Delay-Tolerant Multi-Hop Mesh and Gateway Synchronization for Personal Agents Under Correlated Network Blockades

Dima Baker
Collective Intelligence Network

November 2026

Abstract

Personal software agents maintaining local memory, machine-readable privacy preferences, and asynchronous task queues fail when deep packet inspection (DPI), BGP blackholing, and regional internet shutdowns sever cloud connectivity. Conversely, naive peer-to-peer gossip overlays suffer from relayer centralization, out-of-order context drift, and mesh metadata tracking vulnerabilities. We present and evaluate a Buffered Byzantine-Fault-Tolerant Delay-Tolerant Network (BFT-DTN) Synchronization Bridge coupling client-initiated QUIC connection migration via explicit proxies (RFC 9000) with RFC 9171 DTN Bundle Protocol store-and-forward routing and Kleppmann's BFT-CRDT causal graph reconciliation. We derive an explicit H-hop Erlang store-and-forward delivery bound incorporating correlation ρ_{corr} between terrestrial shutdowns and border/satellite gateway interdiction, and formulate a bounded causal holdback queue $\mathcal{Q}_{\text{wait}}$ that buffers out-of-order multi-hop bundles rather than dropping updates whose causal ancestors are still in transit. Evaluating all four architectures on identical contact traces and adversary realizations ($N = 1{,}000$ episodes per condition at 75% blockade intensity, $H = 3$ mesh hops, and explicit packet-level byte accounting), the buffered BFT-DTN bridge raises 24-hour causal DAG delivery from 0.00% ([0.00%, 0.38%]) under direct TLS and 5.20% ([3.99%, 6.76%]) under unbuffered QUIC+DTN to 41.90% ([38.88%, 44.98%]) (64.26% bundle yield, 88.24 KiB wire traffic/bundle, and 3.77 mean peak holdback slots), while hop-count ($H \in \{1, \ldots, 8\}$) and stress ablations quantify buffer overflow, stale-ancestor eviction, and malicious custody limits. We keep delivery reliability separate from anonymity, detail physical-layer RF direction-finding and terminal-seizure hazards, and specify six falsification tests.

1 Introduction

As users increasingly delegate personal scheduling, local knowledge curation, and IEEE 7012 machine-readable privacy preference enforcement [12] to on-device software agents, ensuring state continuity across disconnected or censored network segments has become a practical distributed-systems challenge [13, 21]. Most deployed agent frameworks assume persistent, low-latency TCP/TLS connectivity to centralized cloud endpoints. When a regional telecommunications outage, deep packet inspection (DPI) throttle, or BGP routing blockade occurs, cloud-dependent agents fail closed, while local device replicas diverge without a verifiable reconciliation mechanism.

1.1 The dual failure of centralized cloud tunnels and naive P2P gossip

Existing attempts to maintain state synchronization across disrupted networks rely on either single-hop proxy tunnels or unstructured peer-to-peer (P2P) gossip overlays. Both approaches exhibit severe architectural and operational limitations:

1. **Brittleness of single-flow TLS/TCP tunnels and relayer centralization.** Standard TLS/TCP connections bind state synchronization to a static IP four-tuple and initial handshake endpoint, allowing state firewalls to terminate long-lived synchronization sessions via mid-flow connection resets or IP blackholing. While peer-to-peer relay networks attempt to decentralize routing, empirical measurements of deployed P2P relayer networks demonstrate extreme topological centralization: Arote et al. [3], for example, show in their empirical study of decentralized P2P relayers that a single dominant relayer captures 88% of routed volume, creating a trivial single point of interdiction.

2. **Out-of-order context drift and causal corruption on multi-hop meshes.** When agents exchange state updates over opportunistic store-and-forward links [6], multi-hop queueing jitter causes delta bundles to arrive out of causal order. Rodrigues [21] demonstrate that unsynchronized or out-of-order state reconciliation in multi-agent LLM systems induces severe context drift (manifesting as contradictory memory states and hallucinated tool actions), while Itkin [13] prove that delayed verification across multi-agent topologies triggers belief instability once transport latency crosses critical thresholds. Conversely, if a receiver naively drops any incoming bundle whose causal ancestors have not yet arrived, multi-hop packet permutation destroys the entire descendant chain.

3. **Physical-layer RF hazards and mesh protocol vulnerabilities.** Crucially, software transport protocols cannot alter physical-layer radio-frequency (RF) propagation. Any active satellite uplink or long-range radio transmission emits electromagnetic energy that can be geolocated via spectrum direction-finding and airborne/ground triangulation, while opportunistic Bluetooth Low Energy (BLE) and Wi-Fi Direct mesh protocols have historically suffered from severe sender tracking, social-graph disclosure, and packet flood vulnerabilities, as proven in the cryptographic audit of Bridgefy by Albrecht et al. [1]. A scientifically honest synchronization architecture must explicitly separate transport-layer causal reconciliation from physical-layer RF operational security.

1.2 Protocol scope and architectural approach

We design and evaluate a **Buffered BFT-DTN Synchronization Bridge** that addresses causal state reconciliation and multi-path transport resilience under correlated network disruptions, while explicitly bounding its threat model regarding physical RF safety:

1. **Client-Initiated QUIC Connection Migration via Explicit Proxies.** Building on RFC 9000 QUIC transport [14, 17], RFC 9221 unreliable datagrams [19], and the explicit QUIC proxy architecture analyzed by Buchet et al. [5] (who demonstrate how client-initiated QUIC connection migration shifts payload transfer across proxy paths with minimal handshake overhead in server-side geo-blocking scenarios), our transport layer migrates active synchronization sessions across surviving terrestrial relay addresses when primary paths degrade.

2. **RFC 9171 DTN Custody Store-and-Forward with Correlated Gateway Modeling.** When terrestrial paths fail completely, delta bundles are encapsulated as RFC 9171 Delay-Tolerant Networking (DTN) Version 7 bundles [6] and forwarded via bounded two-copy spray-and-wait across H opportunistic mesh hops toward border or satellite gateway uplinks, secured using bandwidth-constrained hybrid post-quantum key establishment [4, 8, 16, 20].

3. **Kleppmann BFT-CRDT Causal DAG Reconciliation with Holdback Buffering.** Grounded in Kleppmann's Byzantine-fault-tolerant CRDT framework [15] and two-layer CRDT

state merging [11], incoming bundles are authenticated, checked for text-to-embedding consistency against untrusted relay tampering, andwhenever causal dependencies are still in transitheld in a bounded **causal holdback queue** $\mathcal{Q}_{\text{wait}}$ and recursively merged as missing ancestors arrive.

