Title: 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. Key Modules and Architecture:

1. **QSDL – Quantum Shadow Detection Layer:**
2. Detects presence of photon streams using high-sensitivity polarization and coherence sensors.
3. Filters by wavelength and detects irregularities against expected environmental behavior.
4. **QPRE – Quantum Pattern Recognition Engine:**
5. Uses AI/ML to differentiate between natural noise and encrypted/structured photon behavior.
6. Leverages entropy analysis, time-pattern detection, and multi-spectral recognition.
7. **QDP – Quantum Decoding Probe:**
8. Applies known quantum basis decoding attempts (BB84, B92 logic) without collapsing the signal.
9. Observes how the photon stream reacts to structured decoding probes.
10. Natural light fails randomly; encrypted quantum data maintains statistical structure.
11. Conceptually acts as a filter to differentiate natural vs encrypted sources by simulating decryption and observing behavior.

12. **QELM – Evidence Logging Module:**

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

14. **Optional: QTLS – Quantum Transmission Localization System:**

15. If triangulation is needed, 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: Use high-pass filtering, spectrum mapping, and noise-trained AI models to discard random light activity. The QPRE is trained specifically to distinguish randomness from quantum structure.

Limitation 2: Signal Collapse during Detection
Solution: Passive detection via QDP and QPRE avoids interacting directly with photon data. No quantum state collapse occurs as no measurement is made that extracts key data.

Limitation 3: Tracking Source & Destination of Quantum Streams
Solution: Use QTLS module with GPS-synchronized photon sensors to triangulate approximate trajectory based on time-of-flight and intensity patterning.

Limitation 4: False Positives from Classical/Artificial Light Sources
Solution: Employ entropy analysis, polarization fingerprinting, AI training on classical noise, and known source blacklists to eliminate false alerts.

Limitation 5: Hardware Constraints and Practical Deployment
Solution: Start with controlled military zones and satellite detection, gradually expanding to data centers, battlefield detectors, and national border points.

Optional Feature: Simulated Decryption Differentiation
By attempting passive decoding of detected photon streams, the system can infer artificial origin based on how well the stream aligns with structured key systems (e.g., BB84 logic). Natural particles behave unpredictably; encrypted ones resist predictably. This is implemented in the QDP layer. This conceptual module provides a non-invasive layer for encrypted signal recognition.

---

4. Conclusion:
QIDS provides a first-of-its-kind, passive, structured quantum signal detection system. It ensures that quantum communication does not go undetected in military zones, border surveillance, or high-security data flows. With its modular design and emphasis on signal integrity, QIDS introduces a new layer of national cybersecurity.

This is a conceptual model in pre-prototype stage and aims to open avenues in quantum surveillance and defense research.

Deployment Areas (Planned Use Cases): - Military zones - Government data centers - Border & satellite communication networks - Strategic industrial networks

---

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

Contact:
Sidhant Negi
Email: sidhantnegi68@gmail.com
GitHub: https://github.com/Sidhant1s