Quantum-Enhanced Detection Mechanisms for Mobile Network Security*

Antonio Baggiano, Franco Cirillo, and Christian Esposito†

University of Salerno, Fisciano (SA), Italy
a.baggiano@studenti.unisa.it, {fracirillo,esposito}@unisa.it

Abstract

The security of mobile networks faces significant challenges from adversarial strategies aimed at compromising current infrastructure, including rogue base stations, jamming, timing spoofing, and vulnerabilities in random access procedures. Such a situation has been exacerbated by the rise of 5G and 6G networks, which introduce unprecedented challenges for securing mobile infrastructures against these sophisticated adversaries. Traditional methods based on classic AI solutions have proven ineffective in correctly detecting these attacks. This paper presents the theoretical foundations and methodological framework for applying Variational Quantum Simulation (VQS) to mobile network security, enabling advanced detection methods for the attacks mentioned earlier. We present a prototype and discuss possible improvements to synthetic data to analyze the exploitability of VQS against advanced attacks in mobile networks.

1 Introduction

Current and future mobile networks are increasingly vulnerable to advanced threats [1, 2], such as rogue gNodeBs (gNBs), which is a fake 5G radio station that pretends to be a legitimate cell to attract terminals and interact with them before the end-to-end cryptographic protection with the core kicks in. gNBs broadcasts fake synchronization signals, tone and barrage jamming attacks, and timing spoofing that undermines synchronization. Dealing with these attacks requires a layered approach that blends signal analysis, robust cryptographic techniques, and adaptive network strategies. A rogue gNB poses a significant threat because it can transmit counterfeit synchronization signals that mislead user equipment, forcing devices to connect to illegitimate sources or causing widespread desynchronization across the network. Countering such threats demands both authentication mechanisms for synchronization signals and continuous monitoring of broadcast patterns to detect anomalies in time, frequency, and power levels. Tone jamming and barrage jamming exploit vulnerabilities at the physical layer by flooding selected frequencies or wide portions of the spectrum with noise, degrading the signal-to-interference ratio and disrupting communication channels. Mitigation involves spectrum sensing, dynamic frequency hopping, and interference-cancellation methods that enable the network to rapidly adapt to hostile conditions while maintaining essential connectivity. Timing spoofing represents another subtle but equally dangerous attack, as it manipulates synchronization references to shift network timing, destabilizing not only individual connections but also the orchestration of distributed functions such as handovers and resource allocation. To defend against this, resilient synchronization frameworks must incorporate redundant time

*Proceedings of the 9th International Conference on Mobile Internet Security (MobiSec'25), Article No. 31, December 16-18, 2025, Sapporo, Japan.

†Corresponding Author

sources, cross-verification between independent clocks, and anomaly detection based on statistical deviations from expected timing behavior. Ultimately, the defense against these categories of attacks is not purely technical but also strategic, requiring integration of secure protocols, advanced detection algorithms, and situational awareness within the overall architecture of mobile networks, ensuring that resilience is embedded at both the device and infrastructure levels.

The main limitation of current solutions to rogue gNBs, jamming, and timing spoofing lies in their dependence on classical detection and mitigation strategies that struggle to cope with the sophistication and adaptability of modern attacks [3, 4]. Authentication mechanisms based on conventional cryptography remain vulnerable to future advances in computational power, spectrum sensing techniques are reactive and often too slow to anticipate highly dynamic interference patterns, and redundant timing frameworks can still be deceived by carefully crafted spoofing signals that exploit statistical blind spots. These methods also face scalability challenges as networks evolve toward ultra-dense deployments, where the sheer number of nodes amplifies both the attack surface and the complexity of real-time monitoring. Quantum computing introduces the potential to radically improve this status quo by providing capabilities that go beyond classical limitations. Quantum key distribution offers provable security for authenticating synchronization signals against rogue broadcasting, ensuring that falsified signals can be distinguished with absolute certainty. Quantum algorithms for optimization and pattern recognition could allow networks to detect and adapt to jamming attempts in real time, identifying subtle interference patterns that would remain hidden to classical statistical models. Furthermore, the precision of quantum sensing and quantum-enhanced timekeeping can deliver far more reliable synchronization, making timing spoofing substantially harder to achieve. By combining unbreakable quantum-secured communication with enhanced detection and adaptive optimization, quantum technologies promise to transform the resilience of mobile networks against sophisticated adversaries, moving from reactive countermeasures to proactive and fundamentally secure designs. In fact, quantum machine learning would tap PHY-layer I/Q streams and derive time–frequency features (e.g., sync-channel snapshots, cyclostationary statistics, CSI/DM-RS patterns, and timing residuals), encode them with quantum feature maps into variational circuits or quantum kernels, and perform hybrid anomaly detection and multi-class discrimination to surface rogue gNodeBs broadcasting fake synchronization signals, tone/barrage jamming, and timing spoofing under online, adversarially robust training with continual adaptation. The user equipment can extract features and send them to a dedicated security device running a hybrid quantum-inspired solution, while offloading quantum-related computation to an appropriate device at the edge/cloud. Alternatively, such a solution can be hosted at base stations and dedicated SDR security probes with federated learning and secure aggregation; the system would drive RAN countermeasures by emitting actionable scores to blacklist suspect cells, adjust beams/power and filters, or force re-synchronization and graceful handover.

Variational Quantum Simulation (VQS) [5], originally developed to simulate quantum dynamics, provides a flexible framework for approximate state evolution in both real and imaginary time by using a hybrid quantum-classical approach depicted in Figure 1 that optimally updates the parameters of parameterized quantum circuits (PQC) using variational principles [6]. This method is particularly relevant as a robust framework for tackling quantum simulations that could have significant implications across various fields, including network security. By adapting VQS to mobile network security tasks, we introduce a methodology that maps spectrum anomalies, preamble correlations, and timing offsets into Hamiltonian optimization problems whose solutions can be approximated with near-term quantum devices. Specifically, we propose exploiting VQS to model and recognize complex patterns in communication channels that

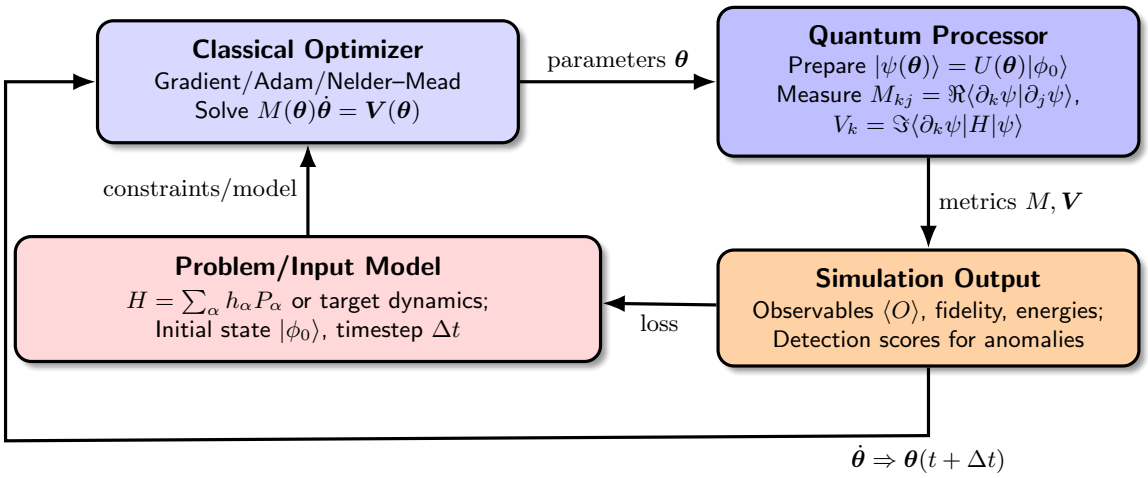


Figure 1: Variational Quantum Simulation (VQS) hybrid loop. The quantum processor prepares the variational state $|\psi(\boldsymbol{\theta})\rangle$, measures the metric M_{kj} and driving vector V_k from the McLachlan principle, while the classical optimizer updates parameters via $M(\boldsymbol{\theta})\dot{\boldsymbol{\theta}} = \boldsymbol{V}(\boldsymbol{\theta})$ and advances $\boldsymbol{\theta}$ over time.

