LifeLink: Resilient Mesh Communication in Contested Environments via Semantic Compression and Economic Asymmetry

The LifeLink Team
Stanford TreeHacks 2026
raghavt3@illinois.edu
tkoduru@umich.edu
rninamdar@wpi.edu
vdaita@stanford.edu

Abstract

In modern conflict zones and disaster scenarios, civilians face a dual threat: the physical destruction of infrastructure and the active suppression of wireless communications. Adversaries increasingly deploy jamming to deny Wi-Fi/Cellular connectivity and GPS spoofing to disrupt navigation. We present **LifeLink**, a decentralized communication architecture designed for these Anti-Access/Area Denial (A2/AD) environments. By utilizing LoRa (915 MHz) hardware, we bypass high-frequency jamming, but incur severe bandwidth constraints. To solve this, we introduce *Semantic Compression*—an edge-AI triage system that reduces natural language to 25-byte payloads. We further demonstrate that LifeLink creates an "Asymmetric Cost Exchange," where the financial and tactical cost to jam the network effectively exceeds the cost of deployment by orders of magnitude.

1 Introduction: The Spectral Denial Problem

Standard emergency communication systems rely on two assumptions: reliable high-bandwidth backhaul (Cellular/Wi-Fi) and reliable positioning (GPS). In contested environments, both assumptions fail.

1.1 The Jamming Threat Model

1. **High-Frequency Denial:** 2.4GHz and 5GHz bands (Wi-Fi) are easily attenuated by walls and effectively jammed by low-cost wide-band interrupters.

2. **GNSS Denial:** GPS signals are weak (-125 dBm) and susceptible to spoofing or jamming, rendering standard location-sharing apps useless.

To address this, LifeLink shifts the physical layer to LoRa (Long Range) at 915 MHz. This lower frequency offers superior penetration through urban obstacles and is significantly harder to jam without high-power military-grade equipment. However, this shift reduces available bandwidth from Megabits/sec to roughly 300 bits/sec. This physical constraint necessitates our primary contribution: *Semantic Compression*.

2 The Economics of Suppression

A key design goal of LifeLink is to leverage the asymmetry of cost between the *suppressor* (the jammer) and the *communicator* (the node). We utilize Commodity-Off-The-Shelf (COTS) hardware (≈$5/node at scale) to force the adversary into a Game Theoretic loss condition.

We define the suppression game outcomes as follows:

1. **Scenario A (Zero Deployment):** If the adversary deploys no jammers, LifeLink operates as a standard high-availability mesh.

2. **Scenario B (Partial Denial):** If the adversary deploys limited jamming, the mesh topology is able to dynamically route around interference holes. The low cost of nodes allows civilians to "swarm" the environment, ensuring that a signal path exists statistically.

3. **Scenario C (Total Saturation):** To fully suppress a city-scale LoRa mesh, the adversary must blanket the noise floor across the entire 900MHz spectrum. This incurs an astronomical power cost and, critically, denies the adversary use of the spectrum for their own communications.

3 Hardware Architecture

The physical node is designed for zero-maintenance operation. It functions entirely off-grid, harvesting solar energy to maintain a continuous listening state.

3.1 Electrical Schematic

The main purpose of our electrical system, which can be seen in the node wiring diagram below, is to mediate between the bursts of power provided by the solar panel through the use of a standard lipo cell.

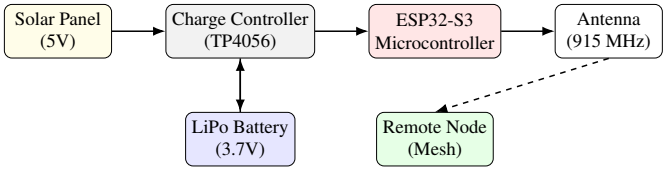

Figure 1: **Node Wiring Diagram.** The Charge Controller isolates the LiPo from over-discharge while regulating Solar input. The ESP32 handles the Protocol Stack and drives the RF interface.

4 Methodology: Semantic Compression

Since we cannot transmit full text over LoRa during high congestion, we implement an AI-driven compression layer.

4.1 Feature Engineering for Embedded Systems

We utilize a lightweight vectorizer suitable for the ESP32's constraints. An input string S is mapped to a feature vector $V \in \mathbb{R}^{82}$ composed of three subspaces:

$$V = [v_{struct} \parallel v_{intent} \parallel v_{ngram}] \tag{1}$$

While v_{struct} captures morphology (e.g., capitalization ratio, punctuation), the critical innovation is v_{ngram}. To avoid storing a large vocabulary on the microcontroller, we employ the **FNV-1a** hash function. Character 4-grams are hashed into 64 fixed bins:

$$v_{ngram}[i] = \sum_{g \in \text{grams}} \mathbb{I}(\text{FNV1a}(g) \pmod{64} = i) \tag{2}$$

This allows the model to learn semantic clusters (e.g., "help", "hlp", "plz") robustly without a dictionary.

