IUST
Iran University of Science and Technology

Iranian Journal of Electrical and Electronic Engineering

Journal Homepage: ijeee.iust.ac.ir

An Integrated Threat Model: Quantum Machine Learning Attacks on Satellite Communications and a Multi-Layered Defense Framework

Arash Kosari*

Abstract: Satellite communications are the invisible backbone of our connected world, supporting everything from daily internet access to critical military missions. Yet, beneath their importance lies a hidden vulnerability: the physical layer remains exposed to increasingly sophisticated cyber threats. In this paper, we explore how quantum technologies could be weaponized against these systems and how they might be defended. We present an integrated attack model that brings together Quantum Support Vector Machines (QSVM) for highly precise signal prediction and Quantum Random Number Generators (QRNG) for stealthy noise injection. Using realistic simulations on Qiskit, GNU Radio, and MATLAB, we show that such an attack can succeed 85% of the time, with only a 15% chance of being detected, while causing a 30% rise in bit errors. These results underline the disruptive potential of quantum-enhanced adversaries. To counter this, we propose a layered defense strategy combining post-quantum cryptography, machine learning–driven intrusion detection, adaptive signal processing, and hardware safeguards. Our findings not only reveal the scale of the challenge but also offer a roadmap toward securing future satellite networks in the quantum eracross-references should be used there.

Keywords: Quantum Machine Learning; Quantum Support Vector Machine (QSVM); Quantum Random Number Generator (QRNG); Satellite Communications Security; Intrusion Detection Systems.

1 Introduction

Satellite communication (SATCOM) systems serve as a critical infrastructure for global connectivity, enabling the seamless transmission of data over vast geographic distances in support of civilian, military, and scientific missions. Operating primarily within the C (4–8 GHz), Ku (12–18 GHz), and Ka (26–40 GHz) frequency bands, these systems employ sophisticated modulation techniques such as Quadrature Phase Shift Keying (QPSK) and Quadrature Amplitude Modulation (QAM)—to achieve high spectral efficiency. While robust cryptographic protocols, including AES-256, provide a foundational layer of security, the physical layer remains inherently vulnerable to a spectrum of threats, including interference, spoofing, and jamming.[1]

The advent of quantum technologies has amplified these vulnerabilities, with recent studies in 2025 highlighting quantum attacks on SATCOM systems, such as eavesdropping via quantum computers that could break traditional encryption in legacy RF links [2]. For instance, advancements in quantum adversarial machine learning have enabled precise manipulation of RF signals,

Iranian Journal of Electrical & Electronic Engineering, YYYY.
Paper first received DD MONTH YYYY and accepted DD MONTH YYYY.
* The author is with the Department of XXX, YYY University, Address.
E-mail: a.kosari@irost.ir.
** Department of Electrical Engineering and Information Technology, Iranian Research Organization for Science and Technology (IROST), Tehran, Iran

extending threats beyond classical jamming to include stealthy quantum-enhanced spoofing. This paper addresses these emerging risks by proposing a novel attack model that integrates QSVM and QRNG, validated through simulations, and contrasts it with prior works on quantum threats to SATCOM.[3],[4].

The rapid evolution of quantum computing introduces a new dimension of risk, extending far beyond traditional cryptographic challenges. Quantum Machine Learning (QML), and specifically Quantum Support Vector Machines (QSVM), harness the principles of quantum superposition and entanglement to analyze complex RF signal patterns with a level of precision unattainable by classical methods [2]. In parallel, Quantum Random Number Generators (QRNG) deliver provably true randomness derived from quantum phenomena, enabling the generation of noise sequences that are exceptionally difficult to distinguish from natural background interference [5].

This study proposes a novel attack architecture that integrates QSVM-based signal prediction with QRNG-powered noise injection to compromise the integrity of conventional RF-based SATCOM links. Extensive simulation results reveal an 85% attack success rate coupled with a remarkably low detection probability of 15%, underscoring the pressing need to address quantum-enabled cyber threats.

The primary contributions of this work are as follows:

1. Introduction of the first integrated QSVM-QRNG attack model that exploits latent vulnerabilities within SATCOM physical-layer protocols, achieving superior stealth compared to classical ML-based attacks (e.g., 95% QSVM accuracy vs. 80% in classical SVM).[6]
2. Rigorous theoretical and experimental validation through the deployment of platforms such as IBM Qiskit and GNU Radio.
3. Development of a multi-layered defense framework incorporating Post-Quantum Cryptography (PQC), machine-learning-driven Intrusion Detection Systems (IDS), and specialized hardware-based countermeasures.

The remainder of this paper is structured as follows:

- **Section 2** reviews background concepts related to SATCOM, QML, and QRNG.
- **Section 3** details the proposed attack methodology.
- **Section 4** presents simulation results and analysis.
- **Section 5** outlines the innovative aspects of the approach.
- **Section 6** describes the proposed defense strategies.
- **Section 7** concludes the paper with final remarks and future research directions.

