TITLE: **MAMAWMAIL**: AN AI-ASSISTED DECENTRALIZED MESSAGING PROTOCOL USING FRACTAL PROPAGATION

WHITEPAPER – VERSION 1.0

Author: Juan Carlos G. Ayeng
Bacolod City, The Philippines
Affiliation: Independent Researcher / Developer

Date: June 20 2025

Abstract

MAMAWMAIL is a decentralized, peer-to-peer messaging protocol that delivers encrypted messages without using central servers or permanent infrastructure. It uses a **fractal propagation model**, where messages branch through multiple devices and self-clean upon successful delivery. The system integrates lightweight learning based on peer performance, allowing intelligent routing decisions without traditional networking overhead. Inspired by natural systems, MAMAWMAIL provides a censorship-resistant, offline-capable, and resilient method of communication.

1. Introduction

In an era of rising digital surveillance, natural disasters, infrastructure dependency, and targeted censorship, there is a critical need for resilient communication systems that do not rely on central servers or continuous internet access. Most modern messaging platforms fail in such environments because they depend on mobile networks, Wi-Fi, or cloud services—making them vulnerable to collapse, restriction, or interception.

MAMAWMAIL addresses this gap through a ***fully decentralized, encrypted, and intelligent peer-to-peer messaging protocol***. It allows messages to move between devices without any central routing authority or server infrastructure, using local communication channels like Bluetooth, Wi-Fi Direct, or local UDP. It achieves delivery through a ***fractal propagation model***, where encrypted packets branch through multiple peers and self-delete after successful forwarding or delivery.

Every participating device runs a lightweight daemon that acts as a relay, scanner, and local learner. These devices form a dynamic ***swarm*** that continuously adapts to the availability and reliability of nearby peers. Once a message is received by its rightful recipient (confirmed by local decryption), a deletion signal is sent to prune the entire propagation tree, ensuring network hygiene and message privacy.

Beyond one-to-one communication, *MAMAWMAIL* is designed to support ***future multicast messaging***—allowing a message to be delivered securely and efficiently to multiple authorized recipients in a group (e.g., field teams, emergency responders, or study groups). This is handled without centralized servers, relying instead on propagation-aware group headers and recipient validation at the device level.

MAMAWMAIL's unique characteristics make it ideal for use in:

1. **Disaster Zones** – enabling rescue teams and civilians to communicate even without mobile signal or Wi-Fi
2. **Military Networks** – providing secure, self-healing field communication without command servers
3. **Enterprise Facilities** – allowing local messaging within disconnected factories, hospitals, or ships
4. **Educational Research** – as a hands-on platform for teaching decentralized networking, swarm logic, and future AI routing

It is also designed for integration with **federated learning** techniques, allowing devices to continuously improve routing strategies without ever sharing user data or message content. Over time, the system evolves into a **self-optimizing communication swarm**, capable of surviving in chaotic, censored, or disconnected environments.

MAMAWMAIL is not just a messaging tool—it is a resilient, intelligent, and autonomous communication mesh for the modern world.

2. System Overview

2.1 Decentralized Design

- No centralized server or routing authority
- Each device acts as both client and relay (a “daemon”)
- Messages are broken into packets and forwarded peer-to-peer

2.2 Message Packet Structure

Component	Size Estimate
Encrypted Message	~10 KB
Routing Header	~0.5 KB
Encryption Overhead	~1 KB
Total	~11.5 KB

3. Fractal Propagation Protocol (IFPP)

MAMAWMAIL uses a custom protocol called IFPP – Intelligent Fractal Propagation Protocol. Messages propagate through the network by branching like a tree, and are pruned after delivery.

3.1 Fractal Growth

- Each packet hops to 3 new devices at every step.
- This grows exponentially (3^1, 3^2, ..., 3^5 = up to 720 concurrent paths).
- Each new device that receives the message becomes a potential forwarder.