4.2 Hierarchical Triage

Inference uses a cascaded Decision Tree ensemble. A binary "Gate" classifier first determines if the message is *Vital*. If true, secondary classifiers predict *Intent* (e.g., MEDIC, EVAC) and *Urgency* ($U \in [0, 3]$).

This reduces a 100-byte SMS to a rigid schema:

$$\text{Payload} = \texttt{INTENT} \mid U_3 \mid F_{flags} \mid N_{count} \mid L_{token} \tag{3}$$

This payload is approximately 8 bytes, reducing Airtime Utilization by $> 90\%$ for critical traffic.

5 Protocol: Hybrid Resilient Routing

LifeLink implements a custom OSI Layer 3 protocol that does not rely on static routing tables.

5.1 Epidemic Gossip

Topology discovery is achieved via "piggybacking." Every heartbeat packet carries a compressed list of the sender's known neighbors. When Node A receives a heartbeat from Node B, it updates its internal cost matrix:

$$Cost(A \to D) = \min(Cost_{curr}, Cost(B \to D) + 1) \tag{4}$$

This propagates connectivity data exponentially ("Epidemic" spread) without flooding the network with control packets.

5.2 Geographic-Gradient Forwarding

Routing decisions for a packet at Node N destined for D follow a prioritized heuristic:

1. **Direct Delivery:** If D is a neighbor, transmit directly.
2. **Geographic Greedy:** If N has high position confidence ($C > 0.3$), forward to the neighbor n that minimizes the Haversine distance to D:
$$n^* = \underset{n \in Neighbors}{\text{argmin}} \ \text{Haversine}(Pos_n, Pos_D) \tag{5}$$
3. **Gradient Fallback:** If Geographic forwarding encounters a local minima (no neighbor is closer), the protocol falls back to the "Hops Away" gradient learned via gossip.

6 Simulation Engine: Physical Fidelity and Robustness

We implement a deterministic, tick-based network simulator (1 tick $\approx$ 100ms at $1\times$ speed) that separates *protocol logic* from *RF environment physics*. This allows controlled stress-testing under contention, jamming, and topology churn.

6.1 Discrete-Time Execution Model

At each tick, the engine executes the following ordered phases:

1. **Environment Update:** clear previous in-air signals and decay interference memory.
2. **FTM Ranging Phase:** non-anchor nodes range all neighbors within FTM radius.
3. **Node Loop:** each node performs neighbor expiry, trilateration update, gossip/heartbeat scheduling, and trust-aware routing state updates.
4. **Transmit Phase:** each node can emit at most one packet per tick (half-duplex TX/RX simplification).

5. **Receive Phase:** each listening node resolves all on-channel candidates using SNR and capture/collision logic.

This strict ordering makes experiments reproducible and prevents event-order ambiguity common in asynchronous simulators.

6.2 Propagation, Noise, and Jamming Model

For a transmitter at distance d (meters), received power is modeled with log-distance path loss:

$$RSSI(d) = P_{tx} - 40 - 20\log_{10}(\max(d, 1)) \text{ dBm} \quad (6)$$

where P_{tx} defaults to 20 dBm. A receiver considers only transmitters within fixed radio radius R_{LoRa}.

Total effective noise is:

$$N_{tot} = N_0 + J(d, c) + I_c \cdot 20 \quad (7)$$

where N_0 is baseline noise floor, $J(d, c)$ is channel-specific jammer contribution, and $I_c \in [0, 1]$ is per-channel interference memory. A single-link decode requires:

$$SNR = RSSI - N_{tot} > 0 \quad (8)$$

otherwise the packet is marked jammed.

6.3 Collision and Capture Effect

For multiple simultaneous candidates on the same channel, we sort by RSSI and apply capture-effect decoding. Let P_1 and P_2 be strongest and second-strongest packets:

$$\Delta = RSSI_1 - RSSI_2 \quad (9)$$

If $\Delta \geq 6$ dB, P_1 is decoded (status *captured*) and others collide; else all collide. This mirrors practical near-far behavior in low-rate links and gives realistic partial-survival under congestion.

6.4 Localization and Topology Estimation

Positioning uses hybrid anchor + FTM ranging:

1. Pairwise FTM distance measurements are simulated with Gaussian measurement noise ($\sigma \approx 0.8$m).
2. Nodes collect at least three confident anchor/peer references.
3. Position is solved by iterative damped least-squares trilateration (Gauss-Newton style).
4. Confidence increases with anchor count and decays through multi-hop gossip.

This explicitly separates *true physics coordinates* (simulator ground truth) from *estimated coordinates* (what the node believes), enabling localization-error-aware routing behavior.

6.5 Routing, Gossip, and Trust Constraints

Routing is trust-aware geographic-gradient forwarding:

1. direct neighbor delivery if destination is one hop away,
2. geographic greedy forwarding if destination position confidence is sufficient,
3. gradient fallback via learned *via-node* from gossip,
4. fail if no admissible next hop exists.

Gossip heartbeats carry compressed neighbor entries, allowing epidemic-style membership propagation without dedicated control floods. TTL bounds and dedup buffers constrain loop persistence.