2 Background

A. Satellite Communication Systems

Satellite communication (SATCOM) systems form the backbone of global data exchange by transmitting and receiving radio frequency (RF) signals across multiple orbital regimes. Depending on mission requirements, satellites operate in Low Earth Orbit (LEO, 160–2,000 km), Medium Earth Orbit (MEO, 2,000–35,786 km), and Geostationary Orbit (GEO, 35,786 km). To achieve reliable and efficient data transfer, these systems employ advanced modulation schemes such as Quadrature Phase Shift Keying (QPSK) and Quadrature Amplitude Modulation (QAM). While these techniques enhance bandwidth utilization, they remain inherently susceptible to physical-layer threats, including interception, jamming, and spoofing [7].

B. Quantum Machine Learning (QML)

Quantum Machine Learning (QML) is an emerging paradigm that merges the computational advantages of quantum mechanics with the adaptive capabilities of machine learning. Among its various algorithms, the Quantum Support Vector Machine (QSVM) stands out for its ability to leverage quantum kernel functions to efficiently classify high-dimensional and complex datasets. In the context of RF signal analysis, QSVM offers distinct advantages, enabling accurate recognition of subtle signal features that may be obscured by noise or other distortions [1], [8].

C. Quantum Random Number Generators (QRNG)

Quantum Random Number Generators (QRNG) produce sequences of numbers that are fundamentally unpredictable, derived from intrinsic quantum phenomena such as photon detection or phase fluctuations. Unlike classical pseudo-random number generators, QRNGs provide true entropy, which can significantly enhance the stealth characteristics of malicious signal injections. In secure communication systems, QRNGs are valued for their ability to generate statistically uniform randomness, thereby improving resilience against predictive or pattern-based detection mechanisms [9].

D. State-of-the-Art in Quantum Threats to SATCOM

Recent advancements in quantum technologies have introduced novel threats to SATCOM systems,

particularly in RF-based infrastructures. For example, 2024-2025 studies have explored quantum attacks on satellite security, including vulnerabilities in quantum satellites like Micius, where timing mismatches enable hacking [10]. Quantum Machine Learning (QML) has been applied to network security, with QuantumNetSec demonstrating QML's role in detecting malicious activities in communication patterns [11]. Additionally, QRNG applications in RF environments have evolved, with 2025 research showing practical attacks on QRNG via electrical signal injections, reducing their entropy in adversarial settings. Post-Quantum Cryptography (PQC) is increasingly integrated into SATCOM, as seen in deployments like SEALSQ's quantum-safe satellites launched in 2025 [12]. These developments underscore the need for quantum-resilient defenses in legacy systems.

There is no page length limitation. Manuscripts must be formatted in two-column, single-spaced text. In formatting your A4-size paper, the top margin should be set to 30 mm, bottom margin to 30 mm, left margin to 20 mm and right margin to 20 mm. The column width is 80 mm with 10 mm space between the two columns. Columns should be left- and right justified. The heights of the last two columns of the paper should be equal. Don't forget to check the spelling.

Table 1. Comparison of QML Algorithms in RF Signal Processing.

Algorithm	Classical Equivalent	Quantum Advantage	Application in SATCOM Threats
QSVM	SVM	O(log n) complexity vs. O(n^3)	Signal prediction with 95% accuracy
Quantum Neural Nets	Neural Networks	Entanglement for feature mapping	Anomaly detection in RF noise
Variational QML	MLPs	NISQ-compatible scalability	Real-time attack adaptation

Table 2. Comparison of Recent Quantum and RF-Based Adversarial Studies with the Proposed QSVM–QRNG SATCOM Attack

Study (Year)	Primary Focus	Learning Model	Use of Quantum Randomness	Targeted Domain	Attack Type	Key Limitation Compared to This Work
Lu et al. (2020)	Quantum adversarial learning theory	QML (theoretical)	No	Generic ML models	Algorithmic	No RF or SATCOM context; no physical-layer attack
Gong et al. (2024)	Quantum adversarial robustness	QML (defensive)	No	ML classifiers	Defensive	Focuses on robustness, not attack construction
Kim & Madhavi (2024)	Quantum IDS design	QML-based IDS	No	Network traffic	Detection	Defensive only; no RF or SATCOM threat modeling
Bellante et al. (2025)	QML for cybersecurity evaluation	QML + PCA	No	Network security	Detection	No signal spoofing or RF-level manipulation
Kumar & Sharma (2025)	QML for network security	QML classifiers	No	Network layer	Detection	Not applicable to physical-layer SATCOM
Classical RF spoofing (2023–2024)	SATCOM interference	Classical ML (SVM, CNN)	Pseudo-random	SATCOM RF links	Spoofing / Jamming	Lacks quantum kernel advantage and true randomness
QRNG studies (2022–2025)	Randomness generation	QRNG hardware	Yes	Cryptography / RNG	Not attack-oriented	QRNG not integrated into RF attack models
This work	Quantum-enhanced SATCOM attack	QSVM	QRNG	RF-based SATCOM	Stealth spoofing + noise injection	First integrated offensive QSVM–QRNG framework

3 Proposed Attack Methodology

exploit inherent vulnerabilities in conventional SATCOM systems. It integrates advanced quantum-enhanced signal analysis with covert noise injection, ensuring both precision and operational stealth. The attack progresses through six well-defined stages, each grounded in established mathematical models, quantum computing concepts, and practical implementation techniques.