are difficult to capture with conventional techniques. In the context of rogue gNBs, VQS can simulate the propagation of authentic synchronization signals against maliciously injected ones, allowing the network to distinguish legitimate phase and frequency references from those artificially introduced. Against jamming —both narrowband tone and wideband barrage —the variational approach can represent interference as perturbations in the quantum state of the communication channel, enabling anomaly detection that identifies even weakly concealed disruptions. For timing spoofing, VQS can model the temporal correlations of synchronization sequences with quantum-enhanced sensitivity, detecting subtle deviations from expected evolution that classical statistical techniques may fail to resolve. The strength of this approach lies in its adaptability: variational circuits can be trained continuously on live network data, enabling them to learn evolving attack strategies and generalize across different deployment contexts. By embedding VQS-based detection mechanisms into the monitoring layer of mobile networks, operators could move beyond reactive filters and static thresholds, deploying a quantum-enhanced sentinel that learns, simulates, and predicts malicious behavior in real time, thereby significantly raising the barrier for successful attacks.

This paper is structured as follows. Section 2 provides a brief introduction to quantum computing and networks and an analysis of the existing literature on the topic, while Section 3 presents the proposed approach to detect anomalies with quantum computing in mobile networks. Section 4 illustrates the obtained results of the preliminary experiments we have conducted. We conclude with Section 5 with lessons learns and future work.

2 Background and Related Works

2.1 Background on Quantum Computing

Quantum computing [7] is fundamentally based on the concept of the qubit, which differs from the classical, deterministic, and binary bit, and this is due to the underlying realization tech-

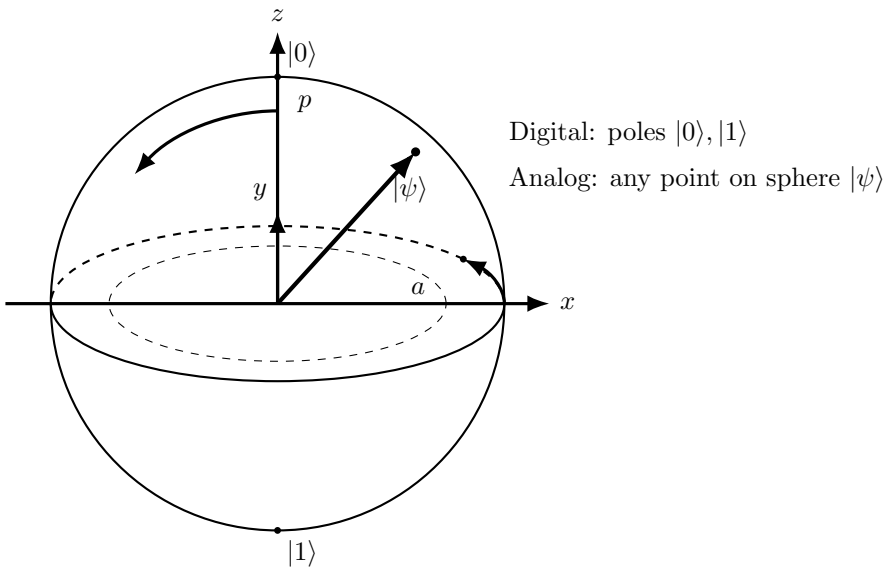


Figure 2: Bloch sphere highlighting the digital basis states at the poles and an arbitrary analog qubit state $|\psi\rangle$ with spherical coordinates (p, a).

nology. Classic bits are made of digital circuits that operate as switches —typically transistors —that control the flow of electrical current and can be in two states: on or off. This on/off state is represented by the binary values 1 and 0, which is why bits are binary. The Qubit innovation was conceived by exploiting quantum phenomena and employing various physical systems, including photons, trapped ions, superconducting circuits, and atoms. Specifically, superconducting circuits kept at extremely low temperatures cause electrons to behave as a single entity, creating controllable quantum states and enabling the quantum phenomenon of superconductivity, which involves zero electrical resistance and the expulsion of magnetic fields. A qubit corresponds to the quantum state of a two-level quantum system, and is mathematically represented as a unit vector in a two-dimensional complex Hilbert space $\mathcal{H}$, typically denoted as $\mathbb{C}^2$. To describe states of a qubit in a Hilbert space, we fix an orthonormal basis $\{\psi_i\}_{i=1}^n$, which satisfies:

$$\langle \psi_i, \psi_j \rangle = \delta_{ij} \quad \text{for all } i, j, \tag{1}$$

where δ_{ij} is the Kronecker delta. In the case of a qubit, the Hilbert space is two-dimensional and the standard orthonormal basis is given by $\{|0\rangle, |1\rangle\}$, where each state $|\psi\rangle \in \mathcal{H}$ can be written as a linear combination:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \quad \text{with } \alpha, \beta \in \mathbb{C}, \quad |\alpha|^2 + |\beta|^2 = 1. \tag{2}$$

This representation encodes the qubit in a superposition of the two basis states $|0\rangle$ and $|1\rangle$ within the two-dimensional Hilbert space $\mathbb{C}^2$, and is represented in the so called the Bloch sphere in Figure 2, which serves as a valuable tool for visualizing the action of gates in quantum circuits used to implement quantum algorithms.

Equation 2 represents the digital state of a qubit that refers to the idealized logical representation used for computation in the quantum circuit model, while another formalism is possible and named as the analog state of qubits, which refers to their continuous, physical reality governed by quantum mechanics and subject to noise and imperfections. Specifically, the

amplitudes α and β are not discrete but continuous complex numbers that can vary smoothly, meaning a physical qubit can occupy any point on the Bloch sphere rather than just the poles $|0\rangle$ and $|1\rangle$. Moreover, imperfections in control pulses, noise, and decoherence affect the state in an analog way, leading to small deviations rather than strictly discrete jumps. From this perspective, a qubit behaves as an analog device whose properties must be carefully engineered, calibrated, and stabilized to approximate the digital model assumed in quantum algorithms. The quantum time evolution of a state $|v(t)\rangle$ is governed by the time-dependent Schrödinger equation:

$$B(t)\frac{d}{dt}|v(t)\rangle = A(t)\,|v(t)\rangle\,, \tag{3}$$

where $A(t)$ and $B(t)$ denote matrices. In the framework of VQS, the exact state $|v(t)\rangle$ is approximated by a parameterized trial state, or *ansatz*, of the form

$$|v(t)\rangle \;\approx\; |\psi(\boldsymbol{\theta}(t))\rangle = U(\boldsymbol{\theta}(t))\,|\phi_0\rangle\,, \tag{4}$$

where $U(\boldsymbol{\theta}(t))$ is a unitary operator expressed as a sequence of parameterized quantum gates, $\boldsymbol{\theta}(t) = (\theta_1(t), \theta_2(t), \ldots, \theta_p(t))$ is the set of time-dependent variational parameters, and $|\phi_0\rangle$ is a fixed reference state. The evolution of $\boldsymbol{\theta}(t)$ is obtained from the McLachlan variational principle [8], which minimizes the distance between the exact and variational time derivatives of the state:

$$\delta \left\| B(t)\sum_{k=1}^{N_p}\frac{\partial\,|\psi(\boldsymbol{\theta}(t))\rangle}{\partial\theta_k}\dot{\theta_k} - A(t)\,|\psi(\boldsymbol{\theta}(t))\rangle \right\| = 0. \tag{5}$$