6.6 Scalability Characteristics

The simulator is designed to model city-scale behavior trends, while remaining computationally tractable for browser-based experimentation:

- **FTM phase:** naive all-pairs proximity check is $\mathcal{O}(N^2)$ per tick.
- **Receive phase:** for each node, decoding cost scales with in-range on-channel contenders; worst-case dense contention approaches $\mathcal{O}(N^2)$.
- **Traffic shaping:** one TX dequeue per node per tick prevents unbounded queue explosion and stabilizes runtime under burst injection.
- **Memory bounds:** bounded dedup buffers, capped gossip entries, and finite event/transmission logs prevent unbounded state growth.

Thus, the framework is primarily a *mesoscopic* simulator: suitable for robust comparative studies (protocol variants, jamming strategies, trust policies), while abstracting away waveform-level PHY details.

6.7 Validation and Robustness Test Matrix

We validate correctness and resilience using scenario-driven tests with observable metrics:

- **Delivery Path Metrics:** total sent, delivered, dropped, collisions, and average hop count.
- **Topology Convergence:** membership coverage (fraction of known peers) under varying beacon jitter and churn.
- **Adversarial Stress:** multi-channel jammers with varying radius/power to evaluate degradation mode (jammed vs captured vs collision).
- **State Robustness:** trust graph persistence across simulator resets triggered by node-set changes, ensuring configured trust edges are not lost during topology updates.

The trust-persistence fix is critical for experimental validity: without it, adding nodes mutates security topology unintentionally, confounding comparisons across runs.

6.8 Model Limitations (Explicit)

To avoid overstating claims, we explicitly note current abstractions:

1. fixed-range cutoff rather than probabilistic reception curves,
2. no fading, shadowing maps, Doppler, or coding-rate/SF adaptation,
3. simplified half-duplex scheduling and per-tick synchronization,
4. simplified trust/crypto semantics for protocol experimentation.

These choices intentionally prioritize reproducibility, parameter sweeps, and systems-level insight over waveform-level emulation.

7 Future Work

While the current LifeLink prototype validates the core architecture of semantic compression and hybrid routing, scaling to city-wide deployment requires further optimization in hardware integration and protocol security.

7.1 Hardware Integration & Miniaturization

The current node utilizes modular components (ESP32 DevKit, TP4056, discrete LoRa module) which increases Size, Weight, and Power (SWaP) and per-unit cost.

To address this, we are working on designing a prototype monolithic Custom PCB (Current state in Figure 4) that integrates the ESP32-S3 SoC, the SX1262 LoRa transceiver, and a dedicated MPPT solar management circuit onto a single board. This integration allows us to:

1. **Reduce Footprint:** Compressing the node volume by ≈60%, allowing for inconspicuous deployment in urban debris.
2. **Optimize RF Path:** Implementing a custom impedance-matched trace antenna to reduce signal loss compared to SMA connectors.
3. **Slash Costs:** Consolidating the Bill of Materials (BOM) drives the unit cost from $40 (prototype) toward our target of $5 at volume.

7.2 Protocol Hardening

Currently, trust is established via heuristic consensus (k-of-n confirmation). Future iterations will implement Lightweight Elliptic Curve Cryptography (ECC) directly on the ESP32. By signing packets with a private key, nodes can build a cryptographic reputation score, preventing ”Sybil attacks” where a single adversary spoofs multiple witness nodes to inject false alerts.

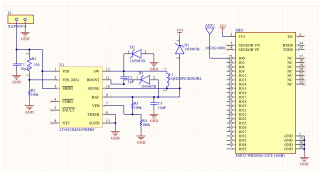

Figure 2: Schematic Design

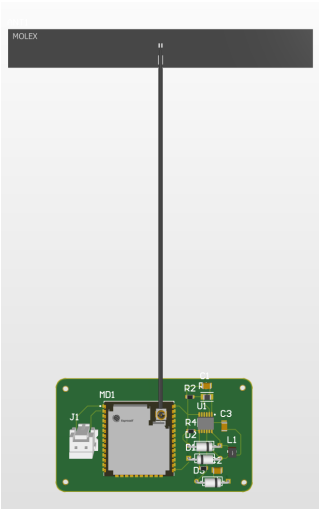

Figure 3: PCB Layout

Figure 4: **Proposed Hardware Integration.** Moving to a single-board design reduces manufacturing cost and improves physical resilience.

7.3 Multilingual Model Generalization

The current semantic compression model is trained on English crisis datasets. To support global humanitarian deployment, we plan to utilize **Federated Learning**. This would allow the global model to be fine-tuned on user devices for local languages and slang without transmitting raw text back to a central server, preserving privacy while adapting to regional dialects.

8 Conclusion

LifeLink validates that civilian communication infrastructure can be hardened against state-level disruption. By combining the physics of LoRa propagation, the economics of cheap hardware, and the efficiency of semantic AI, we render the strategy of spectral jamming fiscally and tactically obsolete.