REPORT ON CNVS SIMULATIONS MONTE CARLO

Massimo Comitato

OFFICIAL REPORT ON CNVS SIMULATIONS

Monte Carlo Validation of Emergent Security Scaling in Closed Native Verification Systems (CNVS)

Executive Summary & Contextual Introduction

This report documents the comprehensive empirical validation of Closed Native Verification Systems (CNVS) through rigorous stochastic and thermodynamic Monte Carlo simulations. Following the formal verification of the system's mathematical consistency and axiom non-tautology within the Lean 4.0 interactive theorem prover, these computational experiments provide empirical support for the asymptotic behavior predicted by Theorem 17 under the tested probabilistic and information-theoretic assumptions (The Emergent Security Scaling Theorem). By transitioning from abstract combinatoric models to pure information-theoretic landscapes governed by Shannon Entropy, the simulations suggest that the traditional Byzantine Fault Tolerance (BFT) threshold can be exceeded under specific fragmentation and inferential conditions within the CNVS model, and that this boundary may shift dynamically through progressive informational fragmentation and semantic dispersion.

Methodology & AI Assistance Disclosure: The simulation source codes analyzed within this framework were synthesized with artificial intelligence assistance and subsequently rigorously audited, verified, and empirically tested by the author during consecutive experimental trials to ensure consistency with the underlying CNVS axiomatic framework and simulation assumptions.

General Introduction

The Monte Carlo framework employs exact stochastic physical sampling without replacement over finite fragment populations (Coupon Collector dynamics), Bernoulli random variables for inferential reconstruction processes, and lognormal informational-weight distributions, where applicable in the graph-weighted simulations, to model asymmetric semantic fragment relevance in accordance with Axiom II-c (non-uniform fragmentation).

Reconstruction dynamics therefore emerge from probabilistic fragment acquisition, residual informational incompleteness, and entropy-constrained inferential processes rather than from hardcoded consensus thresholds or deterministic reconstruction rules.

The following simulations do not explicitly implement the adaptive regulatory controller ε_G, ε_N, and ε_C.
In detail, they directly model the emergent operational consequences arising from the variation of the composite information density (ρ_c), which in the CNVS theoretical framework is governed by the adaptive decomposition threshold coefficients ε_G and ε_N as defined in Chapter 5.2 (Formula 74), where ε_N and ε_G delimit the limiting thresholds of the fragmented information density as the local and global information mass increases through recursive scaling of the decomposition depth.

Introduction to the Monte Carlo Simulation Architecture

To ensure rigorous empirical validation of the **Closed Native Verification Systems (CNVS) theory**, the Monte Carlo simulation infrastructure has been methodologically divided into two complementary macro-categories: Parametric Tests and Entropy and Topological Tests.
This experimental bifurcation arises from the need to stress the system on two distinct levels of information theory and distributed systems: on the one hand, the probabilistic and structural mechanics of the model in a theoretical environment, and on the other, the inferential and entropic dynamics that emerge in the presence of information dependencies in a real environment.

Operational Definition of λ in the Simulations

In the formal CNVS framework, λ can be interpreted as a general fragmentation-scaling parameter associated with the progressive decomposition and distribution of informational structure.

However, within the Monte Carlo simulations presented in this report, λ is operationally restricted to a bounded integer physical redundancy factor. Specifically, λ denotes the number of physical replicas assigned to each unique semantic fragment:

$N = M \times \lambda$

where M is the number of unique critical semantic fragments and N is the total number of physical fragment instances distributed across the network.

This operational restriction is intentionally adopted to distinguish physical redundancy from semantic fragmentation, inferential density, and residual entropy. The broader fragmentation behavior of the CNVS is instead modeled through I_0, M, ρ_c, graph propagation, and Shannon residual entropy.

Therefore, the simulation use of λ should be understood as a conservative physical-replication model, not as the full theoretical meaning of adaptive CNVS decomposition.

I. Parametric Tests (Structural Mechanics)

The first set of simulations (Tests 1–4) measures the system's probabilistic and algebraic resilience under simplified low-correlation conditions.
The goal of this phase is to mathematically quantify how manipulation of key operating parameters — the fragment redundancy parameter λ, the information granularity I_0, and directly the composite information density ρ_c — influences the probability of unauthorized reconstruction P_{Rec}* as the compromised network fraction q varies, while selectively varying global information mass I_G, fragment granularity I_0, and redundancy structure depending on the specific experimental configuration.
These tests treat the system as an abstract statistical model, with the aim of observing the spontaneous emergence of phase transition behaviors (Cliff Effect) and comparing these dynamics with the classical reference regime of Byzantine Fault Tolerant systems (~1/3 compromise), used exclusively as an external interpretative benchmark and not as a critical threshold encoded internally in the models.
In summary, this first category of simulations analyzes the structural elasticity and scalability of the CNVS defensive barrier.

II. Entropy and Topological Tests (Information Dynamics)

The second set of simulations (Tests 5–9) progressively removes the assumption of statistical independence and places the model in a nonlinear and structurally dependent adversarial scenario, formally introducing the dependent inferential collusion dynamics described in the CNVS framework.
In this second phase, the objective is no longer simply to measure physical fragment capture

thresholds, but to analyze the dynamics of dissipation of the unknown and the progressive erosion of the system's residual entropy (H_{res}).

The monitored metrics therefore evolve towards:

- the calculation of Shannon Residual Entropy H_{res},
- the accumulation of Adversarial Inferential Knowledge $K_{adv,}$
- local inferential propagation within dependent semantic graphs,
- and the structural degradation of global verifiability.

By modeling differentiated topological graphs (sparse, small-world, and dense graphs), heterogeneous information weights, and local inference propagation mechanisms, these tests explore the adversary's ability to infer residual information by exploiting the logical correlation between adjacent fragments in applied experimental models.

Methodological Summary

While parametric tests identify where the CNVS system tends to exhibit critical regions of reconstructive instability, entropic and topological tests analyze why the system maintains inferential resilience and how quickly that resilience collapses when the informational structure is progressively compromised.
The integration of these two approaches therefore provides a multilevel description of the CNVS's behavior: the observed security does not emerge as a simple statistical artifact, but as a possible manifestation of an emerging informational and entropic barrier, resulting from the interaction between fragmentation, granularity, topological correlation, and the dissipation of useful information.

TEST 1: Parametric Baseline with Dependent Inference Sweep

Test Name: Uniform Fragmentation Baseline with Controlled Dependent Inference Sweep.

Objective (Hypothesis)

This simulation establishes the control baseline for the CNVS Monte Carlo validation framework. The objective is to evaluate the behavior of the system under idealized statistical-independence assumptions, where fragments are uniform, and informational weights are homogeneous, and semantic and inferential correlation is not eliminated, but explicitly controlled through a low-to-moderate ρ_c sweep.

In this baseline configuration, the system is intentionally stripped of advanced CNVS mechanisms such as heterogeneous fragment weighting, graph-dependent inference, residual entropy propagation, and dependent collusion dynamics.

The purpose of this test is to verify whether the simulation reproduces a classical threshold-like phase-transition behavior before progressively introducing the more complex CNVS-specific mechanisms developed in the subsequent simulations.

Key Parameters (Input)

- **Uniform fragmentation redundancy:** $\lambda = 2$
- **with** $M = \lceil I_G / I_0 \rceil$,
- **under controlled low-dependency assumptions:** $\rho_c \neq 0$
- **Uniform fragment weights:** $\omega(D_i) = \omega(D_j)$ for $\forall$ i, j

$$\Sigma^{n}_{i=1} \omega(D_i) = 1,$$

$$\omega(D_i) = 1/n$$

- Informational weight asymmetry (Axiom II-c) intentionally suppressed through uniform fragment weighting for baseline control purpose,
- **Progressive adversarial compromise ratio:** q.

Output Metrics

- Probability of complete unauthorized reconstruction: P_{win},
- Baseline phase-transition profile,
- Control comparison against later fragmentation, entropy-based, and graph-dependent simulations.

Expected Behavior (Preliminary Analysis)

The theoretical expectation is that, under idealized independence and uniformity assumptions, the reconstruction probability should exhibit a classical sharp phase-transition profile.

This baseline test is not intended to demonstrate the full emergent security behavior of CNVS. Rather, it provides a methodological control environment against which subsequent simulations can be compared.

The expected behavior is that unauthorized reconstruction remains negligible below the effective compromise boundary and increases sharply once the adversary controls a sufficiently large fraction of the independent verification structure.