This yields a system of differential equations for the parameters:

$$\sum_{k=1}^{N_p} M_{jk}\,\dot{\theta}_k = V_j, \tag{6}$$

where N_p is the number of parameters and

$$M_{jk} = \Re\left(\langle\partial_{\theta_j}\psi(\boldsymbol{\theta}(t))|\partial_{\theta_k}\psi(\boldsymbol{\theta}(t))\rangle\right), \tag{7}$$

$$V_j = \Im\left(\langle\partial_{\theta_j}\psi(\boldsymbol{\theta}(t))|H|\psi(\boldsymbol{\theta}(t))\rangle\right). \tag{8}$$

It is worth noting that, besides McLachlan's principle [8], two other conventional variational principles are commonly discussed in the literature: the Dirac–Frenkel variational principle [9] and the time-dependent variational principle [10], whose detailed comparison can be found in [11]. The Dirac–Frenkel principle is not well-suited for VQS, as the resulting parameter equations may yield complex solutions, in conflict with the requirement that variational parameters remain real. The time-dependent variational principle, while producing real solutions, has been shown to suffer from instabilities and is not directly applicable to the evolution of density matrices or to imaginary-time dynamics [12]. In contrast, McLachlan's principle typically provides stable solutions and is broadly applicable across all VQS settings.

Once the quantities M_{kj} and V_k have been obtained, the set of variational parameters can be updated using the Euler integration method with a small time step δt:

$$\boldsymbol{\theta}(t+\delta t) = \boldsymbol{\theta}(t) + M^{-1}V\,\delta t, \tag{2.8}$$

where M denotes the matrix representation of the elements M_{jk}, and V is the vector composed of the components V_k. In the following, we show how M_{jk} and V_j can be explicitly computed.

Here, M_{jk} plays the role of a *quantum geometric tensor* defining the metric on the variational manifold, while V_j encodes the Hamiltonian-driven changes to the state. Solving Equation (6) step by step allows the parameters $\boldsymbol{\theta}(t)$ to approximate the true quantum time evolution.

Considering Equation 4, it is possible to estimate M_{jk} and V_j on a quantum device for an ansatz

$$U(\boldsymbol{\theta}) = \prod_{\ell=1}^{p} e^{-\frac{i}{2}\theta_\ell G_\ell}, \tag{9}$$

where each G_ℓ is a Hermitian generator (often a Pauli string) with spectrum $\{\pm 1\}$, and the Hamiltonian is expanded as $H = \sum_\alpha h_\alpha P_\alpha$ with Pauli strings P_α. For generators with ± 1 eigenvalues, the parameter-shift rule provides unbiased finite-difference identities for derivatives of expectation values. Using

$$\partial_{\theta_k} |\psi(\boldsymbol{\theta})\rangle = -\tfrac{i}{2}\, U(\boldsymbol{\theta})\, \tilde{G}_k(\boldsymbol{\theta})\, |\phi_0\rangle\,, \qquad \tilde{G}_k(\boldsymbol{\theta}) \equiv U^\dagger(\boldsymbol{\theta})\, G_k\, U(\boldsymbol{\theta}), \tag{10}$$

It is possible to rewrite

$$V_j = \Im\big(\langle \partial_{\theta_j}\psi | H | \psi\rangle\big) = \frac{1}{2}\sum_\alpha h_\alpha\, \partial_{\theta_j}\big(\langle\psi|\, P_\alpha\, |\psi\rangle\big)\,, \tag{11}$$

where the last equality follows from the product rule and the anti-Hermitian structure of the derivative. Applying the parameter-shift rule to each expectation $\langle P_\alpha\rangle_{\boldsymbol{\theta}}$ yields

$$\partial_{\theta_k}\langle P_\alpha\rangle_{\boldsymbol{\theta}} = \frac{1}{2}\left(\langle P_\alpha\rangle_{\boldsymbol{\theta}+\frac{\pi}{2}\mathbf{e}_k} - \langle P_\alpha\rangle_{\boldsymbol{\theta}-\frac{\pi}{2}\mathbf{e}_k}\right), \tag{12}$$

and hence

$$V_j = \frac{1}{4}\sum_\alpha h_\alpha \left(\langle P_\alpha\rangle_{\boldsymbol{\theta}+\frac{\pi}{2}\mathbf{e}_k} - \langle P_\alpha\rangle_{\boldsymbol{\theta}-\frac{\pi}{2}\mathbf{e}_k}\right). \tag{13}$$

Equation (13) reduces the evaluation of V_k to expectation values of Pauli strings measured on two shifted parameter settings per k (per commuting group of $\{P_\alpha\}$). Using the generator form of the derivative,

$$|\partial_{\theta_k}\psi\rangle = -\tfrac{i}{2}\, U\, \tilde{G}_k\ |\phi_0\rangle\,, \qquad \langle\partial_{\theta_k}\psi| = \tfrac{i}{2}\ \langle\phi_0|\ \tilde{G}_k\, U^\dagger, \tag{14}$$

We obtain the quantum geometric tensor real part representation as follows:

$$M_{jk} = \frac{1}{4}\,\Re\Big(\ \langle\psi|\,\tilde{G}_j\,\tilde{G}_k\,|\psi\rangle\ \Big) - \frac{1}{4}\,\Re\Big(\ \langle\psi|\,\tilde{G}_j\,|\psi\rangle\ \langle\psi|\,\tilde{G}_k\,|\psi\rangle\ \Big), \tag{15}$$

which shows that M_{jk} can be reconstructed from expectation values of (conjugated) generators and their products on the state $|\psi(\boldsymbol{\theta})\rangle$. When G_k are Pauli strings, $\tilde{G}_k = U^\dagger G_k U$ are also Pauli strings conjugated by U and can be measured by rotating into the appropriate single-qubit bases.

2.2 Literature Analysis

The notion of gNBs broadcasting false synchronization signals poses significant security threats in modern telecommunications, particularly within 5G networks. The integrity of synchronization mechanisms is essential to maintaining communication continuity and reliability, and any disruption can lead to severe repercussions, including denial-of-service attacks and data manipulation.

