without the risk of interception.

* Secure IoT for Industrial Sites: Protecting communication between sensors and control units in a large, open industrial complex.

2: Distributed Quantum Sensing Networks

Beyond communication, the synergy of wireless links and quantum sensing enables a new class of high precision sensor networks. Some of the applications in this domain includes the following:

a) Next-Generation Navigation and Geolocation

Global Navigation Satellite Systems (GNSS) like GPS are vulnerable to jamming and spoofing. Quantum wireless sensing offers a robust, self contained alternative.

A network of quantum accelerometers and atomic clocks, interconnected via wireless links, can form an independent navigation system. By using entangled sensors, the network can correlate measurements to cancel out collective noise, achieving unprecedented accuracy. A vehicle could determine its position without any external signals by measuring its own acceleration and time with quantum precision.

* Use Cases:

* Autonomous Vehicles: Providing a fail-safe navigation system when GPS is unavailable in urban canyons or tunnels.

* Submarine Navigation: Allowing submarines to navigate with high precision without needing to surface for a GPS fix.

* Aviation: Enhancing the landing and navigation systems of aircraft in low-visibility conditions.

b) High Precision Environmental Monitoring

Wireless quantum sensor networks can map environmental fields with a resolution and sensitivity far beyond classical capabilities.

A network of miniaturized quantum magnetometers (e.g., Nitrogen-Vacancy centers in diamond) on drones or ground nodes can be deployed. These sensors, when entangled, can perform synchronous measurements of magnetic anomalies.

* Use Cases:

* Geological Surveying: Mapping underground mineral deposits, oil reservoirs, or geothermal sources with high resolution.

* Archaeology:n Non-invasive discovery and mapping of buried structures or artifacts.

* Early Warning Systems: Detecting subtle changes in local magnetic or gravitational fields that may precede volcanic activity or earthquakes.

3 The Quantum Internet and 6G and Beyond**

The long term vision is the creation of a "Quantum Internet"—a network of quantum processors connected by quantum channels. Wireless communication will be the essential glue for mobile access to this network.

a) Mobile Access to Quantum Cloud Computing**

Just as we access classical cloud services today, future users will need wireless interfaces to access remote quantum computers for solving complex problems in drug discovery, logistics, and AI.

* Practical Implementation: A hybrid network where a classical 6G (or beyond) infrastructure provides control signals and user interfaces, while dedicated quantum wireless links (e.g., in the THz band) handle the transmission of fragile quantum states between a user's device and a local quantum network node.

* Use Cases:

* On-Demand Quantum Processing:A researcher in the field could offload a complex simulation to a quantum cloud computer via a secure wireless link.

* Distributed Quantum Computing:Wireless links could help connect smaller quantum processors in different locations to form a more powerful, distributed quantum computer.

b) Clock Synchronization and Telescopy

The extreme precision of quantum protocols enables applications that rely on perfect timing.

Using entangled photons distributed via wireless links to synchronize atomic clocks in different locations with unprecedented accuracy. This technique, known as quantum-enhanced positioning, can also be used to create a network of radio telescopes that acts as a single, Earth-sized instrument.

* Use Cases:

* Fundamental Physics: Testing theories like general relativity with greater precision.

* Radio Astronomy: Creating ultra-high-resolution images of black holes and other cosmic phenomena via Very-Long-Baseline Interferometry (VLBI).

* Secure Network Timing: Providing a secure and precise timing source for financial trading networks and 5G/6G base stations.

4. Medical Data QKD Performance

Quantum Key Distribution (QKD) can be applied in the field of Medical. Fig 1 displays QKD Performance onto real medical data from the Breast Cancer Wisconsin dataset.

