Network Management Research Group
Internet-Draft
Intended status: Informational
Expires: 6 December 2026

R. Brown
April Labs

June 2026

Constrained Manifold Inference Engine (CMIE): A Research Problem for Deterministic AI-Network Resilience
draft-april-cmie-research-problem-00

Abstract

This document identifies a gap in current AI-native network architectures: the absence of a real-time, hardware-accelerated validation function that checks AI-generated intents against physical causality constraints, including Transmission Time Interval (TTI) bounds, thermal limits, and topological admissibility. We propose the Constrained Manifold Inference Engine (CMIE) as a candidate architectural function and outline research challenges for its implementation on edge Neural Processing Units (NPUs). This work is motivated by the International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) Focus Group on AI Native for Telecommunication Networks (FG-AINN) Gap Analysis (FG-AINN-O-024) and the related liaison statements between FG-AINN and the IETF Operations and Management Area Working Group (OPSAWG).

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 6 December 2026.

Copyright Notice

Table of Contents

1. Introduction

The increasing deployment of autonomous AI agents in telecommunications networks has created a class of operational risk that existing architectures are not equipped to handle. When an AI orchestrator generates a network reconfiguration intent, there is currently no standardized, pre-execution mechanism to verify that the proposed action is consistent with the physical constraints of the underlying hardware and transmission medium. This gap can result in catastrophic cascading failures, as documented in [ITU-UNDRR].

This document articulates the research problem and proposes the Constrained Manifold Inference Engine (CMIE) as a logical network function to address it. The CMIE is intended to sit between AI orchestrators and physical network controllers, providing a hardware-anchored admissibility check before any intent is executed.

The scope of this document is limited to identifying the research gap, describing the proposed architectural function at a high level, and enumerating the key research challenges that must be addressed before practical deployment is feasible. It does not propose new protocols or IANA registrations.

The rest of this document is organized as follows. Section 2 describes the gap in existing architectures and motivating scenarios. Section 3 defines the proposed CMIE function and its inputs and outputs. Section 4 enumerates the research challenges. Section 5 situates the work relative to existing IETF activities. Section 6 addresses security and trust considerations.

1.1. Terminology

The following terms are used in this document:

AI-native network: A network architecture in which autonomous AI agents have operational authority to reconfigure network resources in real time without mandatory human approval for each action.

Intent: A goal-oriented directive issued by an AI orchestrator describing a desired network state or configuration change, expressed in a machine-readable schema (e.g., YANG models or an intent description language).

Post-Threshold Telemetry State (PTTS): A formalized network link condition wherein primary communication objectives are suspended due to performance degradation, but the link is actively repurposed by the network to extract and utilize residual physical measurements (e.g., pilot drift, timing displacement) as a primary distributed environmental sensing resource.

Deterministic Physical Degradation State (DPDS):A mathematically predictable, environment-specific profile of channel attenuation, phase-shift, and polarization changes, serving as a continuous, hardware-rooted authentication and sensing metric independent of stochastic error rates (e.g., traditional SNR or QBER thresholds).

Admissible manifold: The subspace of possible network configurations that simultaneously satisfy all active physical constraints (TTI, thermal, topological, and latency).

Recursive Topological Consistency (RTC): A network control paradigm wherein global physical manifold admissibility constraints are continuously projected downward to govern local routing, beamforming, and error-correction decisions, ensuring that distributed optimizations do not violate the global stability of the network topology.

Constrained Manifold Inference Engine (CMIE):
An AI-native network function or validation layer that evaluates stochastic AI/ML outputs, sensor fusion data, or intent translations against hard causal limits (e.g., latency, Transmission Time Interval [TTI], and Doppler bounds) and discrete spatial priors, systematically pruning and rejecting physically impossible network states prior to execution.

Unified Coordination State Vector (UCSV): The output artifact of the

RTC process: a structured representation of the current feasibility boundaries, consumable by orchestrators, controllers, and audit systems.

2. Problem Statement

2.1. Gap in Existing Network Architectures

Modern AI-native networks (e.g., those under study in ITU-T SG13/FG-AINN and 3GPP SA5) rely on autonomous agents to reconfigure network resources in real time. However, current architectures lack a standardized mechanism to validate whether an AI-generated intent (e.g., a traffic rerouting decision) respects fundamental physical causality, including:

* Transmission Time Interval (TTI) bounds,

* thermal degradation limits of radio and backhaul links,

* topological admissibility under partial failure, and

* latency budgets for closed-loop control.