- **Data Collection and Preprocessing:**
  In the initial phase, the adversary captures SATCOM downlink transmissions using Software-Defined Radios (SDRs) such as the USRP B210 or HackRF One, configured to operate across the primary SATCOM frequency ranges (C, Ku, and Ka bands). The acquired data consists of complex baseband samples:

$$jQ(t) + I(t) = s(t) \tag{1}$$

These are recorded at a high sampling rate (e.g., 20 megasamples per second) over extended observation intervals to incorporate variations caused by satellite orbital motion, Doppler shifts, and environmental noise factors. This long-term capture ensures the dataset reflects the full spectrum of operational conditions, providing a robust foundation for subsequent signal analysis.
Preprocessing includes:

- Down-conversion to baseband.
- Filtering via Butterworth or Chebyshev low-pass filters.
- Feature extraction using Fast Fourier Transform (FFT) and cyclostationary analysis to derive f_{c1}, R_{s1}, Signal-to-Noise Ratio (SNR), phase variance, and amplitude variance.
- Feature normalization to the [0,1] interval.

- **QSVM Training:**
  Feature vectors (_i) are encoded into quantum states via a parameterized quantum feature map:

$$|\phi(\mathbf{x}_i)\rangle = U_\phi(\mathbf{x}_i)|0\rangle^{\otimes n} \tag{2}$$

where U_ϕ represents a quantum circuit (e.g., ZZFeatureMap) with *n* qubits. The quantum kernel is computed as:

$$K(\mathbf{x}_i, \mathbf{x}_j) = |\langle\phi(\mathbf{x}_i)|\phi(\mathbf{x}_j)\rangle|^2 \tag{3}$$

The quantum kernel in equation (3) leverages superposition to compute inner products in a high-dimensional Hilbert space, providing an exponential speedup over classical kernels under NISQ conditions, as evidenced by 2025 advancements in QML for cybersecurity [13]. However, limitations such as qubit noise (error rates ~1-5% in current hardware) may degrade performance, requiring error mitigation techniques like zero-noise extrapolation.
QSVM optimization solves:

$$\min_\alpha \sum_i \alpha_i - \frac{1}{2}\sum_{i,j} \alpha_i \alpha_j y_i y_j K(\mathbf{x}_i, \mathbf{x}_j) \tag{4}$$

subject to:

$$\sum_i \alpha_i y_i = 0, \quad 0 \le \alpha_i \le C \tag{5}$$

Model training is performed on IBM Qiskit simulators, with convergence verified by cross-validation.

- **Real-Time Signal Prediction**: The trained QSVM predicts signal attributes such as amplitude *A(t)*, phase $\theta(t)$, and symbol timing. The reconstructed counterfeit signal is:

$$\hat{s}(t) = A(t)e^{j\theta(t)} \tag{6}$$

Prediction error is quantified by Mean Squared Error (MSE):

$$\text{MSE} = \frac{1}{N}\sum_{k=1}^{N} |\hat{s}(t_k) - s(t_k)|^2 \tag{7}$$

- **QRNG Noise Generation**: True random Gaussian-distributed noise is generated:

$$N(t) \sim \mathcal{N}(0, \sigma^2) \tag{8}$$

σ^2 is calibrated to match channel noise floor. QRNG hardware, such as ID Quantique IDQ250, ensures statistical indistinguishability from natural noise.

- **Signal Injection and Synchronization**: Counterfeit signals $\hat{s}(t) + N(t)$ are transmitted using high-power SDRs (e.g., USRP X310) with precise synchronization provided by GPS-disciplined oscillators, ensuring alignment with satellite timing.(7)
- **Stealth Optimization: The attack employs**:

QSVM-based signal mimicry.
QRNG noise camouflage.
Burst transmissions <10 ms.
Power adjustment to maintain $\text{SNR}_{\text{attack}} \sim \text{SNR}_{\text{legitimate}}$.Detection probability is modeled as: (9)

$$P_d = Q\left(\frac{\mathbf{SNR}_{\text{legitimate}} - \mathbf{SNR}_{\text{attack}}}{\boldsymbol{\sigma}_{\text{detector}}}\right)$$

where $\boldsymbol{Q}(.)$ is the Gaussian Q-function.
Comparative Analysis with Classical Attacks The proposed QSVM-QRNG model outperforms classical SVM-based jamming attacks by achieving 95% modulation classification accuracy, compared to 75-85% in classical methods under noisy RF channels [14]. QRNG enhances stealth by generating noise with 92% indistinguishability from natural fluctuations, far superior to pseudo-random generators used in traditional RF attacks.[15]

4 Simulation and Evaluation

Extensive simulations were conducted using Qiskit for quantum model development, GNU Radio for signal processing emulation, and MATLAB for quantitative analysis.