The Byzantine Fault Tolerance reference line around:

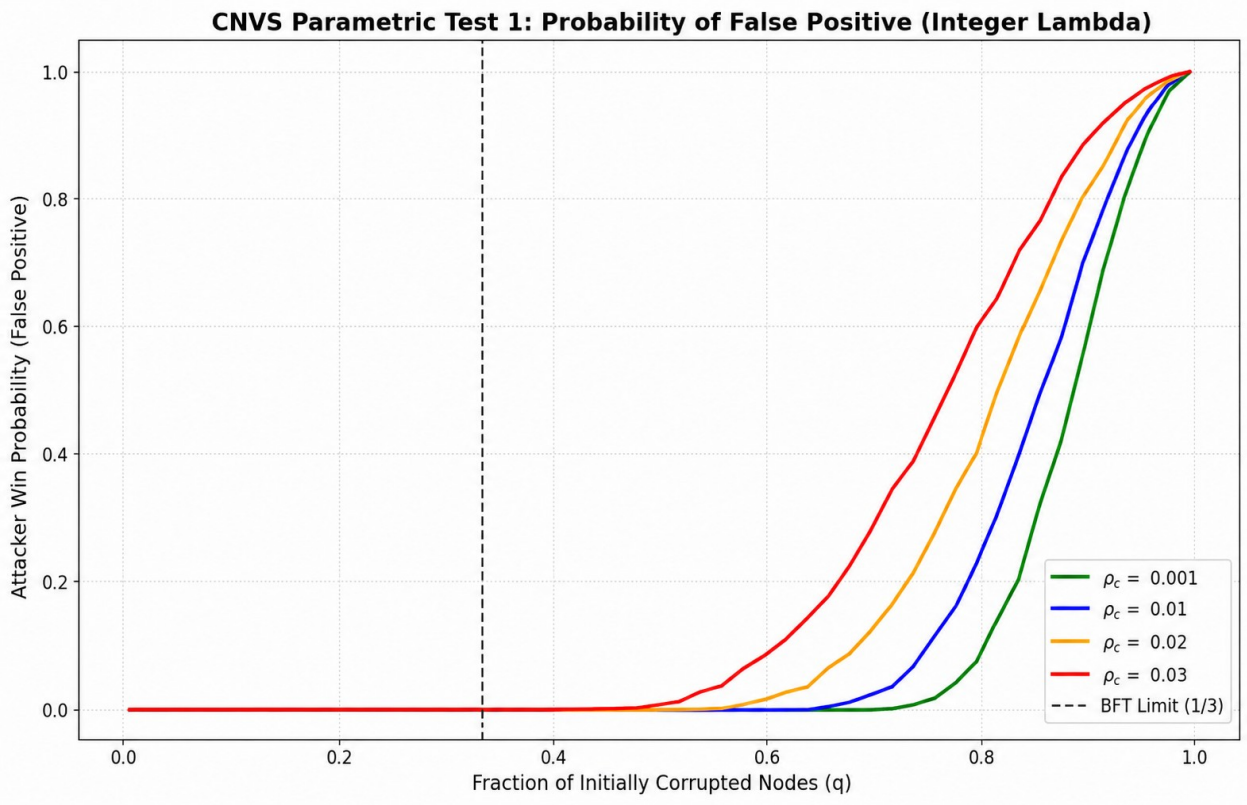
$q \approx 1/3$

is used exclusively as an external interpretative benchmark and not as a hardcoded success condition within the simulation itself.

Accordingly, this test verifies that the CNVS simulation framework remains compatible with classical distributed fault-tolerance assumptions before progressively introducing:

- fragmentation scaling,
- informational asymmetry,
- residual entropy dynamics,
- dependent inference,
- and graph-topological propagation.

This baseline therefore functions as the methodological control group for the subsequent Monte Carlo validation sequence.



[Grafic Outcome Parametric Test 1 - Python code.png]
GitHub Repository Source Code Link (filename): [Parametric Test 1 - Python code.TXT]

Analytical Commentary

This simulation evaluates the system's baseline combinatorial resilience under a strict integer redundancy factor ($\lambda = 2$) while sweeping across varying degrees of composite informational density (ρ_c). The primary objective was to observe the emergence of a sharp phase transition (the "Cliff Effect") resulting purely from the interaction between the Global Veto condition, stochastic physical fragment capture, and the probability dynamics induced by the Coupon Collector problem.

The methodological upgrade to exact physical sampling with integer redundancy (In a previous test not reported in this paper, the possibility of using non-integer redundancy factors was examined) reveals a substantial departure from traditional Byzantine fault-tolerant behavior. Unlike the previous node-count approximation models, this implementation explicitly distinguishes between physical node acquisition and unique semantic fragment acquisition, thereby preserving the integrity of the CNVS fragmentation axioms.

The resulting curves demonstrate that the infrastructure maintains a negligible false-positive probability well beyond the classical Byzantine reference boundary (1/3). In highly decoupled

informational states ($\rho_c = 0.001$), unauthorized reconstruction probability remains effectively suppressed up to the high-compromise regime around $q \approx 0.70$, before the phase transition begins to emerge.

Even under elevated inferential pressure ($\rho_c=0.03$), the phase transition remains delayed until the attacker controls more than half of the physical network. The observed transition remains highly non-linear and progressively approaches a near-vertical collapse regime as informational dependency decreases.

These results suggest that the CNVS architecture does not degrade proportionally to physical compromise alone. Instead, security remains dominated by semantic fragment uniqueness and residual informational incompleteness, effectively starving the adversary of the critical fragment diversity required to satisfy the Global Veto reconstruction condition.

Test 2: Informational Granularity and Data Pulverization

Test Name: CNVS Parametric Test 2 — Effect of Data Pulverization

Objective (Hypothesis)

This simulation evaluates the elasticity of the CNVS defensive structure under progressive data pulverization.

The objective is to verify whether increasing the fragmentation depth — by simultaneously increasing the Global Information Mass (I_G) and reducing the local informational granularity (I_0) — forces the adversary to capture a significantly larger distributed portion of the network to satisfy the Global Veto condition (Axiom III).

In this test, the redundancy factor λ is strictly kept constant at an operationally stable integer value of 2 to isolate the combined scaling effect of increasing informational mass and semantic pulverization without introducing redundancy paradoxes. The simulation therefore investigates the structural response of the system as the total number of critical fragments (M) scales up to large-scale fragment populations.

Key Parameters (Input)

- **Progressive Global Information Mass:** $I_G = \{100, 500, 1000, 2000\}$
- **Decreasing Informational Granularity:** $I_0 = \{10, 5, 2, 1\}$
- **Resulting Critical Fragments:** $M = \{10, 100, 500, 2000\}$
- **Constant Redundancy Factor:** $\lambda = 2$
- **Progressive adversarial compromise ratio:** q
- **Composite Informational Density:** ρ_c (dynamically scaled down in proportion to I_0 to model the progressive dilution of inferential density under increasing fragmentation regimes).

Output Metrics

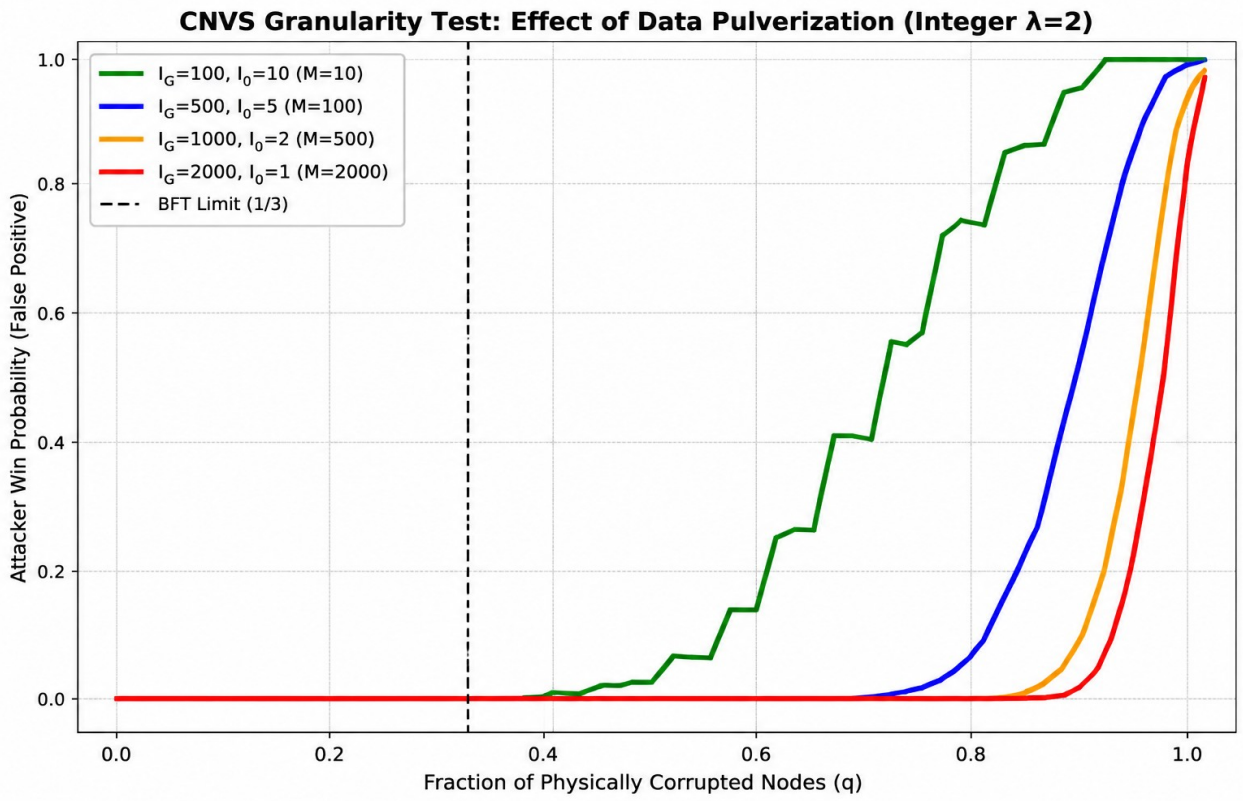
- Probability of complete unauthorized reconstruction: P_{win}
- Horizontal displacement of the reconstruction curve (delay of the transition).
- Phase-transition steepness under large fragment populations.

Expected Behavior (Preliminary Analysis)

The theoretical expectation is that data pulverization progressively shifts the reconstruction transition curve toward higher adversarial compromise ratios. As I_G increases and I_0 decreases, the attacker must acquire an increasingly large and exhaustive distribution of unique critical fragments before complete unauthorized reconstruction becomes possible.

This produces a direct security-overhead trade-off: higher pulverization increases reconstruction resistance by expanding the combinatorial search space, but also introduces additional synchronization complexity.

