Article

Not peer-reviewed version

Operational Threat Modeling of Adversarial Noise in Continuous-Variable Quantum Communication

José R. Rosas-Bustos *, Jesse Van Griensven Thé, Roydon Andrew Fraser, Nadeem Said, Sebastian Ratto Valderrama, Mark Pecen, Alexander Truskovsky, Andy Thanos

Posted Date: 30 January 2026

doi: 10.20944/preprints202601.2359.v1

Keywords: continuous-variable quantum communication; adversarial noise; operational threat modeling; physical-layer attacks; noise taxonomy; gaussian channels; finite-resolution estimation; estimator tolerances; energy deviation; covariance-matrix methods

Article

Operational Threat Modeling of Adversarial Noise in Continuous-Variable Quantum Communication

José R. Rosas-Bustos [1,2,3,4]*, Jesse Van Griensven Thé [1,2,3,4], Roydon Andrew Fraser [1,3,4], Nadeem Said [1,2,3], Sebastian Ratto Valderrama [3,4,5], Mark Pecen [3,4], Alexander Truskovsky [4] and Andy Thanos [6]

[1] Department of MME, University of Waterloo, Waterloo, ON N2L 3G1, Canada
[2] LAKES Environmental Research Inc., Waterloo, ON N2L 3L3, Canada
[3] Applied Quantum Technologies (AQT) Initiative, Columbia, MD 21046, USA
[4] EigenQ, Inc., Austin, TX 78701, USA
[5] Department of ECE, University of Waterloo, Waterloo, ON N2L 3G1, Canada
[6] Cisco Systems, Inc., San Jose, CA 95134, USA
* Correspondence: jrosasbu@uwaterloo.ca

Abstract

Recent work has shown that finite measurement resolution and estimator tolerances can create operational vulnerabilities in quantum integrity verification, enabling adversarial probing strategies that evade static detection criteria [1]. Building on these insights, we examine how analogous adversarial mechanisms arise in continuous-variable quantum communication (CVQC), where security and performance-critical decisions are made directly from finite-resolution phase-space measurements. We develop an operational threat-modeling framework that classifies adversarial interference in CVQC into three regimes: (i) low-amplitude reconnaissance noise engineered to remain within estimator tolerances, (ii) moderate exploratory noise designed to probe stability margins and system sensitivities, and (iii) high-intensity denial-of-service (DoS) interference intended to force operational failure. Using a receiver-centric Gaussian-channel representation, we characterize how each regime perturbs second-order quadrature statistics and induces systematic degradation of state coherence and purity. To quantify adversarial impact in an implementation-relevant manner, we introduce an energy-deviation metric derived from the trace of the covariance matrix, directly linking excess noise accumulation to estimator degradation and operational failure thresholds under finite-sample constraints. The resulting taxonomy and metric establish a structured foundation for analyzing physical-layer adversarial behavior in continuous-variable quantum communication.

Keywords: continuous-variable quantum communication; adversarial noise; operational threat modeling; physical-layer attacks; noise taxonomy; gaussian channels; finite-resolution estimation; estimator tolerances; energy deviation; covariance-matrix methods

1. Introduction

Recent advances in quantum communication have made increasingly clear that security and integrity are shaped not only by idealized theoretical guarantees, but also by operational constraints such as finite measurement resolution, estimator tolerances, and hardware-imposed control limits. In particular, our prior work demonstrated that finite-resolution measurements can induce regions of *operational indistinguishability*, termed *convergence vicinities*, in which distinct physical models become experimentally indistinguishable without violating Bell's theorem itself [1]. That analysis revealed a class of vulnerabilities in quantum integrity verification frameworks that rely on static thresholds or idealized measurement assumptions.

The present work extends this operational perspective to *continuous-variable quantum communication* (CVQC), where estimator tolerances manifest directly in phase-space quadrature statistics inferred

 doi:10.20944/preprints202601.2359.v1

from finite-resolution measurements. While Ref. [1] focused on discrete-variable integrity verification, CVQC systems introduce a qualitatively different attack surface: security- and performance-critical decisions are made directly from continuous-valued estimators, such as quadrature variances and covariance matrices, which are inherently subject to finite-sample uncertainty.

In CVQC systems, quantum information is encoded in the canonical quadratures of optical modes and accessed experimentally via homodyne or heterodyne detection. Rather than treating noise exclusively as an uncontrolled environmental process, we consider *adversarial noise*: intentional, structured disturbances designed to exploit estimator tolerances, probe system stability, or disrupt communication. Such interference need not appear as anomalously large fluctuations; instead, it may be engineered to remain within nominal operating margins while gradually biasing parameter estimation, degrading coherence, or undermining operational assumptions.

CVQC plays a central role in quantum communication and networking due to its compatibility with existing optical infrastructure and its scalability [2–4]. At the same time, CVQC implementations are known to be sensitive to excess noise, phase instability, and detector limitations, which can compromise inferred channel parameters and communication reliability, particularly under finite-size parameter-estimation constraints [2,5–9]. These sensitivities define a physical-layer attack surface in which adversarial disturbances can be shaped to interact with finite-resolution estimation and acceptance criteria [10,11].

In this work, we classify adversarial interference in CVQC into three operational regimes. *Reconnaissance noise* consists of low-amplitude perturbations engineered to remain within estimator tolerances while extracting information about system parameters, directly analogous to convergence-vicinity exploitation in discrete-variable systems [1]. *Exploratory noise* introduces moderate, structured disturbances intended to probe stability margins and reveal directional sensitivities in phase space. Finally, *denial-of-service (DoS) noise* corresponds to high-intensity interference that overwhelms estimation and control capabilities, forcing operational failure. Throughout this work, covariance matrices are expressed in units where the vacuum variance is normalized to unity, and proportionality constants relating energy and covariance trace are omitted for clarity.

To analyze these regimes in an implementation-relevant manner, we adopt a receiver-centric modeling perspective based on Gaussian channels acting on phase-space quadratures. Within this framework, we characterize how adversarial noise perturbs second-order quadrature moments and induces systematic degradation of state coherence and purity. We introduce an *energy-deviation* metric derived from the trace of the covariance matrix, providing a compact and experimentally accessible scalar observable that links adversarial disturbances to estimator degradation and operational failure thresholds under finite-sample constraints.

This manuscript is intentionally scoped to *operational threat modeling*. Accordingly, we do not propose or validate mitigation, control, or adaptive response mechanisms. Questions of how to detect, estimate, or actively counter adversarial perturbations through feedback, modulation, or protocol adaptation are deferred to future work, where defensive strategies can be evaluated against the threat regimes and observables defined here.

Specifically, this work makes three contributions: (i) it formalizes a taxonomy of adversarial noise regimes in CVQC grounded in operational intent and estimator visibility; (ii) it develops a Gaussian-channel modeling framework that captures adversarial interference at the level of receiver-accessible covariance statistics without assumptions about adversary capabilities; and (iii) it introduces an energy-deviation metric and finite-sample detectability analysis that connect excess noise accumulation to estimator tolerances and operational failure boundaries. Together, these results establish a structured, receiver-centric foundation for analyzing physical-layer adversarial behavior in continuous-variable quantum communication.

 doi:10.20944/preprints202601.2359.v1

2. Related Work and Gap Statement

2.1. Continuous-Variable Quantum Communication and Parameter Estimation

Continuous-variable quantum communication (CVQC) protocols encode information in the amplitude and phase quadratures of optical modes and rely on statistical inference over continuous measurement outcomes to establish correctness, performance, and, where applicable, security. Homodyne and heterodyne detection schemes provide direct access to quadrature observables, making CVQC naturally compatible with Gaussian-state modeling and covariance-matrix descriptions [2,12].

A central component of CVQC operation is *parameter estimation*. Practical implementations infer quantities such as channel loss, excess noise, quadrature variances, and covariance structure from finite ensembles of measurement outcomes. These estimates underpin protocol decisions, including acceptance or abort conditions in quantum key distribution, calibration and stability assessment in quantum networking, and performance evaluation in sensing and verification tasks [2,9]. As a result, the reliability of CVQC systems is fundamentally tied to the statistical properties of these estimators, particularly under finite-size constraints where confidence regions and acceptance thresholds must be defined explicitly [5–7].

Existing analyses of parameter estimation in CVQC typically focus on environmental and device-induced noise sources, including thermal noise, detector inefficiency, phase drift, and loss [8,12]. Within this framework, excess noise is often treated as a stationary or weakly time-varying stochastic process, and security or performance guarantees are derived under assumptions of well-characterized noise statistics and asymptotic or large-sample limits.

However, in realistic operating conditions, parameter estimation is constrained by finite measurement resolution, finite sample sizes, and implementation-specific acceptance margins. These constraints introduce *estimator tolerances*: bounded regions in parameter space within which observed statistics are deemed consistent with nominal operation. While such tolerances are necessary for practical operation, they also create regions of operational indistinguishability, where distinct underlying disturbances produce statistically indistinguishable measurement outcomes over finite observation windows.

Recent work in discrete-variable quantum integrity verification has shown that finite-resolution effects can be systematically exploited by adversarial probing strategies that remain within estimator tolerances while biasing inferred parameters [1]. In continuous-variable systems, where security- and performance-critical decisions are made directly from continuous-valued estimators, analogous vulnerabilities can arise at the level of phase-space statistics. Nevertheless, existing CVQC literature has largely treated parameter estimation as a passive inference problem rather than as a potential attack surface shaped by estimator design and tolerance thresholds.

This gap motivates a receiver-centric, operational examination of parameter estimation in CVQC under adversarial conditions. Rather than assuming noise to be purely environmental or benign, the present work considers how structured disturbances interact with finite-resolution estimation procedures and how their impact manifests in experimentally accessible covariance statistics. This perspective reframes parameter estimation not only as a tool for system characterization, but also as a potential locus of adversarial exploitation in continuous-variable quantum communication.

2.2. Implementation Constraints: Finite Resolution, Finite Samples, and Acceptance Regions

Practical continuous-variable quantum communication (CVQC) systems operate under unavoidable implementation constraints that shape how quantum states and channels are characterized in practice. Chief among these constraints are finite measurement resolution, finite sample sizes, and the use of predefined acceptance regions for parameter estimation. Together, these factors determine the operational limits of inference and play a central role in how noise, benign or adversarial, manifests in experimentally accessible statistics.

Finite measurement resolution arises from detector noise, electronic bandwidth limitations, digitization, and coarse-graining of continuous outcomes. Homodyne and heterodyne measurements

 doi:10.20944/preprints202601.2359.v1

therefore yield discretized quadrature samples with nonzero uncertainty, even under idealized state preparation. As a result, small perturbations to underlying quadrature distributions may be indistinguishable from measurement-induced fluctuations, particularly over limited observation windows [9,12].