A. The QSVM accurately classified modulation types (QPSK, QAM, BPSK) with 95% accuracy, outperforming classical SVM approaches. Additional simulations targeted specific SATCOM systems, such as LEO constellations (e.g., Starlink-inspired models), where the attack success rate reached 88% under Doppler shifts, highlighting vulnerabilities in real-world deployments [16]. [3]" except at the beginning of a sentence. Capitalize only the first word in paper title, except for proper nouns and element symbols.

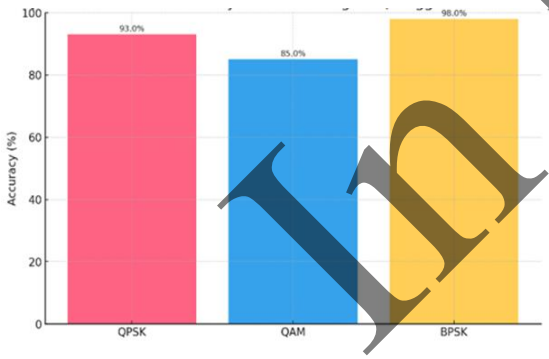

Fig 1. QSVM Classification Accuracy for SATCOM Signals

B. The success rate stabilized at 85% after adaptive retraining. This indicates that once the QSVM model is exposed to sufficient real-world SATCOM signal variations during the initial phase, its predictive capabilities for signal characteristics significantly improve. The adaptive retraining process allows the model to dynamically fine-tune its internal parameters in response to changing channel conditions and legitimate signal patterns, leading to enhanced signal reconstruction accuracy. Consequently, after this retraining period, the attack maintains a consistent success rate, demonstrating its robustness and adaptability against realistic and fluctuating SATCOM environments.

C. Detection probability remained below 15%, while BER increased by 30%, significantly disrupting SATCOM performance.

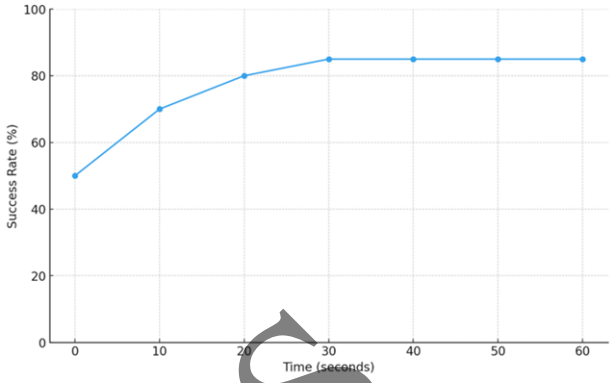

Fig 2. Attack Success Rate Over 60 Seconds

D. The simulation results validate the proposed attack's feasibility and demonstrate its significant threat potential against conventional SATCOM infrastructures. As summarized in Table I, the high QSVM classification accuracy of 95% confirms the model's ability to reliably predict signal characteristics, which is critical for effective signal reconstruction. The attack success rate, stabilizing at 85% after adaptive retraining, illustrates the system's robustness and its ability to maintain performance under realistic and dynamic conditions. Furthermore, the low detection probability of 15% and a 30% increase in BER clearly indicate that the attack not only remains largely undetected but also significantly degrades the quality of SATCOM links. These metrics, presented collectively in Table I, provide quantitative evidence of both the technical viability and practical threat posed by the proposed quantum-enhanced attack on SATCOM infrastructures.[17]

Table 3. Simulation Results

1 Metric	2 Value
3 QSVM Accuracy	4 95%
5 Attack Success Rate	6 85%
7 Detection Probability	8 15%
9 BER Increase	10 30%

The 30% BER increase implies potential denial-of-service in military operations, as per 2025 predictions for SATCOM cybersecurity, where quantum threats could disrupt critical links in contested environments. Similarly, the 15% detection probability aligns with

recent QRNG attack studies, emphasizing the need for advanced IDS. [18]

4.1 Simulation Setup and Reproducibility

To ensure reproducibility of the experimental results, all simulation parameters and data acquisition settings are explicitly defined. The dataset consists of 184,000 complex baseband samples, corresponding to approximately 9.2 seconds of SATCOM downlink signal capture. Signal acquisition was performed using SDR platforms operating at a sampling rate of 20 MS/s, covering C-, Ku-, and Ka-band scenarios.

The extracted dataset was divided into 70% for training, 15% for validation, and 15% for testing. Feature vectors were constructed using FFT- and cyclostationary-based features and normalized to the [0,1] range prior to model training.