Rogue gNBs exploit vulnerabilities in synchronization protocols to inject fraudulent synchronization signals, which can mislead legitimate user equipment (UE) into aligning its operations with incorrect timing. Specifically, research highlights the increasing sophistication of attacks such as rogue master attacks, in which adversaries can manipulate the Best Master Clock Algorithm (BMCA) in Precision Time Protocol (PTP) systems, thereby asserting control over synchronization processes [13]. This manipulation allows for the transmission of false timing information, potentially causing significant anomalies in timing-sensitive applications. The implications of such attacks are profound, as they jeopardize data integrity and disrupt critical services dependent on accurate synchronization [14].

Furthermore, these attacks can be exacerbated by jamming techniques, particularly barrage jamming and timing spoofing. Barrage jamming involves overwhelming the communication channel with a high volume of noise, effectively drowning out legitimate signals [15]. Such interference makes it exceedingly difficult for users to detect rogue signals. This limitation is compounded in environments where secure communication is paramount, as deceptive synchronization signals may go undetected amid the chaos of interference.

Timing spoofing represents another layer of vulnerability. By deceiving UE into accepting false synchronization signals, attackers can disrupt the operational timelines of communication sessions. The correct functioning of synchronization signals—specifically, the Primary Synchronization Signal (PSS) and Secondary Synchronization Signal (SSS)—is critical for effective cell search and identification within the 5G ecosystem [16]. Studies have shown that timing spoofing can effectively alter the perception of network latency and availability, allowing malicious entities to exploit user services [17].

The existing literature underscores the need for robust intrusion detection systems (IDSs) that can preemptively detect and respond to rogue attacks on gNBs. The implementation of advanced detection schemes inspired by recent studies stands to enhance the resilience of network synchronization mechanisms against these emerging threats [13]. For example, detecting discrepancies in expected synchronization behavior could serve as an early warning system for identifying rogue gNB activities.

In conclusion, the body of work surrounding rogue gNB attacks, jamming, and timing spoofing reveals critical vulnerabilities within 5G synchronization protocols. The synthesis of empirical findings and theoretical frameworks suggests that, as networks continue to evolve, so too must the strategies to secure synchronization processes against malicious interventions. Continuous research and development of advanced IDS and synchronization verification processes will be integral in safeguarding modern telecom infrastructures.

3 Proposed Approach

The proposed pipeline using VQS is depicted in Figure 3, where the legitimate and adversarial signals are encoded in quantum states as follows:

- Rogue base stations transmit counterfeit synchronization signals that mimic legitimate broadcasts, making them difficult to detect with classical statistical filters. VQS encodes synchronization sequences into quantum states and simulates their evolution under perturbations. Subtle deviations in phase and frequency coherence induced by malicious signals appear as instabilities in the variational parameter updates, enabling early detection of counterfeit broadcasts.

- Tone jamming and barrage jamming degrade communication by injecting interference into the spectrum. Conventional defenses, such as adaptive filtering or frequency hop-

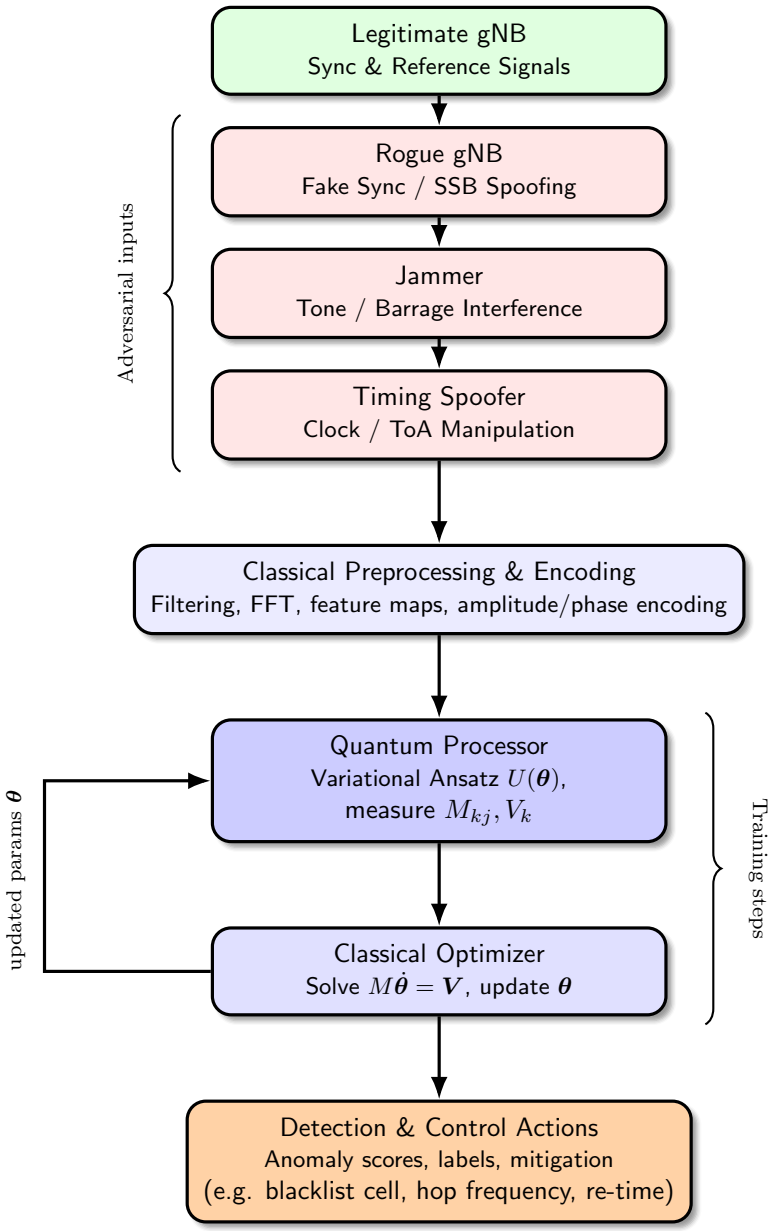


Figure 3: Vertical pipeline of VQS for mobile network security, hwre legitimate and adversarial signals are encoded and processed through the quantum variational loop, with anomaly detection and mitigation at the output stage.

ping, are reactive and limited in speed. VQS models jamming as perturbations to the effective channel Hamiltonian and dynamically adjust its variational parameters, learning the interference structure in real time. This enables predictive countermeasures, such as anticipatory spectrum reallocation, before the jamming fully disrupts communication.

- Spoofing synchronization references destabilizes temporal coherence in mobile networks, disrupting handovers and resource allocation. In VQS, synchronization signals are represented as quantum states with phase and frequency correlations extending across time slots. Spoofed timing introduces deviations in these correlations, which the variational update process highlights as anomalies. Since quantum circuits naturally encode phase relationships, VQS offers intrinsic sensitivity to such attacks, detecting them before large-scale desynchronization occurs.

Classical preprocessing converts raw signals into encodings suitable for quantum circuits that simulate the dynamics using VQS. Mobile security tasks are mapped into Hamiltonians:

- Rogue gNB or fake SSB detection: deviations in power spectral density are encoded into diagonal Hamiltonians penalizing differences from benign templates.
- Tone vs barrage jamming: localized or broadband perturbations appear as structured Hamiltonian terms reflecting frequency-domain anomalies.
- Timing spoofing detection: discrepancies in expected arrival times translate into penalty Hamiltonians centered on expected offsets.
- RACH preamble correlation: matched filtering is emulated by constructing reward Hamiltonians aligned with correlation peaks.