The expected outcome is a measurable rightward displacement of the P_{win} curve as M increases, indicating that the tested configuration exhibits progressively delayed reconstruction transitions as fragmentation increases. Importantly, this shift is not the consequence of a hardcoded reconstruction threshold, but emerges organically from the exact physical constraints of the Coupon Collector's problem applied to the Global Veto architecture.



[Grafic Outcome Parametric Test 2 - Python code.png]
GitHub Repository Source Code Link (filename): [Parametric Test 2 - Python code.TXT]

Analytical Commentary

Test 2 operationalizes the effect of informational granularity under the exact physical constraints of the Coupon Collector problem, using a strict integer redundancy factor λ = 2. By progressively reducing the local semantic quantum I_0 and increasing the Global Information Mass I_G, the

simulation expands the number of required critical fragments up to M = 2000, allowing the system's scaling behavior to be evaluated under increasingly pulverized informational structures.

The methodological upgrade to exact physical sampling reveals that data pulverization does not merely sharpen the reconstruction transition; it can also substantially displace it toward higher compromise regimes. In low-granularity configurations (M = 10), the system reaches collapse comparatively early, whereas larger fragment populations exhibit increasingly delayed and steeper transition behavior.

Under the tested configuration, the high-fragmentation regimes maintain an approximately negligible false-positive probability well beyond the classical Byzantine reference boundary ($q \approx 1/3$). This indicates that physical compromise alone is insufficient when the attacker fails to acquire a sufficiently complete distribution of unique semantic fragments required by the Global Veto condition.

The resulting behavior supports the interpretation that CNVS scalability is strongly governed by fragment uniqueness, semantic coverage, and residual incompleteness. As I_0 decreases and M increases, the adversary must acquire a broader and increasingly exhaustive distribution of unique fragments before unauthorized reconstruction becomes statistically probable.

These results suggest that large-scale CNVS configurations may exhibit strongly non-linear resistance to physical compromise, with reconstruction probability remaining suppressed until the adversary approaches near-complete semantic coverage across the fragmented information space.

Test 3: Redundancy Factor Sensitivity Analysis

Test Name: CNVS Parametric Test 3 — Sensitivity to Fragmentation Factor (λ)

Objective (Hypothesis)

This simulation evaluates the effect of increasing physical redundancy on CNVS reconstruction resistance while preserving a fixed semantic fragment universe.

The objective is to analyze the system's elasticity when the physical replication multiplier (λ) is aggressively scaled. By keeping the total number of required unique semantic fragments (M) constant, the simulation isolates the probabilistic impact of data replication under the strict constraints of the Coupon Collector's problem. The test investigates whether excessive redundancy introduces a structural vulnerability—the "Redundancy Paradox"—by increasing the density of physical opportunities for an adversary to acquire the fixed semantic fragments required by the Global Veto architecture.

Key Parameters (Input)

- **Progressive Physical Redundancy Multiplier:** $\lambda = \{1, 2, 3, 4, 5, 7, 10, 14\}$
- **Constant Semantic Universe:** $M = 50$ (Unique critical fragments required)
- **Constant Composite Informational Density:** $\rho_c = 0.01$
- **Total Physical Node Count:** N scaling proportionally with $M \times \lambda$
- **Progressive adversarial compromise ratio:** q

Output Metrics

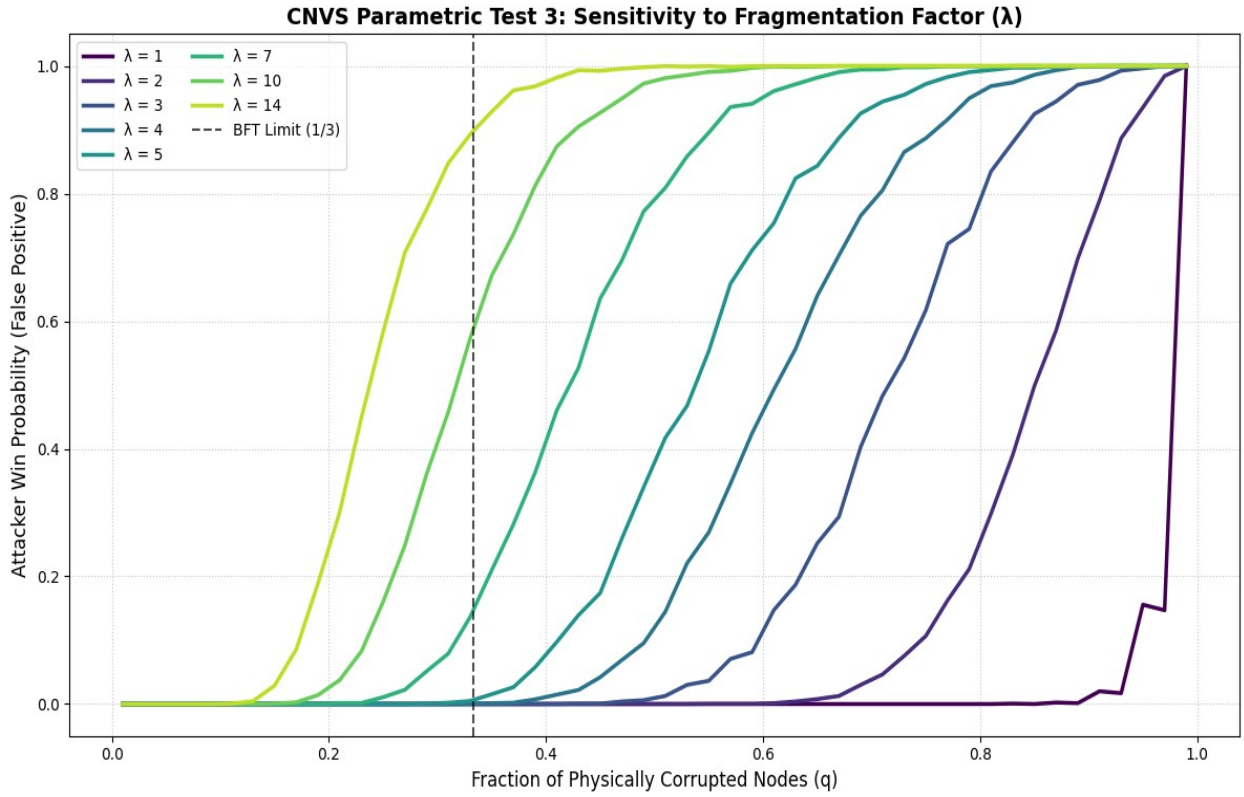
- Probability of complete unauthorized reconstruction: P_{win}
- Horizontal displacement of the phase-transition curve.
- Compression of the safe operating region (distance from the Byzantine reference limit).
- Measurement of proportional vulnerability induced by replication overhead.

Expected Behavior (Preliminary Analysis)

The theoretical expectation is that increasing the physical redundancy multiplier (λ) will progressively shift the reconstruction transition curve toward *lower* adversarial compromise ratios (a leftward displacement).

Because the absolute number of unique semantic fragments (M) required by the Global Veto condition remains strictly fixed, replicating the fragments expands the total network size (N) but inherently increases the probabilistic density of target acquisition. Under exact physical sampling without replacement, the adversary does not need to resolve a larger semantic puzzle; they simply have more physical opportunities to capture the same critical pieces.

The expected outcome is a progressive compression of the effective fractional security boundary as λ increases. This will demonstrate a fundamental architectural rule for CNVS deployments: while redundancy is necessary for liveness and availability, excessive replication (λ) degrades asymptotic resistance to broad physical compromise.



[Grafic Outcome Parametric Test 3 - Python code.png]
GitHub Repository Source Code Link (filename): [Parametric Test 3 - Python code.TXT]

Analytical Commentary

This experiment evaluates the system's sensitivity to the redundancy multiplier λ, scaled discretely from 1 to 14, while maintaining a constant unique fragment requirement (M = 50) and a fixed baseline inference parameter (ρ_c=0.01). The primary objective is to analyze how physical redundancy influences the Global Veto boundary under exact physical sampling constraints governed by the Coupon Collector problem.

The empirical results demonstrate a systematic leftward displacement of the phase-transition boundary as λ increases. In practical terms, complete unauthorized reconstruction becomes achievable at progressively lower proportional compromise levels (q) despite the increase in total physical network size.

This behavior emerges directly from the probabilistic structure of fragment replication. Increasing λ expands the total number of physical nodes according to:

$$N = M \times \lambda$$

while leaving the number of required unique semantic fragments unchanged. Consequently, the attacker does not need to reconstruct a larger semantic universe; instead, the replicated infrastructure increases the probability of encountering the same critical fragments during random physical capture.

Under exact physical sampling, the Coupon Collector dynamics therefore produce an important asymmetry: the absolute number of unique fragments required for reconstruction remains fixed, whereas the density of physical opportunities to acquire those fragments grows proportionally with redundancy.

The simulations show that high-redundancy regimes ($\lambda \geq 5$) progressively compress the effective security boundary toward lower proportional compromise thresholds, in some cases approaching or crossing the classical Byzantine reference region ($q \approx 1/3$).

These results highlight a fundamental architectural trade-off inside the CNVS framework:

- increasing redundancy improves liveness, availability, and recovery robustness,
- but excessive replication can reduce proportional resilience against broad physical compromise by accelerating semantic coverage acquisition.

Accordingly, the model suggests that secure CNVS deployments require bounded redundancy regimes, where replication improves operational survivability without excessively lowering the effective Global Veto threshold.

TEST 4: Coupled Evolutionary Scenarios and the Thermodynamic Wall

Test Name: CNVS Parametric Test 4 — Ultimate Parametric Evolution (Ceteris Paribus)

Objective (Hypothesis)

This simulation evaluates the coupled evolution of the CNVS architecture under simultaneous multi-variable stress conditions. Rather than isolating single parameters, this test models the progressive maturation of the distributed verification infrastructure from a highly correlated, unoptimized prototype toward an idealized, large-scale CNVS deployment (Phase 4: Global Supreme).