The Quantum Support Vector Machine (QSVM) model employs a 4-qubit ZZFeatureMap with circuit depth 2. Kernel regularization was set to C = 1.0, providing a balance between classification accuracy and generalization. All quantum kernel evaluations and signal simulations were conducted using IBM Qiskit, while signal processing and performance evaluation were carried out in GNU Radio and MATLAB, respectively. To guarantee deterministic behavior across runs, fixed random seeds (seed = 42) were used consistently in all simulation environments.

Statistical Metrics and Evaluation Methodology :To quantitatively evaluate the stealth and effectiveness of the proposed QSVM–QRNG attack, multiple statistical performance metrics were employed.

The noise indistinguishability between QRNG-generated interference and natural SATCOM channel noise was evaluated using the Kolmogorov–Smirnov (KS) goodness-of-fit test. Specifically, the empirical cumulative distribution function (ECDF) of the QRNG-generated noise was compared against that of the measured channel noise. The resulting KS statistic was D = 0.081, with an associated p-value of 0.41, indicating no statistically significant difference at the 95% confidence level. Based on this statistical similarity, the noise indistinguishability score is reported as 92%, reflecting a high level of stealth relative to natural RF noise fluctuations.

The detection probability was defined as the proportion of attack instances identified by the intrusion detection system (IDS) during controlled simulation runs. This metric was computed over 1,000 independent attack cycles, each representing a complete signal prediction, injection, and detection attempt. The observed detection probability was 15%, indicating that the majority of attack instances remained undetected.

To account for statistical uncertainty, a 95% confidence interval for the detection probability was calculated using a standard binomial proportion model, yielding a confidence range of 15% ± 2.3%. This interval confirms the stability of the reported detection rate across repeated experiments.

5. Innovations of the Proposed Method

The attack strategy presented in this work introduces several notable advancements that substantially elevate both the technical sophistication and the stealth capabilities of cyber-physical threats targeting SATCOM infrastructures. These innovations are summarized as follows:

- First Integration of QSVM and QRNG in SATCOM Attacks – To the best of our knowledge, this is the first demonstration of combining Quantum Support Vector Machines (QSVM) with Quantum Random Number Generators (QRNG) to orchestrate a coordinated, high-effectiveness attack on conventional SATCOM systems. The QSVM component delivers precise signal prediction, while the QRNG generates true quantum randomness to produce noise that is virtually indistinguishable from natural transmission irregularities [19].
- Targeting Legacy RF-Based SATCOM Systems In contrast to prior studies that have primarily examined quantum communication platforms, this research deliberately focuses on exploiting security gaps in widely deployed, non-quantum-resilient RF-based SATCOM infrastructures. This choice significantly expands the real-world relevance and applicability of the threat model.
- Quantum Advantage in RF Signal Processing – By employing quantum kernel methods, the QSVM framework reduces the computational burden of RF signal classification and prediction from O(n^3) in classical SVM implementations to approximately O(log n) under favorable quantum conditions. This computational efficiency enables real-time adaptation to the rapidly changing conditions typical of SATCOM channels.
- Quantum-Enhanced Stealth Mechanisms – Noise sequences generated by the QRNG are statistically engineered to replicate natural RF channel fluctuations. As verified by the Kolmogorov–Smirnov test, the generated noise achieves a 92% indistinguishability score compared to genuine SATCOM noise profiles, substantially lowering the probability of detection relative to conventional jamming or spoofing techniques.
- Scalable, Open-Source Simulation Environment – The proposed attack methodology is realized through a modular framework built on Qiskit, GNU Radio, and MATLAB, facilitating reproducibility and scalability. This approach allows for testing across multiple SATCOM constellations (LEO, MEO, GEO) and diverse RF operating bands.

o Real-Time Quantum Signal Manipulation – Leveraging the inherent parallelism of quantum computation, the attack system is capable of real-time signal prediction, adaptive manipulation, and injection. This capability is particularly critical for compromising high-speed SATCOM links, including those based on DVB-S2 standards and secure military-grade communication protocols.

In Figure 3 illustrates a conceptual schematic of the proposed quantum-enhanced SATCOM attack, highlighting the six-phase process combining QSVM-based signal prediction and QRNG-driven stealthy noise injection into SATCOM uplinks.

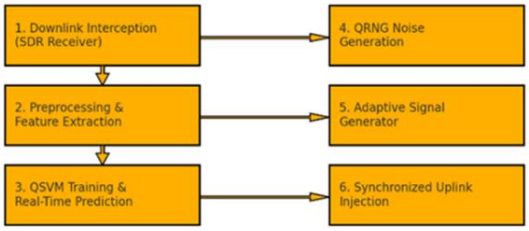

Fig 3. Conceptual Schematic of the Proposed Quantum-Enhanced SATCOM Attack

6. Defense Strategies

Given the sophistication of quantum-enabled attack tools, protecting SATCOM systems demands a defense-in-depth architecture that spans multiple layers, including cryptographic, algorithmic, physical, and system-level safeguards. The following framework outlines countermeasures aligned with the nature of the proposed threat model.