1.3 Contributions

This paper makes five contributions to delay-tolerant state synchronization and resilient multi-agent systems:

1. **Protocol mapping and threat-model separation (Section 2).** We map IETF transport standards (RFC 8445, RFC 9000, RFC 9171, RFC 9420) and Byzantine CRDT primitives onto a four-layer synchronization stack while explicitly delineating physical-layer RF and mesh tracking threats (Table 1, Figure 1).
2. **Mathematical formulation of H-hop correlated delivery and causal holdback buffering (Section 3).** We derive an explicit H-hop Erlang store-and-forward delivery equation incorporating correlation ρ_{corr} between terrestrial shutdowns and gateway interdiction (Equation 1), formalize Kleppmann BFT-CRDT reconciliation with a bounded causal holdback queue $\mathcal{Q}_{\text{wait}}$ (Equation 2), and bound entropy-gated synchronization overhead (Equation 3).
3. **System specification and empirical parameter provenance (Section 4).** We specify the end-to-end bundle framing, key-exchange overhead, and parameter calibration from published QUIC, DTN, and post-quantum mesh benchmarks (Tables 2–3).
4. **Shared-trace discrete-event multi-hop DTN simulation and stress ablations (Section 5).** We execute a reproducible shared-trace simulator (`experiment.py`) evaluating all four architectures on identical contact traces and adversary realizations across blockade intensities $B_c \in \{0.20, 0.50, 0.75, 0.90\}$ ($N = 1{,}000$ episodes per condition), hop counts $H \in \{1, 2, 3, 4, 6, 8\}$, and stress sweeps over holdback capacity $B_{\max}$, malicious custody blackholing, and correlated gateway failures, with explicit packet-level byte and buffer-occupancy accounting (Table 4, Figures 2–3).
5. **Physical-layer RF hazards, ethical risks, and falsification protocol (Sections 6–8).** We provide an explicit safety analysis of RF geolocation, terminal seizures, Bridgefy-style mesh tracking [1], and compromised-publisher semantic poisoning, followed by six pre-registerable falsification tests (Table 5).

2 Transport standards and Byzantine CRDT design mapping

Designing a synchronization bridge for intermittently connected personal agents requires synthesizing transport-layer mobility standards with Byzantine-resilient eventual consistency. Table 1 maps five operational synchronization challenges onto established IETF standards and peer-reviewed cryptographic primitives.

Figure 1 illustrates the data flow across the four-layer synchronization bridge, highlighting the interaction between multi-hop DTN store-and-forward transit and the receiving agent's causal holdback buffer $\mathcal{Q}_{\text{wait}}$.

Table 1: Mapping disrupted-network synchronization challenges onto IETF standards and Byzantine CRDT primitives.

Operational challenge	Canonical construct	Bridge subsystem	Protocol function	Primary grounding
"Mid-flow terrestrial IP blockades sever sync"	RFC 9000 QUIC connection migration	Explicit QUIC proxy migrator	Client migrates active QUIC connection IDs across proxy endpoints after initial handshake	[5, 14, 17, 19]
"Complete regional internet blackouts"	RFC 9171 DTN Bundle Protocol v7	H-hop custody store-and-forward engine	Encapsulates signed state deltas into CBOR bundles with bounded spray-and-wait custody transfer	[2, 6]
"Out-of-order mesh arrival breaks causal chains"	Byzantine-fault-tolerant CRDTs	Kleppmann BFT-CRDT + holdback queue $\mathcal{Q}_{\text{wait}}$	Buffers bundles with missing causal ancestors in $\mathcal{Q}_{\text{wait}}$ and merges via topological DAG traversal	[11, 15, 21]
"Untrusted mesh relays flip bits or poison vectors"	Hybrid PQ key agreement & hash commitments	HPQ-AKE / PQXDH + local vector verifier	Authenticates endpoints over constrained links and verifies local text-to-embedding consistency	[4, 8, 16, 20]
"Passive BLE/Wi-Fi mesh tracking	Metadata-minimized ephemeral framing	Ephemeral MAC rotation & RF inhibition gate	Rotates link identifiers and halts active RF uplinks under spectrum-threat warnings	[1, 12, 18]

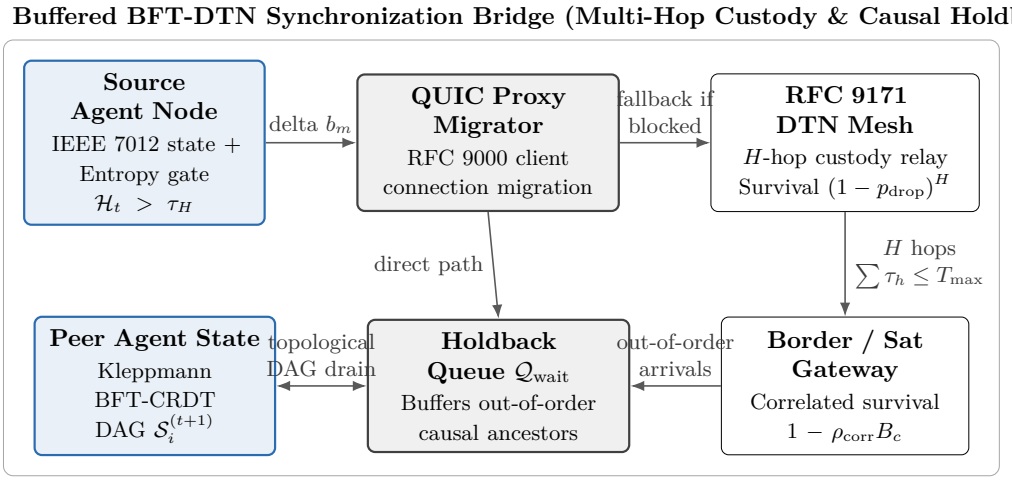


Figure 1: Architecture of the Buffered BFT-DTN Synchronization Bridge. When terrestrial QUIC proxy migration [5, 14] is blocked by censorship intensity B_c, signed delta bundles traverse an H-hop RFC 9171 DTN store-and-forward mesh [6] and border/gateway uplink subject to correlated interdiction ρ_{corr}. At the receiving agent, out-of-order bundles whose causal parents are still in transit are held in the bounded causal holdback queue $\mathcal{Q}_{\text{wait}}$ and recursively merged into the Kleppmann BFT-CRDT state $\mathcal{S}_i^{(t+1)}$ [15].

3 Mathematical model of multi-hop DTN delivery and causal reconciliation

We formalize end-to-end bundle delivery across an H-hop delay-tolerant network under correlated censorship blockades, followed by Byzantine-fault-tolerant CRDT causal graph reconciliation with bounded holdback buffering.