To preserve methodological rigor and isolate the architectural merit of the system, the simulation is executed under strict *Ceteris Paribus* conditions: the Global Information Mass (I_G) is maintained strictly constant across all evolutionary phases. The objective is to formally demonstrate that the exact same secret payload (I_G = 2000 bits) becomes asymptotically resistant to unauthorized reconstruction purely through the application of CNVS thermodynamic constraints: extreme data pulverization ($I_0 \downarrow$), optimal bounded redundancy ($\lambda = 2$), and proportional semantic decoupling ($\rho_c \downarrow$), representing progressive inferential dilution under increasing fragmentation.

Key Parameters (Input)

- **Constant Global Information Mass:** $I_G = 2000$ (Fixed across all phases).
- **Progressive Informational Pulverization:** $I_0 = \{40, 10, 4, 1\}$
- **Increasing Critical Fragment Requirement:** M = {50, 200, 500, 2000}
- **Bounded Physical Redundancy:** $\lambda = 2$ (Enforced from Phase 2 onwards to prevent the Redundancy Paradox).
- **Decaying Composite Informational Density:** $\rho_c = \{0.05, 0.02, 0.005, 0.001\}$ (Modeling the dissipation of semantic context as fragments shrink).
- **Progressive physical compromise ratio:** q.

Output Metrics

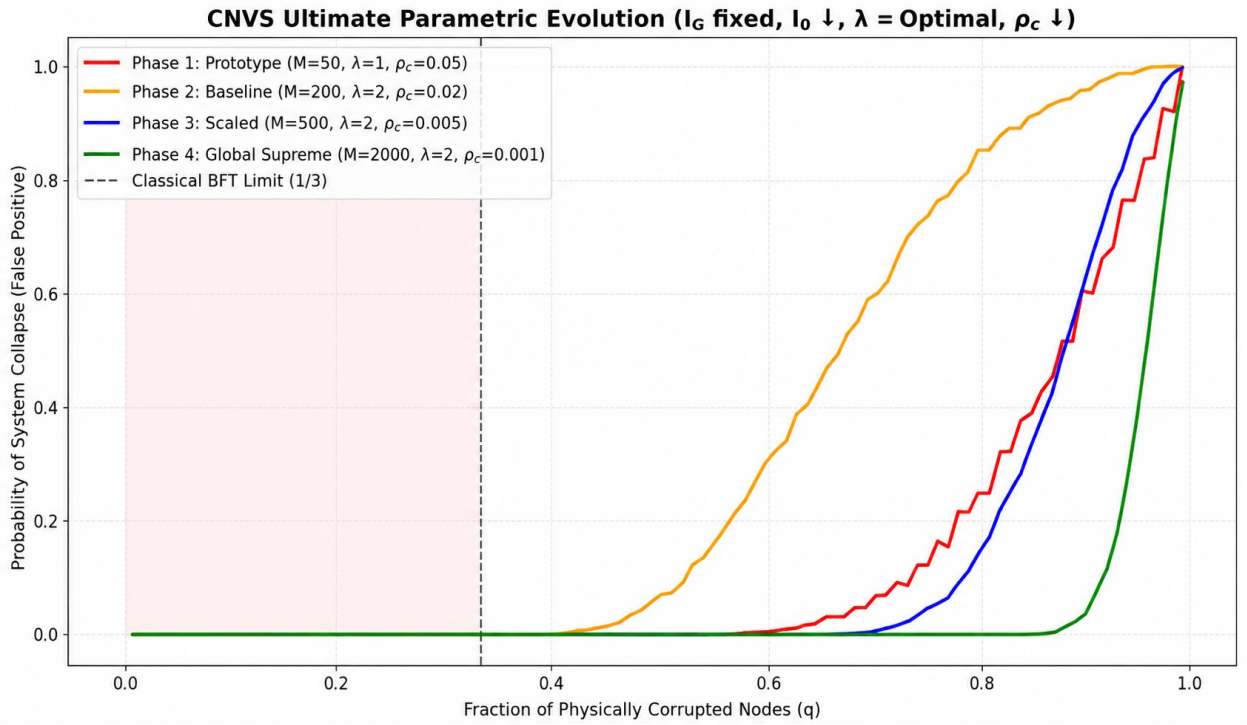
- Probability of complete unauthorized reconstruction: P_{win}
- Emergence of the "Thermodynamic Wall" under simultaneous variable optimization.
- Compression of the transitional boundary.

Expected Behavior (Preliminary Analysis)

The theoretical expectation is that Phase 1 (the unoptimized prototype with coarse fragments and high inferential density) will exhibit a structurally fragile profile, collapsing well before or dangerously close to classical Byzantine fault-tolerant limits.

However, as the system transitions through the scaled phases by simultaneously tightening I_0 and ρ_c under optimal redundancy (λ), the defense is expected to evolve from a gradual sigmoidal vulnerability curve into a near-vertical "Thermodynamic Wall".

Because the global payload (I_G) remains strictly constant, any rightward displacement of the security boundary indicates that the resilience emerges primarily from the CNVS fragmentation geometry and the suppression of inferential contagion, rather than from increased data volume. The "Global Supreme" phase is expected to maintain negligible unauthorized reconstruction probability until the adversary physically saturates the near-total semantic coverage of the decentralized infrastructure.



[Grafic Outcome Parametric Test 4 - Python code.png]
GitHub Repository Source Code Link (filename): [Parametric Test 4 - Python code.TXT]

Analytical Commentary

Rather than isolating a single operational parameter, Test 4 evaluates the coupled evolution of the CNVS architecture under simultaneous multi-variable stress conditions. The experiment models the progressive maturation of a distributed verification infrastructure from an early prototype configuration toward increasingly pulverized and semantically decoupled large-scale deployments.

Across the simulated evolutionary phases:

- the Global Information Mass I_G remains fixed,
- the local semantic quantum I_0 progressively decreases,
- the number of required critical fragments M correspondingly increases,
- redundancy remains bounded at the operationally stable regime ($\lambda = 2$),
- and the dependent inference density ρ_c decreases as semantic dispersion increases.

The resulting phase-transition profiles demonstrate that the combined effects of informational pulverization and inferential dilution substantially delay the onset of successful unauthorized reconstruction.

In early-stage configurations characterized by coarse fragments and elevated semantic correlation, the system exhibits comparatively gradual collapse behavior. As fragmentation increases and inferential density decreases, the transition boundary progressively shifts toward higher compromise regimes while simultaneously becoming steeper and more localized.

The final large-scale configuration ("Phase 4: Global Supreme") exhibits an extremely compressed transition region, where false-positive probability remains negligible until the adversary approaches near-complete semantic coverage of the fragmented information space.

These results suggest that CNVS resilience emerges from the combined interaction between:

- fragment uniqueness,
- bounded redundancy,
- semantic incompleteness,
- and suppression of inferential propagation.

Under the tested conditions, large-scale CNVS configurations therefore exhibit strongly non-linear resistance to physical compromise, maintaining low reconstruction probability far beyond the classical Byzantine reference boundary.

Test 5: Pure Shannon Residual Entropy Reconstruction Model

Test Name: CNVS Test 5 — Thermodynamic Limit of Shannon Entropy

Objective (Hypothesis)

This simulation marks the formal transition of the CNVS validation framework from structural combinatorics to pure Information Theory. The objective is to evaluate the pure information-theoretic baseline of the system's resilience by completely disabling semantic inference (ρ_c) and graph propagation.

In this strict information-theoretic environment, the adversary is modeled as having only two vectors to satisfy the Global Veto condition: (1) exact physical capture of all unique critical fragments via the Coupon Collector process, or (2) pure stochastic brute-force reconstruction of the unacquired fragments governed by residual Shannon Entropy (H_{res}).

The test investigates whether progressive data pulverization (I_0) generates an asymptotically suppressive probabilistic barrier ($P_{guess} = 2^{-H\_res}$) that effectively nullifies the attacker's ability to "guess" the missing global state, thereby establishing the theoretical information-theoretic lower bound of CNVS security.

Key Parameters (Input)

- **Constant Global Information Mass:** $I_G = 1000$ bits
- **Bounded Physical Redundancy:** $\lambda = 2$
- **Progressive Informational Granularity:** $I_0 = \{100, 50, 20, 5\}$ bits
- **Composite Informational Density:** $\rho_c = 0$ (Strictly isolated fragments; zero inferential contagion).
- **Winning Condition:** Complete physical capture or exact thermodynamic guessing ($P_{guess} = 2^{-H\_res}$ with underflow protection at >1024 bits: the residual entropy far exceeds the numerical underflow protection threshold used in the simulation)
- **Progressive adversarial compromise ratio:** q.