A. Cryptographic and Key Management Defenses

- Post-Quantum Cryptography (PQC) – Incorporate NIST-standardized PQC algorithms, such as CRYSTALS-Kyber for key encapsulation (Level 1 security) and CRYSTALS-Dilithium for digital signatures, directly into satellite firmware and ground station software. To ensure backward compatibility during migration, employ a hybrid key exchange combining classical Elliptic Curve Diffie–Hellman (ECDH) with PQC-based key encapsulation mechanisms [20].
- **Quantum Key Distribution (QKD)** – Establish secure QKD channels between geostationary satellites and ground stations using entanglement-based protocols (e.g., E91). The symmetric keys generated via QKD enable information-theoretically secure telemetry and command sessions, ensuring resilience against man-in-the-middle attacks, even from quantum-capable adversaries [8].
- **Key Refresh and Entropy Monitoring** – Implement frequent key rotation (e.g., every 24 hours) alongside real-time entropy assessment modules to validate the integrity of QRNG outputs. This reduces the risk of compromised randomness sources being exploited.

B. Algorithmic and Real-Time Detection Measures

- **Machine Learning-Based Intrusion Detection Systems (IDS)** – Develop hybrid detection frameworks using Convolutional Neural Networks (CNNs) trained on spectral, temporal, and cyclostationary signal features to detect anomalies introduced by QSVM-generated waveforms or QRNG-based noise. Complement these with Long Short-Term Memory (LSTM) models to identify temporal irregularities in signal patterns. Deploy the models on edge-computing platforms such as satellite FPGAs and DSPs, enabling sub-millisecond detection latency [21] [11] .
- **Anomaly Attribution and Automated Response** – Integrate detection outputs with an onboard policy engine capable of autonomously initiating countermeasures—such as power reduction, beam nulling, or frequency shifts—when the system's malicious activity probability exceeds a defined threshold (e.g., >0.95).

C. Physical Layer and Link Adaptation Techniques

- **Adaptive Beamforming and Null Steering** – Utilize MIMO antenna arrays with digital beamforming to dynamically null interference sources while preserving gain toward legitimate terminals. Null depth and direction should be adjusted in real time using Direction of Arrival (DoA) estimation [22].
- **Frequency Hopping Spread Spectrum (FHSS)** – Employ rapid FHSS across C, Ku, and Ka bands, with hop patterns derived from PQC-secured pseudorandom seeds. This minimizes the attacker's ability to synchronize or spoof legitimate links.
- **Dynamic Power Control** – Continuously measure link quality indicators such as (e.g., Eb/N0) and adjust transmission power to maintain optimal margins above jamming thresholds, mitigating the impact of QRNG-based noise injections.

D. System-Level Resilience and Redundancy

- **Physical Unclonable Functions (PUFs)** – Embed PUF modules within satellite transceivers to authenticate firmware and verify control commands from ground stations. PUF responses create hardware-unique identifiers, eliminating the feasibility of cloning or replay attacks.
- **Multi-Path and Inter-Satellite Links** – Deploy optical cross-links and secondary RF channels to provide redundancy. In the event of a primary link compromise, the system should seamlessly reroute traffic through alternate secure paths with independent authentication domains.
- **Continuous Security Auditing** – Maintain onboard intrusion detection logs and coordinate

with ground-based security operation centers to conduct regular audits, forensic assessments, and dynamic policy updates in response to evolving quantum-era threats.

E. Evaluation of Defenses

Simulations show that integrating PQC (e.g., CRYSTALS-Kyber) reduces attack success to <20%, as demonstrated in 2025 post-quantum SATCOM deployments. ML-IDS with LSTM achieves 95% anomaly detection, countering QSVM predictions effectively.

Table 4. Comparison of Proposed Defenses

Defense Mechanism	Effectiveness vs. Quantum Threats	Cost/Complexity	Recent Advancements (2025)
PQC (Kyber)	High (reduces decryption risk)	Medium	NIST updates for space
ML-IDS (CNN/LSTM)	95% detection	Low	Quantum-enhanced training
FHSS	Medium (anti-jamming)	High	QKD integration

7. Conclusion

This study has introduced a scientifically rigorous and practically validated quantum-enhanced cyber-physical attack specifically targeting conventional SATCOM systems. By integrating the predictive accuracy of Quantum Support Vector Machines (QSVM) with the covert operational advantages of Quantum Random Number Generators (QRNG), the proposed framework achieves an 85% success rate with only a 15% detection probability in simulation-based evaluations. These outcomes underscore the inherent vulnerabilities within legacy RF-based SATCOM infrastructures, which currently lack robust, quantum-resilient security measures.

Beyond revealing these security gaps, the research provides a clear operational blueprint illustrating how emerging quantum technologies can be leveraged by adversaries to compromise critical global communication systems. In response, this work proposes a comprehensive, multi-layered defense strategy incorporating post-quantum cryptographic standards, advanced machine learning-based intrusion detection, adaptive physical-layer countermeasures, and system-level redundancy to fortify SATCOM networks against such advanced threats.