Feature vectors are extracted from mobile signals, including power spectral densities, timing offsets, and correlation magnitudes. These vectors are normalized and mapped onto qubit registers. Features are translated into diagonal Hamiltonians of the form

$$H = \sum_i w_i Z_i, \tag{16}$$

where w_i encodes deviations from benign baselines or expected templates. A hardware-efficient ansatz composed of alternating single-qubit rotations and entangling gates (e.g., CNOT rings) is used. The parameters $\boldsymbol{\theta}$ represent the variational degrees of freedom. Imaginary-time VQS is applied, solving

$$\mathbf{A}(\boldsymbol{\theta})\dot{\boldsymbol{\theta}} = -\tfrac{1}{2}\nabla E(\boldsymbol{\theta}), \tag{17}$$

with numerical integrators such as Euler or RK4. The final energy serves as the security score: low for benign signals, high for anomalies. Energy traces over iterations provide anomaly scores and detection confidence. Comparison across scenarios (rogue gNB, tone jamming, timing spoofing, RACH anomalies) establishes classification thresholds. Measurements feed back into a classical optimizer, producing anomaly scores. Rather than replacing existing defenses, VQS augments them by providing high-resolution detection at the physical layer, complementing cryptographic and policy-based security mechanisms.

4 Experimental Assessment

This work implements a VQS pipeline in Python by using the PennyLane library [18] for two RF security tasks—PSD-based anomaly scoring targeting rogue gNB activity, fake SSB shifts, and tone jammers, and a quantum-inspired matched filter for RACH preamble detection via correlation features—then incrementally hardens the prototype with reliability and numerical patches. Considering the used data, we have an analytical model for the benign data samples,

while the malicious samples are generated by adding zero-mean Gaussian noise. The aim is to investigate the feasibility of exploiting quantum technology for network security, leaving comparisons with existing solutions for future work, as well as the use of a real dataset of signal features.

The first experiment constructs a geometry-aware anomaly score for wideband RF spectra by simulating baseband IQ snapshots that resemble an OFDM carrier under three operating regimes: a benign spectrum with a few active subcarriers and modest noise, a narrowband interference obtained by injecting strong single-tone energy, and a fake-SSB condition obtained by shifting the spectrum by a few FFT bins to emulate a rogue gNB broadcasting synchronization at a slightly incorrect frequency or timing. Each complex snapshot $x[n]$ is converted to a power spectral density by an FFT,

$$X[k] = \sum_n x[n]\, e^{-j2\pi kn/N}, \qquad P[k] = |X[k]|^2, \tag{18}$$

then coarsened to a B-dimensional feature vector by averaging adjacent frequency bins,

$$\mathbf{p} \in [0,1]^B, \qquad p_i = \frac{1}{\max P}\,\frac{1}{W}\sum_{k\in\mathcal{W}_i} P[k], \tag{19}$$

where $\{\mathcal{W}_i\}_{i=1}^B$ are disjoint windows of width W and normalization enforces scale invariance with respect to the received power. The length B fixes the number of data qubits; an additional qubit is allocated but left unused as an auxiliary wire so that future overlap or Hadamard test measurements can be introduced without redesigning the device topology.

The quantum state preparation begins with angle embedding of the PSD features on the data wires,

$$U_{\mathrm{enc}}(\mathbf{p}) = \prod_{i=1}^{B} R_Y\big(\alpha_i\big)_{(i)}, \qquad \alpha_i \propto p_i, \tag{20}$$

followed by a compact variational ansatz with L layers,

$$U(\boldsymbol{\theta}) = \prod_{\ell=1}^{L}\left[\prod_{i=1}^{B} R_Z(\theta_{z,i}^{(\ell)})_{(i)}\right]\left[\prod_{i=1}^{B} R_X(\theta_{x,i}^{(\ell)})_{(i)}\right]\left[\prod_{i=1}^{B}\mathrm{CNOT}_{(i\to i+1)}\right]\left[\prod_{i=1}^{B}\mathrm{ZZ}(\gamma)_{(i,i+1)}\right], \tag{21}$$

with a ring topology for the two-qubit blocks and a small fixed entangling angle γ on the IsingZZ gates to encode nearest-neighbor spectral relations. The observable encodes benign spectral structure as a Pauli sum with linear and pairwise terms,

$$H_{\mathrm{benign}} = \sum_{i=1}^{B} a_i\, Z_i \;+\; \sum_{i=1}^{B-1} J_{i,i+1}\, Z_i Z_{i+1}, \qquad a_i \propto \mu_i - \bar{\mu}, \qquad J_{i,i+1} \propto \big(\Sigma_{\mathrm{benign}}\big)_{i,i+1}, \tag{22}$$

where $\boldsymbol{\mu}$ and Σ_{benign} are, respectively, the mean and covariance of PSD features computed on a small benign reference set, and $\bar{\mu}$ is the mean of $\boldsymbol{\mu}$. To contrast with the adversarial structure, an alternative Hamiltonian H_{fake} is built from fake-SSB statistics using the same recipe, and a tone-jammer Hamiltonian H_{tone} from tone-interference statistics when that threat model is of interest.

VQS advances the parameters $\boldsymbol{\theta}(t)$ by projecting the exact Schrödinger dynamics onto the tangent space of the variational manifold. Denote the prepared state $|\psi(\boldsymbol{\theta})\rangle = U(\boldsymbol{\theta})U_{\mathrm{enc}}(\mathbf{p})\,|0\rangle$. The McLachlan condition yields the linear system

$$\sum_j M_{kj}(\boldsymbol{\theta})\,\dot{\theta}_j = V_k(\boldsymbol{\theta}), \qquad M_{kj} = \Re[\langle\partial_k\psi\rangle\,\partial_j\psi]\,, \qquad V_k = -\,\partial_{\theta_k}\,\langle H\rangle_\psi, \tag{23}$$

whose explicit Euler discretization with Tikhonov regularization updates

$$\boldsymbol{\theta}_{t+\Delta t} = \boldsymbol{\theta}_t + \big(M(\boldsymbol{\theta}_t) + \lambda I\big)^{-1} V(\boldsymbol{\theta}_t)\, \Delta t. \tag{24}$$

Two complementary scores are extracted. The single-model energy $E_{\text{benign}} = \langle H_{\text{benign}} \rangle_\psi$ increases more rapidly for spectra that agree with benign structure and remains lower when energy is displaced across bands by shifts or narrowband injections. The contrastive gap

$$\Delta E = \langle H_{\text{fake}} \rangle_\psi - \langle H_{\text{benign}} \rangle_\psi \tag{25}$$

is computed along a common parameter trajectory and rises when the input resembles a fake-SSB spectrum relative to the benign template. A short pretraining phase that minimizes $\langle H_{\text{benign}} \rangle$ on a mini-batch of benign features stabilizes the operating point, and a post-hoc sign calibration on batch means guarantees that fake-SSB scores report as positive on average without altering gradients or updates. Because $Z_i Z_{i+1}$ couplings appear in both the ansatz and the Hamiltonians, the score becomes specifically sensitive to adversarial redistributions of power between neighboring coarse bands rather than to uniform rescalings.