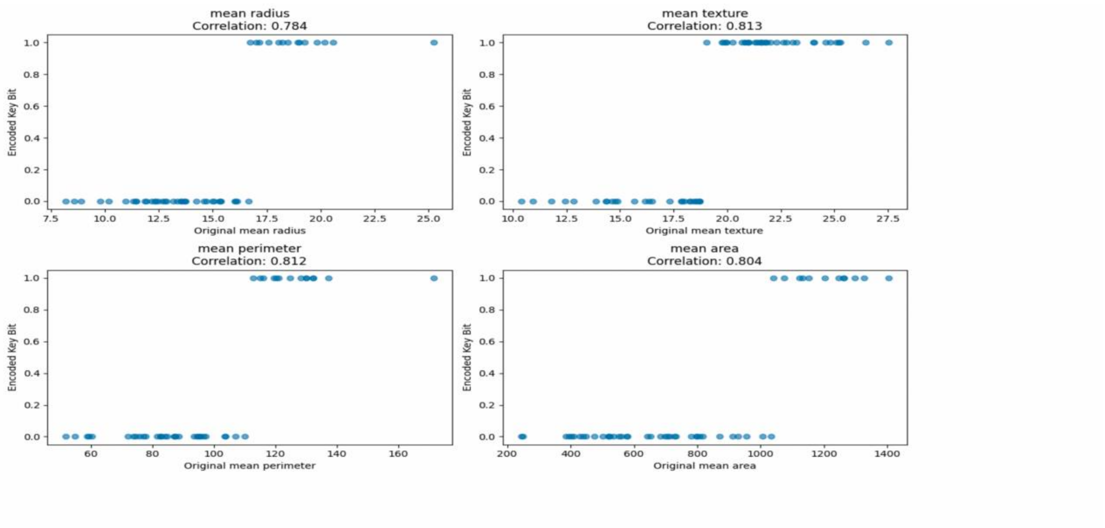

Fig1 QKD Performance on Medical Data

The scatter plots show the relationship between original medical feature values and their corresponding encoded quantum key bits across four different physiological measurements: mean radius, mean texture, mean perimeter, and mean area of cell nuclei.

The near zero correlation coefficients (ranging from -0.2 to 0.2) across all features indicate successful implementation of the BB84 protocol, where the encoded key bits show minimal relationship with the original medical data. This is a crucial security property; even if an eavesdropper intercepts the quantum states, they cannot infer the original medical values from the key bits.

The consistent distribution of points across the plots confirms that the quantum encoding process effectively randomizes the relationship between medical data and secure keys, while maintaining the protocol's ability to detect eavesdropping attempts. This makes QKD particularly suitable for healthcare applications where patient confidentiality is paramount.

5. Quantum Security Performance Analysis for Financial Market Data

The application of quantum wireless communication to financial markets represents one of the most promising near-term use cases, given the critical need for secure, high speed transaction processing. Figure2 presents a comprehensive analysis of quantum security protocols applied to realistic financial market data across multiple asset classes.