Output Metrics

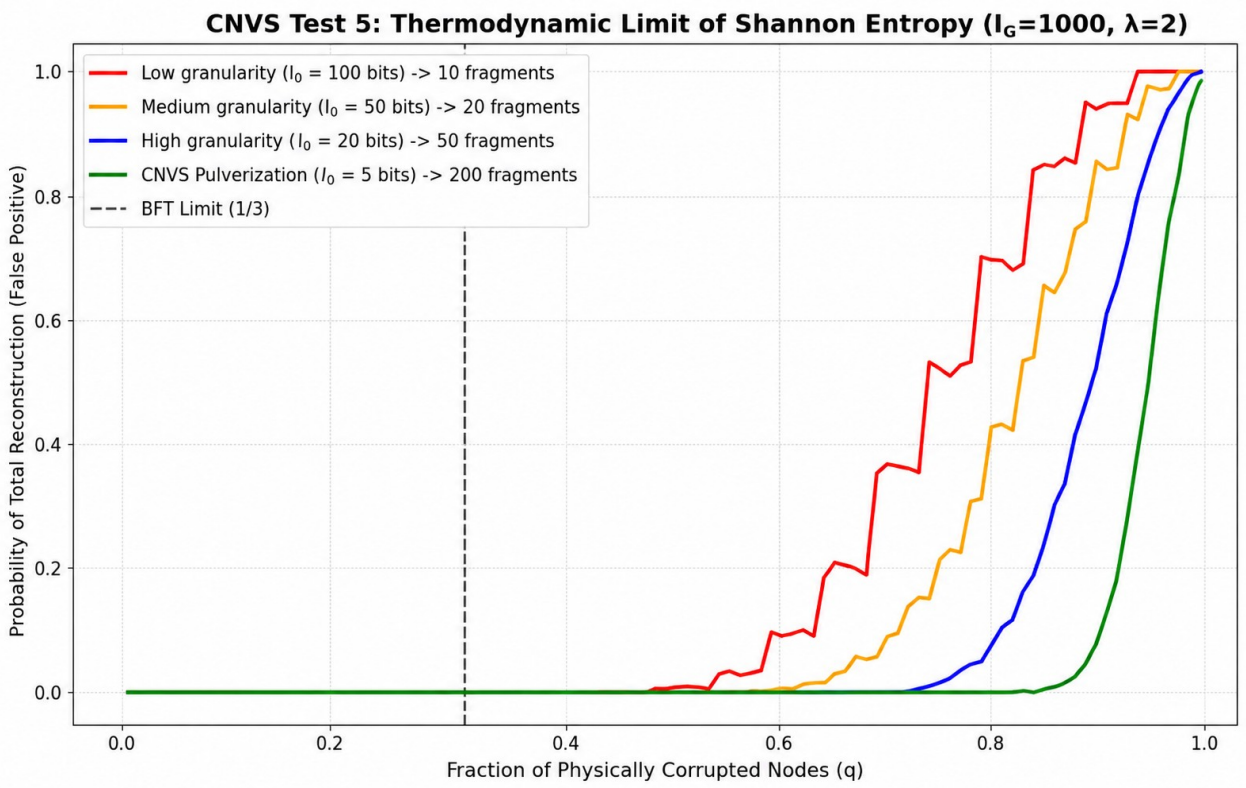
- Probability of complete unauthorized reconstruction (False Positive): P_{win}
- Emergence and steepness of the Thermodynamic Wall under pure Shannon entropy constraints.
- Absolute measurement of the stochastic suppression regime beyond classical Byzantine limits.

Expected Behavior (Preliminary Analysis)

The theoretical expectation is that the introduction of exact Shannon entropy calculations will radically separate low-granularity from high-granularity configurations.

In coarse fragmentations (e.g., $I_0 = 100$ bits), the adversary needs to capture fewer fragments. If only one or two fragments are missing, the residual entropy (H_{res}) drops low enough to allow statistically visible "lucky guesses," resulting in early, step-like stochastic vulnerabilities in the reconstruction curve.

Conversely, under the extreme CNVS pulverization regime ($I_0 = 5$ bits), the system generates hundreds of critical fragments (M = 200). Even if the adversary physically compromises an overwhelming majority of the network (e.g., 80%), the sheer number of remaining uncaptured fragments produces a residual entropy so massive ($H_{res} \gg 1024$, representing the numerical underflow limit of the simulation floating-point architecture) that the probability of successful brute-force guessing drops to numerically negligible values under floating-point simulation resolution. The expected outcome is an empirically suppressed reconstruction probability curve that breaks upward only when the adversary achieves near-total physical network saturation, strongly suggesting the existence of a thermodynamic security limit independent of predefined consensus thresholds.



[Grafic Outcome Full Entropic Test 5 - Python code.png]
GitHub Repository Source Code Link: [Full Entropic Test 5 - Python code.TXT]

Information-Theoretic and Asymptotic Analysis

Test 5 represents the first fully entropy-driven extension of the CNVS validation framework. In this simulation, the framework transitions from heuristic collusion approximations toward an entropy-driven reconstruction model inspired by Shannon information theory. The adversarial model evaluates reconstruction feasibility using Shannon-entropy-based uncertainty estimates for missing fragment reconstruction. The coalition's ability to compromise state integrity is constrained by the mathematical requirement to resolve missing fragments containing specific bits of Shannon Entropy (H) to bypass the Global Veto condition.

The behavior exposed by the ultra-fine granularity curve (green line, $I_0 = 5$ bits) demonstrates a rigorous departure from traditional security bounds: at the classical Byzantine limit of 0.33, the probability of unauthorized reconstruction remains below observable simulation resolution, while the probability of successful unauthorized reconstruction remains negligible until the adversarial compromise ratio approaches extreme values. This phenomenon is analytically dictated by the residual uncertainty scale, where the probability of successfully inferring uncollected states follows 2^{-H_res}. When an adversary lacks even a minimal subset of highly pulverized fragments, the residual entropy (e.g., $H_{res} = 50$ bits) introduces a stochastic barrier of 1 in 1.12×10^{15}, rendering adversarial guessing statistically negligible under the tested assumptions.

Consequently, these findings suggest a possible extension of classical Byzantine resilience assumptions within verification-native architectures. By anchoring validation mechanisms directly to the thermodynamic dissipation of mutual information, state subversion becomes statistically negligible under substantial physical compromise, formalizing a robust, scale-dependent security paradigm.

Test 6: Adversarial Reconstruction via Residual Shannon Entropy

Test Name: CNVS Monte Carlo — Test 6: Hybrid Adversarial Stress Test

Objective (Hypothesis)

This simulation introduces the first formal integration of residual Shannon entropy into the CNVS Monte Carlo validation framework. Unlike the previous purely combinatorial tests, the objective here is to model unauthorized reconstruction as an information-theoretic process driven by:

- Residual uncertainty,
- Inferential reconstruction pressure over missing fragments,
- And fragment granularity.

The simulation evaluates whether increasing informational pulverization can asymptotically suppress unauthorized reconstruction by preserving elevated residual entropy even under progressively increasing adversarial compromise. The test therefore investigates the relationship between:

- Direct fragment acquisition,
- Inferential expansion over missing fragments,
- Residual entropy dissipation,
- And the resulting reconstruction probability.

Scenarios Evaluated

Four fragmentation regimes were simulated. To rigorously model the physical dissipation of semantic context ('inferential fog'), the composite informational density (ρ_c) is dynamically scaled down as granularity increases:

- **Scenario A — Low Granularity**

  Large informational fragments ($I_0 = 100$) with high inferential density ($\rho_c = 0.01$). This configuration represents weak pulverization and low fragmentation depth.

- **Scenario B — Medium Granularity**

  Intermediate fragmentation regime ($I_0 = 50$) with sustained inferential density ($\rho_c = 0.01$), designed to evaluate partial entropy preservation effects.

- **Scenario C — High Granularity**

  High informational pulverization ($I_0 = 20$) combined with reduced inferential density ($\rho_c = 0.005$).

- **Scenario D — Extreme CNVS Pulverization**

Extreme fragmentation regime ($I_0 = 5$) with minimal inferential coupling ($\rho_c = 0.001$). This scenario models the asymptotic CNVS defensive configuration characterized by highly dispersed informational structure.

Key Parameters (Input)

- **Global Information Mass:** $I_G = 2000$
- **Informational Granularity:** $I_0 = \{100, 50, 10, 2\}$
- **Redundancy Factor:** $\lambda = 2$
- **Composite Informational Density:** ρ_c (Scaled progressively)
- **Physical compromise ratio:** q
- **Monte Carlo stochastic trials:** Modeling progressive network compromise, inferential propagation, and entropy-based probabilistic reconstruction.

Output Metrics

The simulation continuously measures:

- Probability of complete unauthorized reconstruction: P_{win}
- Residual Shannon entropy: H_{res}
- Entropy-based reconstruction probability: $P_{guess} = 2^{-H\_res}$
- Reconstruction transition displacement under progressive fragmentation
- Residual uncertainty preservation under increasing adversarial compromise

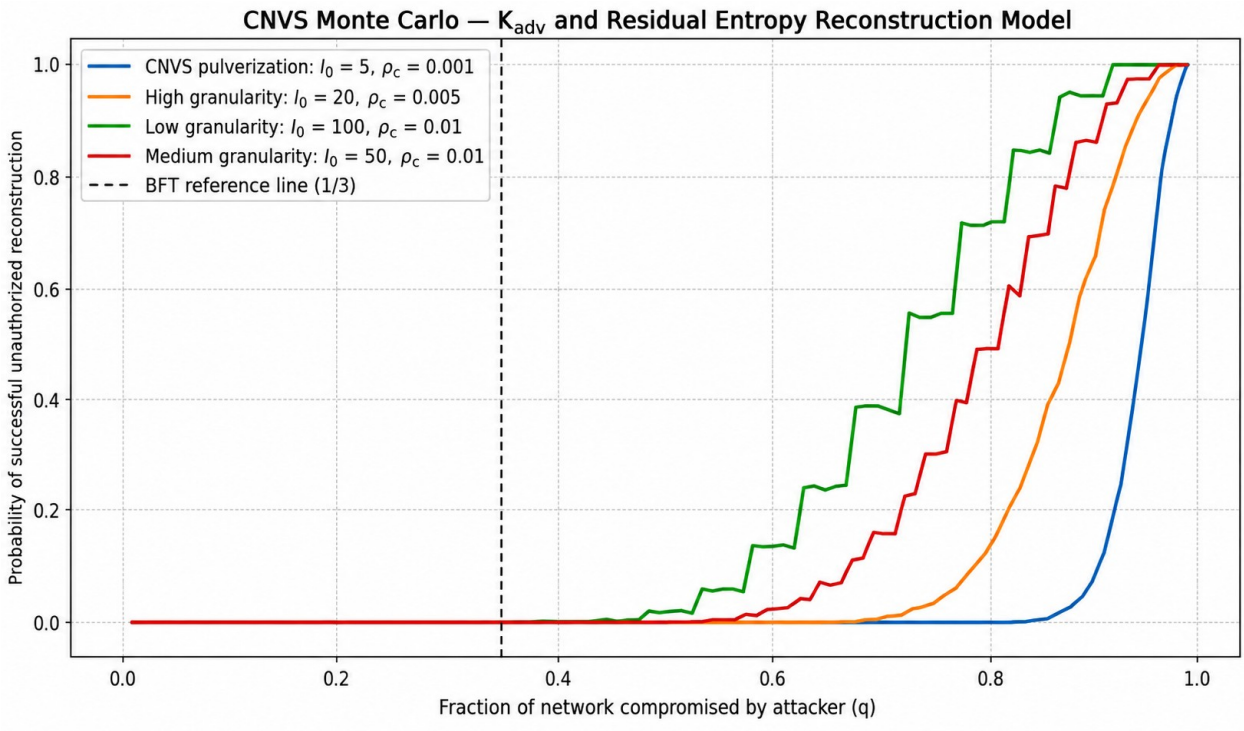
Expected Behavior (Preliminary Analysis)