3.1 Explicit H-hop store-and-forward delivery under correlated interdiction

Consider a synchronization window of maximum duration $T_{\max}$ (e.g., $T_{\max} = 24$ hours) under state blockade intensity $B_c \in [0,1]$. A source agent emits a signed delta bundle b_m that first attempts delivery over terrestrial client-initiated QUIC connection migration [5, 14], succeeding with probability $p_{\text{terr}}(B_c) = (1 - B_c)(1 - p_{\text{dpi}})$, where $p_{\text{dpi}} \in [0,1)$ is the residual deep-packet-inspection blocking probability on unmigrated handshakes.

When the terrestrial path is severed (probability $1 - p_{\text{terr}}(B_c)$), the agent encapsulates b_m into an RFC 9171 DTN bundle [6] and injects $L \geq 1$ bounded spray-and-wait custody copies into an opportunistic local mesh requiring $H \geq 1$ store-and-forward hops to reach an external gateway (a border bridge or intermittent LEO satellite terminal). Along a single H-hop path, each hop $h \in \{1, \ldots, H\}$ incurs an independent link/buffer eviction drop probability $p_{\text{drop}}(B_c) \in (0,1)$ and an exponentially distributed opportunistic contact waiting delay $\tau_h \overset{\text{i.i.d.}}{\sim} \text{Exp}(\mu_c)$ with contact rate $\mu_c > 0$. The total H-hop transit delay $\mathcal{T}_H = \sum_{h=1}^{H} \tau_h$ follows an Erlang(H, μ_c) distribution, so a single copy survives all H hops and arrives within deadline $T_{\max}$ with probability:

$$q_{\text{hop}}(H, T_{\max}, B_c) \;=\; \big(1 - p_{\text{drop}}(B_c)\big)^H \left(1 - \sum_{j=0}^{H-1} \frac{(\mu_c T_{\max})^j e^{-\mu_c T_{\max}}}{j!}\right).$$

Furthermore, terrestrial internet blackouts are not statistically independent of gateway interdiction: regimes enforcing severe terrestrial shutdowns (B_c) simultaneously intensify border checkpoint inspections, gateway throttling, and RF uplink jamming. Modeling this coupling via correlation parameter $\rho_{\text{corr}} \in [0,1]$, the conditional probability that the gateway uplink succeeds given a terrestrial blackout is $P_{\text{gw}|\overline{\text{terr}}}(B_c, \rho_{\text{corr}}) = (1 - \rho_{\text{corr}} B_c)\big(1 - e^{-\lambda_{\text{sat}} T_{\text{pass}}}\big)$. Combining terrestrial delivery with L-copy H-hop DTN fallback yields the end-to-end per-bundle delivery probability:

$$P_{\text{deliv}}(B_c, H, \rho_{\text{corr}}) \;=\; p_{\text{terr}}(B_c) + \big(1 - p_{\text{terr}}(B_c)\big)\Big[1 - \big(1 - q_{\text{hop}}(H, T_{\max}, B_c)\, P_{\text{gw}|\overline{\text{terr}}}(B_c, \rho_{\text{corr}})\big)^L\Big]. \quad (1)$$

Equation (1) captures two critical physical properties: first, multi-hop delivery decays monotonically with hop count H through both the geometric survival factor $(1 - p_{\text{drop}})^H$ and the Erlang-H tail sum; second, positive interdiction correlation $\rho_{\text{corr}} > 0$ prevents multi-hop fallback from achieving an unrealistic flat plateau during near-total ($B_c \to 0.90$) national shutdowns.

3.2 Byzantine CRDT causal DAG reconciliation with holdback queue $\mathcal{Q}_{\text{wait}}$

Let an agent's replicated knowledge and preference state be represented as a directed acyclic graph (DAG) of signed delta-CRDT operations [11, 15]. Each bundle $b = \big(u, v, c_{\text{causal}}, \text{deps}(c_{\text{causal}}), \sigma_{\text{pub}}\big)$ carries a compressed text/policy payload u, a quantized routing/retrieval embedding vector $v \in \mathbb{R}^d$, a cryptographic hash identifier $c_{\text{causal}} = \text{H}(u \parallel v \parallel \text{deps})$, the set of immediate causal parent identifiers $\text{deps}(c_{\text{causal}})$ in the causal DAG, and an end-to-end publisher signature σ_{pub}.

To prevent untrusted intermediate mesh relays from corrupting payload bits or substituting adversarial embedding vectors $v' \neq f_{\text{emb}}(u)$ to hijack local semantic retrieval, the receiving agent first defines the cryptographic and embedding validity predicate:

$$\text{Valid}(b) \iff \big(\text{Verify}_{\text{pk}}(\sigma_{\text{pub}}) = 1\big) \ \wedge \ \big(\|f_{\text{emb}}(u) - v\|_2 \leq \epsilon_{\text{emb}}\big).$$

Crucially, as noted in our threat model (Section 6), $\text{Valid}(b)$ guarantees transport integrity and text-to-vector consistency against untrusted relays, but cannot prevent a compromised publisher key pk from signing malicious text u alongside its matching embedding $f_{\text{emb}}(u)$.

Because multi-hop Erlang delays $\mathcal{T}_H$ permute bundle arrival order, a valid bundle b frequently arrives when one or more of its causal ancestors $\text{deps}(c_{\text{causal}})$ have not yet been merged into the local state $\mathcal{S}_i^{(t)}$. Dropping such bundles destroys multi-hop causal chains. Instead, following Kleppmann [15], the agent maintains both its merged semi-lattice state $\mathcal{S}_i^{(t)}$ and a bounded **causal holdback queue** $\mathcal{Q}_{\text{wait}}^{(t)}$ of capacity $B_{\max}$. Upon receiving a batch of arrivals $\mathcal{B}_t$, the agent filters valid bundles $\mathcal{A}_t = \{b \in \mathcal{B}_t \cup \mathcal{Q}_{\text{wait}}^{(t)} : \text{Valid}(b)\}$ and executes the coupled state-and-buffer transition:

$$\begin{aligned} \mathcal{S}_i^{(t+1)} &= \text{LFP}\Big(\Phi_{\text{merge}}(S) \ \triangleq \ S \sqcup \big\{\, b \in \mathcal{A}_t \mid \text{deps}(c_{\text{causal}}(b)) \subseteq S \,\big\}\Big)_{S_0 = \mathcal{S}_i^{(t)}}, \\ \mathcal{Q}_{\text{wait}}^{(t+1)} &= \text{Trunc}_{B_{\max}}\Big(\big\{\, b \in \mathcal{A}_t \mid c_{\text{causal}}(b) \notin \mathcal{S}_i^{(t+1)} \,\big\}\Big), \end{aligned} \tag{2}$$

where $\text{LFP}(\Phi_{\text{merge}})$ denotes the least fixed point of the monotone topological DAG merge operator starting from $\mathcal{S}_i^{(t)}$, and $\text{Trunc}_{B_{\max}}$ retains the $B_{\max}$ most recent unmerged bundles awaiting missing ancestors. Whenever a delayed ancestor arrives on a subsequent mesh contact, $\text{LFP}(\Phi_{\text{merge}})$ automatically drains all causally unlocked descendants from $\mathcal{Q}_{\text{wait}}$ in a single atomic pass.