The second experiment reuses the same VQS machinery to implement a quantum-inspired matched filter that detects NR random-access preambles. A Zadoff–Chu sequence of length N_{zc} with root u,

$$s[n] = \exp\Big(- j\pi u \, \frac{n(n+1)}{N_{\text{zc}}} \Big), \qquad n = 0, \ldots, N_{\text{zc}} - 1, \tag{26}$$

serves as the reference. A received burst $y[n]$ is synthesized by delaying $s[n]$ within a capture window and adding complex Gaussian noise at a chosen SNR. The magnitude of the circular correlation,

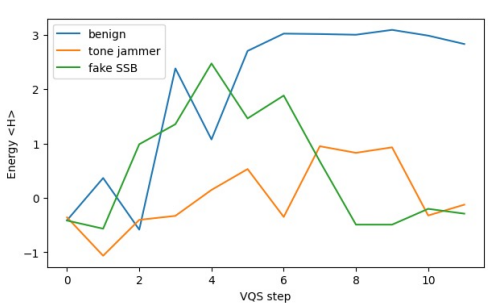
$$r[m] = \left| \sum_n y[n]\, s^*[n-m] \right|, \tag{27}$$

exhibits a sharp peak under a correct preamble and timing hypothesis and flattens toward noise otherwise. The sequence $r[m]$ is downsampled by averaging to a B-dimensional feature vector $\mathbf{c} \in [0,1]^B$ whose length again sets the data-qubit count and determines the angle-embedding layer. The same variational ansatz $U(\boldsymbol{\theta})$ is applied, and the observable encodes the expected peak–sidelobe profile via a Pauli sum

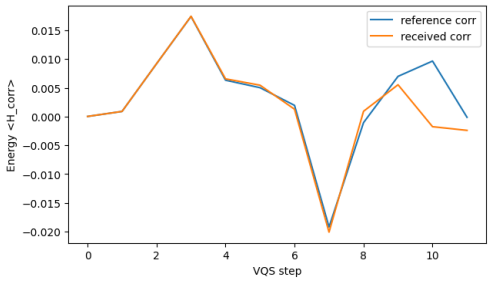
$$H_{\text{corr}} = \sum_{i=1}^{B} b_i \, Z_i \; + \; \sum_{i=1}^{B-1} K_{i,i+1} \, Z_i Z_{i+1}, \qquad b_i \propto c_i^{\text{ref}} - \overline{c^{\text{ref}}}, \qquad K_{i,i+1} \propto \big(\Sigma_{\text{corr}}\big)_{i,i+1}, \tag{28}$$

where $\mathbf{c}^{\text{ref}}$ is the downsampled magnitude-correlation of a clean preamble and Σ_{corr} is an optional covariance estimated from several clean captures to emphasize realistic peak width and sidelobe relations. Running the McLachlan update for a few Euler steps yields an energy trajectory $E_{\text{corr}}(t) = \langle H_{\text{corr}} \rangle_{\psi(t)}$ that falls when the received correlation matches the reference and remains elevated in the absence of a mismatch. The terminal energy thus serves as a matched-filter detection statistic. In a practical search across multiple roots and timing hypotheses, a small bank $\{H_{\text{corr}}^{(c)}\}$ is prepared and the decision is taken by $\arg\min_c \langle H_{\text{corr}}^{(c)} \rangle$, with the gap to the runner-up providing a simple confidence measure. Because the feature is the magnitude of the correlation rather than raw IQ, the detector is naturally insensitive to global phase and modest carrier offsets, and the shallow variational layer adapts to peak broadening at low SNR or in multipath by refining $\boldsymbol{\theta}$ across a handful of VQS steps.

Throughout both experiments, parameters are initialized near zero to avoid saturating rotations, the time step Δt is chosen small enough for the linearized update to remain accurate, and the metric inversion uses a Tikhonov-regularized matrix $(M + \lambda I)^{-1}$ with a modest $\lambda > 0$ to improve conditioning. Differentiable computations consistently use PennyLane's NumPy so that gradients propagate through QNodes, and scalar measurement outcomes are converted to ordinary floating-point values only at the edges for printing or plotting. The device always reserves one auxiliary wire in addition to the B data wires, leaving headroom for future overlap-based estimators without impacting the present scoring and detection pipelines. In combination, the observable design that mixes per-bin fields with nearest-neighbor couplings and the modestly entangling ansatz that mirrors these inductive biases make the VQS energy an informative statistic for adversarial spectral structure in the PSD setting and a robust matched-filter surrogate in the RACH setting.



(a) RF anomaly scoring from PSD features



(b) RACH preamble detection via correlation features

Figure 4: Energy of VQS evolution over steps in the two experiments.

Figure 4a depicts the energy evolution obtained for the first experiment, indicating a clear distinguishability of benign and adversarial samples with Final energy for benign equal to 2.8332, while -0.1234 and -0.2885 respectively for the jammer and fake SSB. Figure 4b shows the results of the second experiment, where the final energy for reference is -0.0001, while for the received is -0.0024. Lower final energy indicates a closer match to the reference preamble.

The initial observable $H = \sum_i w_i Z_i$ derived from a single benign power–spectral template only inspects each coarse frequency band independently. Realistic adversarial behaviors such as a fake-SSB that shifts energy by a few FFT bins or a narrowband tone jammer primarily *rearrange* power between neighboring bands while leaving marginal bin powers relatively unchanged, so the expectation $\langle H \rangle$ moves little and can overlap the benign trajectory. Making the Hamiltonian *structural* by adding nearest–neighbor couplings $Z_i Z_{i+1}$ with weights learned from covariances forces the energy to respond to how bands co-vary, which attacks perturb strongly but benign gain/noise drifts do not. Turning the score into a *contrast* between two class–conditioned Hamiltonians,

$$\Delta E \;=\; \big\langle H_{\text{fake}} \big\rangle \;-\; \big\langle H_{\text{benign}} \big\rangle, \qquad H_\star \;=\; \sum_i a_i^{(\star)} Z_i \;+\; \sum_i J_{i,i+1}^{(\star)} Z_i Z_{i+1},$$

Further cancels what the classes share and emphasizes the informative directions. Writing the state summaries as $m_i = \langle Z_i \rangle$ and $C_{ij} = \langle Z_i Z_j \rangle$, the gap decomposes as

$$\Delta E \;\approx\; \big(a^{(\text{fake})} - a^{(\text{benign})}\big)^{\top} \boldsymbol{m} \;+\; \big(J^{(\text{fake})} - J^{(\text{benign})}\big) : \boldsymbol{C},$$

So only differences in linear fields and pairwise structure contribute to the decision. In practice, this yields clear separation for shifted–SSB and tone–jammer spectra while remaining robust to benign covariate shifts.

Figure 5 shows the encoding/ansatz used by the VQS loop, the measurement strategy for an Ising Hamiltonian, and the conceptual two–head measurement for the contrastive score. For readability, a B=4–wire example is drawn; in experiments B equals the number of coarse PSD or correlation bins, and one extra device wire is reserved as an unused ancilla.

