Author Rebuttal

Rebuttal to Reviewer gVe4

We sincerely thank the reviewer for the thorough, thoughtful, and technically grounded evaluation of our manuscript. We greatly appreciate the recognition of the novelty of the proposed GAN-based anomaly detection framework, particularly the innovative feature extraction mechanism, the incorporation of expert-informed regularization, and the inclusion of comprehensive ablation studies. These observations directly align with the core technical contributions of the paper, and we are grateful for the reviewer's careful engagement with our work.

To provide clarity and transparency, we respond below to all comments and questions raised. We also explicitly indicate where each concern has been addressed in the revised manuscript.

Appreciation of Strengths Identified

We are grateful to the reviewer for acknowledging:

- The novel GAN-based feature extraction strategy, including the use of quantum-simulated embeddings to capture higher-order correlations relevant to camouflage attacks.
- The methodologically grounded integration of discriminator loss with expert-designed regularization, namely the Angle-of-Incidence Optimization (AIO) and squared residual constraints.
- The inclusion of a full ablation study, which strengthens empirical validation and isolates the contribution of each model component.

These elements—QVAL, AIO, and TET—constitute the primary methodological contributions of this work, and we appreciate the reviewer's recognition of their significance.

Responses to Identified Weak Points

1. Clarity and Rigor of Presentation

We thank the reviewer for this important observation and fully agree that clarity and rigor can be improved. In the revised manuscript, we have made the following changes:

- Simplified complex sentence structures and replaced unconventional terminology with standard language used in GAN and IDS literature.

- Added an intuition-driven explanation of the quantum embedding (QVAL), clarifying how it captures higher-order, non-linear feature interactions relevant to camouflage attacks.
- Explicitly detailed the generator and discriminator architectures, including layer sizes, activations, and training parameters.
- Clarified the training protocol, explicitly stating that the model is trained on benign traffic and that no full retraining is assumed during deployment.

These revisions improve rigor without altering the underlying methodology.

2. Marginal Improvements over Classical GANs

We appreciate the reviewer's careful comparison with classical GAN baselines. While headline accuracy gains are necessarily small due to near-saturation performance regimes, we clarify that:

- The primary contribution is robustness and stability, not raw accuracy.
- Improvements are statistically significant, supported by paired tests and large effect sizes.
- Ablation results demonstrate that each proposed component contributes consistently to robustness, even when headline metrics appear saturated.

This clarification is explicitly stated at the end of Section 1 (Introduction) and reinforced in Section 4.2.

3. Baselines and Benchmarks

We thank the reviewer for highlighting the need for stronger baseline clarity. In the revised manuscript:

- A dedicated benchmarking subsection has been added describing the dataset, its relevance to polymorphic attacks, and its limitations.
- All baselines are explicitly defined, including how the classical GAN baseline is obtained by disabling QVAL, AIO, and TET.
- FGSM and PGD are clearly positioned as robustness stress tests, not competing anomaly detectors.

This ensures transparency, reproducibility, and fair comparison.

4. Temporal Dynamics and Evolving Threats

We appreciate this important feedback. The revised manuscript now explicitly clarifies that:

- The Temporal Evolution Tracking (TET) mechanism does not model arbitrary or population-level dataset drift.
- TET is designed to capture adversarial evolution relative to a stable benign centroid.

- Temporal regularization operates on sequential deviations from the benign reference rather than treating samples independently.

This clarification appears in Section 2, immediately after Equation (5), preventing overclaiming and ensuring correct interpretation.

5. Formatting and CPAIOR Compliance

We acknowledge the formatting issue and appreciate the reviewer's understanding. The camera-ready version will fully comply with CPAIOR and LNCS guidelines. This issue does not affect the technical validity of the work.

Responses to Explicit Rebuttal Questions

Q1: Are QVAL, AIO, and TET original contributions?

Yes. All three components are original contributions introduced in this work:

Component	Purpose
QVAL	Captures high-order, non-linear feature interactions
AIO	Detects geometric camouflage and directional drift
TET	Models slow adversarial evolution relative to a benign centroid

Their non-interchangeability is demonstrated through ablation, where removing AIO or TET results in the largest degradation in performance.

Q2: More Details on Quantum Embeddings (QVAL)

The quantum embedding mechanism uses variational quantum circuits simulated on classical hardware. Classical features are encoded using parameterized rotation gates, followed by entanglement layers that enable representation of non-linear, high-order correlations. The resulting embeddings reshape the adversarial loss landscape, improving convergence stability and robustness rather than raw accuracy. Additional intuition and circuit design rationale are included in Section 3.1.

Q3: More Details on Baselines and Benchmarks

A standard network traffic benchmark associated with contemporary polymorphic attacks is used. Baselines include a classical GAN and all ablated variants of the proposed model. Evaluation employs multiple performance metrics and paired statistical validation consistent with current IDS literature. These clarifications are presented in Section 4.2.

Integration of Reviewer-Requested Clarifications

All reviewer concerns are now explicitly mapped in the manuscript as follows:

- Temporal scope clarification: Section 2 (after Equation 5)

- Baseline definition: Section 2 (Equation 2)
- QVAL, AIO, TET justification: Section 3 and Section 4.2
- Ablation and statistical validation: Tables 3 and 4
- Robustness framing: Introduction and Section 4.2
- Decision logic: Section 3.3
- Adversarial benchmarking: Section 4.2

Final Remarks

We sincerely thank the reviewer for the time, expertise, and constructive feedback invested in this review. While we acknowledge that improvements in clarity, framing, and presentation were necessary, we believe that the fundamental methodological contributions are sound, original, and now clearly articulated. All concerns raised have been carefully addressed through targeted revisions, additional explanations, and reproducible code.

We also extend our gratitude to the Program Chairs, Area Chairs, and Reviewers for the opportunity to strengthen this work. The revised manuscript reflects their guidance and significantly improves clarity, rigor, and transparency.