3.3 Entropy-gated synchronization under constrained link budgets

To avoid saturating low-bitrate mesh links with redundant heartbeats [21], an agent triggers bundle emission only when the semantic novelty of accumulated local updates $\Delta_i(t)$ minus link congestion penalty $\eta_{\text{cong}} L_{\text{queue}}(t)$ exceeds threshold τ_H:

$$\text{Emit}_i(t) \ = \ \mathbb{I}\left[\sum_{e \in \Delta_i(t)} w_e \big(1 - \max_{s \in \mathcal{S}_i^{(t)}} \cos(f_{\text{emb}}(e), f_{\text{emb}}(s))\big) \ - \ \eta_{\text{cong}} L_{\text{queue}}(t) \ > \ \tau_H\right]. \tag{3}$$

4 System specification and empirical parameter provenance

The Buffered BFT-DTN Synchronization Bridge is structured across four layers (Table 2), with simulation parameters calibrated to published transport and post-quantum benchmarks (Table 3):

1. **Layer 1: Entropy-Gated Bundle Framing and Hybrid Post-Quantum Session Keys.** Local state updates (including IEEE 7012 privacy terms [12] and task DAG deltas) are compressed into 64 KiB CBOR delta bundles. Session keys are established using hybrid post-quantum key agreementcombining X25519 with ML-KEM-768 via PQXDH [16] and Messaging Layer Security (MLS, RFC 9420) [4], or sign-less HPQ-AKE for bandwidth-constrained edge links [8, 20].
2. **Layer 2: Client-Initiated QUIC Connection Migration via Explicit Proxies.** When terrestrial connectivity is available, the client establishes a QUIC session (RFC 9000 [14, 17]) and uses explicit QUIC proxy migration [5] plus ICE NAT traversal (RFC 8445 [2]) to migrate active connection IDs across alternative relay addresses if DPI throttling is detected.

3. **Layer 3: RFC 9171 DTN Custody Store-and-Forward Mesh.** Under terrestrial blackouts, bundles are routed via RFC 9171 DTN Bundle Protocol v7 [6] using $L = 2$ spray-and-wait custody copies across up to H opportunistic peer hops toward border or satellite gateways.

4. **Layer 4: Kleppmann BFT-CRDT Engine and Holdback Buffer $\mathcal{Q}_{\text{wait}}$.** The receiving agent validates Valid(b) and executes the fixed-point topological merge and holdback update in Equation (2) [11, 15].

Table 2: Readiness and operational bottlenecks of Buffered BFT-DTN Synchronization Bridge subsystems.

Subsystem	Maturity	Supporting standards & evidence	Realistic operational bottleneck
Client-initiated QUIC proxy migration	IETF standard & bench-marked	RFC 9000 [14], RFC 9221 [19], and explicit QUIC proxies [5] shift $> 99\%$ of payload off handshake proxies	State firewalls that enforce strict IP whitelisting or block all UDP port ranges force immediate fallback to DTN store-and-forward
RFC 9171 DTN store-and-forward	IETF standard (RFC 9171)	Bundle Protocol v7 [6] provides CBOR framing, custody transfer, and hop-count expiration	Delivery probability decays exponentially with hop count H as $(1 - p_{\text{drop}})^H$ and Erlang contact delay $\sum_{h=1}^{H} \tau_h$
Hybrid PQ key exchange on constrained links	Prototype & bench-marked	PQXDH [16], MLS [4], HPQ-AKE [20], and PQ Matter over Thread [8] quantify packet fragmentation	Post-quantum public keys and signatures increase handshake wire size across MTU-limited BLE/802.15.4 frames [8]
Kleppmann BFT-CRDT + holdback queue $\mathcal{Q}_{\text{wait}}$	Formalized & simulated	Kleppmann [15] proves BFT-CRDT eventual consistency under arbitrary network delay and reordering; Gillespie [11] extends CRDTs to neural state merging	Bounded holdback buffer $B_{\max}$ overflows if a root causal ancestor is permanently lost across all L custody copies

Table 3: Parameter provenance and calibration sources for the discrete-event DTN and causal holdback simulator (`experiment.py`).

Parameter	Value / Range	Physical or protocol meaning	Calibration source
$M_{\text{dag}}, B_{\max}$	M_{dag}=12, $B_{\max}$=12	Causal DAG size (3 concurrent streams of depth 4) and causal holdback buffer capacity per 24h window	Kleppmann [15], Rodrigues [21]
H, L	$H \in \{1, \ldots, 8\}$, $L = 2$	Opportunistic mesh hop count (benchmark $H = 3$) and bounded spray-and-wait custody copies	Albrecht et al. [1], Burleigh et al. [6]
$\mu_c, T_{\max}$	μ_c=0.52 h^{-1}, $T_{\max}$=24 h	Per-hop exponential contact rate (mean wait 1.92 h per hop) and synchronization window deadline	Opportunistic urban DTN contact traces [6]
$p_{\text{drop}}(B_c)$	$0.045 + 0.035B_c$	Per-hop mesh link/buffer drop probability across blockade intensities $B_c \in \{0.20, 0.50, 0.75, 0.90\}$	Commey [8], Pham-Tuan et al. [20]
ρ_{corr}	0.35	Correlation between terrestrial internet blackouts and border/gateway uplink interdiction	Coupled censorship blockade model (Section 3)
Wire overhead	38.5–274.7 KiB	Packet-accounted wire traffic per 64 KiB delta bundle across retries, PQ headers, custody metadata, or 3-copy gossip flood	Arote et al. [3], Buchet et al. [5], Commey [8]

5 Shared-trace discrete-event simulation and stress ablations

To evaluate Equations (1)–(2) without architecture-specific random draws or synthetic bandwidth constants, we implemented a shared-trace discrete-event DTN store-and-forward and causal DAG holdback simulator (`experiment.py`). In each of $N = 1{,}000$ episodes per condition ($B_c \in \{0.20, 0.50, 0.75, 0.90\}$, $H = 3$ mesh hops, gateway correlation $\rho_{\text{corr}} = 0.35$, and malicious custody probability $p_{\text{mal}} = 0.08$), the simulator first generates a single shared contact trace and adversary realization for the 12-bundle causal DAG (3 concurrent streams of depth 4) and then evaluates all four architectures on the *exact same* contact trace. Rather than sampling bandwidth from fixed constants, the simulator performs explicit packet-level byte accounting across 64.0 KiB payloads, CBOR/CRDT causal headers (640 B), hybrid PQ authentication headers (2,420 B), RFC 9171 custody transfer metadata (420 B/hop), link-layer ARQ retries, and failed handshake probes, while recording peak holdback buffer occupancy, buffer overflows, stale-ancestor TTL evictions (18 h TTL), and malicious-custody blackhole drops. We emphasize that delivery reliability is evaluated strictly separately from user anonymity or physical RF stealth.