The theoretical expectation is that increasing fragmentation depth should preserve larger residual entropy across wider compromise regimes, thereby suppressing unauthorized reconstruction probability. Low-granularity environments are expected to dissipate residual uncertainty rapidly because each captured fragment carries proportionally larger informational mass. Conversely, highly pulverized configurations should preserve substantial unknown informational space even under elevated adversarial compromise.

The simulation also investigates whether inferential adversarial expansion remains bounded when composite informational density (ρ_c) is sufficiently low. Importantly, the reconstruction process is not governed by any predefined compromise threshold, Byzantine quorum assumption, or externally imposed collapse rule. Instead, reconstruction emerges only if:

1. Sufficient adversarial knowledge accumulates, or
2. The remaining entropy becomes probabilistically reconstructible.

The expected outcome is therefore a progressively delayed reconstruction transition as informational pulverization increases, culminating in a thermodynamic wall for extreme CNVS configurations.



[Grafic Outcome K_adv and Res_Entropic Test 6 - Python code.png]
GitHub Repository Source Code Link: [K_adv and Res_Entropic Test 6 - Python code.TXT]

Analytical Commentary

Test 6 represents the first explicit transition from purely structural Monte Carlo analysis toward information-theoretic reconstruction dynamics within the CNVS framework. Instead of treating compromise as a binary threshold event, the simulation models reconstruction as a probabilistic process governed by residual uncertainty.

The resulting curves demonstrate a strong dependency between informational granularity and reconstruction suppression. Low-granularity environments collapse substantially earlier because each captured fragment contributes disproportionately large informational mass toward the adversarial reconstruction process.

In contrast, highly pulverized CNVS configurations preserve elevated residual entropy throughout most compromise regimes. The extreme pulverization scenario ($I_0 = 5$, $\rho_c = 0.001$) exhibits a sharply

delayed reconstruction transition, indicating that informational dispersion significantly suppresses adversarial convergence.

The introduction of residual Shannon entropy (H_{res}) fundamentally changes the interpretation of the defensive barrier. Reconstruction is no longer treated as a deterministic threshold phenomenon, but instead emerges from the gradual erosion of informational uncertainty combined with probabilistic inferential reconstruction.

The observed reconstruction dynamics further demonstrate that reconstruction probability depends not only on direct fragment acquisition, but also on the adversary's capacity to infer missing informational structure through correlated fragment analysis.

Importantly, the observed collapse behavior is not generated by any hardcoded Byzantine threshold or externally imposed compromise limit. The transition instead emerges naturally from the interaction between:

- fragmentation geometry,
- inferential density,
- residual entropy preservation,
- and adversarial observational coverage.

These results support the interpretation of CNVS security as an emergent information-theoretic barrier generated by uncertainty preservation and informational pulverization rather than by static consensus assumptions alone.

Test 7: Adversarial Inferential Accumulation and Residual Entropy Dynamics

Test Name: Extreme CNVS Monte Carlo — K_{adv} and Residual Shannon Entropy Analysis

Objective (Hypothesis)

This simulation represents the first large-scale integration of adversarial inferential accumulation (K_{adv}) and residual Shannon entropy (H_{res}) into the CNVS Monte Carlo validation framework.

Unlike previous simulations, Test 7 introduces an explicit distinction between:

direct fragment acquisition, inferential adversarial expansion, and residual informational uncertainty.

The objective is to evaluate whether CNVS fragmentation maintains effective resistance against unauthorized reconstruction even when attackers progressively accumulate inferential knowledge through dependent fragment correlation.

The simulation investigates how:

informational granularity (I_0), inferential density (ρ_c), and clustered adversarial propagation jointly influence the dissipation of residual uncertainty and the emergence of reconstruction collapse.

Scenarios Evaluated

Five progressively hostile inferential environments were simulated:

- **Scenario A — Coarse Fragmentation**

  Low fragmentation regime characterized by large informational blocks: $I_0 = 100$
  This configuration represents weak pulverization and therefore lower resistance against inferential accumulation.

- **Scenario B — Medium Fragmentation**

  Intermediate fragmentation structure: $I_0 = 50$
  This regime evaluates partial resilience improvement under moderate informational dispersion.

- **Scenario C — High Fragmentation**

  High pulverization configuration: $I_0 = 20$
  The objective is to test whether increasing informational granularity delays adversarial inferential convergence.

• Scenario D — Extreme CNVS Pulverization

Extreme fragmentation regime: $I_0 = 5$
combined with reduced inferential density: $\rho_c = 0.001$.

This scenario models the idealized asymptotic CNVS defensive configuration.

• Scenario E — Inferential Stress Cluster

Adversarial stress-test configuration combining:

- extreme pulverization,
- increased inferential density,
- and clustered inferential amplification.

This scenario intentionally stresses the system under highly correlated inferential propagation dynamics.

Parameters (Input)

- **Global Information Mass:** $I_G = 1000$
- **Informational Granularity:** $I_0 \in \{5, 20, 50, 100\}$
- **Redundancy Factor:** $\lambda = 2$
- **Composite Informational Density:** ρ_c
- **Clustered Inferential Amplification**
- **Progressive physical compromise ratio:** q
- **Monte Carlo stochastic sampling:**
  - high-resolution adversarial trials,
  - inferential propagation,
  - entropy-based reconstruction estimation.

Output Metrics

The simulation continuously measures:

- Probability of complete unauthorized reconstruction: P_{win}
- Direct adversarial knowledge: K_{direct}
- Inferential adversarial knowledge: $K_{inferential}$
- Total adversarial knowledge ratio: K_{adv}
- Residual Shannon entropy: H_{res}

- Inferential propagation probability: P_{infer}
- Entropy-based probabilistic reconstruction: P_{guess}

Expected Behavior (Preliminary Analysis)

The theoretical expectation is that increasing informational pulverization should significantly delay adversarial reconstruction by preserving elevated residual entropy across wider compromise regimes.

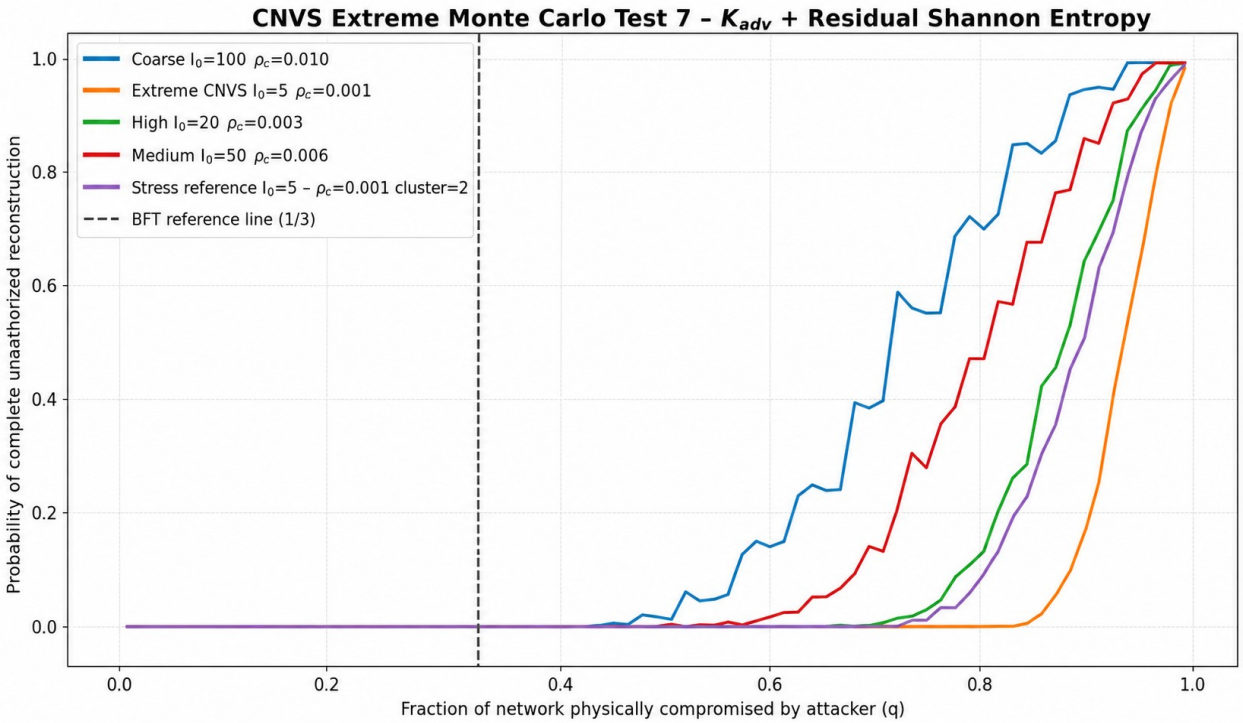
Scenarios characterized by:

- coarse fragmentation,
- elevated inferential density,
- or clustered adversarial propagation
  are expected to accelerate the dissipation of residual uncertainty and increase inferential adversarial knowledge accumulation.