The ITU-T FG-AINN Gap Analysis [FG-AINN-O-024] identifies this as multiple related gaps: GS14 (absence of a unified architecture), G8-1 (lack of traceability for AI decisions), and G9 (undefined accountability framework). The analysis concludes that no existing standard from IETF, 3GPP, or ETSI defines a pre-execution validation function that bridges the gap between stochastic AI inference and deterministic physical constraints.

2.2. Motivating Scenarios

Consider a compound stress event (e.g., an extreme heatwave coinciding with peak grid load). As links cross their nominal performance thresholds:

* An AI orchestrator, optimizing for Quality of Service (QoS), may generate an intent to reroute critical traffic through a thermally degraded path.

* Without a validation layer, the network would attempt to execute this intent, causing a cascading collapse (the "invisible failure" described in [ITU-UNDRR]).

* Post-failure logs cannot recover the lost services; the damage is already done.

What is missing is a real-time, hardware-anchored function that can reject infeasible intents before they reach the physical network controllers, while simultaneously providing an auditable trace of why a particular intent was denied.

3. Proposed Architectural Function: CMIE

This document proposes the Constrained Manifold Inference Engine (CMIE) as a logical network function that addresses the above gap. The CMIE is designed to be deployed on edge Neural Processing Units (NPUs) to meet sub-10ms latency requirements.

3.1. Input State Spaces

The CMIE consumes three classes of input state:

(1) Deterministic Physical Degradation State (DPDS)

Extracted from post-threshold telemetry (e.g., phase drift, attenuation profiles) when links enter a Post-Threshold Telemetry State (PTTS). This provides a deterministic, hardware-rooted ground truth of physical limits.

(2) Network Topology and TTI State

Real-time constraints from RAN, backhaul, and core network, including synchronization bounds and remaining time budgets for closed-loop actions.

(3) AI Intent and Policy State

Proposals generated by autonomous orchestrators (e.g., Non-RT RIC, intent-based networking controllers), expressed in a common schema (e.g., YANG models or an intent description language).

3.2. Core Inference Operation

The CMIE evaluates the AI intent against the physical state using a hybrid discrete-continuous constraint solver. The solver determines whether the proposed configuration lies within the admissible manifold defined by:

* TTI synchronization windows,

* thermal safety margins,

* topological connectivity constraints, and

* maximum allowable latency for critical services.

If the intent is admissible, the CMIE issues a signed Admissibility Certificate to the network controllers. If the intent violates any constraint, the CMIE rejects the proposal and triggers a deterministic fallback (e.g., a pre-validated degraded-mode service profile).

3.3. Output: Recursive Topological Consistency (RTC)

Upon rejection or modification, the CMIE projects the physical constraints downward to all local AI agents. This process, called Recursive Topological Consistency (RTC), ensures that every agent operates with a globally consistent view of what is physically feasible. The output is a Unified Coordination State Vector (UCSV) that can be consumed by orchestrators, controllers, and audit systems.

4. Research Challenges

The following research challenges must be addressed to enable practical CMIE deployment.

4.1. Real-Time Constraint Solving on Edge NPUs

Formulating physical causality into a mathematical structure that can be solved within sub-10ms TTI bounds is non-trivial. Initial experiments suggest that mixed-precision integer inference, implemented on NPU architectures (e.g., those optimized for graph-based constraint solving), is a promising direction. Research is needed on:

* efficient encoding of TTI and thermal constraints as differentiable or linearizable forms,

* hardware-aware solver design for edge NPUs, and

* trade-offs between solver accuracy and latency.

4.2. Telemetry Extraction in Degraded States

The PTTS concept requires extracting Deterministic Physical Degradation Signatures from highly attenuated or noisy pilot signals. This may require new physical-layer signal processing techniques that operate without full demodulation.

4.3. Multi-Agent Conflict Resolution

When a CMIE rejects an intent, local AI agents may resist the imposed constraints (e.g., by repeatedly submitting similar infeasible proposals). Research is needed on:

* stable coordination protocols between the CMIE and multiple agents,
* escalation and human-in-the-loop procedures for deadlock situations, and
* distributed CMIE instances that maintain global consistency across domains.