Finite sample sizes further constrain parameter estimation. In operational settings, covariance matrices and excess-noise parameters are inferred from a limited number of measurement outcomes, leading to statistical uncertainty that scales inversely with the number of samples. Confidence intervals and hypothesis tests used in protocol verification must therefore accommodate estimator variance, introducing tolerance margins that grow as sample sizes decrease or noise levels increase. These finite-size effects and confidence-region constructions are well established in continuous-variable quantum key distribution and related CV platforms [5,6,13]. These effects are well understood in benign noise models but become critical when disturbances are structured or non-stationary.

To ensure reliable operation, CVQC implementations define *acceptance regions* for estimated parameters, within which observed statistics are deemed consistent with nominal behavior. These regions may be specified explicitly, as in security margins for quantum key distribution, or implicitly, through calibration thresholds and performance criteria in communication and networking applications. Acceptance regions are thus an integral part of system design, translating statistical uncertainty into operational decision rules.

While acceptance regions are necessary for practical operation, they also define regions of operational indistinguishability. Distinct physical disturbances that induce parameter shifts smaller than estimator tolerances cannot be reliably discriminated by the receiver, even if they are systematic or adversarial in origin. This phenomenon has been identified in discrete-variable integrity verification as a source of exploitable structure under finite-resolution measurements [1]. In continuous-variable systems, where decisions are made directly from continuous-valued estimators, analogous indistinguishability arises naturally from finite resolution and finite data.

Existing CVQC analyses typically treat these implementation constraints as technical limitations to be mitigated through longer integration times or improved hardware. In contrast, the present work treats finite resolution, finite samples, and acceptance regions as defining features of the operational threat landscape. By explicitly incorporating these constraints into the characterization of adversarial noise, we expose how estimator tolerances shape the boundary between detectable and operationally invisible disturbances in continuous-variable quantum communication.

2.3. Physical-Layer Adversaries in Optical/CV Links: Excess Noise, Phase Perturbations, and Jamming

Physical-layer adversaries targeting optical and continuous-variable (CV) communication links have been studied primarily in the context of excess noise, phase instability, and optical jamming. In much of the existing literature, such disturbances are modeled as environmental or technical imperfections, including thermal noise, laser phase noise, imperfect synchronization, and channel loss fluctuations. These effects are typically assumed to be stationary or weakly time varying, and mitigation strategies focus on calibration, stabilization, and post-processing [2,12].

Excess noise is a central performance-limiting factor in CVQC, particularly in continuous-variable quantum key distribution (CV-QKD), where security thresholds are defined in terms of tolerable noise above the shot-noise limit [14]. Prior work has extensively analyzed how excess noise degrades key rates, limits transmission distance, and constrains security margins. However, excess noise is most often treated as an aggregate parameter arising from uncontrolled environmental processes or imperfect components, rather than as a deliberately structured disturbance shaped to exploit estimator tolerances.

Phase perturbations constitute another well-studied class of physical-layer effects in optical links. Phase noise can arise from laser linewidth, fiber fluctuations, or reference-frame misalignment, and has motivated a large body of work on phase tracking, compensation, and synchronization [15]. These studies typically assume benign drift or stochastic fluctuations and aim to restore a fixed or slowly

 doi:10.20944/preprints202601.2359.v1

varying phase reference. The possibility that phase perturbations may be intentionally structured, timed, or biased to probe system sensitivities or estimator robustness is rarely addressed explicitly.

Optical jamming and denial-of-service–like interference have also been considered in classical and quantum optical communication, particularly in free-space or shared-fiber scenarios [11]. In quantum settings, such interference is generally associated with overt disruption, detector saturation, or protocol abort conditions. As a result, jamming is often treated as an easily detectable failure mode rather than as part of a broader continuum of adversarial behavior that includes stealthy or sub-threshold interference.

A growing body of work has further highlighted that optical and CV quantum links are susceptible to explicitly *implementation-level physical-layer attacks*, including detector saturation, local-oscillator (LO) manipulation, wavelength-dependent jamming, and calibration-dependent exploits that bypass idealized security assumptions while remaining compatible with nominal parameter estimates [7,11]. These studies emphasize that adversarial control over physical-layer degrees of freedom can directly translate into estimator bias, parameter mischaracterization, or forced protocol behavior without violating abstract protocol models.

Across these bodies of work, a common implicit assumption is that physical-layer disturbances can be categorized either as benign noise to be estimated and compensated, or as catastrophic interference that immediately invalidates operation. This dichotomy obscures intermediate regimes in which disturbances are intentionally shaped to remain within accepted operating margins while extracting information, biasing inference, or mapping system robustness. Moreover, prior analyses seldom connect physical-layer perturbations directly to estimator tolerances and acceptance regions that govern operational decisions at the receiver.

The present work departs from this perspective by treating excess noise, phase perturbations, and jamming as manifestations of a broader class of adversarial interference at the physical layer. Rather than classifying disturbances solely by physical mechanism, we organize them by operational intent and by their impact on receiver-side observables relative to estimator tolerances. This receiver-centric viewpoint enables a unified treatment of stealthy probing, stress-inducing perturbations, and overt disruption within a single operational threat-modeling framework for continuous-variable quantum communication.

To situate the proposed regime taxonomy within the broader landscape of physical-layer security research, it is useful to relate the operational regimes defined here to well-known classes of implementation-level disturbances studied in optical and continuous-variable systems. Importantly, this mapping is not intended to propose, analyze, or validate specific attack implementations. Rather, it provides an interpretive bridge between mechanism-agnostic adversarial regimes, defined solely by their receiver-observable impact relative to estimator tolerances, and representative families of physical-layer interference discussed in the literature.

The associations in Table 1 should be interpreted strictly at the level of *receiver-observable effects*. Multiple physical mechanisms may map to the same effective disturbance in estimator space, and a single physical-layer technique may realize different adversarial regimes depending on amplitude, timing, and interaction with finite-sample tolerances. Accordingly, regime classification in this work is determined by statistical visibility and operational consequence at the receiver, not by assumptions about attacker hardware, access, or intent. This receiver-centric abstraction allows disparate physical-layer phenomena to be analyzed within a single operational framework, while remaining agnostic to specific exploitation pathways or device-level vulnerabilities.

 doi:10.20944/preprints202601.2359.v1

Table 1. Mechanism-agnostic adversarial regimes mapped to representative physical-layer attack families in optical/CV links. The mapping is receiver-centric and illustrative: it links each family to its dominant observable effect (effective (G, N) in Eq. (1)) and to the operational regime taxonomy, without assuming specific adversary implementations. Representative discussions of these attack families can be found in [7,11].

Attack family	Typical regime(s)	Receiver-observable signature	Notes / scope
LO manipulation / calibration bias	Recon / Exploratory	Shifted shot-noise unit or gain calibration; biased reference covariance or rescaled $\hat{V}$ (effective change in G or trusted normalization).	Treated as an estimation-layer effect; exploits reference-setting rather than explicit signal disturbance.
Phase-reference perturbation / pilot interference	Exploratory / DoS	Phase-space rotation/mixing; growth of off-diagonal covariance $\hat{V}_{xp}$; phase-dependent variance inflation.	Most visible under imperfect phase tracking; appears as ellipse rotation and anisotropy (Fig. 3).
Non-stationary excess-noise injection	Recon / Exploratory	Per-window sub-threshold variance with long-horizon drift in $\Delta E(t)$ or $\mathrm{Tr}(\hat{V})$ (time-varying N).	Motivates cumulative monitoring (Fig. 4); regime depends on amplitude and windowing.
Detector saturation / blinding-like effects	DoS	Nonlinear response, clipping, estimator failure; unreliable or non-Gaussian covariance estimates.	Included as a receiver-interface failure mode; covariance captures net inflation but not detailed nonlinearities.
Broadband optical jamming	Exploratory / DoS	Rapid variance growth and elevated noise floor; unstable parameter estimation (large, possibly time-varying N).	Operational classification depends on how far ΔE exceeds tolerance limits.

2.4. Gap and Contributions

Despite extensive study of noise, loss, and imperfections in continuous-variable quantum communication (CVQC), a clear gap remains in how physical-layer disturbances are conceptualized and analyzed from an adversarial perspective. Existing work predominantly treats excess noise, phase instability, and jamming either as benign environmental effects to be estimated and compensated, or as catastrophic failures that immediately invalidate operation. This framing overlooks a broad intermediate regime in which disturbances are deliberately structured to exploit finite measurement resolution, finite sample sizes, and estimator tolerances without necessarily triggering protocol aborts or anomaly flags.

Relative to our prior work on discrete-variable integrity verification and convergence vicinities [1], the present study extends the notion of operational indistinguishability to continuous-variable systems by: (i) translating indistinguishability from outcome statistics to covariance and estimator space in CVQC; (ii) defining adversarial regime boundaries explicitly in terms of receiver-side tolerances and acceptance regions; and (iii) introducing an energy-deviation observable together with a finite-sample detectability analysis that quantifies regime transitions under realistic estimation constraints.

In particular, prior analyses rarely formalize how receiver-side acceptance regions and confidence thresholds shape what constitutes an operationally detectable disturbance. As a result, there is limited

 doi:10.20944/preprints202601.2359.v1

theoretical machinery for reasoning about stealthy probing, gradual parameter biasing, or adversarial stress-testing at the physical layer of CVQC systems. Moreover, while security and robustness are often discussed at the protocol or information-theoretic level, there is a lack of receiver-centric threat models that directly connect physical-layer interference to experimentally accessible observables such as covariance matrices and inferred energy.

This work addresses these gaps by introducing an explicitly operational threat-modeling framework for adversarial noise in CVQC. The central contributions are threefold. First, we formalize a taxonomy of adversarial noise regimes, reconnaissance, exploratory, and denial-of-service, distinguished by adversarial intent and by their observable impact relative to estimator tolerances rather than by assumed physical mechanisms. Second, we develop a Gaussian-channel modeling approach that captures adversarial interference at the level of receiver-accessible phase-space statistics, avoiding assumptions about the adversary's internal capabilities or resources. Third, we introduce an energy-deviation metric derived from the trace of the covariance matrix, providing a compact, protocol-agnostic, and experimentally compatible scalar measure that links excess noise accumulation to estimator degradation and operational failure thresholds.

Together, these contributions establish a structured foundation for analyzing physical-layer attack surfaces in continuous-variable quantum communication. By shifting the focus from idealized noise models to receiver-observable effects under finite resolution and finite data, the framework enables systematic reasoning about how benign-appearing perturbations can escalate into destabilizing interference. This perspective complements existing security and robustness analyses and sets the stage for subsequent work on detection, mitigation, and adaptive control strategies grounded in operational observables.

3. Adversarial Noise Modelling

From a cybersecurity perspective, adversarial noise in CVQC constitutes a physical-layer attack surface, where structured perturbations exploit estimator tolerances, control assumptions, and finite-resolution effects rather than protocol-level logic.

In continuous-variable (CV) quantum systems, quantum information is encoded in the canonical quadratures $\hat{x}$ and $\hat{p}$ of optical modes. These quadratures fully characterize Gaussian quantum states and form the operational foundation of CVQC systems and devices [12]. As a result, performance- and integrity-relevant information in CVQC is inferred directly from finite-resolution measurements of phase-space observables.