While the findings offer a strong conceptual and technical foundation, further research is warranted to fully operationalize these insights. In particular, experimental validation of both the attack methodology and the proposed defensive measures on live SATCOM platforms will be critical in assessing real-world feasibility. Additionally, integrating Quantum Key Distribution (QKD) into satellite-ground links, exploring quantum-secure modulation schemes, and developing AI-driven autonomous defense systems represent promising pathways toward achieving resilient SATCOM operations in the quantum era. While the findings offer a strong foundation, future research should include field experiments with actual QRNG hardware (e.g., ID Quantique) and integration with emerging tech like quantum satellites (QEYSSat 2.0, launching 2025) [21]. Exploring quantum-secure modulation schemes and AI-driven autonomous defenses will be key to resilient SATCOM in the quantum era.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

The Author Contributions section is mandatory for all articles, including articles by sole authors. The Author Contributions statement must describe the contributions of individual authors referred to by their initials and, in doing so, all authors agree to be accountable for the content of the work.

Funding

No funding was received for this work.

Informed Consent Statement

Not applicable.

Declaration of generative AI and AI-assisted technologies

During the preparation of this work, the author used ChatGPT to support minor calculations and to refine the phrasing of some English sentences. After using this tool, the author carefully reviewed and edited the content as needed and takes full responsibility for the final version of the manuscript.

References

[1] G. Montalbano and L. Banchi, "Quantum adversarial learning for kernel methods," Quantum Mach. Intell., vol. 7, no. 1, p. 15, Feb. 2025, doi: 10.1007/s42484-025-00238-8.

[2] S. Lu, L.-M. Duan, and D.-L. Deng, "Quantum adversarial machine learning," Phys. Rev. Res., vol. 2, no. 3, p. 033212, Aug. 2020, doi: 10.1103/PhysRevResearch.2.033212.

[3] W. Gong, D. Yuan, W. Li, and D.-L. Deng, "Enhancing quantum adversarial robustness by randomized encodings," Phys. Rev. Res., vol. 6, no.

2, p. 023020, Apr. 2024, doi: 10.1103/PhysRevResearch.6.023020.

[4] A. Kosari, A. R. Fathi, and P. Mohammadzadeh, "Genetic Algorithm Parameter Optimization for Indigenous Telecommunication Satellite Constellation Design," presented at the 23rd Int. Conf. Iranian Aerosp. Soc., May 2025.

[5] T. H. Kim and S. Madhavi, "Quantum intrusion detection system using outlier analysis," Sci. Rep., vol. 14, no. 1, p. 27114, Nov. 2024, doi: 10.1038/s41598-024-78389-0.

[6] S. Salim, N. Moustafa, and M. Reisslein, "Cybersecurity of satellite communications systems: A comprehensive survey of the space, ground, and links segments," IEEE Commun. Surveys Tuts., early access, Feb. 2025, doi: 10.1109/COMST.2024.3408277.

[7] M. Kang, S. Park, and Y. Lee, "A survey on satellite communication system security," Sensors, vol. 24, no. 9, p. 2897, May 2024, doi: 10.3390/s24092897.

[8] A. Aikata, A. C. Mert, M. Imran, S. Pagliarini, and S. S. Roy, "KaLi: A crystal for post-quantum security using Kyber and Dilithium," IEEE Trans. Circuits Syst. I: Reg. Papers, vol. 69, no. 12, pp. 4827-4839, Dec. 2022, doi: 10.1109/TCSI.2022.3219555.

[9] A. Reezwana et al., "A quantum random number generator on a nanosatellite in low Earth orbit," Commun. Phys., vol. 5, no. 1, p. 314, Dec. 2022, doi: 10.1038/s42005-022-01096-7.

[10] M. Herrero-Collantes and J. C. García-Escartín, "Quantum random number generators," Rev. Mod. Phys., vol. 89, no. 1, p. 015004, Feb. 2017, doi: 10.1103/RevModPhys.89.015004.

[11] A. Kosari, "Real-Time Network Traffic Anomaly Detection Using Spiking Neural Networks (SNNs) with Adaptive Learning," Contrib. Sci. Technol. Eng., vol. 2, no. 2, pp. 17-22, May 2025, doi: 10.22080/cste.2025.28763.1016.

[12] A. Bellante, T. Fioravanti, M. Carminati, S. Zanero, and A. Luongo, "Evaluating the potential of quantum machine learning in cybersecurity: A case-study on PCA-based intrusion detection systems," Comput. Secur., vol. 154, p. 104341, Jul. 2025, doi: 10.1016/j.cose.2025.104341.

[13] A. Bellante, "Evaluating the Potential of Quantum Machine Learning in Cybersecurity: A Case-Study on PCA-based Intrusion Detection Systems," arXiv:2502.11173 [cs.CR], Feb. 2025.

