Quantum Intrusion Detection System (QIDS): Passive Detection of Encrypted Quantum Communication in Open Environments
Conceptual Model

Inventor: Sidhant Negi
Status: Confidential and Not Patented
Tags: #Cybersecurity #QuantumDefense #PassiveQuantumDetection #QIDS #NationalSecurity

---

Abstract

This conceptual white paper presents the design and architecture of a novel passive quantum intrusion detection system (QIDS) capable of identifying unauthorized encrypted quantum communication in real-world environments. The system distinguishes between natural/random light and artificial/encrypted quantum particles by analyzing structured behavior, coherence, and response to simulated decoding logic. This paper also discusses limitations inherent to such a system and provides tactical solutions for overcoming them. While still under development, the system is envisioned for deployment in national defense and critical infrastructure environments.

---

1. Objective

To conceptually build a quantum-aware intrusion detection system that detects the presence of unauthorized quantum communication (e.g., QKD, entangled photon transfer) in passive mode—without collapsing the signal—and alerts relevant authorities while optionally tracking source and destination.

---

2. System Architecture and Key Modules

2.1 QSDL – Quantum Shadow Detection Layer

- Detects presence of photon streams using high-sensitivity polarization and coherence sensors.
- Filters by wavelength and detects irregularities against expected environmental behavior.

2.2 QPRE – Quantum Pattern Recognition Engine

- Uses AI/ML to differentiate between natural noise and encrypted/structured photon behavior.
- Leverages entropy analysis, time-pattern detection, and multi-spectral recognition.

2.3 QDP – Quantum Decoding Probe

- Applies known quantum basis decoding attempts (BB84, B92 logic) without collapsing the signal.
- Observes how the photon stream reacts to structured decoding probes.
- Natural light fails randomly; encrypted quantum data maintains statistical structure.

2.4 QELM – Evidence Logging Module

- Logs metadata (time, spectrum, polarization, intensity) for forensic and legal purposes.

2.5 QTLS – Quantum Transmission Localization System *(Optional)*

- Uses synchronized detectors to infer source/destination of the photon stream based on time-of-arrival difference.

---

3. Limitation Analysis and Tactical Solutions

Limitation 1: Natural Environmental Disruptions (Sunlight, Weather, EM noise)

Solution: High-pass filtering, spectrum mapping, and noise-trained AI models are employed to discard random light activity. QPRE is specifically trained to distinguish randomness from quantum structure.

Limitation 2: Signal Collapse During Detection

Solution: Passive detection through QDP and QPRE avoids direct interaction with photon data. No quantum state collapse occurs since no data-extracting measurements are made.

Limitation 3: Tracking Source & Destination of Quantum Streams

Solution: QTLS with GPS-synchronized photon sensors enables trajectory triangulation based on time-of-flight and intensity analysis.

Limitation 4: False Positives from Classical/Artificial Light Sources

Solution: Uses entropy analysis, polarization fingerprinting, AI training, and source blacklists to eliminate false alerts.

Limitation 5: Hardware Constraints and Practical Deployment

Solution: Initial deployment in controlled military zones and satellites, later expanding to data centers and national border checkpoints.

Optional Feature: Simulated Decryption Differentiation

By passively simulating known quantum key protocols, QDP observes whether a photon stream responds with structured resilience—indicative of encrypted quantum data—without collapsing it. This serves as a powerful filter to detect artificial streams among natural ones.

---

4. Conclusion

QIDS introduces a passive, structured, and modular quantum detection system for identifying encrypted communication. Its relevance in national defense, strategic surveillance, and secure infrastructure monitoring marks it as a vital cybersecurity innovation for the quantum age.

This is a conceptual model in the pre-prototype stage and aims to inspire research and development in quantum surveillance and defense.

---

5. Deployment Scenarios

- Military Zones and Warfields
- Government and Defense Data Centers
- Border Surveillance Installations
- Satellite and Strategic Communication Infrastructure
- Critical Industrial Networks

Legal Disclaimer

This document is published for educational and conceptual discussion purposes only. Commercial use without inventor's permission is prohibited.

Contact Information

Inventor: Sidhant Negi
📧Email: sidhantnegi68@gmail.com
🔗GitHub: https://github.com/Sidhant1s