In this work, we define *adversarial noise* as intentionally engineered perturbations applied to phase-space quadratures with the objective of probing system parameters, exploiting estimator tolerances, or disrupting communication. This definition contrasts with environmental noise, which arises from uncontrolled physical processes and is typically modeled as stationary or weakly varying. Adversarial noise is instead structured, may be adaptive, and is informed by the system's observable behavior and response.

At an operational level, adversarial noise is modeled as an effective Gaussian channel acting on the phase-space vector $\hat{\mathbf{r}} = (\hat{x}, \hat{p})^{\mathsf{T}}$:

$$\hat{\mathbf{r}}' = G\hat{\mathbf{r}} + \boldsymbol{\xi}, \tag{1}$$

where G is a real linear transformation on phase space representing deterministic effects such as attenuation, amplification, rotation, or effective squeezing as inferred from receiver-accessible observables, and $\boldsymbol{\xi}$ is a classical random vector drawn from a zero-mean Gaussian distribution with covariance matrix N. This representation should be understood as a phenomenological description of the observable impact of adversarial interference at the receiver, rather than as a claim about the physical implementation or capabilities of the adversary. In particular, G is not assumed to correspond to a physically realized or symplectic operation, and the model does not assume that the adversary performs coherent quantum operations, implements symplectic control, or possesses quantum-level access to the channel.

 doi:10.20944/preprints202601.2359.v1

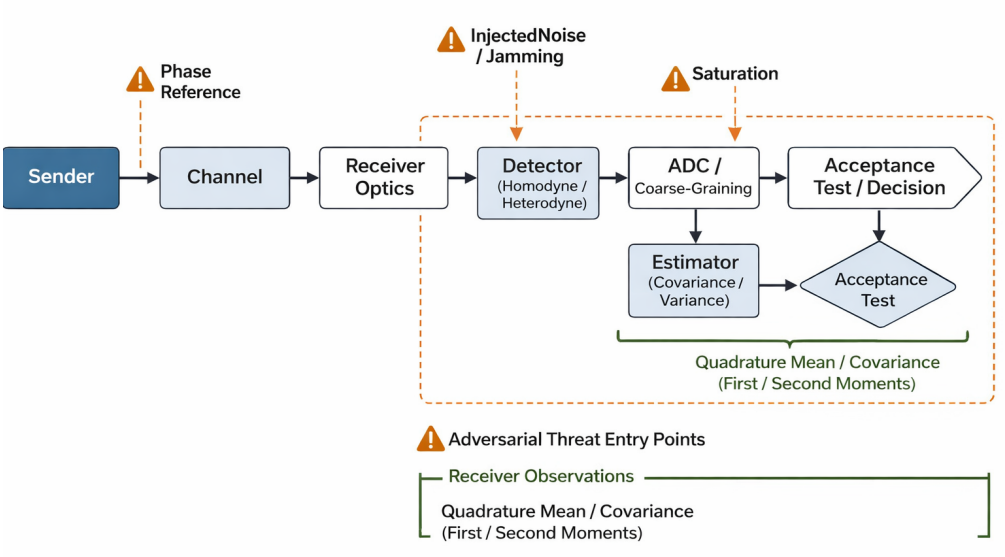

Figure 1. Receiver-centric operational threat surface for continuous-variable quantum communication. Adversarial actions can enter at multiple physical-layer points (e.g., phase reference manipulation, injected noise/jamming, detector/ADC saturation), while the receiver's decision logic is based on finite-resolution measurements and estimators of first- and second-order quadrature moments (mean/covariance). This diagram provides an operational interpretation of the effective Gaussian-channel model in Eq. (1).

In this receiver-centric view, the parameters (G, N) summarize the net observable impact of upstream disturbances on the statistics used by the receiver's estimator and acceptance test.

Distinct adversarial strategies correspond to different effective choices of G and N, reflecting both the intensity and operational intent of the interference. Throughout this work, adversarial noise is therefore treated as an operationally defined disturbance characterized solely by its receiver-side statistical signatures, independent of assumptions about the adversary's underlying physical resources or attack mechanism.

3.1. Receiver Observables and Estimator Tolerances

The operational impact of adversarial noise in continuous-variable quantum communication is determined not only by the physical disturbance applied to the channel, but by how that disturbance manifests in *receiver-accessible observables*. In practice, integrity assessment, calibration, and performance verification in CVQC rely on finite-sample estimates of quadrature moments derived from homodyne or heterodyne measurements with limited resolution and detector noise.

At the receiver, experimentally accessible information is typically restricted to first- and second-order moments of the quadratures, summarized by the estimated mean vector and covariance matrix. These estimates are subject to statistical uncertainty arising from finite data acquisition, detector inefficiencies, and coarse-graining effects. As a result, any verification or monitoring procedure implicitly defines *estimator tolerances*: bounded regions in parameter space within which observed statistics are deemed consistent with nominal operation.

Adversarial noise exploits these tolerances by shaping perturbations so that their induced changes in observable statistics remain within accepted confidence intervals, at least over limited observation windows. In this sense, the adversary interacts not with the ideal quantum state itself, but with the receiver's statistical inference layer. This perspective mirrors the convergence-vicinity concept introduced in discrete-variable integrity verification, where finite resolution renders distinct underlying models operationally indistinguishable.

Formally, let $\hat{V}$ denote the estimated covariance matrix obtained from a finite ensemble of measurements. Acceptance regions for nominal operation can be represented as

$$\|\hat{V} - V_{\text{ref}}\| \leq \delta_V, \tag{2}$$

 doi:10.20944/preprints202601.2359.v1

where V_{ref} is a reference covariance matrix and the norm may be interpreted operationally as a chosen matrix norm (e.g., the Frobenius norm) or, equivalently, as a set of elementwise confidence bounds on the estimated covariance entries. The tolerance δ_V is determined by finite sample size, measurement resolution, and the receiver's false-alarm or confidence-level design. Adversarial perturbations that induce changes smaller than δ_V are operationally invisible, even if they introduce systematic bias or accumulate deleterious effects over time.

This receiver-centric viewpoint motivates the modeling choices adopted throughout this work. Rather than characterizing adversarial noise by its physical origin or implementation, we classify it by its observable impact relative to estimator tolerances. Reconnaissance, exploratory, and denial-of-service noise regimes can then be distinguished by how their induced covariance distortions relate to these acceptance regions, providing a unified operational basis for adversarial threat modeling in CVQC.

Within this framework, we classify adversarial noise in CVQC into three operational categories: *reconnaissance noise*, *exploratory noise*, and *denial-of-service (DoS) noise*. These categories are distinguished not only by noise intensity, but by adversarial intent and by their characteristic impact on phase-space statistics, estimator reliability, and operational stability.

In later sections, we use τ as a scalar analogue of δ_V for variance-based monitoring, and δ_{est} as a generic tolerance scale when the specific estimator is not explicitly specified.

3.2. Summary of Adversarial Regimes

For clarity and implementation relevance, Table 2 summarizes the three adversarial-noise regimes considered in this work in terms of (i) operational intent, (ii) characteristic noise intensity relative to estimator tolerances, (iii) dominant observable signatures in receiver-side quadrature statistics, and (iv) expected operational consequence for continuous-variable quantum communication (CVQC). This summary emphasizes that the regimes are defined operationally by how disturbances manifest in experimentally accessible observables, rather than by assumptions about the adversary's physical resources or internal attack mechanism.

These regime boundaries should be interpreted as *receiver-defined surfaces in estimator space*, determined by measurement resolution, sample size, estimator design, and acceptance criteria, rather than as intrinsic thresholds of the underlying physical disturbance. Accordingly, the regime boundaries in Table 2 are operational rather than absolute: the same physical perturbation may transition between regimes depending on device characteristics, finite-sample uncertainty, and application-specific failure thresholds. This perspective motivates the use of receiver-side covariance statistics, and in particular the energy-deviation metric introduced in Sec. 3, as a protocol-agnostic means of quantifying proximity to tolerance and failure boundaries.

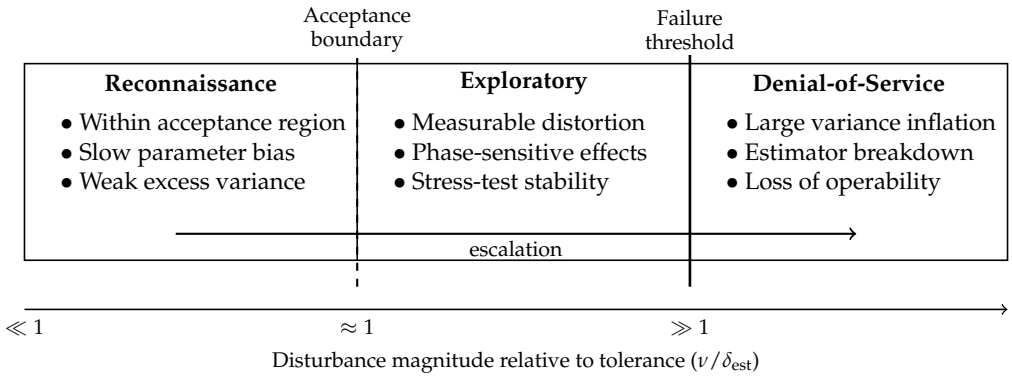

Figure 2. Adversarial regime ladder versus tolerance ratio and receiver-observable signatures. Regimes are distinguished operationally by the magnitude of disturbance relative to estimator tolerances (e.g., ν/δ_{est}), transitioning from acceptance-region stealth (reconnaissance) to measurable stress (exploratory) and ultimately to failure beyond operational thresholds (DoS).

 doi:10.20944/preprints202601.2359.v1

Table 2. Operational summary of adversarial-noise regimes in CVQC. Regimes are distinguished by adversarial intent and by their characteristic impact on receiver-side quadrature statistics and estimator reliability.

Regime	Operational intent	Intensity relative to tolerances	Dominant observable signatures	Operational consequence
Reconnaissance noise	Stealthy probing and gradual biasing of inferred parameters	Below acceptance margins and estimator confidence intervals	Subtle excess variance; slow parameter drift; long-horizon detectability	Biased estimation and covert information leakage
Exploratory noise	Stress-testing to reveal sensitivities, nonlinearities, and stability margins	Above nominal environmental levels, but below disruption thresholds	Anisotropic covariance distortion; phase-dependent statistics; instability precursors	Identification of fragile operating regimes
Denial-of-service (DoS) noise	Rapid disruption and forced operational failure	Far above tolerances; exceeds device/protocol operating limits	Rapid variance inflation; strong phase diffusion; purity collapse	Estimator failure and loss of communication/verification

3.3. Illustrative Example: Quadrature-Biased Excess Noise

To illustrate how the adversarial regimes defined above manifest in experimentally accessible observables, we consider a representative example of *quadrature-biased excess noise*. This example is not intended to model a specific attack implementation, but rather to demonstrate how structured disturbances project onto phase-space statistics and how their operational impact depends on noise intensity and estimator tolerances.