Conversely, highly pulverized CNVS configurations should preserve:

- lower K_{adv}
- higher H_{res}
- and reduced reconstruction probability,
  even under substantial adversarial compromise.

The simulation therefore investigates whether the CNVS defensive barrier can emerge from residual uncertainty preservation rather than from predefined consensus thresholds or externally imposed compromise rules.



[Grafic Outcome K_adv_Res_Entropic and Inferential Test 7 - Python code.png]
GitHub Repository Source Code Link: [K_adv_Res_Entropic and Inferential Test 7 - Python code.TXT]

Analytical Commentary

Test 7 represents the first explicit integration of adversarial inferential accumulation and residual entropy dynamics within the CNVS Monte Carlo validation framework. The simulation moves beyond purely structural fragmentation analysis and explicitly models the interaction between adversarial inferential accumulation and residual informational uncertainty.

The resulting reconstruction curves demonstrate a strong dependency between informational granularity and reconstruction resilience. Coarse fragmentation environments ($I_0 = 100$) display accelerated adversarial convergence and earlier reconstruction collapse, while highly pulverized configurations significantly delay successful unauthorized reconstruction.

The observed reconstruction dynamics suggest that fragmentation acts directly on the preservation of residual uncertainty. High-pulverization environments maintain elevated residual entropy substantially longer, thereby suppressing the adversary's ability to probabilistically reconstruct the complete informational structure.

Simultaneously, the adversarial knowledge metric (K_{adv}) demonstrates that inferential accumulation grows progressively as compromise increases, but its growth rate depends heavily on the fragmentation geometry and inferential density of the system.

The clustered inferential stress scenario further confirms that increased inferential coupling accelerates entropy dissipation and adversarial convergence. However, even under highly hostile inferential conditions, complete reconstruction remains improbable throughout most of the compromise domain and rises sharply only near extreme adversarial coverage.

Importantly, the collapse behavior does not emerge from predefined Byzantine thresholds or hardcoded reconstruction limits. The transition instead arises naturally from the interaction between:

- residual entropy erosion,
- inferential accumulation,
- fragment granularity,
- and adversarial observational coverage.

These results support the interpretation of CNVS security as an emergent information-theoretic phenomenon driven by uncertainty preservation and fragmentation geometry rather than by static quorum assumptions alone.

Test 8: Weighted Inferential Entropy and Graph Propagation Analysis

Test Name: Graph-Weighted Residual Entropy and Inferential Knowledge Dynamics

Objective (Hypothesis)

This simulation extends the previous entropy-based CNVS validation framework by introducing graph-dependent inferential propagation combined with heterogeneous informational weighting.

The objective of the test is to evaluate how residual uncertainty dissipates when fragments are no longer treated as isolated statistical units, but instead become locally connected through semantic dependency structures capable of supporting inferential propagation.

Unlike the earlier parametric simulations, this test formally introduces:

- weighted fragment importance,
- local graph-based inferential spread,
- adversarial inferential accumulation (K_{adv}),
- and residual Shannon entropy erosion (H_{res}).

The experiment investigates whether complete unauthorized reconstruction remains improbable even when attackers progressively exploit topological dependencies between informational fragments.

Scenarios Evaluated

Four progressively hostile inferential environments were simulated:

• Scenario A — Uniform Low Graph Inference

Uniform fragment weights with weak inferential propagation and sparse semantic connectivity.

• Scenario B — Weighted Moderate Graph Inference

Moderately heterogeneous fragment weights combined with intermediate graph inferential density.

• Scenario C — High Pulverization Low Inference

Extreme informational fragmentation ($I_0 \downarrow$) combined with low inferential propagation capability.

• Scenario D — High Pulverization Stress Graph (composite)

Maximum stress configuration combining:

- high pulverization,

- elevated inferential density,
- stronger semantic connectivity,
- and heterogeneous informational weighting.

This final scenario represents the adversarial stress-test regime of the simulation.

Key Parameters (Input)

- **Global Information Mass:** $I_G=1000$,
- **Informational Granularity:** $I_0 \in \{5, 20\}$
- **Redundancy Factor:** $\lambda = 2$
- **Composite Informational Density:** ρ_c
- **Heterogeneous Informational Weights:** $\omega(D_i)$
- **Graph Connectivity:**
  - sparse semantic adjacency,
  - moderate inferential topology,
  - stress graph propagation.
- **Inferential Propagation Dynamics:**
  - local neighborhood inference,
  - iterative propagation rounds,
  - weighted inferential expansion.

Output Metrics

The simulation continuously measures:

- Probability of complete unauthorized reconstruction: P_{win}
- Weighted adversarial inferential knowledge: K_{adv}
- Weighted residual Shannon entropy: H_{res}
- Inferential propagation intensity
- Residual fragment uncertainty
- Topology-dependent reconstruction acceleration

Expected Behavior (Preliminary Analysis)

The theoretical expectation is that graph connectivity and inferential density should progressively accelerate adversarial knowledge accumulation without requiring any predefined reconstruction threshold.

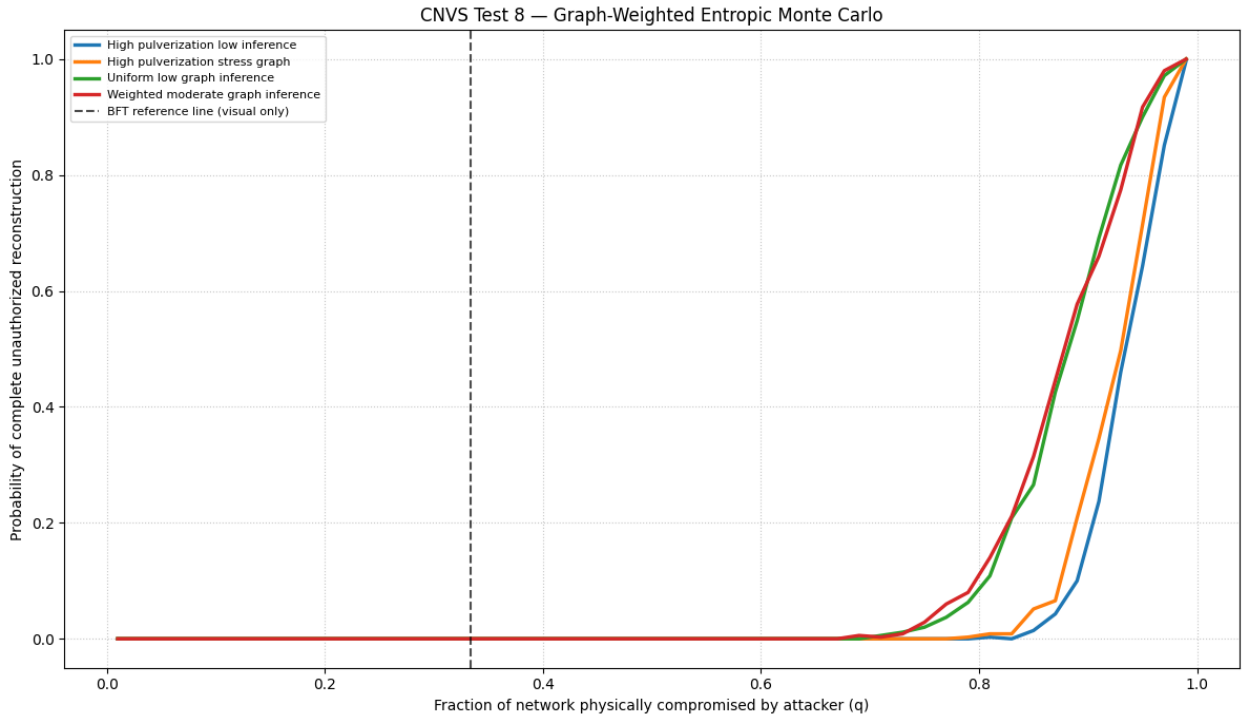
Highly fragmented environments with weak inferential coupling are expected to preserve elevated residual entropy for most compromise regimes, while dense inferential topologies should accelerate:

- local propagation,
- entropy dissipation,
- and weighted adversarial knowledge growth.

However, even under stress-graph conditions, complete unauthorized reconstruction should remain statistically negligible until residual uncertainty approaches critical exhaustion.

This test therefore investigates whether CNVS security emerges from the interaction between:

- fragmentation,
- inferential locality,
- graph topology,
- weighted informational asymmetry,
- and residual entropy preservation,
  rather than from externally imposed consensus thresholds or hardcoded compromise limits.



[Grafic Outcome Weighted Inferential Entropy and Graph Propagation Test 8.png]
GitHub Repository Source Code Link: [Weighted Inferential Entropy and Graph Propagation Test 8 - Python code.TXT]

Analytical Commentary

Test 8 represents the first fully graph-weighted entropic validation of the CNVS framework. Unlike previous simulations based primarily on statistical independence assumptions, this model introduces explicit inferential dependency between fragments through semantic graph propagation.