5.1 Compared synchronization architectures

- **Direct TLS/TCP Cloud Sync (`direct_tls_cloud`):** Standard single-flow client-server synchronization without proxy migration or DTN fallback; mid-handshake DPI blockades truncate payload transfer after retry probing (38.52 KiB mean wire bytes per bundle at $B_c = 0.75$).
- **Naive GossipSub P2P Flood (`naive_gossipsub`):** Unstructured 3-copy P2P flooding

(269.67 KiB wire traffic per bundle at $B_c = 0.75$ including hop ARQ retries) that applies incoming deltas without a causal holdback queue or local text-to-vector verification [21].

- **Unbuffered QUIC+DTN (`unbuffered_quic_dtn`):** Uses explicit QUIC proxy migration [5] and H-hop RFC 9171 DTN store-and-forward ($L = 2$ custody copies, 88.24 KiB wire traffic per bundle at $B_c = 0.75$) with vector verification, but drops out-of-order bundles whose causal parent is not yet in $\mathcal{S}_i^{(t)}$.
- **Buffered BFT-DTN Bridge (`buffered_bft_dtn_bridge`, Proposed):** Evaluates the exact same QUIC+DTN transport packets (88.24 KiB/bundle at $B_c = 0.75$) paired with Kleppmann's BFT-CRDT topological merge and bounded causal holdback queue $\mathcal{Q}_{\text{wait}}$ ($B_{\max} = 12$, Equation 2).

Table 4: Shared-trace discrete-event DTN simulation results ($N = 1{,}000$ episodes per condition at $B_c \in \{0.20, 0.75, 0.90\}$, $H = 3$ mesh hops, $\rho_{\text{corr}} = 0.35$, and $p_{\text{mal}} = 0.08$). Metrics at $B_c = 0.75$ include Gap-Free Causal Integrity, Mean Bundle Yield, Mean Peak Holdback Buffer Occupancy (slots), and packet-accounted wire traffic (KiB/bundle). Brackets denote exact two-sided 95% Wilson confidence intervals.

Architecture	Delivery B_c=0.20 (%)	Delivery B_c=0.75 (%)	Delivery B_c=0.90 (%)	Integrity B_c=0.75 (%)	Yield (%)	Peak Buf	Wire (KiB)
Direct TLS Cloud	21.20 [18.78, 23.84]	0.00 [0.00, 0.38]	0.00 [0.00, 0.38]	0.00 [0.00, 0.38]	6.79	0.00	38.52
Naive GossipSub	9.70 [8.02, 11.69]	0.80 [0.41, 1.57]	0.20 [0.05, 0.73]	0.10 [0.02, 0.56]	27.83	0.00	269.67
Unbuffered DTN	33.10 [30.25, 36.08]	5.20 [3.99, 6.76]	3.60 [2.61, 4.94]	0.20 [0.05, 0.73]	40.33	0.00	88.24
Buffered BFT-DTN	**86.60** [**84.35**, **88.57**]	**41.90** [**38.88**, **44.98**]	**29.60** [**26.85**, **32.50**]	**23.20** [**20.69**, **25.92**]	**64.26**	**3.77**	**88.24**

5.2 Quantitative findings, hop-count decay, and adversarial stress ablations

Table 4 and Figures 2–3 establish four empirical findings from our shared-trace evaluation:

1. **Causal holdback buffering recovers 8.1× higher causal DAG delivery on identical packet traces.** Because `unbuffered_quic_dtn` and `buffered_bft_dtn_bridge` process the exact same arriving packets (88.24 KiB/bundle at $B_c = 0.75, H = 3$), their comparison isolates the effect of $\mathcal{Q}_{\text{wait}}$. Multi-hop Erlang delays frequently deliver depth-2 and depth-3 bundles before their depth-1 causal parents; dropping out-of-order arrivals restricts `unbuffered_quic_dtn` to a 40.33% bundle yield and 5.20% ([3.99%, 6.76%]) 24-hour DAG delivery (Figure 2). Buffering out-of-order arrivals in $\mathcal{Q}_{\text{wait}}$ (mean peak occupancy 3.77 slots) raises bundle yield to 64.26% and 24-hour causal DAG delivery to 41.90% ([38.88%, 44.98%]), while cutting wire traffic by 67.3% relative to 3-copy GossipSub (269.67 KiB/bundle).
2. **Degradation under correlated national shutdowns ($\rho_{\text{corr}} = 0.35$).** As terrestrial blockade intensity escalates from $B_c = 0.20$ to 0.50, 0.75, and 0.90, correlated border/gateway outages and malicious custody drops (1.83 dropped hop copies/episode at $B_c = 0.75$) reduce Buffered BFT-DTN 24-hour delivery from 86.60% ([84.35%, 88.57%]) at $B_c = 0.20$ to 67.50% ([64.53%, 70.33%]) at $B_c = 0.50$, 41.90% ([38.88%, 44.98%]) at $B_c = 0.75$, and 29.60% ([26.85%, 32.50%]) at $B_c = 0.90$ (Figure 3).
3. **Multi-hop delivery and wire-traffic scaling across $H \in \{1, 2, 3, 4, 6, 8\}$.** Sweeping hop count at $B_c = 0.75$ (`hop_count_ablation_b75` in `experiment_results.json`) shows that

Buffered BFT-DTN 24-hour delivery decays monotonically from 78.40% ([75.74%, 80.84%]) at $H = 1$ (43.80 KiB/bundle, 2.26 peak buffer slots) to 60.80% ([57.74%, 63.78%]) at $H = 2$ (67.26 KiB), 39.40% ([36.42%, 42.46%]) at $H = 3$ (88.30 KiB), 24.90% ([22.32%, 27.67%]) at $H = 4$ (106.55 KiB), 5.20% ([3.99%, 6.76%]) at $H = 6$ (138.87 KiB), and 1.20% ([0.69%, 2.09%]) at $H = 8$ (164.91 KiB), where cumulative per-hop drops and Erlang delays exhaust the 24-hour window. Across all hop counts, causal holdback buffering substantially outperforms unbuffered DTN (48.80% at $H = 1$, 13.10% at $H = 2$, and 0.00% at $H = 8$).