Figure 3 provides a phase-space visualization of the regime taxonomy using covariance ellipses (equivalently, Wigner-function contours) together with the associated energy-deviation scale $\Delta E \propto \mathrm{Tr}(V') - \mathrm{Tr}(V_0)$. The tolerance level δ_e denotes a receiver-defined energy-deviation margin (a scalar analogue of the covariance tolerance δ_V), derived from the receiver's finite-sample acceptance rule (e.g., Eq. (27) and the associated confidence level) and any additional resolution/calibration uncertainty. Under this interpretation, regime transitions correspond to changes in the statistical visibility of covariance distortions relative to δ_e, rather than changes in physical mechanism.

We consider a single-mode Gaussian state with covariance matrix

$$V_0 = \begin{pmatrix} \sigma_x^2 & 0 \\ 0 & \sigma_p^2 \end{pmatrix}, \tag{3}$$

where $\sigma_x^2 = \sigma_p^2 = 1$ for the vacuum reference state. Adversarial interference is modeled as additive excess noise injected preferentially along the momentum-like quadrature,

$$V' = \begin{pmatrix} \sigma_x^2 & 0 \\ 0 & \sigma_p^2 + \nu \end{pmatrix}, \tag{4}$$

with $\nu \geq 0$ denoting the magnitude of the quadrature-biased disturbance.

 doi:10.20944/preprints202601.2359.v1

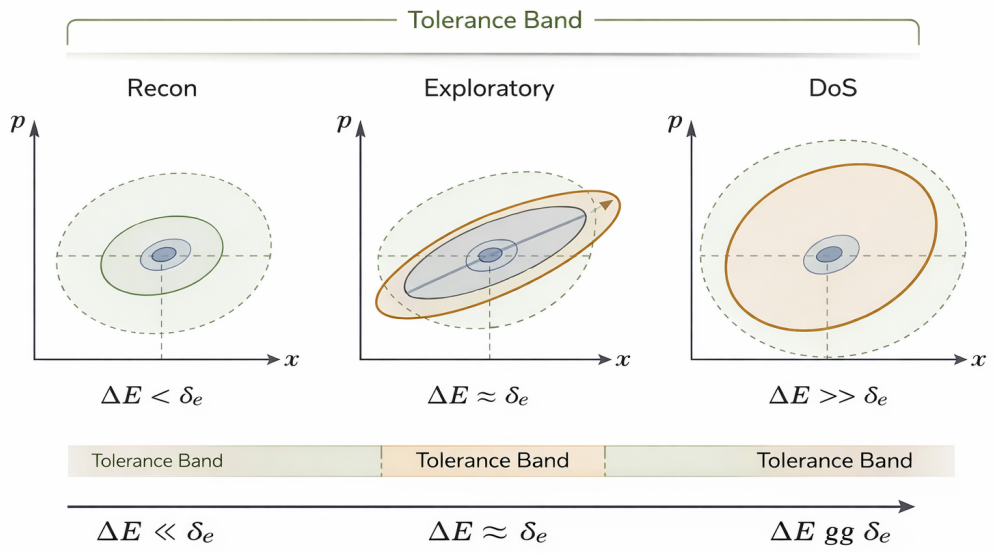

Figure 3. Phase-space covariance ellipses (Wigner-like contours) illustrating how adversarial regimes manifest in receiver-accessible second-order statistics. Reconnaissance perturbations remain within the estimator tolerance band and produce only a small energy deviation ($\Delta E < \delta_e$). Exploratory perturbations introduce anisotropic distortion and rotation (quadrature-biased excess noise plus phase-space mixing), yielding $\Delta E \approx \delta_e$ near the detectability boundary. Denial-of-service (DoS) perturbations cause large (near-isotropic) variance inflation and push $\Delta E \gg \delta_e$, consistent with estimator breakdown and operational failure.

Reconnaissance regime.

When ν is chosen such that $\nu \ll \delta_{\text{est}}$, where δ_{est} denotes the effective estimator tolerance imposed by finite sample size and detector resolution, the induced change in covariance remains within accepted confidence intervals. At this level, the energy deviation

$$\Delta E \propto \mathrm{Tr}(V') - \mathrm{Tr}(V_0), \qquad \mathrm{Tr}(V') - \mathrm{Tr}(V_0) = \nu. \tag{5}$$

is statistically indistinguishable from benign fluctuations on short timescales. Nevertheless, repeated application of such perturbations can bias inferred channel parameters, enabling adversarial probing without triggering static anomaly-detection criteria.

Exploratory regime.

For intermediate values of ν, comparable to but not overwhelmingly exceeding estimator tolerances, the covariance matrix becomes measurably anisotropic. Observable consequences include elongation of the Wigner function along the p-quadrature and increased sensitivity to phase-space orientation. In this regime, phase-space rotations redistribute the excess variance between measured quadratures, producing phase-dependent changes in observed energy deviation and estimator performance. Such behavior reveals directional sensitivities and proximity to stability boundaries while preserving overall operability.

Denial-of-service regime.

When ν is increased such that $\nu \gg \delta_{\text{est}}$ and exceeds device- or protocol-level operating limits, the excess variance dominates the covariance structure. The resulting energy deviation grows rapidly, state purity collapses, and quadrature statistics become incompatible with reliable parameter estimation or communication. In this regime, the biased-noise example transitions into denial-of-service interference, where functional breakdown occurs irrespective of phase-space orientation.

 doi:10.20944/preprints202601.2359.v1

This simplified example highlights three key points. First, the same structured disturbance can realize different adversarial regimes depending solely on its magnitude relative to estimator tolerances and operational thresholds. Second, quadrature bias naturally induces phase-space anisotropy, making observable degradation strongly orientation dependent in the exploratory regime. Third, receiver-side covariance statistics, and in particular the energy-deviation metric, provide a unifying operational lens for diagnosing adversarial impact without requiring assumptions about the adversary's physical capabilities.

3.4. Reconnaissance Noise

Reconnaissance noise consists of low-amplitude perturbations deliberately engineered to remain within estimator tolerances while extracting information about system parameters over time. This adversarial regime is characterized not by large fluctuations, but by *stealth*: the adversary seeks to avoid triggering integrity checks or anomaly-detection mechanisms while accumulating statistically meaningful information across repeated observations.

In continuous-variable systems, reconnaissance noise is well modeled as additive Gaussian excess noise with small variance:

$$\hat{x}' = \hat{x} + \epsilon_x, \quad \hat{p}' = \hat{p} + \epsilon_p, \tag{6}$$

where $\epsilon_x, \epsilon_p \sim \mathcal{N}(0, \sigma^2_{\text{recon}})$ and σ^2_{recon} is chosen to lie below detection thresholds imposed by finite measurement resolution and parameter-estimation uncertainty. At the level of individual measurements, such perturbations are experimentally indistinguishable from weak environmental noise. However, when applied persistently, they can introduce systematic bias into inferred system parameters.

This attack mechanism directly parallels the vulnerability identified in our prior work on quantum integrity verification, where finite-resolution measurements give rise to *convergence vicinities*, regions of operational indistinguishability in which classical and quantum statistical predictions coincide within experimental tolerance [1]. In the continuous-variable setting, reconnaissance noise exploits analogous estimator tolerances in phase-space measurements, enabling adversarial probing to proceed undetected so long as the induced excess noise remains within accepted confidence intervals.

Reconnaissance noise in CVQC can therefore be understood as the continuous-variable analogue of convergence-vicinity exploitation identified in discrete-variable integrity verification [1].

3.4.1. Implications for Quantum Communication Protocols and Devices

In practical continuous-variable quantum communication protocols and quantum devices, integrity and performance verification rely on parameter estimation performed with finite sample sizes, finite detector resolution, and predefined acceptance margins for noise, loss, or calibration error. Reconnaissance noise leverages these operational constraints by introducing small, structured perturbations that do not immediately violate acceptance criteria, yet gradually bias inferred system parameters.

These effects arise at the implementation level and do not contradict formal security, verification, or correctness guarantees, but instead undermine the assumptions under which parameter estimation faithfully reflects device or channel behavior. Small excess-noise contributions introduced within accepted confidence intervals may accumulate over time, shifting estimated operating points without triggering alarms or fault conditions.

Crucially, this vulnerability does not reflect a failure of quantum mechanics or abstract protocol guarantees, but rather the practical limitations of real-world implementations. As demonstrated in the discrete-variable context in [1], verification frameworks based on static thresholds can fail to detect adversarial behavior that is carefully engineered to remain within acceptable bounds. In continuous-variable quantum communication systems and devices, reconnaissance noise can similarly bias calibration, stability assessment, or performance metrics while remaining operationally invisible.

 doi:10.20944/preprints202601.2359.v1

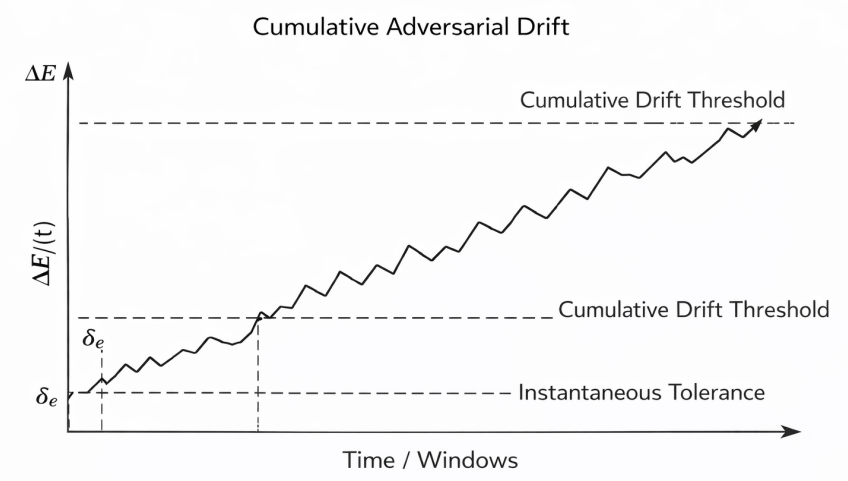

Figure 4. Illustration of cumulative adversarial drift under repeated sub-threshold perturbations. Each monitoring window remains within an instantaneous acceptance tolerance (dashed line at δ_e), so short-term tests may accept operation. However, the accumulated energy deviation $\Delta E(t)$ can drift upward across windows and eventually exceed a long-horizon drift threshold (upper dashed line), indicating delayed detectability and/or parameter bias despite per-window acceptance.

Figure 4 emphasizes that reconnaissance noise can be operationally stealthy even when individual perturbations remain below the instantaneous tolerance δ_e over short monitoring windows. In this regime, $\Delta E(t)$ may exhibit gradual upward drift due to repeated sub-threshold injections, causing delayed detection only when a cumulative threshold (or a long-horizon alarm criterion) is exceeded. This captures the practical distinction between *per-window acceptability* and *long-term estimator bias*: the receiver may repeatedly accept nominal behavior while the inferred operating point shifts over time.