5. Relationship to Existing IETF Work

The CMIE concept complements and extends several IETF activities:

* IETF NMRG (Network Management Research Group): provides a natural home for the research challenges identified above.
* IETF ANIMA (Autonomic Networking Integrated Model and Approach): the CMIE could serve as a validation layer for autonomic functions described in ANIMA.
* IETF OPSAWG (Operations and Management Area Working Group): a liaison from ITU-T FG-AINN [IETF-LS] (May 2026) already invites collaboration on AI-native network operations.

This document does not propose protocol changes; it identifies a research gap that, if filled, could inform future protocol work (e.g., extensions to YANG models, new RPCs for intent validation).

6. Security Considerations

The CMIE is designed to improve the security and resilience of AI-native networks. However, as a new architectural function interposed between AI orchestrators and physical network controllers, it also introduces a set of security considerations that must be addressed before deployment.

6.1. Security Benefits

The CMIE provides several security and trust properties:

* It prevents hallucinated or adversarially manipulated reconfigurations from reaching the physical network, reducing the attack surface for AI-layer exploits.

* It provides an auditable trail of rejected intents, including the specific physical constraints that caused each rejection, directly addressing the accountability gaps (G9) identified in [FG-AINN-O-024].

* When implemented on trusted execution environments or NPUs with attestation capabilities, the CMIE can provide hardware-rooted trust for the constraint evaluation function.

6.2. Threats and Open Problems

The following threat categories are identified as requiring attention in future specifications based on this research problem statement:

Telemetry integrity attacks: An adversary with access to physical-layer measurement systems could forge or manipulate the Physical Degradation State (DPDS) data fed to the CMIE. If the CMIE is presented with falsified telemetry indicating that a degraded path is healthy, it may issue an Admissibility Certificate for an infeasible configuration. Mitigations (e.g., cryptographic attestation of telemetry, anomaly detection on DPDS streams) are out of scope for this document and must be addressed in future work.

Constraint solver poisoning: If the CMIE's constraint definitions or policy state are updatable at runtime, an adversary could modify them to either over-restrict feasible intents (denial of service) or under-restrict infeasible ones (bypass). The integrity and provenance of constraint definitions must be protected, for example through signed policy updates and a change-control process.

Denial of service via solver exhaustion: An adversary controlling one or more AI agents could submit a high volume of complex, near-boundary intents, exhausting the CMIE's computational budget and delaying or blocking the evaluation of legitimate intents. Rate limiting and computational quotas per agent are candidate mitigations.

Multi-agent coordination attacks: As described in Section 4, local

agents may repeatedly resubmit rejected intents. In an adversarial context, colluding agents could use this behavior to probe the constraint space and infer sensitive information about the physical state of the network. Escalation and human-in-the-loop procedures should be designed with this threat in mind.

Admissibility Certificate forgery: If the signed certificates issued by the CMIE are not properly validated by downstream controllers, an adversary could present a forged certificate to bypass the validation function entirely. Future protocol work should define the certificate format, signing algorithm, and validation procedures.

Detailed treatment of these threats, including threat modeling, attack trees, and mitigation specifications, is out of scope for this research problem statement and must be addressed in subsequent documents.

7. IANA Considerations

This document has no IANA actions.

8. References

8.1. Normative References

8.2. Informative References

[FG-AINN-O-024]
ITU-T Focus Group on AI Native for Telecommunication Networks (FG-AINN), "Standardization Gap Analysis of the FG-AINN", Output Document FG-AINN-O-024, ITU-T, Geneva, May 2026.

[IETF-LS] ITU-T Focus Group on AI Native for Telecommunication Networks (FG-AINN), "Liaison Statement to IETF OPSAWG on Completion of FG-AINN Vocabulary Deliverable", Liaison Statement LS-FG-AINN-OPSAWG-2026-05, ITU-T, Geneva, May 2026.

[ITU-UNDRR]
International Telecommunication Union (ITU) and United Nations Office for Disaster Risk Reduction (UNDRR), and Sciences Po Technology and Global Affairs Innovation Hub, "When Digital Systems Fail: The Hidden Risks of Our Digital World", ITU/UNDRR/Sciences Po Joint Report, Geneva, May 2026, <https://www.itu.int/hub/publication/s-rep-wtisd-2026/>

Author’s Address

Ricardo Brown
April Labs
Hong Kong
Email: info@aprillabs.xyz