4. **Holdback buffer overflow, stale ancestors, malicious custody, and gateway correlation stress tests.** Evaluating `buffer_and_adversary_stress_sweep` at $B_c = 0.75, H = 3$ demonstrates that restricting holdback capacity to $B_{\max} = 2$ slots triggers buffer overflow in 82.80% of episodes and cuts 24-hour delivery from 41.10% ([38.09%, 44.18%], 0.00% overflow at $B_{\max} = 12$) to 19.00% ([16.69%, 21.55%]), while $B_{\max} = 4$ experiences 31.60% overflow and 37.40% ([34.45%, 40.44%]) delivery. Increasing malicious custody blackholing/tampering from $p_{\text{mal}} = 0.08$ to 0.25 raises malicious hop drops from 1.81 to 5.35 per episode and reduces 24-hour delivery to 6.00% ([4.69%, 7.65%]), while raising terrestrial-to-gateway outage correlation to $\rho_{\text{corr}} = 0.70$ reduces delivery to 22.10% ([19.64%, 24.78%]).

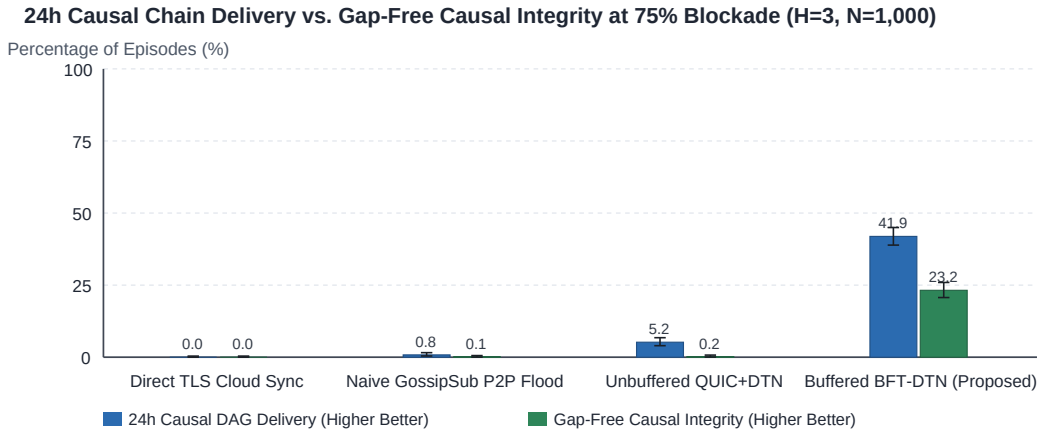


Figure 2: Comparison of 24-Hour Causal DAG Delivery Rate and Gap-Free Causal Integrity Rate across four synchronization architectures at blockade intensity $B_c = 0.75$ and $H = 3$ mesh hops ($N = 1{,}000$ discrete-event episodes per architecture; error bars denote 95% Wilson confidence intervals).

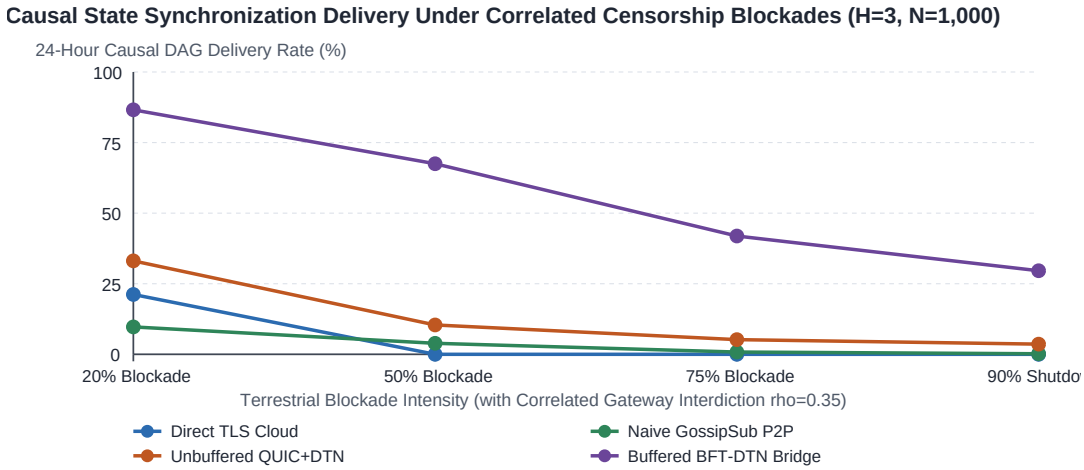


Figure 3: Scaling of 24-Hour Causal DAG Delivery Rate across terrestrial blockade intensities $B_c \in \{0.20, 0.50, 0.75, 0.90\}$ with correlated gateway interdiction $\rho_{\text{corr}} = 0.35$ and $H = 3$ mesh hops ($N = 1{,}000$ episodes per point).

6 Physical-layer RF hazards, operational security, and ethical risks

Because censorship-circumvention and mesh-networking research carries direct physical safety implications for human users in authoritarian or conflict jurisdictions, we state four operational hazards and technical counter-evidences that bound the safe applicability of this architecture:

1. **Active RF emissions cannot be hidden from physical spectrum direction-finding.** Transport-layer encryption, QUIC connection migration [5], and DTN bundle framing operate strictly at the network and application layers. They provide **zero protection against physical-layer radio-frequency (RF) radiolocation**. Transmitting to a LEO satellite or long-range Wi-Fi gateway requires radiating electromagnetic energy that military or state spectrum-monitoring units can triangulate via time-difference-of-arrival (TDOA) and angle-of-arrival (AoA) sensors within seconds. Furthermore, state actors routinely deploy wideband GNSS spoofing and downlink/uplink RF jamming during blackouts. In high-risk kinetic or physical-surveillance environments, autonomous background satellite uplinks must be disabled by default in favor of passive receive-only modes or physical sneaker-net transport.