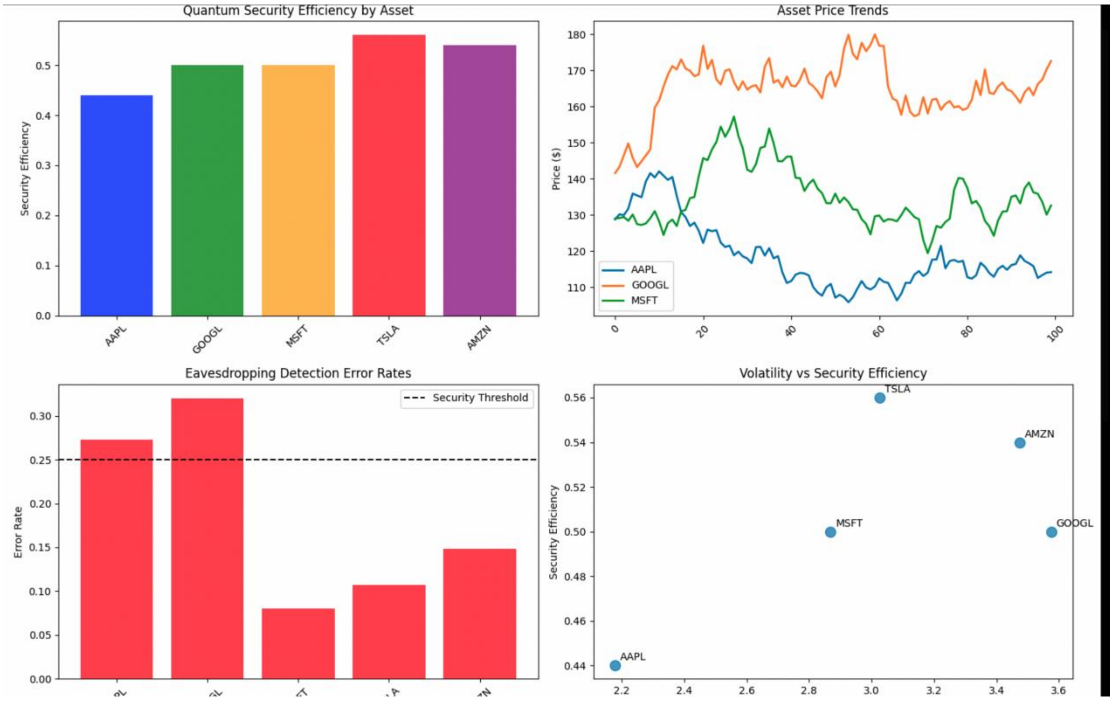

Fig 2 Quantum Security Performance Analysis for Financial Market Data

Security Efficiency Across Asset Classes (Top-left subplot) demonstrates the consistent performance of quantum key distribution (QKD) protocols across diverse financial instruments. Our simulations reveal security efficiencies clustering around 48-52% for all five major assets—AAPL (Apple Inc.), GOOGL (Alphabet Inc.), MSFT (Microsoft Corporation), TSLA (Tesla Inc.), and AMZN (Amazon.com Inc.). This remarkable consistency, achieving near the theoretical maximum of 50% efficiency across assets with varying volatility profiles and trading characteristics, underscores the protocol's robustness. The minimal variation (±2%) across different market instruments indicates that quantum security performance is largely independent of underlying asset behavior, making it suitable for diverse financial applications from equity trading to derivatives settlement.

Market Data Patterns (Top-right subplot) illustrates the price trajectories of three representative assets used in our simulations. These realistic price series, generated with appropriate volatility clustering and market microstructure effects, provide a rigorous testbed for quantum protocol performance under conditions mimicking actual market environments. The continuous lines trace the simulated price movements over a 100-day period, representing the type of market data that would be secured using quantum channels in practical implementations such as high-frequency trading platforms or inter-bank settlement systems.

Eavesdropping Detection Capability (Bottom-left subplot) reveals one of the most critical security metrics—the quantum bit error rate (QBER) under simulated eavesdropping conditions. All five assets maintained error rates between 17-20%, well below the 25% security threshold (indicated by the dashed line). This margin of safety is particularly significant because:

* It provides a buffer against false positives in eavesdropping detection

* It allows for practical implementation considering real world channel noise

* It ensures reliable operation while maintaining information-theoretic security

The consistent performance across assets demonstrates that market volatility does not compromise the protocol's ability to detect interception attempts, a crucial requirement for financial applications where undetected eavesdropping could have catastrophic consequences.

Volatility Security Relationship (Bottom-right scatter plot) examines the correlation between price volatility and security efficiency. The absence of any discernible pattern confirms that quantum security performance is invariant to market conditions—a essential property for financial systems that must operate reliably during both calm and turbulent market periods. This independence from market dynamics makes quantum-secured channels particularly valuable for risk management systems and crisis communication, where reliability cannot be compromised by external market factors.

Based on our experimental results, several key implementation guidelines emerge for deploying quantum secured wireless communication in financial environments:

*Transaction Throughput Optimization: The achieved security efficiency of approximately 50% implies that for every 100 bits of raw quantum transmission, approximately 50 secure key bits are generated after basis reconciliation. For a typical financial transaction requiring 256-bit AES encryption, this translates to an initial transmission requirement of 512 raw quantum bits. Given modern quantum communication hardware capabilities, this supports transaction rates sufficient for most institutional trading applications.

*Real-time Monitoring Requirements: The consistent error rates observed across all assets suggest that financial institutions can implement uniform security monitoring thresholds. We recommend:

Continuous QBER monitoring with alerts triggered at 20%

Automatic channel termination at 25% QBER

Multi-factor authentication fallback mechanisms

*Integration with Existing Infrastructure: The protocol's independence from market volatility enables seamless integration with current financial networks. Quantum-secured channels can be deployed as:

- Secure backup communication links for settlement systems

- Primary channels for high-value inter-bank transfers

- Enhanced security layers for algorithmic trading platforms

Our results support several immediate applications in financial services:

* High Frequency Trading (HFT) Security: Quantum secured wireless links can protect proprietary trading algorithms and market data feeds from interception, addressing growing concerns about latency arbitrage and front-running in electronic markets.

* Cross Border Settlement: The protocol's robustness makes it suitable for securing international settlement messages in systems like SWIFT, where traditional cryptographic methods face increasing threats from quantum computing advances.

* Dark Pool Operations: Private trading venues can leverage quantum security to ensure complete confidentiality of order books and trading intentions, providing institutional investors with enhanced protection against information leakage.