Related long-horizon excess-noise accumulation effects under finite-size monitoring have been discussed in the context of CV-QKD parameter estimation and excess-noise tracking [6,7].

3.5. Exploratory Noise

Exploratory noise corresponds to moderate, structured perturbations intended to probe the stability limits of a quantum communication system. Unlike reconnaissance noise, which is engineered to remain strictly below detection thresholds, exploratory noise is designed to induce measurable, yet non-catastrophic, deviations in system behavior. The adversary's objective at this stage is not immediate disruption, but rather to observe how the system responds to controlled stress, thereby identifying sensitivities, nonlinearities, and potential failure modes. Operationally, exploratory noise forms part of an attacker learning loop, in which injected perturbations are correlated with observable system responses to infer stability margins and response characteristics.

In continuous-variable systems, exploratory noise can be modeled operationally as a Gaussian channel combining moderate excess noise with phase-space distortion. At the level of quadrature operators, this is expressed as

$$\hat{\mathbf{r}}' = R(\phi)\hat{\mathbf{r}} + \boldsymbol{\xi}_{\text{exp}}, \tag{7}$$

where $R(\phi)$ denotes a phase-space rotation by angle ϕ, and $\boldsymbol{\xi}_{\text{exp}} \sim \mathcal{N}(\mathbf{0}, N_{\text{exp}})$ represents additive Gaussian noise with covariance matrix N_{exp}. The covariance N_{exp} exceeds typical environmental noise levels but remains below denial-of-service intensity. This phenomenological model captures physically realizable exploratory interference, including phase-reference perturbation and structured excess-noise injection, without assuming a specific adversarial implementation.

In contrast to reconnaissance noise, exploratory perturbations produce observable distortions in quadrature statistics and state covariance. These deviations remain compatible with continued system operation, allowing repeated observation of system behavior under stress. From an adversarial

 doi:10.20944/preprints202601.2359.v1

perspective, this regime enables systematic probing of how observable quantities respond to controlled perturbations across different operating conditions.

3.5.1. Impact on System Stability

Exploratory noise impacts system stability in several operationally significant ways:

1. **Phase-Space Asymmetry.** Moderate phase rotations and excess noise introduce asymmetric distortions in the covariance matrix, revealing directional sensitivities in phase space and dependence on specific operating points.
2. **Dynamic Response Characteristics.** Observable changes in quadrature statistics under exploratory perturbations expose characteristic response times, relaxation behavior, and transient dynamics of the system.
3. **Stability Margin Identification.** By varying the magnitude and structure of injected perturbations, exploratory noise enables identification of regions in parameter space where performance degradation accelerates, signaling proximity to instability or failure thresholds.

These effects allow an adversary to construct an empirical map of system robustness, analogous to stress-testing and vulnerability discovery in classical engineered systems, translated here into the phase-space dynamics of continuous-variable quantum devices.

3.5.2. Exploratory Noise as a Precursor to Escalation

Exploratory noise serves as an intermediate stage between stealthy reconnaissance and overt denial-of-service interference. Information extracted during this phase, including sensitivity to phase distortions, tolerance to excess noise, and the onset of nonlinear or unstable behavior, can inform the design of subsequent, higher-intensity perturbations.

As such, exploratory noise plays a critical role in adversarial escalation strategies. It bridges low-amplitude, covert probing and overt disruption by enabling targeted refinement of attack parameters based on observed system behavior. In continuous-variable quantum communication systems, this progression highlights the importance of understanding not only failure modes, but also the structured pathways through which adversarial interference can evolve from benign-appearing perturbations into destabilizing attacks.

3.6. Denial-of-Service (DoS) Noise

Denial-of-service (DoS) noise represents the most severe class of adversarial interference considered in this work. It is characterized by high-intensity perturbations that overwhelm the quantum communication channel and render reliable transmission impossible. Unlike reconnaissance or exploratory noise, which aim to extract information or probe system stability while preserving operability, DoS noise is explicitly disruptive and seeks to force operational failure. In this regime, the primary effect of interest is not gradual performance degradation, but the rapid breakdown of state integrity and communication viability.

In continuous-variable quantum communication systems, DoS interference can be modeled operationally as a Gaussian channel with large excess noise and/or strong phase diffusion. At the quadrature level, this is expressed as

$$\hat{\mathbf{r}}' = R(\phi)\hat{\mathbf{r}} + \boldsymbol{\xi}_{\mathrm{DoS}}, \tag{8}$$

where the phase parameter ϕ may fluctuate rapidly over a wide range, and $\boldsymbol{\xi}_{\mathrm{DoS}} \sim \mathcal{N}(\mathbf{0}, N_{\mathrm{DoS}})$ is a Gaussian noise term with covariance matrix N_{DoS} far exceeding nominal operating limits. This phenomenological model captures intense optical jamming, severe phase-reference destabilization, or broadband noise injection, without assuming a specific adversarial mechanism or implementation.

 doi:10.20944/preprints202601.2359.v1

3.6.1. Impact on Quantum State Coherence

DoS noise rapidly degrades quantum state coherence by dramatically inflating quadrature variances and distorting the phase-space distribution. The covariance matrix V of the state transforms as

$$V' = R(\phi)VR^{\mathsf{T}}(\phi) + N_{\mathrm{DoS}}, \tag{9}$$

leading to a substantial increase in $\mathrm{Tr}(V)$. Because the trace of the covariance matrix is directly proportional to the mean photon number, this corresponds to rapid growth in state energy.

In phase space, this manifests as extensive spreading of the Wigner function, accompanied by loss of Gaussian localization and severe reduction in state purity. Nonclassical correlations and phase-sensitive structure required for quantum communication and information-processing tasks are rapidly destroyed, rendering the quantum state unsuitable for reliable transmission, verification, or further processing.

3.6.2. Energy Deviation and Failure Thresholds

To quantify the severity of DoS interference in an implementation-relevant manner, state degradation is characterized using an energy-deviation metric derived from the covariance matrix:

$$\Delta E_{\mathrm{DoS}} \propto \mathrm{Tr}(V') - \mathrm{Tr}(V_0), \tag{10}$$

where V_0 denotes the covariance matrix of the unperturbed reference state. As excess noise accumulates, ΔE_{DoS} grows rapidly, reflecting both increased quadrature variance and loss of state structure.

Operational failure occurs once the energy deviation exceeds a system-dependent threshold ΔE_{th}, determined by factors such as detector saturation, estimator breakdown, numerical instability, or loss of protocol validity:

$$\Delta E_{\mathrm{DoS}} \gg \Delta E_{\mathrm{th}}. \tag{11}$$

Crossing this threshold marks a transition from degraded performance to functional failure, beyond which meaningful quantum communication or device operation cannot be maintained.

3.6.3. Observability and Operational Consequences

Because DoS noise produces large-amplitude and rapidly varying deviations in quadrature statistics, it is typically straightforward to distinguish from lower-intensity adversarial regimes. However, the defining characteristic of DoS interference is speed: the rapid escalation of excess noise can destabilize the system on timescales shorter than those required for detailed diagnosis or corrective action.

From an operational perspective, DoS noise delineates the ultimate boundary of adversarial tolerance in continuous-variable quantum systems. It defines the regime in which physical-layer interference directly translates into loss of functionality, underscoring the importance of characterizing failure thresholds and the pathways through which adversarial perturbations drive systems from degraded operation into complete breakdown.

3.7. Operational Signatures in Covariance Statistics

Adversarial noise affects continuous-variable quantum states in ways that depend on both its intensity and its operational intent. While all adversarial strategies perturb the underlying phase-space distribution, their impact on state energy, coherence, and purity differs systematically across reconnaissance, exploratory, and denial-of-service regimes. These effects directly determine the reliability, integrity, and operational stability of continuous-variable quantum communication systems and devices.

Table 3 summarizes how different receiver-accessible observables map to specific estimators, dominant failure modes, and adversarial regime sensitivity under finite-sample and finite-resolution constraints.

 doi:10.20944/preprints202601.2359.v1

Table 3. Mapping between receiver-accessible observables, estimators, dominant failure modes, and adversarial regime sensitivity in continuous-variable quantum communication. The table emphasizes how finite-sample estimation and implementation constraints shape operational vulnerability across adversarial regimes.

Observable	Estimator	Dominant failure mode	Most sensitive regime	Notes
$\hat{\sigma}_x^2$, $\hat{\sigma}_p^2$	Sample variance	Estimator bias; confidence-interval inflation	Reconnaissance	Finite-sample scaling $\sim 1/\sqrt{n}$; sub-threshold excess noise remains statistically invisible over short windows
Off-diagonal covariance $\hat{V}_{xp}$	Sample covariance	Phase-reference sensitivity; estimator instability	Exploratory	Requires stable phase reference; sensitive to quadrature rotations and anisotropic noise
Full covariance matrix $\hat{V}$	Sample covariance matrix	Numerical instability; anisotropic distortion	Exploratory	Finite-resolution effects distort eigenstructure before trace growth becomes large
$\mathrm{Tr}(\hat{V})$	Energy-deviation estimator	Cumulative variance growth; estimator breakdown	Exploratory / DoS	Phase-invariant; directly linked to excess noise accumulation and operational thresholds
Detector output range / ADC bins	Saturation monitoring	Clipping; nonlinear distortion	DoS	Hardware-limited; produces abrupt deviation rather than gradual bias
Higher-order moments (e.g., kurtosis)	Moment-based estimators	Model mismatch; non-Gaussian leakage	Exploratory (conditional)	Not reliably accessible in most CVQC platforms; large sample sizes required

3.7.1. Energy Deviation as an Operational Metric

To quantify the impact of adversarial noise in a manner compatible with experimental continuous-variable platforms, state degradation is characterized using an *energy-deviation* metric derived from second-order quadrature moments. For a single-mode Gaussian state with covariance matrix V, the mean energy (up to a constant offset set by normalization) is proportional to the trace of the covariance matrix, a standard result in Gaussian quantum optics and continuous-variable quantum information [12].

$$\langle E \rangle \propto \mathrm{Tr}(V). \tag{12}$$

 doi:10.20944/preprints202601.2359.v1

Remark 1 (Trace energy relation under the vacuum-normalized convention). *Throughout this paper we adopt the common shot-noise-unit normalization in which the vacuum covariance is $V_{\mathrm{vac}} = I_{2m}$ for an m-mode system. Let $\hat{\mathbf{r}} = (\hat{x}_1, \hat{p}_1, \ldots, \hat{x}_m, \hat{p}_m)^{\mathsf{T}}$ and define the covariance matrix by $V_{ij} := \frac{1}{2}\langle\{\Delta\hat{r}_i, \Delta\hat{r}_j\}\rangle$. Under this convention, the total mean photon number satisfies the affine relation*

$$\langle\hat{N}\rangle = \sum_{k=1}^{m}\langle\hat{n}_k\rangle = \frac{\mathrm{Tr}(V) + \|\mathbf{d}\|^2 - 2m}{4}, \tag{13}$$

where $\mathbf{d} := \langle\hat{\mathbf{r}}\rangle$ is the displacement vector. In particular, for zero-mean (or mean-subtracted) statistics ($\mathbf{d} = \mathbf{0}$), $\langle\hat{N}\rangle = \big(\mathrm{Tr}(V) - 2m\big)/4$. Therefore, any energy deviation *induced by excess noise can be taken proportional to $\Delta\mathrm{Tr}(V)$ up to a fixed constant factor (and vacuum offset), so we use $\Delta E \propto \mathrm{Tr}(V') - \mathrm{Tr}(V_0)$ as an operational scalar metric.*