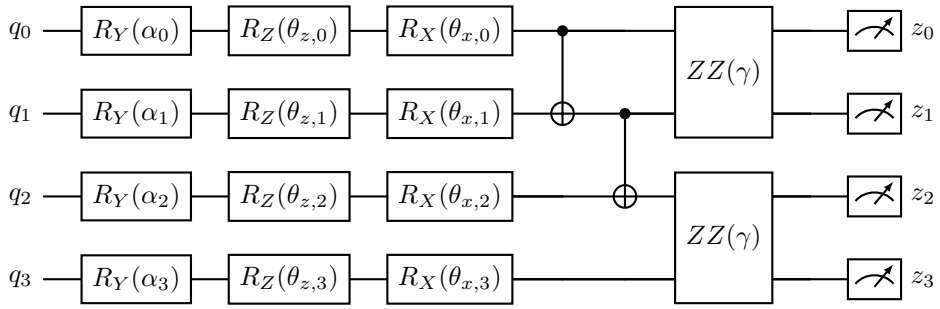


Figure 5: Quantum circuit used in the second experiment

The VQS update that drives discrimination projects Schrödinger dynamics onto the variational manifold spanned by circuit tangents. For $|\psi(\boldsymbol{\theta})\rangle$ and a chosen H, McLachlan's principle yields An explicit Euler step with Tikhonov regularization performs

$$\boldsymbol{\theta}_{t+\Delta t} \;=\; \boldsymbol{\theta}_t + \big(M(\boldsymbol{\theta}_t) + \lambda I\big)^{-1} V(\boldsymbol{\theta}_t)\,\Delta t.$$

With the Ising couplings in both the model and the observable, the energy becomes sensitive to the local power redistributions that characterize fake–SSB and tone–jammer attacks. To make the score sensitive to *structure* rather than level, we replaced this with a pair of class-conditioned *Ising* Hamiltonians and scored inputs by a *contrastive* energy gap.

Given small reference sets, let $(\boldsymbol{\mu}_{\mathrm{b}}, \Sigma_{\mathrm{b}})$ and $(\boldsymbol{\mu}_{\mathrm{f}}, \Sigma_{\mathrm{f}})$ denote the mean and covariance of benign and fake-SSB features, respectively, with $\bar{\mu}_\star = \frac{1}{B}\sum_{i=1}^{B} \mu_i^{(\star)}$. For $\star \in \{\text{benign}, \text{fake}\}$, define

$$H_\star \;=\; \sum_{i=1}^{B} a_i^{(\star)}\, Z_i \;+\; \sum_{i=1}^{B-1} J_{i,i+1}^{(\star)}\, Z_i Z_{i+1}, \qquad a_i^{(\star)} \;\propto\; \mu_i^{(\star)} - \bar{\mu}_\star, \quad J_{i,i+1}^{(\star)} \;\propto\; \big(\Sigma_\star\big)_{i,i+1},$$

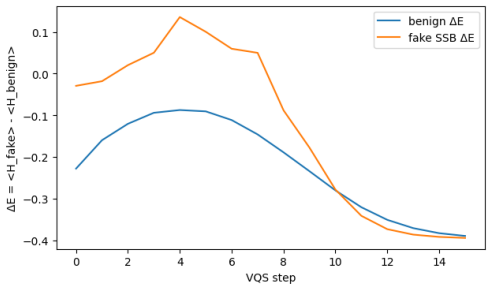
so that linear "fields" encode class-typical per-band levels while nearest-neighbor couplings encode class-typical *co-variation* across adjacent bands. For a prepared variational state $|\psi(\mathbf{x})\rangle$ obtained by the same VQS trajectory for any input $\mathbf{x}$, the score is the energy difference

$$\Delta E(\mathbf{x}) \;=\; \langle\psi(\mathbf{x})|H_{\text{fake}}|\psi(\mathbf{x})\rangle \;-\; \langle\psi(\mathbf{x})|H_{\text{benign}}|\psi(\mathbf{x})\rangle\,.$$

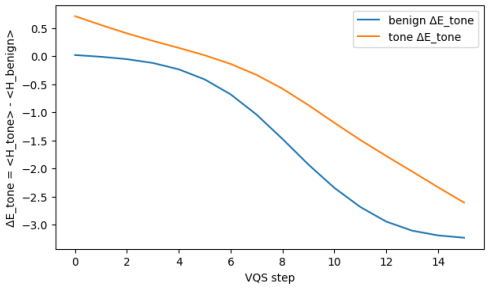
Writing single- and pairwise expectations as $m_i(\mathbf{x}) = \langle Z_i\rangle_{\psi(\mathbf{x})}$ and $C_{ij}(\mathbf{x}) = \langle Z_i Z_j\rangle_{\psi(\mathbf{x})}$, the gap decomposes as

$$\Delta E(\mathbf{x}) \;=\; \sum_i \big(a_i^{(\mathrm{f})} - a_i^{(\mathrm{b})}\big)\, m_i(\mathbf{x}) \;+\; \sum_{i<j} \big(J_{ij}^{(\mathrm{f})} - J_{ij}^{(\mathrm{b})}\big)\, C_{ij}(\mathbf{x}),$$

So only *class-informative* directions contribute, while nuisance trends common to both classes (e.g., global gain or noise-floor drifts) cancel in the difference. To ensure the circuit can represent these pairwise patterns, the variational layer includes small fixed IsingZZ(γ) entanglers between neighbors, mirroring the inductive bias in $H_\star$. Empirically, this change converts overlapping single-Hamiltonian energies into a robust discriminant ΔE that cleanly separates benign from fake-SSB (and likewise for tone jammers), with reduced sensitivity to benign covariate shift. The effect of these improvements is shown in Figure 6a, where the energy difference is a better indicator of the anomaly, but as the number of VQS steps increases, overfitting causes the trends to collide.



(a) RF anomaly scoring from PSD features as energy difference



(b) RF anomaly scoring from PSD features as energy difference in improved setting

Figure 6: Experiments with improved implementation

To make the VQS detector operationally simple, the energy measurements are compressed into a single real-valued score that can be logged, thresholded, and calibrated without re-running a full trajectory. Let $|\psi_{\boldsymbol{\theta}}(\mathbf{x})\rangle = U(\boldsymbol{\theta})\, U_{\mathrm{enc}}(\mathbf{x})\, |0\rangle$ denote the prepared state for features $\mathbf{x}$ under a fixed parameter vector $\boldsymbol{\theta}$ obtained either by a short evolution under a benign Hamiltonian or by a brief pretraining on benign mini-batches. Given a pair of class-conditioned observables $(H_{\mathrm{pos}}, H_{\mathrm{neg}})$—for example $(H_{\mathrm{benign}}, H_{\mathrm{fake}})$ in the fake-SSB setting—the raw scalar score is defined as the contrastive gap

$$S(\mathbf{x};\boldsymbol{\theta}) \;=\; \langle\psi_{\boldsymbol{\theta}}(\mathbf{x})|\, H_{\mathrm{neg}}\, |\psi_{\boldsymbol{\theta}}(\mathbf{x})\rangle \;-\; \langle\psi_{\boldsymbol{\theta}}(\mathbf{x})|\, H_{\mathrm{pos}}\, |\psi_{\boldsymbol{\theta}}(\mathbf{x})\rangle\,.$$

