Hop-History Relay

by Nick Clark | Published April 25, 2026

What Hop-History Records

The hop-history field accumulates as a message propagates. Each relaying device appends an entry containing the relaying device's credential, the timestamp of relay, the device's signature over the message-plus-prior-history, and any relay-specific metadata (signal strength, geographic location for credentialed-position-bearing relays, reception channel).

The history is part of the message's verifiable structure. A receiver evaluates every entry's signature against the credentialing chain, producing a verified path record.

Why Path Information Matters Operationally

Origin authentication answers 'who said this' but not 'how did it reach me.' For non-adversarial use cases, this is sufficient. For adversarial deployment (defense mesh, contested-environment commercial operation, 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.

Hop-history evaluation produces diagnostic information that origin-only evaluation does not. 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); less sophisticated adversaries fail signature-chain validation and their tampering is rejected at protocol level.

What This Enables for Adaptive Routing

Routes that consistently produce unmolested messages gain weight in the receiving system's routing assessment; routes with frequent signature failures or adversarial-appearing relays lose weight. The architecture supports adaptive mesh routing without exposing routing decisions to adversarial manipulation.

Forensic reconstruction benefits from the architectural path information. After-event analysis can trace exactly how a message propagated. The patent positions the primitive at the layer that mesh-network forensics requires.