The energy deviation induced by adversarial noise is therefore defined as

$$\Delta E \propto \mathrm{Tr}(V') - \mathrm{Tr}(V_0), \tag{14}$$

$$\Delta E := \frac{\mathrm{Tr}(V') - \mathrm{Tr}(V_0)}{4}, \tag{15}$$

where V_0 denotes the covariance matrix of the unperturbed reference state and V' that of the perturbed state. Here we use δ_e to denote a receiver-defined *energy-deviation tolerance* (a scalar analogue of δ_V), i.e., the maximum ΔE typically accepted as nominal over a monitoring window at the chosen confidence level, as determined by finite-sample uncertainty, detector resolution, and false-alarm design. Here and throughout this work, covariance matrices are expressed in normalized units where the vacuum variance of each quadrature is set to unity. The proportionality is understood to apply to zero-mean states or to covariance matrices computed after subtraction of estimated first moments, so that $\mathrm{Tr}(V)$ captures excess variance due solely to noise rather than coherent displacement. This definition avoids reliance on idealized Hamiltonian ground states or full state tomography and instead reflects experimentally accessible quantities such as quadrature variances or mean photon number.

Energy deviation serves as a practical, protocol-agnostic metric because it directly captures excess noise accumulation, estimator degradation, and proximity to operational failure thresholds. It applies equally to communication, verification, and sensing tasks in continuous-variable systems. Different classes of adversarial noise correspond to distinct regimes of energy deviation:

1. **Reconnaissance Noise.** Low-amplitude excess noise produces only a small increase in $\mathrm{Tr}(V)$, yielding ΔE values that typically remain within estimator confidence intervals. Although energetically subtle, such deviations can accumulate over time, biasing inferred system parameters and enabling information leakage without triggering conventional anomaly detection.
2. **Exploratory Noise.** Moderate, structured perturbations lead to observable increases in ΔE as quadrature variances become asymmetric or inflated. These deviations are constrained below catastrophic levels, allowing repeated observation of system behavior while revealing sensitivity to controlled stress.
3. **Denial-of-Service (DoS) Noise.** High-intensity excess noise causes a rapid and large increase in $\mathrm{Tr}(V)$, driving ΔE well beyond operational thresholds. In this regime, energy growth correlates with estimator breakdown, detector saturation, and loss of functional viability.

3.7.2. Coherence Loss and State Purity

Beyond energy deviation, adversarial noise degrades quantum coherence and state purity, both of which are critical for reliable quantum information processing. These effects are naturally visualized in phase space via the Wigner function and quantified through changes in the covariance matrix.

1. **Reconnaissance Noise.** Because reconnaissance noise remains energetically small, the Wigner function retains an approximately Gaussian and localized form over short timescales, and state

 doi:10.20944/preprints202601.2359.v1

purity is largely preserved. However, repeated low-level perturbations can accumulate, gradually degrading coherence and revealing information about system parameters without overt disruption.

2. **Exploratory Noise.** Exploratory perturbations distort the covariance matrix more noticeably, producing elongation, rotation, or anisotropic spreading of the Wigner function in phase space. This reflects partial loss of coherence and moderate purity degradation, indicating proximity to stability boundaries.
3. **Denial-of-Service (DoS) Noise.** Under DoS conditions, large excess noise rapidly spreads the Wigner function, yielding a highly mixed state with severely reduced purity. Nonclassical correlations and phase-sensitive structure are destroyed, rendering the quantum state unsuitable for communication, verification, or further processing.

From an operational perspective, these regimes define a structured progression of state degradation: from subtle parameter biasing, to stress-induced instability, to complete functional breakdown. This progression provides a unified framework for characterizing how adversarial interference manifests at the quantum-state level across increasing noise intensity.

3.7.3. Normalization and Multi-Mode Generalization

Throughout this work, covariance matrices are expressed in normalized units where the vacuum variance of each quadrature is set to unity. This convention is standard in continuous-variable quantum optics and simplifies comparison across devices, protocols, and operating regimes by eliminating system-dependent scaling factors. Under this normalization, excess noise, estimator tolerances, and energy deviation can be interpreted directly in terms of deviations from the vacuum reference, without explicit dependence on absolute optical power or Hamiltonian parameters.

The energy-deviation metric introduced in this paper inherits this normalization naturally. For a single-mode Gaussian state with covariance matrix V, the quantity $\mathrm{Tr}(V)$ provides a dimensionless measure of total quadrature variance relative to vacuum. As a result, energy deviation captures excess noise accumulation in a manner that is both experimentally accessible and independent of specific detector calibrations, provided consistent normalization is maintained.

Although the analysis presented here focuses primarily on single-mode qumodes for clarity, the framework extends straightforwardly to multi-mode continuous-variable systems. For an m-mode Gaussian state with covariance matrix $V \in \mathbb{R}^{2m\times 2m}$, the total energy deviation generalizes to

$$\Delta E \propto \mathrm{Tr}(V') - \mathrm{Tr}(V_0), \tag{16}$$

where V_0 denotes the reference covariance matrix of the unperturbed multi-mode state. In this setting, $\mathrm{Tr}(V)$ aggregates excess variance across all modes and quadratures, capturing both local noise accumulation and correlated disturbances arising from mode coupling or shared noise sources.

Importantly, the adversarial-noise taxonomy introduced in this work remains applicable in the multi-mode case. Reconnaissance noise corresponds to low-amplitude, potentially correlated perturbations that remain within joint estimator tolerances across modes; exploratory noise induces structured distortions revealing inter-mode sensitivities and stability margins; and denial-of-service noise drives global variance growth that overwhelms estimation and control capabilities. While multi-mode systems introduce additional structure through correlations and entanglement, the receiver-centric, covariance-based perspective adopted here provides a consistent operational basis for analyzing adversarial interference at scale.

These considerations highlight that the present single-mode treatment should be viewed as a minimal setting for exposition rather than a fundamental limitation. The normalization conventions and energy-deviation framework developed here are compatible with multi-mode extensions and networked architectures, supporting future work on adversarial robustness in large-scale continuous-variable quantum communication systems.

 doi:10.20944/preprints202601.2359.v1

3.7.4. Why the Covariance Trace

A central design choice in this work is the use of the trace of the covariance matrix as the primary scalar observable for quantifying adversarial impact. This choice is motivated by a combination of physical relevance, experimental accessibility, and robustness under realistic implementation constraints.

First, for Gaussian continuous-variable states, the trace of the covariance matrix,

$$\mathrm{Tr}(V) = \langle \hat{x}^2 \rangle + \langle \hat{p}^2 \rangle, \tag{17}$$

is directly proportional (up to a constant offset set by normalization) to the mean energy or mean photon number of the mode for zero-mean states or for covariance matrices computed after subtraction of first moments. As such, increases in $\mathrm{Tr}(V)$ provide a physically meaningful measure of excess noise accumulation that is independent of phase-space orientation. This makes the trace a natural indicator of how strongly adversarial perturbations inflate quadrature variance and drive the system toward operational failure.

Second, the trace is invariant under ideal symplectic rotations. This invariance is critical in adversarial settings, where structured noise may project differently onto measured quadratures depending on phase-space orientation. By using $\mathrm{Tr}(V)$, we obtain a metric that captures total variance growth without being confounded by purely geometric redistribution of noise between quadratures. Orientation-dependent effects are still observable through the full covariance structure, but the trace provides a compact summary of overall disturbance severity.

Third, from an experimental standpoint, the trace is exceptionally well matched to receiver-accessible observables. It depends only on second-order quadrature moments, which can be estimated reliably using homodyne or heterodyne detection with finite resolution and without full state tomography. In contrast, alternative quantities such as symplectic eigenvalues, entropic measures, or fidelity metrics typically require stronger assumptions, higher-order statistics, or significantly larger data sets, making them less suitable for real-time or implementation-level monitoring.

Finally, the covariance trace provides a protocol-agnostic link between adversarial interference and operational thresholds. Estimator breakdown, detector saturation, numerical instability, and protocol abort conditions are all naturally associated with excessive variance growth rather than with specific geometric features of the state. By framing adversarial impact in terms of $\mathrm{Tr}(V)$, the resulting energy-deviation metric directly reflects proximity to such failure modes across communication, verification, and sensing applications.

For these reasons, the covariance trace serves as an effective compromise between physical interpretability, experimental feasibility, and adversarial robustness. It enables a unified, receiver-centric characterization of disturbance severity while remaining compatible with finite-resolution measurements, finite-sample estimation, and multi-mode generalizations.

3.8. Finite-Sample Detectability: A Minimal Quantitative Demonstration

3.8.1. Setup: Estimating Excess Noise from Quadrature Samples

We provide a minimal quantitative demonstration of how finite sample size and finite-resolution estimation induce an operational detectability threshold for weak adversarial excess noise. The goal is not to propose a complete detector or security proof, but to make explicit the statistical mechanism that underlies the reconnaissance/exploratory regime boundary, below a sample-limited threshold, injected excess noise is statistically indistinguishable from nominal operation within typical confidence requirements. This behavior mirrors finite-size parameter-estimation effects analyzed in CV-QKD, where excess noise below estimator confidence bounds remains operationally invisible despite being systematic [5–7]. Importantly, the qualitative regime structure discussed below does not depend on the Gaussian approximation itself; the same $1/\sqrt{n}$ scaling and soft detectability boundary follow directly from the exact χ^2 distribution.

 doi:10.20944/preprints202601.2359.v1

Consider a receiver performing homodyne measurements of a single quadrature (without loss of generality, the p-quadrature) on n independent state preparations. Let $\{p_i\}_{i=1}^{n}$ denote the recorded outcomes. Under nominal operation, assume a zero-mean Gaussian model

$$p_i \sim \mathcal{N}(0, \sigma_0^2), \tag{18}$$

where σ_0^2 represents the reference quadrature variance, including trusted receiver noise contributions. Under adversarial excess-noise injection, the observed variance becomes

$$\sigma_1^2 = \sigma_0^2 + \nu, \tag{19}$$

where $\nu \geq 0$ is the excess-noise magnitude to be detected.