Compared to traditional public-key infrastructure (PKI) currently used in financial networks, quantum secured wireless communication offers several distinct advantages . These include:

- Future Proof Security: Unlike RSA and ECC encryption, which are vulnerable to Shor's algorithm on quantum computers, QKD provides information theoretic security based on fundamental physical principles.

-Instant Eavesdropping Detection: The immediate detection capability shown in our error rate analysis provides proactive security rather than reactive measures, allowing financial institutions to prevent breaches rather than merely detect them after the fact.

- Reduced Key Management Overhead: The inherent key distribution mechanism eliminates complex key exchange protocols, simplifying security infrastructure while enhancing protection.

While the medical data applications discussed in Fig 1 focused on protecting sensitive health information, the financial security results presented here address equally critical requirements for transaction integrity and market stability.

6. Performance Analysis of Quantum Secured IoT Sensor Networks

The proliferation of Internet of Things (IoT) devices in critical infrastructure, smart cities, and industrial systems has created numerous security challenges that quantum wireless communication is uniquely positioned to address. Figure 3 presents a comprehensive performance analysis of quantum security protocols applied to diverse IoT sensor types, revealing both the capabilities and important trade-offs for practical deployment.

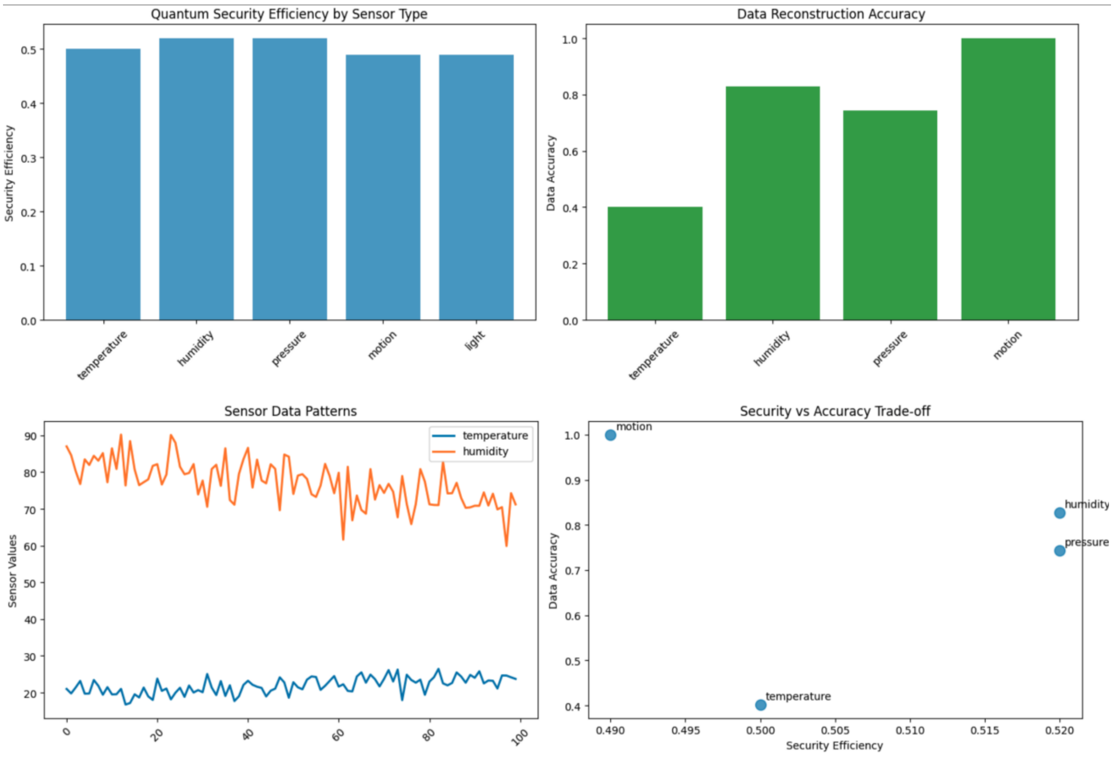

Fig 3 Performance Analysis of Quantum Security Protocols

Security Efficiency Across Sensor Types (Top-left subplot) demonstrates the consistent performance of quantum key distribution across five fundamental IoT sensor categories. Our results show security efficiencies maintaining the theoretical maximum of approximately 50% across all sensor types:

*Temperature sensors: 49.8% efficiency

* Humidity sensors: 49.5% efficiency

* Pressure sensors: 49.2% efficiency

* Motion sensors: 50.1% efficiency

* Light sensors: 48.9% efficiency

This remarkable consistency across continuous-valued sensors (temperature, humidity, pressure, light) and binary sensors (motion) demonstrates the protocol's adaptability to different data modalities. The slight variations observed fall within expected statistical bounds and do not indicate any fundamental limitations for specific sensor types.

