Hop-History Relay and Byzantine Custody Chain

by Nick Clark | Published April 25, 2026

What Hop History Records

Each device that relays a governed mesh message appends an entry to the message's hop-history field. The entry includes: the relaying device's identifier (its credentialed device hash), the timestamp of relay, the device's signature over the message-plus-prior-history, and any relay-specific metadata (reception channel, signal strength, geographic location for credentialed-position-bearing relays).

The history accumulates as the message propagates. A message that traveled through three relays has a hop history of three signed entries. The history is part of the message's verifiable structure: receiving units evaluate every entry's signature against the credentialing chain.

Why Path Evaluation Adds What Origin Evaluation Misses

Origin evaluation answers 'who said this' but not 'how did it reach me.' For most non-adversarial use cases, this is sufficient. For adversarial use cases (defense mesh, contested-environment commercial deployment, critical-infrastructure messaging), the path matters. A valid message from a trusted origin that arrives via an adversarial relay is operationally suspect even though origin authentication passes.

Adversarial relays may delay messages, replay messages, or alter messages within their physical scope. Origin authentication doesn't detect any of these without path information. Hop-history evaluation does: a message whose hop history shows a known-adversarial relay or whose hop pattern is structurally unusual triggers elevated scrutiny in the receiving system's admissibility evaluation.

How Adversarial Relays Self-Disclose

When an adversarial device participates in mesh relay, it has two structural options: append a valid hop record (with its own credential, signature, and timestamp) or modify the message and produce an invalid signature chain. The first option discloses the adversary's presence at a specific point in the network. The second option causes signature-chain validation to fail at the next legitimate relay.

The architecture forces adversaries to choose between disclosure and detection. Sophisticated adversaries may choose disclosure (operate openly within the mesh while attempting to influence message routing) — but this is itself useful operational information. Less sophisticated adversaries fail signature-chain validation and their tampering is rejected at protocol level.

What This Enables for Mesh Resilience

Mesh networks can identify reliable propagation routes through historical hop-history analysis. Routes that consistently produce unmolested messages gain weight; routes with frequent signature failures or adversarial-appearing relays lose weight. The architecture supports adaptive routing without exposing routing decisions to adversarial manipulation.

Forensic reconstruction of mesh events benefits from the architectural path information. After-event analysis can trace exactly how a message propagated, when

each hop occurred, and what each relay's state was. The patent positions the primitive at the layer that mesh-network forensics and adaptive-routing both require.