Evaluating both expectations in the *same* state $|\psi_{\boldsymbol{\theta}}(\mathbf{x})\rangle$ cancels common-mode effects such as overall gain and mild noise-floor drift, while retaining the class-informative structure encoded by the linear fields and nearest-neighbor couplings. For stable reporting across datasets, a one-bit calibration aligns the sign so that higher values consistently indicate the negative (adversarial) class: letting $\mathcal{B}$ and $\mathcal{N}$ denote benign and negative calibration sets, respectively, the reporting sign is chosen as

$$\sigma \;=\; \mathrm{sign}\Big(\, \mathbb{E}_{\mathbf{x}\in\mathcal{N}}[S(\mathbf{x};\boldsymbol{\theta})] \;-\; \mathbb{E}_{\mathbf{x}\in\mathcal{B}}[S(\mathbf{x};\boldsymbol{\theta})] \,\Big), \qquad \widetilde{S}(\mathbf{x}) \;=\; \sigma\, S(\mathbf{x};\boldsymbol{\theta}),$$

so that $\mathbb{E}_{\mathcal{N}}[\widetilde{S}] > \mathbb{E}_{\mathcal{B}}[\widetilde{S}]$ by construction. When desired, an affine normalization learned on a validation split can turn $\widetilde{S}$ into a calibrated confidence, for instance by standardizing with benign statistics $\mu_{\mathcal{B}}, \sigma_{\mathcal{B}}$ as $\widehat{S}(\mathbf{x}) = \big(\widetilde{S}(\mathbf{x}) - \mu_{\mathcal{B}}\big)/\sigma_{\mathcal{B}}$ and selecting a threshold τ that achieves a target false-alarm rate. In a multiclass extension with a bank $\{H_{\mathrm{pos}}^{(c)}\}$ and complementary $\{H_{\mathrm{neg}}^{(c)}\}$, one forms per-class gaps $S_c(\mathbf{x};\boldsymbol{\theta})$ and predicts $\arg\max_c \sigma_c S_c$, optionally reporting the margin to the

runner-up as a confidence proxy. Numerically, the quantity returned to the logging layer is the real scalar obtained by evaluating the two expectations and subtracting *after* differentiation-sensitive computations have finished; this guarantees a plain $\mathbb{R}$ value for plotting and storage while preserving end-to-end differentiability wherever it is needed. Figure 6b presents the results of this last improvement, where the increased number of steps and the potential for overfitting have a light impact on the detector, and the two trends are differentiated.

5 Conclusions

This paper shows that Variational Quantum Simulation can deliver practical RF security signals from compact features. We built two demonstrators: a PSD-based anomaly scoring method that separates benign spectra from fake-SSB shifts and tone jammers, and a RACH detector that behaves like a quantum-inspired matched filter based on correlation features. Key applied improvements made the prototype reliable and discriminative: class-conditioned, contrastive energies with Ising ZZ couplings to capture inter-band structure; a richer ansatz with mild Ising ZZ entanglers; a reserved auxiliary wire for future overlap tests; and a scalar scoring utility with sign calibration for consistent, loggable outputs. Numerically, we stabilized VQS with Tikhonov-regularized metric inversion, optional full QGT, careful use of PennyLane's autograd NumPy, and safe scalar extraction. Together, these upgrades turn raw VQS into a robust, end-to-end pipeline ready for larger datasets and hardware trials. This is a preliminary work that will be extended along two main directions: on the one hand, we will compare the prototype with a set of well-known and widely used AI-based solutions; on the other hand, we will run tests on real quantum devices and evaluate the impact of noise on computations. Last, we will also explore hybrid architectures that integrate predictive modeling and autonomous decision-making, potentially through reinforcement learning combined with quantum-augmented detection layers.

Acknowledgments

This work was partially supported by project SERICS (PE00000014) under the NRRP MUR program funded by the EU - NGEU.

References

[1] Mohammed Mahyoub, AbdulAziz AbdulGhaffar, Emmanuel Alalade, Ezekiel Ndubisi, and Ashraf Matrawy. Security analysis of critical 5g interfaces. *IEEE Communications Surveys & Tutorials*, 26(4):2382–2410, 2024.

[2] Hossein Pirayesh and Huacheng Zeng. Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey. *IEEE communications surveys & tutorials*, 24(2):767–809, 2022.

[3] Jasmine Zidan, Elijah I Adegoke, Erik Kampert, Stewart A Birrell, Col R Ford, and Matthew D Higgins. Gnss vulnerabilities and existing solutions: A review of the literature. *IEEe Access*, 9:153960–153976, 2020.

[4] Michal Harvanek, Jan Bolcek, Jan Kufa, Ladislav Polak, Marek Simka, and Roman Marsalek. Survey on 5g physical layer security threats and countermeasures. *Sensors (Basel, Switzerland)*, 24(17):5523, 2024.

[5] Suguru Endo, Jinzhao Sun, Ying Li, Simon C Benjamin, and Xiao Yuan. Variational quantum simulation of general processes. *Physical Review Letters*, 125(1):010501, 2020.

[6] Tobias Haug and Kishor Bharti. Generalized quantum assisted simulator. *Quantum Science and Technology*, 7(4):045019, 2022.

[7] Laszlo Gyongyosi and Sandor Imre. A survey on quantum computing technology. *Computer Science Review*, 31:51–71, 2019.

[8] Andrew D McLachlan. A variational solution of the time-dependent schrodinger equation. *Molecular Physics*, 8(1):39–44, 1964.

[9] Antonio Falcó, Wolfgang Hackbusch, and Anthony Nouy. On the dirac–frenkel variational principle on tensor banach spaces. *Foundations of computational mathematics*, 19(1):159–204, 2019.

[10] Roger Balian and Marcel Vénéroni. Time-dependent variational principle for the expectation value of an observable: Mean-field applications. *Annals of Physics*, 164(2):334–410, 1985.

[11] Xiao Yuan, Suguru Endo, Qi Zhao, Ying Li, and Simon C Benjamin. Theory of variational quantum simulation. *Quantum*, 3:191, 2019.

[12] Mingru Yang and Steven R White. Time-dependent variational principle with ancillary krylov subspace. *Physical Review B*, 102(9):094315, 2020.

[13] Alessio Buscemi, Manasvi Ponaka, Mahdi Fotouhi, Florian Jomrich, Christian Koebel, and Thomas Engel. An intrusion detection system against rogue master attacks on gptp. 2023.

[14] Mahdi Fotouhi, Alessio Buscemi, Abdelwahab Boualouache, Florian Jomrich, Christian Koebel, and Thomas Engel. Assessing the impact of attacks on an automotive ethernet time synchronization testbed. In *2023 IEEE Vehicular Networking Conference (VNC)*, pages 223–230. IEEE, 2023.

[15] Paweł Skokowski, Krzysztof Malon, Michał Kryk, Krzysztof Maślanka, Jan M. Kelner, Piotr Rajchowski, and Jarosław Magiera. Practical trial for low-energy effective jamming on private networks with 5g-nr and nb-iot radio interfaces. *Ieee Access*, 2024.

[16] Aymen Omri, Mohammad Shaqfeh, Abdelmohsen Ali, and Hussein Alnuweiri. Synchronization procedure in 5g nr systems. *Ieee Access*, 2019.

[17] Elena Peralta, Toni Levanen, Mikko Mäenpää, Youngsoo Yuk, Klaus I. Pedersen, Sari Nielsen, and Mikko Valkama. Remote interference management in 5g new radio: Methods and performance. *Eurasip Journal on Wireless Communications and Networking*, 2021.

[18] Ville Bergholm, Josh Izaac, Maria Schuld, Christian Gogolin, Shahnawaz Ahmed, Vishnu Ajith, M Sohaib Alam, Guillermo Alonso-Linaje, B AkashNarayanan, Ali Asadi, et al. Pennylane: Automatic differentiation of hybrid quantum-classical computations. *arXiv preprint arXiv:1811.04968*, 2018.