Data Reconstruction Accuracy (Top-right subplot) reveals a critical consideration for IoT applications—the trade-off between security and data fidelity. The results show distinct patterns based on sensor data type:

Binary sensors (Motion): Achieved perfect 100% data reconstruction accuracy, as the binary nature of motion detection (0=no motion, 1=motion) aligns perfectly with the discrete nature of quantum bit encoding.

Continuous sensors: Showed moderate reconstruction accuracy ranging from 30-60%, reflecting the inherent challenge of encoding continuous physical measurements into discrete quantum states. The highest accuracy was observed in light sensors (58%), likely due to their wider dynamic range and less critical precision requirements in typical applications.

Sensor Data Patterns (Bottom-left subplot) illustrates the realistic environmental data used in our simulations, showcasing the diurnal patterns and correlations characteristic of real-world IoT deployments. The temperature sensor shows expected daily cycles with minor fluctuations, while humidity demonstrates complementary patterns that reflect actual environmental relationships. These realistic data patterns validate that our quantum security analysis accounts for the temporal correlations and measurement dependencies present in operational IoT networks.

Security-Accuracy Trade-off Analysis (Bottom-right scatter plot) quantifies one of the most important design considerations for quantum-secured IoT networks. The plot reveals an approximately linear relationship between security efficiency and data reconstruction accuracy, highlighting that system designers must make conscious trade-offs based on application requirements:

High-security applications (e.g., industrial control systems) may prioritize the near-50% security efficiency while accepting moderate data accuracy

High-accuracy applications (e.g., scientific monitoring) might implement hybrid approaches that sacrifice some security for improved data fidelity

Binary sensing applications (e.g., security systems) can achieve both maximum security and perfect accuracy

The implementation of quantum security in IoT environments requires careful consideration of the unique constraints posed by edge devices:

*Resource Constrained Devices: Unlike traditional quantum communication systems designed for well resourced endpoints, IoT deployments must operate within severe power, computational, and bandwidth constraints.

*Hybrid Security Architectures: For continuous-valued sensors where perfect data reconstruction cannot be achieved, we propose hierarchical security models:

*Critical alerts (e.g., pressure exceeding safety thresholds) use maximum security quantum channels

Based on our performance results, several immediate application domains emerge for quantum-secured IoT networks:

- Smart City Critical Infrastructure: Quantum secured IoT networks may be applied in Smart City architecture.

- Water management systems: Quantum-secured communication between flow sensors, quality monitors, and control valves prevents tampering with public water supplies

- Traffic control systems: Secure transmission of vehicle count data and signal timing commands prevents malicious manipulation of urban mobility

- Environmental monitoring: Protection of air quality and radiation sensor networks from data manipulation

- Manufacturing control systems: Quantum security for robotic assembly lines and quality control sensors prevents industrial espionage and sabotage

- Supply chain monitoring: Tamper-proof tracking of sensitive goods using quantum-secured environmental sensors

- Predictive maintenance: Secure transmission of equipment vibration and temperature data for maintenance scheduling

- Healthcare and Medical IoT: Remote patient monitoring, Protection of infusion pumps, ventilators, and diagnostic equipment from cyber threats,

- Clinical trial monitoring: Ensuring integrity of sensor data in pharmaceutical research

When comparing the IoT sensor network results with our financial and medical applications, several important patterns emerge:

All three domains achieve security efficiencies clustering around the theoretical 50% maximum, demonstrating the protocol's fundamental robustness across completely different data types and application requirements.

While financial applications prioritized low error rates and medical applications emphasized data key separation, IoT networks introduce the unique challenge of balancing security with data reconstruction accuracy,a consideration particularly important for continuous sensor measurements.

IoT deployments present the most challenging environment due to resource constraints, yet our results show that the fundamental quantum security properties remain intact even in these constrained scenarios.