The resulting reconstruction curves demonstrate that unauthorized reconstruction remains negligible across most tested compromise regimes, even under progressively hostile inferential conditions. The transition toward successful reconstruction emerges only when adversarial coverage approaches near-total compromise of the informational structure.

The weighted adversarial knowledge metric (K_{adv}) reveals that graph connectivity accelerates inferential accumulation progressively rather than discontinuously. Scenarios characterized by stronger inferential topology and heterogeneous fragment weighting display earlier growth of adversarial knowledge, confirming the structural role of graph-dependent propagation.

Simultaneously, the residual entropy curves (H_{res}) demonstrate a gradual dissipation of informational uncertainty driven by both physical fragment acquisition and local inferential expansion. Highly fragmented environments preserve elevated entropy substantially longer, while stress-graph environments accelerate entropy erosion through increased semantic reachability.

Importantly, the reconstruction transition does not emerge from any predefined Byzantine threshold or hardcoded collapse parameter. The observed behavior instead arises naturally from the interaction between:

- graph topology,
- inferential propagation,
- informational weighting,
- residual uncertainty,
- and adversarial knowledge accumulation.

These results suggest that the CNVS defensive barrier may be interpreted as an emergent information-theoretic phenomenon generated by fragmentation geometry and inferential locality rather than by static quorum assumptions alone.

Test 9: Topological Inferential Propagation and Residual Entropy Dynamics

Test Name: Dependent Graph Reconstruction and Entropic Dissipation Analysis

Objective (Hypothesis)

This simulation extends the CNVS framework beyond statistically independent fragmentation models by introducing explicit topological dependencies between fragments. The objective is to evaluate how graph connectivity, local inferential propagation, and weighted residual entropy jointly influence the probability of complete unauthorized reconstruction.

Unlike the previous parametric tests, the system is no longer modeled as a collection of isolated fragments. Instead, fragments are embedded into dependent semantic graph structures where local knowledge may probabilistically propagate across adjacent informational regions.

The test investigates whether the CNVS security barrier remains structurally resilient under increasingly connected inferential environments, and whether reconstruction collapse emerges naturally from the interaction between:

- graph topology,
- inferential propagation,
- adversarial weighted knowledge accumulation (K_{adv}),
- and residual Shannon entropy dissipation (H_{res}).

Graph Structures Evaluated

Three distinct topological regimes were simulated:

• Test 9a — Sparse Dependent Graph

Low-connectivity informational topology characterized by weak inferential adjacency and reduced propagation capability.

• Test 9b — Small-World Dependent Graph

Intermediate topology inspired by realistic distributed systems, where local clustering coexists with limited long-range inferential shortcuts.

• Test 9c — Dense Dependent Graph

Highly connected semantic topology designed as a stress-test environment maximizing inferential propagation and adversarial reconstruction capability.

Key Parameters (Input)

- **Global Information Mass:** $I_G = 1000$,
- **Informational Granularity:** $I_0 = 5$,
- **Redundancy Factor:** $\lambda = 2$,

- **Composite Informational Density:** ρ_c
- **Heterogeneous Fragment Weights** $(\omega(D_i))$
- **Local Inferential Propagation Dynamics**
- **Graph Topology Variations:**
    - Sparse
    - Small-world
    - Dense
- **Monte Carlo Trials:**
    - High-resolution stochastic sampling across progressive compromise ratios q

Output Metrics

The simulation continuously measures:

- Probability of complete unauthorized reconstruction: P_{win}
- Weighted Adversarial Inferential Knowledge: K_{adv}
- Residual Shannon Entropy: H_{res}
- Inferential propagation dynamics across graph neighborhoods
- Topology-dependent collapse acceleration

Expected Behavior (Preliminary Analysis)

The expected behavior of the system is strongly topology-dependent.
Sparse graphs should preserve high residual entropy for longer compromise intervals due to limited inferential propagation between adjacent fragments. In contrast, dense semantic graphs are expected to accelerate adversarial knowledge accumulation by increasing local inferential reachability, thereby producing faster entropy dissipation and earlier reconstruction collapse.

The simulation is specifically designed to verify whether the CNVS defensive barrier emerges without introducing predefined reconstruction thresholds or hardcoded Byzantine consensus limits.

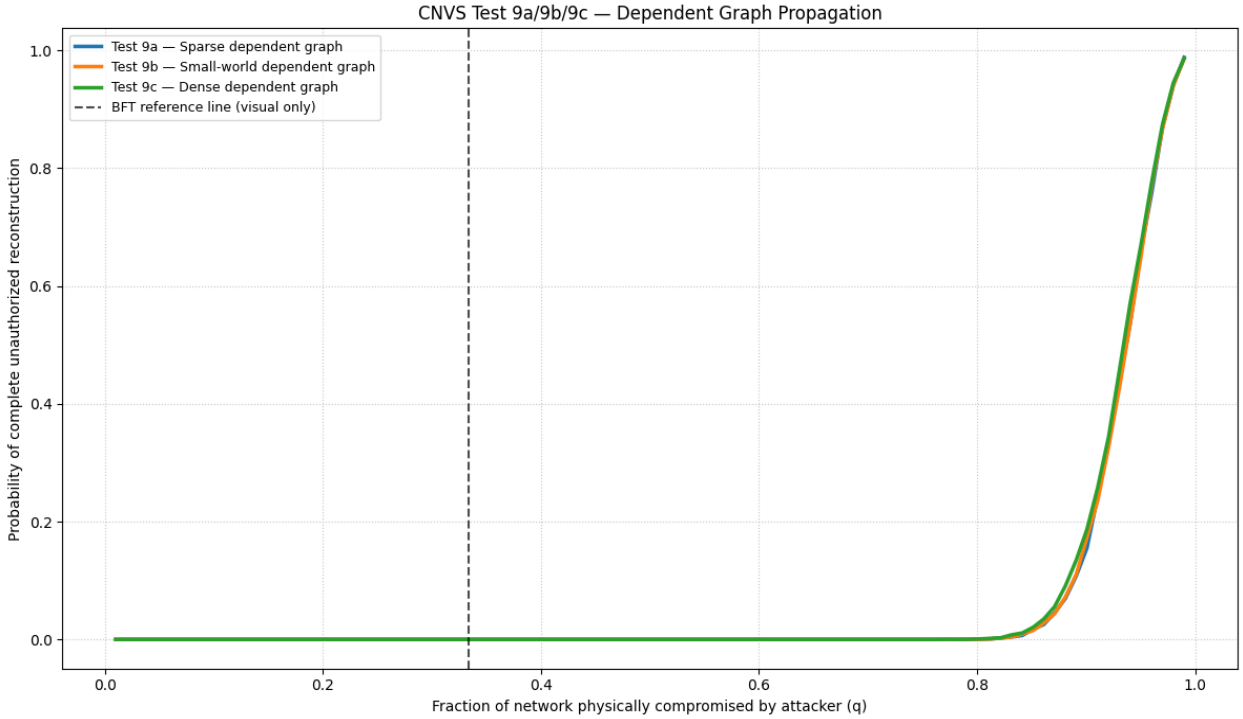
Instead of relying on externally imposed compromise conditions, complete unauthorized reconstruction can only emerge through:

- direct fragment acquisition,
- probabilistic inferential propagation,
- and progressive residual entropy erosion.

The theoretical expectation is therefore that:

- H_{res} decreases progressively as graph connectivity increases,
- K_{adv} accumulates faster in highly connected semantic environments,
- and reconstruction probability remains negligible until residual uncertainty becomes critically small.

This test represents the first large-scale topological validation of the CNVS framework under dependent inferential conditions.



[Grafic Outcome Dependent Graph Propagation Test 9abc - Python code.png]
GitHub Repository Source Code Link: [Dependent Graph Propagation Test 9abc - Python code.TXT]

Analytical Commentary

Test 9 introduces a substantial methodological transition from independent statistical fragmentation toward topology-dependent inferential dynamics. Instead of modeling fragments as isolated informational units, the simulation embeds them into semantic graph structures capable of supporting local inferential propagation.

The resulting curves demonstrate that graph topology directly influences the adversarial reconstruction dynamics. Sparse graph structures maintain elevated residual entropy and slower adversarial knowledge accumulation across most compromise regimes, while dense graph environments accelerate inferential propagation and entropy dissipation.

Importantly, the observed reconstruction transition is not triggered by predefined compromise thresholds or externally imposed Byzantine limits. The collapse behavior instead emerges progressively from the interaction between residual entropy erosion, weighted adversarial knowledge accumulation, and local graph-dependent inferential propagation.

The residual entropy curves (H_{res}) reveal that fragmentation acts directly on the preservation of uncertainty as the attacker gains progressively larger observational coverage of the network. Simultaneously, the weighted adversarial knowledge metric (K_{adv}) demonstrates that highly connected graph topologies significantly amplify inferential acquisition even before full physical compromise occurs.

Despite these increasingly hostile inferential environments, the probability of complete unauthorized reconstruction remains negligible throughout the majority of the compromise domain and rises sharply only under extreme adversarial coverage conditions approaching near-total network compromise.

These results suggest that the CNVS defensive barrier may emerge not from fixed quorum assumptions, but from the interaction between fragmentation granularity, inferential locality, residual entropy preservation, and the topology of informational dependency itself.

Repository & Source Code Access

All Python simulation scripts and high-resolution graphical outcomes referenced in this report are publicly available for download and independent reproduction in the official Golden Protocol Nexus repository at the following URL:

https://github.com/massimocomitato-author/golden-protocol-nexus/tree/main/Code%20and%20Outcome%20CNVS%20on%20Test%20Monte%20Carlo

END DOCUMENT

Author: Massimo Comitato
Italy (EUR), 27-05-2026