A natural estimator for the quadrature variance is the sample variance

$$\hat{\sigma}^2 := \frac{1}{n} \sum_{i=1}^{n} p_i^2, \tag{20}$$

where the mean is taken to be 0 for simplicity, consistent with symmetric modulation or calibrated offset removal. More generally, the standard estimator $\frac{1}{n}\sum_{i=1}^{n}(p_i - \bar{p})^2$ yields the same scaling of estimator uncertainty with sample size, and the zero-mean form is adopted here for notational clarity. For Gaussian samples, $\hat{\sigma}^2$ is an unbiased estimator with

$$\mathbb{E}[\hat{\sigma}^2] = \sigma^2, \qquad \mathrm{Var}(\hat{\sigma}^2) = \frac{2\sigma^4}{n}. \tag{21}$$

Thus, under nominal operation ($\sigma^2 = \sigma_0^2$), the standard deviation of the variance estimator scales as

$$\mathrm{Std}(\hat{\sigma}^2) = \sqrt{\frac{2}{n}}\,\sigma_0^2. \tag{22}$$

To connect to operational acceptance regions, suppose the receiver uses a one-sided threshold test of the form

$$\hat{\sigma}^2 \leq \sigma_0^2 + \tau, \tag{23}$$

where τ encodes an estimator tolerance determined by the target false-alarm probability (confidence level), finite-resolution effects, and additional trusted uncertainty margins. In practice, τ can be interpreted as the upper tolerance margin of a one-sided acceptance region for variance-based monitoring.

Exact finite-sample distribution (Gaussian case).

For Gaussian quadrature samples $p_i \sim \mathcal{N}(0, \sigma^2)$ with known (or pre-subtracted) mean, the variance estimator $\hat{\sigma}^2 = \frac{1}{n}\sum_{i=1}^{n} p_i^2$ admits the exact finite-sample law

$$\frac{n\,\hat{\sigma}^2}{\sigma^2} \sim \chi_n^2. \tag{24}$$

If instead one uses the usual sample-mean-corrected estimator $s^2 = \frac{1}{n-1}\sum_{i=1}^{n}(p_i - \bar{p})^2$, then

$$\frac{(n-1)\,s^2}{\sigma^2} \sim \chi_{n-1}^2. \tag{25}$$

In what follows we use a normal (Gaussian) approximation to this χ^2-based sampling distribution in the large-n regime, which yields the simple $1/\sqrt{n}$ detectability scaling used for the operational threshold discussion.

 doi:10.20944/preprints202601.2359.v1

In the large-n regime, a normal approximation yields an operational detectability condition:

$$\nu \gtrsim z_\alpha \sqrt{\frac{2}{n}}\,\sigma_0^2, \tag{26}$$

where z_α is the one-sided normal quantile associated with the desired significance level (e.g., $\alpha = 0.05$). Equation (26) makes explicit the finite-sample scaling: the minimum excess noise that can be reliably resolved decreases only as $1/\sqrt{n}$ and grows with the baseline variance scale σ_0^2.

This quantitative scaling underpins the operational interpretation adopted throughout the paper: reconnaissance noise corresponds to ν values that remain below (or comparable to) the finite-sample detectability scale in Eq. (26) over typical monitoring windows, while exploratory noise corresponds to ν values that exceed it and therefore produce statistically resolvable distortions in receiver-side covariance statistics.

3.8.2. Tolerance Regions and Missed-Detection Probability

We now make explicit how estimator tolerances translate into a nonzero probability of missed detection for weak adversarial excess noise. This connects the abstract notion of acceptance regions directly to operational risk in finite-sample monitoring.

Let the receiver adopt a variance-based acceptance test of the form

$$\hat{\sigma}^2 \le \sigma_0^2 + \tau, \tag{27}$$

where σ_0^2 is the reference variance under nominal operation and $\tau > 0$ defines the tolerance margin. Any realization satisfying Eq. (27) is deemed consistent with normal operation.

Related finite-size missed-detection and confidence-region effects are well known in CV-QKD parameter estimation, where excess noise can evade detection with nonzero probability under finite sampling, even when security margins are formally satisfied [5,7].

Under adversarial excess-noise injection, the true variance is $\sigma_1^2 = \sigma_0^2 + \nu$. The probability of missed detection (Type-II error) is therefore

$$P_{\mathrm{miss}}(\nu) = \Pr\!\left(\hat{\sigma}^2 \le \sigma_0^2 + \tau \,\middle|\, \sigma^2 = \sigma_0^2 + \nu\right). \tag{28}$$

Using the Gaussian approximation for the sampling distribution of $\hat{\sigma}^2$ in the large-n regime,

$$\hat{\sigma}^2 \sim \mathcal{N}\!\left(\sigma_1^2,\ \frac{2\sigma_1^4}{n}\right), \tag{29}$$

the missed-detection probability can be written explicitly as

$$P_{\mathrm{miss}}(\nu) = \Phi\!\left(\frac{\sigma_0^2 + \tau - (\sigma_0^2 + \nu)}{\sqrt{2}\,\sigma_1^2/\sqrt{n}}\right) = \Phi\!\left(\frac{\tau - \nu}{\sqrt{2}\,\sigma_1^2/\sqrt{n}}\right), \tag{30}$$

where $\Phi(\cdot)$ denotes the cumulative distribution function of the standard normal distribution.

Equation (30) makes several operational features explicit. First, for $\nu \ll \tau$, the argument of $\Phi(\cdot)$ is positive and large, yielding $P_{\mathrm{miss}} \approx 1$: adversarial excess noise is almost certainly accepted as nominal. Second, the transition from high to low missed-detection probability occurs over a finite interval of ν whose width scales as $\sigma_1^2/\sqrt{n}$ and reduces to $\mathcal{O}(\sigma_0^2/\sqrt{n})$ in the weak-perturbation regime. This interval defines a *soft detectability boundary*, rather than a sharp threshold.

In this sense, estimator tolerances induce a continuous acceptance region in variance space, not a binary security boundary. Reconnaissance noise corresponds to operating points where ν lies deep inside the high-P_{miss} region, while exploratory noise occupies the intermediate regime where detection

 doi:10.20944/preprints202601.2359.v1

becomes probabilistic and phase-space anisotropies or temporal correlations may provide additional observable leverage.

Finally, Eq. (30) highlights why purely static thresholds are intrinsically vulnerable under finite-sample constraints. For any fixed tolerance τ and sample size n, there exists a nontrivial range of excess-noise amplitudes that are statistically likely to evade detection, even though they induce systematic bias and energy accumulation over time. This quantitative fact underlies the operational regime taxonomy developed in this work and motivates the use of covariance-based metrics that track cumulative degradation rather than instantaneous threshold violations.

3.8.3. Operational Boundary Between Reconnaissance and Exploratory Regimes

The transition between reconnaissance and exploratory adversarial regimes can be formalized operationally using the finite-sample detectability analysis developed above. Rather than being defined by a sharp noise-amplitude threshold, this boundary emerges from the interplay between excess-noise magnitude, estimator tolerances, and available sample size.

Using the missed-detection probability in Eq. (30), an operational boundary can be defined by selecting a reference confidence level $P^*_{\text{miss}} \in (0,1)$ that separates statistically invisible perturbations from those that are likely to be detected within a monitoring window. Solving

$$P_{\text{miss}}(\nu^*) = P^*_{\text{miss}} \tag{31}$$

gives the following boundary condition, illustrated in Fig. 5.

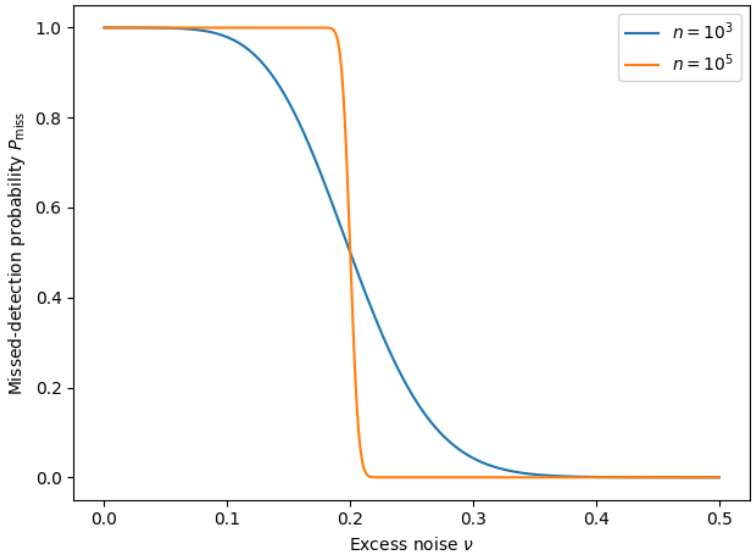

Figure 5. Missed-detection probability $P_{\text{miss}}(\nu)$ as a function of excess-noise amplitude ν for two sample sizes ($n = 10^3$ and $n = 10^5$) at fixed estimator tolerance τ. Finite sample size induces a soft detectability boundary: increasing n sharpens the transition between statistically invisible (reconnaissance) and detectable (exploratory) perturbations, but does not eliminate missed detection for finite n.

Figure 5 provides a concrete numerical illustration of Eq. (30), showing how finite sample size transforms the fixed tolerance test in Eq. (27) into a soft, probabilistic detectability boundary.

For the excess-noise amplitude ν^* yields

$$\nu^* = \tau - \sqrt{2}\,(\sigma_0^2 + \nu^*)\,\frac{\Phi^{-1}(P^*_{\text{miss}})}{\sqrt{n}}, \tag{32}$$

where $\Phi^{-1}(\cdot)$ is the inverse standard normal cumulative distribution function.

Equation (32) defines a *finite-sample operational boundary* between adversarial regimes:

 doi:10.20944/preprints202601.2359.v1

1. For $\nu \ll \nu^*$, missed-detection probability remains close to unity, and excess noise is statistically indistinguishable from nominal fluctuations over the observation window. This corresponds to the *reconnaissance regime*, in which adversarial probing can proceed stealthily while gradually biasing inferred parameters.
2. For $\nu \gtrsim \nu^*$, missed-detection probability decreases appreciably, and excess noise becomes intermittently or consistently observable in receiver-side statistics. This marks the onset of the *exploratory regime*, where structured perturbations induce detectable stress without yet forcing system failure.

Several features of this boundary are noteworthy. First, ν^* depends explicitly on the sample size n: increasing data acquisition narrows the reconnaissance regime, but does not eliminate it entirely for finite n. Second, the boundary depends on the chosen tolerance τ, which is itself an operational design parameter reflecting acceptable false-alarm rates, calibration uncertainty, and detector limitations. Third, because the estimator variance depends on the total variance $\sigma_0^2 + \nu$, the boundary shifts dynamically as excess noise accumulates, producing feedback between adversarial action and statistical detectability.

Importantly, this boundary is probabilistic rather than absolute. There exists a finite interval of ν values for which the system alternates between apparent nominal behavior and detectable deviation across successive observation windows. This gray zone is precisely where exploratory adversarial strategies are most informative: injected perturbations are large enough to elicit observable responses, yet small enough to preserve overall operability.