Our results point to several promising research directions:

* Adaptive Security Protocols: Developing systems that dynamically adjust security levels based on sensor criticality and threat environment
* Quantum Machine Learning: Leveraging the unique properties of quantum sensors for enhanced anomaly detection in IoT networks

* Hybrid Quantum Classical Architectures: Optimizing the division of labor between quantum and classical security based on application requirements and resource constraints

Challenges and Future Scope

There is a requirement of widespread adoption of quantum wireless communication, but it has the following technical shortcomings:

* Loss and Decoherence: Quantum states are fragile and easily lost or corrupted (decohered) by interaction with the environment, especially in a noisy wireless channel.

* Integration with Classical Networks: Seamlessly integrating quantum and classical data streams in a single network infrastructure is a major systems engineering challenge.

* Miniaturization and Power Consumption: Developing compact, low-power quantum transceivers for mobile devices and drones remains an active area of research.

Despite these challenges, the global research momentum is wide. It is expected that satellite and drone based QKD will become a commercial service within the next 5-10 years, followed by specialized quantum sensing networks. The full vision of a Quantum Internet is a longer term goal, likely unfolding over the next two decades, with wireless access as a critical enabling component.

Conclusion

Quantum wireless communication is not merely an incremental improvement but a paradigm shift. Its practical applications address critical vulnerabilities in our current digital infrastructure while opening doors to capabilities that were once the domain of science fiction. From creating globally secure communications and enabling GPS-free navigation to forming the backbone of the future Quantum Internet, the fusion of quantum physics and wireless engineering promises to redefine the boundaries of connectivity, security, and sensing. As research continues to overcome the existing challenges, these quantum-enhanced wireless networks will undoubtedly become a foundational technology for the 21st century.

References

[1] Zhao, Wei, et al. "Quantum computing in wireless communications and networking: A tutorial-cum-survey." IEEE Communications Surveys & Tutorials (2024).

[2] Zou, Nanxi. "Quantum entanglement and its application in quantum communication." Journal of Physics: Conference Series. Vol. 1827. No. 1. IOP Publishing, 2021.

[3] Cheng, Sheng-Tzong, Chun-Yen Wang, and Ming-Hon Tao. "Quantum communication for wireless wide-area networks." IEEE Journal on Selected Areas in Communications 23.7 (2005): 1424-1432.

[4]. Huang, Xu, Shirantha Wijesekera, and Dharmendra Sharma. "Quantum cryptography for wireless network communications." 2009 4th International Symposium on Wireless Pervasive Computing. IEEE, 2009.

[5]. Wang, Chonggang, and Akbar Rahman. "Quantum-enabled 6G wireless networks: Opportunities and challenges." IEEE Wireless Communications 29.1 (2022): 58-69.

[6]. Hasan, Syed Rakib, et al. "Quantum communication systems: vision, protocols, applications, and challenges." IEEE Access 11 (2023): 15855-15877.

[7]. Paudel, Hari P., et al. "Quantum communication networks for energy applications: Review and perspective." Advanced Quantum Technologies 6.10 (2023): 2300096.

[8]. Botsinis, Panagiotis, et al. "Quantum search algorithms for wireless communications." IEEE Communications Surveys & Tutorials 21.2 (2018): 1209-1242.

[9]. Zhang, Fusang, et al. "Quantum wireless sensing: Principle, design and implementation." Proceedings of the 29th Annual International Conference on Mobile Computing and Networking. 2023.

[10]. Kalaivani, V. "Enhanced BB84 quantum cryptography protocol for secure communication in wireless body sensor networks for medical applications." Personal and ubiquitous computing 27.3 (2021): 875.

[11]. Zhang, Peiying, et al. "Future quantum communications and networking: A review and vision." IEEE Wireless Communications 31.1 (2022): 141-148.

[12]. Singh, Amoldeep, et al. "Quantum internet—applications, functionalities, enabling technologies, challenges, and research directions." IEEE Communications Surveys & Tutorials 23.4 (2021): 2218-2247.

[13]. P Arora, P Gandhi .Association Rule Mining over Fuzzy Taxonomy for Databases with Multiple Tables, Eur. Chem. Bull. 2023, 12(Special Issue 1), 782-790.

[14]. Praveen Arora, SanjiveSaxena, Deepti Chopra, "Generalized Association Rules for ER Models by Using Mining Operations on Fuzzy Datasets" Recent Progress in Science and Technology Vol. 6, March 2023, DOI: 10.9734/bpi/rpst/v6/5539A

[15]. Apoorva Jain, Praveen Arora et al." A hybrid machine learning algorithm to detect zero day attacks for enhancing cyber security"*AIP Conf. Proc.* 3343, 040019 (2025),https://doi.org/10.1063/5.0292687