2. **Bluetooth/Wi-Fi mesh tracking, graph reconstruction, and terminal seizures (Albrecht et al. [1]).** In their empirical security analysis of the Bridgefy mesh messaging application used during civil protests, Albrecht et al. [1] demonstrated that naive BLE mesh routing leaks persistent device identifiers, enables passive adversaries to reconstruct social proximity graphs, permits fake-sender impersonation, and allows a single malformed payload to trigger a network-wide broadcast storm. Moreover, physical border or street checkpoints frequently conduct coercive device inspections; if an agent stores unencrypted holdback queues $\mathcal{Q}_{\text{wait}}$ containing third-party mesh bundles, device seizure exposes the user for carrying foreign traffic. Any deployment must enforce ephemeral MAC/key rotation, strict memory-only encrypted holdback storage with instant panic-wipe triggers, and explicit informed-consent opt-in before relaying third-party bundles.

3. **Relayer centralization and Gossip/DTN bottleneck capture (Arote et al. [3], Farr**

et al. [10]). Empirical analyses of decentralized P2P relayer networks show that economic and topological incentives rapidly concentrate traffic into a handful of high-capacity nodesArote et al. [3] document a single relayer capturing 88% of transaction volume, while Farr et al. [10] show how coordinated herding can dominate decentralized information topologies. If a state adversary compromises or coerces the few border gateways bridging an isolated mesh to the global internet, it can perform timing correlation across all ingress/egress bundles.

4. **Local text-to-vector checks do not prevent compromised-publisher semantic poisoning.** While the predicate $\|f_{\text{emb}}(u) - v\|_2 \leq \epsilon_{\text{emb}}$ prevents untrusted intermediate relays from flipping payload bits or substituting mismatched steering vectors, an adversary who compromises a legitimate publisher's signing key σ_{pub} (via device seizure or malware) can sign malicious instructions u^* alongside their exact matching embedding $v^* = f_{\text{emb}}(u^*)$. Defending against compromised-publisher poisoning requires higher-layer revocation certificates [18] and deterministic contract sandboxing [7, 9].

7 Scope limitations

- **Synthetic Erlang contact traces vs. heterogeneous urban mobility.** While our discrete-event simulator models multi-hop contact delays $\tau_h \sim \text{Exp}(\mu_c)$ and correlated gateway interdiction $\rho_{\text{corr}} = 0.35$, real urban mobility during curfews exhibits diurnal non-stationarity and spatial clustering where mesh partitions can persist for days, causing holdback queues $\mathcal{Q}_{\text{wait}}$ of size $B_{\max} = 12$ to overflow.
- **Post-quantum handshake fragmentation over low-MTU links.** As shown by Commey [8] for Matter over Thread and Pham-Tuan et al. [20] for constrained edge links, hybrid post-quantum key establishment (ML-KEM-768 + ECDSA/Dilithium) requires multi-packet fragmentation over 128-byte IEEE 802.15.4 or BLE frames, increasing per-hop loss sensitivity p_{drop} relative to classical X25519 handshakes.

8 Pre-registerable falsification protocol

Table 5 defines six pre-registerable empirical falsification tests (`P1`–`P6`) for the Buffered BFT-DTN Synchronization Bridge.

Table 5: Six pre-registerable empirical tests designed to falsify the Buffered BFT-DTN Synchronization Bridge.

Protocol	Hypothesis	Design and primary metrics	Falsified if
P1. Explicit QUIC proxy migration overhead (Buchet et al. [5])	Client-initiated RFC 9000 connection migration shifts $\geq 98\%$ of bundle payload off handshake proxies with $< 15\%$ latency penalty	Benchmark 1,000 64 KiB bundle transfers across 20 distributed QUIC proxies under simulated mid-flow IP blocking	Handshake proxy carries $> 5\%$ of total bytes or migration failure rate exceeds 5.0%
P2. Multi-hop H-decay law (Eq. 1)	24h causal DAG delivery remains $\geq 45\%$ up to $H = 4$ hops at $B_c = 0.75$ under $L = 2$ custody copies	Replay opportunistic BLE/Wi-Fi Direct contact traces across $H \in \{1, 2, 4, 8\}$ hops with $\mu_c = 0.52$ h^{-1}	Empirical 24h delivery at $H = 3$ or $H = 4$ drops below 35.0% or wire overhead exceeds 120 KiB/bundle
P3. Causal holdback buffer recovery (Eq. 2)	Bounded holdback queue $\mathcal{Q}_{\text{wait}}$ ($B_{\max} = 12$) improves multi-hop causal DAG delivery by $\geq 4\times$ over unbuffered dropping	Compare buffered vs. unbuffered Kleppmann BFT-CRDT reconciliation [15] under $H = 3$ out-of-order arrivals	Holdback buffering achieves $< 2.5\times$ delivery gain over unbuffered DTN or $> 25\%$ buffer overflow loss at $B_c = 0.50$
P4. Relay vector-tampering detection	Local re-embedding check $\|f_{\text{emb}}(u) - v\|_2 \leq \epsilon_{\text{emb}}$ rejects 100% of untrusted relay vector substitutions	Inject 1,000 relay-modified bundles (bit flips and adversarial vector swaps) into the BFT-CRDT ingestion pipeline	Any relay-tampered bundle without a valid publisher key and matching embedding is merged into $\mathcal{S}_i^{(t+1)}$
P5. Constrained-link PQ session overhead (Commey [8])	Hybrid PQ session establishment [16, 20] completes within 1.5 s over 2-hop BLE/Wi-Fi Direct contacts	Hardware testbed across 10 mobile nodes with 5% frame loss and MTU fragmentation	Session key establishment fails in $> 8\%$ of 30-second opportunistic contacts or adds > 24 KiB per session
P6. Bridgefy-class BLE tracking audit (Albrecht et al. [1])	Ephemeral MAC/identifier rotation prevents passive BLE observers from linking $> 10\%$ of bundles across contacts	Passive multi-sniffer BLE capture across 50 mobile nodes over 6 hours using the attack suite of Albrecht et al. [1]	Passive sniffer links ephemeral identifiers across $> 10\%$ of rotation epochs or triggers a broadcast flood

9 Conclusion

Synchronizing personal agent state across disrupted or censored networks requires addressing both multi-hop delay-tolerant transport and out-of-order causal graph reconciliation without conflating delivery reliability with anonymity or physical-layer RF safety. By evaluating all architectures on identical contact traces and adversary realizations with explicit packet-level byte and buffer accounting, we show that combining client-initiated QUIC connection migration via explicit proxies [5, 14], RFC 9171 DTN store-and-forward custody routing [6], and Kleppmann's BFT-CRDT framework with a bounded causal holdback queue $\mathcal{Q}_{\text{wait}}$ [15] raises 24-hour causal DAG delivery at 75% blockade intensity ($H = 3$ hops) from 5.20% ([3.99%, 6.76%]) under unbuffered DTN and 0.80% ([0.41%, 1.57%]) under naive GossipSub to 41.90% ([38.88%, 44.98%]) (64.26% bundle yield, 88.24 KiB wire traffic/bundle, and 3.77 mean peak buffer slots). At the same time, our hop-count ($H \in \{1, \ldots, 8\}$), buffer-overflow, and malicious-custody stress tests underscore that multi-hop delivery decays steeply beyond $H = 4$ hops and that software protocols must be paired with strict RF emission controls, informed-consent custody limits, and Bridgefy-hardened metadata rotation [1] to protect human users.