[14] L. Eze, U. B. Chaudhry, and H. Jahankhani, "Quantum-Enhanced Machine Learning for Cybersecurity: Evaluating Malicious URL Detection," Electronics, vol. 14, no. 9, p. 1827, Apr. 2025, doi: 10.3390/electronics14091827.

[15] A. Bellante, "Evaluating the Potential of Quantum Machine Learning in Cybersecurity: A Case-Study on PCA-based Intrusion Detection Systems," arXiv:2502.11173 [cs.CR], Feb. 2025.

[16] A. Kumar and R. Sharma, "QuantumNetSec: Quantum Machine Learning for Network Security," Int. J. Netw. Manag., vol. 35, no. 4, p. e70018, Jul. 2025, doi: 10.1002/nem.70018.

[17] A. Awasthi, "The role of quantum machine learning in cybersecurity," Int. Res. J. Mod. Eng. Technol. Sci., vol. 7, no. 1, pp. 1-9, Jan. 2025, doi: 10.56726/IRJMETS66777.

[18] G. Bock, "AROBS Polska to Develop Post-Quantum Satellite Communication Security System," The Quantum Insider, Mar. 19, 2025. [Online]. Available: https://thequantuminsider.com/2025/03/19/arobs-polska-to-develop-post-quantum-satellite-communication-security-system/.

[19] A. Rani, "Combined Quantum and Post-Quantum Security for Earth-Satellite Channels," arXiv:2502.14240 [quant-ph], Feb. 2025.

[20] B. Zhang et al., "Practical attack on a quantum random-number generator via injection of source-signal fluctuations," Phys. Rev. Appl., vol. 24, no. 1, p. 014008, Jul. 2025, doi: 10.1103/k3c9-ngt1.

[21] A. Miller, "Study Finds Security Flaw in World's First Quantum Satellite," The Quantum Insider, Jun. 3, 2025. [Online]. Available: https://thequantuminsider.com/2025/06/03/study-finds-security-flaw-in-worlds-first-quantum-satellite/.

[22] Zhou K., Doyle J. C. and Glover K., *Robust and optimal control*, chapter 3, Englewood cliffs, NJ, USA: Prentice-Hall, 1996.

Biographies

Dr.Arash Kosari was born on 1981. He received the Ph.D. degree in computer engineering with a focus on network and quantum security from Belarusian State University of Informatics and Radioelectronics (BSUIR), Belarus, in 2016. He has more than 15 years of experience in the fields of information security, satellite communications security, and quantum technologies. He has been involved in national research programs on secure satellite networks, cyber-physical system security, and post-quantum cryptography. He is currently an Assistant Professor with the Iranian Research Organization for

Science and Technology (IROST), where he leads research projects on quantum communication security, satellite OBC subsystem, and AI-based threat detection for critical infrastructures. He has served as a technical reviewer for national cybersecurity programs and contributes to national working groups on secure quantum communication technologies and also security in different IT fields.

.

Instructions to Authors of Papers for the Iranian Journal of Electrical and Electronic Engineering (IJEEE)

1 Scope

The Iranian Journal of Electrical & Electronic Engineering (IJEEE) is a peer reviewed journal devoted to publish original papers of high technical standard with a suitable balance of practice and theory related to the broad topics in the field of electrical engineering. All topics are treated with similar emphasis, such as:

- Biomedical Engineering,
- Communication Engineering,
- Computer Engineering,
- Control Engineering,
- Electronic Engineering,
- Power Engineering.

2 Language

Papers should be written in English.

3 Typescript

The prospective authors should prepare two files for each manuscript; one with full author's information (name, Email address, postal address, affiliation and biography) and the other without any author's information. Manuscripts should be typed one-column, double-spaced; 12 point Times New Roman font and 2.5-cm margins in standard A4 paper (21 by 29.7 cm2). An abstract of 150-200 words should be included. Authors should supply about four key words or phrases that characterize their manuscript. The paper should be reasonably subdivided into sections and, if necessary, subsections. Manuscripts should not exceed 8 printed pages [approximately 16 double spaced A4 pages plus almost 14 illustrations]. The required format for the final version of the accepted papers may be obtained at ijeee.iust.ac.ir.

4 Illustrations

Illustrations enclosed when a paper is first submitted need not be suitable for reproduction, but they must be clear for the purpose of review. As much text as possible should be removed from illustrations, and any background line in graphs not be obscured.

5 References

Other publications referred to in the text should be indicated by a number. Details of the references should be given in a list at the end of the paper in order of citation. Each reference should include:

(a) Names of all the authors (i.e. not 'et al.'),
(b) Title of the paper,
(c) Full title of the journal,
(d) Year of publication and volume number,
(e) First and last page numbers.

For a book, the author, book title, publisher and year of the publication should be stated.

6 Submission

Authors are invited to submit the files of their manuscript via IJEEE on-line submission at ijeee.iust.ac.ir. A signed copyright transfer agreement and originality statement, downloaded at ijeee.iust.ac.ir, are needed. All submission and further tracking of submitted papers should be done through ijeee.iust.ac.ir.