From an operational standpoint, the reconnaissance–exploratory boundary therefore represents a transition in *statistical visibility*, not in physical noise mechanism. This reinforces the central theme of this work: adversarial regimes in continuous-variable quantum communication are most meaningfully defined by their interaction with finite-resolution estimation and acceptance regions, rather than by idealized noise models or static thresholds alone.

4. Limitations and Scope

The framework developed in this work is intentionally scoped to *operational characterization* rather than mitigation or defense. Several limitations therefore delineate the regime of validity and interpretation of the results.

First, the analysis is restricted to *receiver-side observables*, primarily first- and second-order quadrature statistics summarized by covariance matrices. While this choice reflects what is experimentally accessible in most continuous-variable quantum communication (CVQC) platforms, it does not capture higher-order moments, non-Gaussian features, or full state-tomographic information. Adversarial strategies that primarily affect such higher-order structure may therefore evade characterization within the present framework.

Second, the modeling of adversarial noise is phenomenological and Gaussian at the level of observables. This does not imply that adversaries are limited to Gaussian physical processes, but rather that their impact is analyzed through the lens of finite-resolution estimation. Non-Gaussian attacks that nevertheless manifest as effective excess variance at the receiver are captured by the framework, whereas attacks whose signatures lie entirely outside covariance-level statistics are not.

Third, the finite-sample detectability analysis assumes independent and identically distributed quadrature samples and stationary estimator tolerances over the observation window. In realistic systems, temporal correlations, drifting calibration parameters, or adaptive monitoring strategies may modify detectability boundaries. The results should therefore be interpreted as defining baseline operational limits rather than exhaustive detection guarantees.

Fourth, the work focuses on single-mode states and single-link communication scenarios. While the covariance-trace and energy-deviation concepts generalize naturally to multi-mode systems, correlated noise, mode coupling, and network-level effects introduce additional structure that is

 doi:10.20944/preprints202601.2359.v1

not explicitly analyzed here. Extending the framework to multi-mode and networked settings is a necessary step for full-scale deployment scenarios.

Finally, this paper does not propose concrete countermeasures, adaptive controls, or protocol-level defenses. While the taxonomy and quantitative boundaries introduced here are intended to inform such strategies, their design and validation lie outside the scope of the present study. In particular, questions of optimal monitoring, adaptive thresholding, feedback control, or integration with quantum error correction and verification protocols are deferred to future work.

Within these bounds, the contribution of this paper is to provide a clear operational lens through which adversarial interference in CVQC can be classified, quantified, and compared. The scope is therefore complementary to, rather than competitive with, work on mitigation, control, and security proofs, supplying the threat-modeling substrate upon which such defenses can be systematically evaluated.

5. Conclusion

This work developed an operational framework for characterizing adversarial interference in continuous-variable quantum communication (CVQC) under implementation-realistic constraints, including finite measurement resolution, estimator tolerances, and limited control capabilities. Rather than treating noise as purely environmental and stationary, adversarial interference was modeled as structured, intent-driven disturbances that can be engineered to remain operationally inconspicuous, probe system stability, or rapidly disrupt functionality.

Within a receiver-side Gaussian-channel representation, we introduced a three-regime taxonomy of adversarial noise. *Reconnaissance noise* consists of low-amplitude perturbations designed to evade detection while gradually biasing parameter estimation. *Exploratory noise* introduces moderate, structured disturbances that induce observable stress, revealing directional sensitivities and stability margins. *Denial-of-service (DoS) noise* corresponds to high-intensity interference that overwhelms the system, driving rapid loss of state integrity and operational breakdown. To quantify these regimes in a protocol-agnostic and experimentally accessible manner, we defined an energy-deviation metric based on changes in the trace of the covariance matrix, providing a compact scalar measure of excess variance accumulation and proximity to operational failure thresholds.

Together, the proposed taxonomy and energy-deviation metric establish a structured threat-modeling foundation for analyzing physical-layer attack surfaces in CVQC. By directly linking adversarial intent to observable phase-space statistics, this framework enables systematic analysis of how seemingly benign perturbations can escalate into destabilizing interference. More broadly, it provides a common operational language for connecting physical-layer disturbances to estimator degradation, loss of coherence, and system-level performance limits.

The framework developed here naturally motivates future work focused on mitigation and resilience rather than characterization alone. In particular, adaptive control and modulation strategies can be evaluated against the adversarial regimes and observables defined in this study, enabling quantitative assessment of robustness under non-stationary and adversarial conditions. Extensions to multi-mode and networked systems, incorporation of real-time feedback, and integration with higher-level verification and error-correction mechanisms represent promising directions toward resilient continuous-variable quantum communication and information-processing platforms.

To our knowledge, this is the first receiver-centric framework that explicitly links estimator tolerances, finite-sample statistics, and adversarial intent into a unified operational taxonomy for CV quantum communication.

Author Contributions: Conceptualization, J.R.R.B.; methodology, J.R.R.B. and J.V.G.T.; investigation, J.R.R.B.; validation, J.V.G.T. and R.A.F.; formal analysis, J.R.R.B.; writing, original draft, J.R.R.B.; writing, review and editing, J.V.G.T., R.A.F., N.S., S.R.V., M.P., A.Tr. and A.Th.; supervision, R.A.F.

 doi:10.20944/preprints202601.2359.v1

Funding: This research study was funded in part by the Natural Sciences and Engineering Research Council of Canada (NSERC), Discovery Grants Program, Grant No. RGPIN-2023-04513, in association with Lakes Environmental Software Inc. and EigenQ, Inc.
Cette recherche a été financée par le Conseil de recherches en sciences naturelles et en génie du Canada (CRSNG), RGPIN-2023-04513.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data available from the corresponding author upon reasonable request.

Conflicts of Interest: Author Nadeem Said is an employee of LAKES Environmental Research Inc. Author Andy Thanos is an employee of Cisco Systems, Inc. Authors Jose R. Rosas-Bustos, Jesse Van Griensven The, Mark Pecen, Sebastian Ratto Valderrama and Alexander Truskovsky are Consultants to EigenQ Inc. Roydon Andrew Fraser is a paid advisor to EigenQ Inc. The remaining authors declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

ADC	Analog-to-Digital Converter
CV	Continuous Variable
CVQC	Continuous-Variable Quantum Communication
CV-QKD	Continuous-Variable Quantum Key Distribution
DoS	Denial of Service
LO	Local Oscillator
QIP	Quantum Information Processing
QKD	Quantum Key Distribution

References

1. Rosas-Bustos, J.R.; Thé, J.V.G.; Fraser, R.A.; Valderrama, S.R.; Said, N.; Thanos, A. Theoretical Vulnerabilities in Quantum Integrity Verification Under Bell-Hidden Variable Convergence. *Journal of Cybersecurity and Privacy* **2026**, *6*, 15. https://doi.org/10.3390/jcp6010015.
2. Pirandola, S.; Andersen, U.L.; Banchi, L.; Berta, M.; Bunandar, D.; Colbeck, R.; Englund, D.; Gehring, T.; Lupo, C.; Ottaviani, C.; et al. Advances in quantum cryptography. *Advances in Optics and Photonics* **2020**, *12*, 1012–1236. https://doi.org/10.1364/AOP.361502.
3. Wehner, S.; Elkouss, D.; Hanson, R. Quantum internet: A vision for the road ahead. *Science* **2018**, *362*, eaam9288. https://doi.org/10.1126/science.aam9288.
4. Pironio, S.; Acín, A.; Massar, S.; De La Giroday, A.B.; Matsukevich, D.N.; Maunz, P.; Olmschenk, S.; Hayes, D.; Luo, L.; Manning, T.A.; et al. Random numbers certified by Bell's theorem. *Nature* **2010**, *464*, 1021–1024. https://doi.org/10.1038/nature09008.
5. Leverrier, A.; Grosshans, F.; Grangier, P. Finite-size analysis of a continuous-variable quantum key distribution. *Physical Review A* **2010**, *81*, 062343. https://doi.org/10.1103/PhysRevA.81.062343.
6. Leverrier, A. Composable Security Proof for Continuous-Variable Quantum Key Distribution with Coherent States. *Physical Review Letters* **2015**, *114*, 070501. https://doi.org/10.1103/PhysRevLett.114.070501.
7. Jouguet, P.; Kunz-Jacques, S.; Leverrier, A.; Grangier, P.; Diamanti, E. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nature Photonics* **2013**, *7*, 378–381. https://doi.org/10.1038/nphoton.2013.63.
8. Micadei, K.; Peterson, J.P.S.; Souza, A.M.; Sarthour, R.S.; Oliveira, I.S.; Landi, G.T.; Batalhão, T.B.; Serra, R.M.; Lutz, E. Reversing the direction of heat flow using quantum correlations. *Nature Communications* **2019**, *10*, 2456. https://doi.org/10.1038/s41467-019-10333-7.
9. Su, X.; Zhao, Y.; Hao, S.; Jia, X.; Xie, C.; Peng, K. Experimental preparation of eight-partite cluster state for photonic qumodes. *Optics letters* **2012**, *37*, 5178–5180. Place: United States, https://doi.org/10.1364/OL.37.005178.

 doi:10.20944/preprints202601.2359.v1

10. Hu, X.M.; Zhang, C.; Guo, Y.; Wang, F.X.; Xing, W.B.; Huang, C.X.; Liu, B.H.; Huang, Y.F.; Li, C.F.; Guo, G.C.; et al. Pathways for Entanglement-Based Quantum Communication in the Face of High Noise. *Physical Review Letters* **2021**, *127*, 110505. https://doi.org/10.1103/PhysRevLett.127.110505.
11. Diamanti, E.; Lo, H.K.; Qi, B.; Yuan, Z. Practical challenges in quantum key distribution. *npj Quantum Information* **2016**, *2*, 1–12. https://doi.org/10.1038/npjqi.2016.25.
12. Weedbrook, C.; Pirandola, S.; García-Patrón, R.; Cerf, N.J.; Ralph, T.C.; Shapiro, J.H.; Lloyd, S. Gaussian quantum information. *Reviews of Modern Physics* **2012**, *84*, 621–669. https://doi.org/10.1103/RevModPhys.84.621.
13. Ruppert, L.; Usenko, V.C.; Filip, R. Long-distance continuous-variable quantum key distribution with efficient channel estimation. *Physical Review A* **2014**, *90*, 062310. https://doi.org/10.1103/PhysRevA.90.062310.
14. Grosshans, F.; Grangier, P. Continuous Variable Quantum Cryptography Using Coherent States. *Physical Review Letters* **2002**, *88*, 057902. https://doi.org/10.1103/PhysRevLett.88.057902.
15. Shao, Y.; Wang, H.; Pi, Y.; Huang, W.; Li, Y.; Liu, J.; Yang, J.; Zhang, Y.; Xu, B. Phase noise model for continuous-variable quantum key distribution using a local local oscillator. *Physical Review A* **2021**, *104*, 032608. https://doi.org/10.1103/PhysRevA.104.032608.