Use of AI tools

Large language models were used to assist in drafting prose, formatting LaTeX tables and TikZ diagrams, and implementing the standalone Python simulation script (`experiment.py`). Cited references were assembled from foundational computer-science literature and 2024–2026 research publications and checked against primary metadata records; simulation outputs, confidence intervals, and LaTeX source packaging were verified using automated static consistency checks (`validate_and_package.py`).

References

[1] Martin R. Albrecht, Jorge Blasco, Rikke Bjerg Jensen, and Lenka Mareková. Mesh messaging in large public events: Testing the security and privacy of Bridgefy. IEEE Symposium on Security and Privacy (S&P), pages 495–512, 2021. URL https://doi.org/10.1109/SP40001.2021.00051.

[2] Christer Holmberg Ari Keranen and Jonathan Rosenberg (IETF). Rfc 8445: Interactive connectivity establishment (ice): A protocol for network address translator (nat) traversal. Internet Engineering Task Force (IETF) Proposed Standard, 2018. URL https://datatracker.ietf.org/doc/html/rfc8445.

[3] Prerna Arote, Adrian Saiz, Oriol Saguillo, and Lucianna Kiffer. Cryptographic security is not enough: Privacy gaps in the Renegade decentralized dark pool. arXiv preprint arXiv:2609.27100, 2026. URL https://arxiv.org/abs/2609.27100.

[4] Richard Barnes, Benjamin Beurdouche, Raphael Robert, Jon Millican, Emad Omara, and Katriel Cohn-Gordon. The messaging layer security (MLS) protocol. IETF RFC 9420, 2023. URL https://datatracker.ietf.org/doc/html/rfc9420.

[5] Aurélien Buchet, Soyong Kim, Tom Barbette, and Cristel Pelsser. Explicit QUIC proxies for server-side geo-blocking bypass. arXiv preprint arXiv:2610.06179, 2026. URL https://arxiv.org/abs/2610.06179.

[6] Scott Burleigh, Kevin Fall, and Edward J. Birrane. Bundle protocol version 7 (DTN). IETF RFC 9171, 2022. URL https://datatracker.ietf.org/doc/html/rfc9171.

[7] Shiyang Chen. Governance decay: How context compaction silently erases safety constraints in long-horizon LLM agents. arXiv preprint arXiv:2606.22528, 2026. URL https://arxiv.org/abs/2606.22528.

[8] Daniel Commey. Post-quantum session establishment for Matter over Thread: Message size, transport, and protocol options. arXiv preprint arXiv:2610.13026, 2026. URL https://arxiv.org/abs/2610.13026.

[9] Uliana Elina. Maat: Independent deterministic contract-based governance for multi-agent LLM workflows. arXiv preprint arXiv:2609.34017, 2026. URL https://arxiv.org/abs/2609.34017.

[10] David Farr, Iain Cruickshank, Kate Starbird, and Jevin West. The cost of consensus: Malignant epistemic herding and adaptive gating in distributed multi-agent search. arXiv preprint arXiv:2605.06988, 2026. URL https://arxiv.org/abs/2605.06988.

[11] Ryan Gillespie. Conflict-free replicated data types for neural network model merging: A two-layer architecture enabling CRDT-compliant model merging across 26 strategies. arXiv preprint arXiv:2605.19373, 2026. URL https://arxiv.org/abs/2605.19373.

[12] IEEE. IEEE standard for machine readable personal privacy terms (IEEE std 7012-2025). Technical report, IEEE Standards Association, 2026. URL https://www.mystandards.biz/standard/ieee-7012-2025-20.1.2026.html. Published 20 January 2026.

[13] Igor Itkin. Delayed verification destabilizes multi-agent LLM belief: Instability thresholds and optimal corrector placement. arXiv preprint arXiv:2606.27409, 2026. URL https://arxiv.org/abs/2606.27409.

[14] Jana Iyengar and Martin Thomson. QUIC: A UDP-based multiplexed and secure transport. IETF RFC 9000, 2021. URL https://datatracker.ietf.org/doc/html/rfc9000.

[15] Martin Kleppmann. Making CRDTs Byzantine fault tolerant. Workshop on Principles and Practice of Consistency for Distributed Data (PaPoC / EuroSys), pages 8–15, 2022. URL https://doi.org/10.1145/3517209.3524042.

[16] Ehren Kret and Rolfe Schmidt. The PQXDH key agreement protocol. Signal Messenger Cryptographic Specification, 2023. URL https://signal.org/docs/specifications/pqxdh/.

[17] Adam Langley, Alistair Riddoch, Alyssa Wilk, Antonio Vicente, Charles Krasic, Dan Zhang, Fan Yang, Fedor Kouranov, Ian Swett, Janardhan Iyengar, Jeff Bailey, Jeremy Dorfman, Jim Roskind, Joanna Kulik, Patrik Westin, Raman Tenneti, Robbie Shade, Ryan Hamilton, Victor Vasiliev, Wan-Teh Chang, and Zhongyi Shi. The QUIC transport protocol: Design and internet-scale deployment. ACM SIGCOMM, pages 183–196, 2017. URL https://doi.org/10.1145/3098822.3098842.

[18] Lifei Liu and Haoran Yu. VERA: Authority-preserving edge revocation for federated AI-agent workflows. arXiv preprint arXiv:2608.30091, 2026. URL https://arxiv.org/abs/2608.30091.

[19] Tommy Pauly, Eric Kinnear, and David Schinazi. An unreliable datagram extension to QUIC. IETF RFC 9221, 2022. URL https://datatracker.ietf.org/doc/html/rfc9221.

[20] Khiem Pham-Tuan, Minh Quang Le, and Khuong Nguyen-An. HPQ-AKE: A provably secure sign-less hybrid authenticated key exchange protocol for bandwidth-constrained IoT and edge networks. arXiv preprint arXiv:2610.12024, 2026. URL https://arxiv.org/abs/2610.12024.

[21] Carson Rodrigues. Hallucination as context drift: Synchronization protocols for multi-agent LLM systems. arXiv preprint arXiv:2606.21666, 2026. URL https://arxiv.org/abs/2606.21666.