3.2 Transition to Linear Crawl

After reaching 5 fractal hops, the protocol slows down propagation to single-hop only.

Devices mark received packets with a “been here” flag to prevent loops or resending.

This ensures continued delivery without flooding the network.

3.3 Delivery & Deletion Logic

When the correct recipient device is found (verified by decrypting the message), the message is saved locally.

A delete signal with the same header is propagated to clean up sibling messages across the network.

Devices that forward the message to a new, unvisited device delete their local copy and log a “been here” tag.

4. Local Learning & AI Readiness

MAMAWMAIL integrates a lightweight, AI-ready framework that allows each device to learn optimal forwarding strategies over time without requiring any centralized coordination.

4.1 Stats-Based Learning (Phase 1)

In the initial deployment, each device keeps a local routing scorecard for nearby peers. For each peer, it tracks:

How many messages were sent to that peer

How many of those reached their destination

Example:

json

CopyEdit

```json
{
  "peer_stats": {
    "device_X": { "sent": 10, "success": 8 },
    "device_Y": { "sent": 5, "success": 1 }
  }
}
```

This is used to rank peers when deciding which neighbor to forward messages to, ensuring better chances of success.

4.2 Deletion-Based Memory Logic

Even after a message is forwarded and deleted from a device, the learning survives in the form of updated peer stats. These records are:

- Stored as small JSON files (~10–50 KB total)
- Loaded into memory when the daemon runs
- Updated incrementally after every hop

There is no need for training complex models—this is pure statistics, and it runs efficiently even on older phones.

5. Storage & Performance Analysis

5.1 Message Footprint

Component	Size (KB)
Message body	~10.0 KB
Header + Routing Info	~0.5 KB
Encryption Overhead	~1.0 KB
Total per message	~11.5 KB

5.2 Storage Scenarios

Device Allocation	Approx. Messages
1 MB	~89 messages
20 MB	~1,780 messages
100 MB	~8,900 messages

This makes MAMAWMAIL deployable even on budget Android phones with limited storage.

5.3 Background Learning Overhead

- Local peer stats consume <50 KB
- Memory use during routing: <1 MB
- Weekly growth for logs: ~10 KB/week
- 5-year lifetime data: ~2.5 MB total

Even if the device never resets its data, the learning layer stays lightweight and invisible to the user.

6. Swarm Intelligence & Federated Learning Readiness

6.1 Local Daemons as Swarm Nodes

Every device running MAMAWMAIL acts as an autonomous **message-carrying agent** or **daemon**. Collectively, these daemons form a **swarm**—a peer-driven mesh network that works without any traffic controller or central authority.

Key characteristics:

- Devices are **zero-trust**, but **cooperative**.
- Each daemon performs scanning, hopping, learning, and cleanup.
- All routing decisions are made **locally**, based on past peer performance.

This behavior is modeled after swarm systems in nature—ants, bees, and mycelial networks—which spread and adapt through **simple local rules** that create intelligent global outcomes.

6.2 Federated Learning Potential (Phase 2)

In future upgrades, MAMAWMAIL can integrate **Federated Learning (FL)** to improve peer selection network-wide without violating privacy.

How FL Would Work:

Local Learning
Each device builds a tiny model (or score table) to track peer performance.
→ No raw messages or user data are ever shared.

Peer-to-Peer Knowledge Sharing
Devices periodically sync their stats (e.g., once per day).
→ This includes success ratios, top peers, dead-end paths.

Weighted Merging
Devices **merge peer stats** with others to improve routing accuracy.
→ This builds a **network-wide intelligence** without a central server.

Optional Aggregators
In more organized networks, a trusted aggregator device could **gather anonymized learning data** and send improved routing hints back into the swarm.

6.3 Why This Matters

Feature	**Benefit**
Federated Learning	Smarter peer selection, faster delivery
Local stats only	No private data leaves the device
Device-to-device FL	No need for cloud infrastructure
Hive behavior	The network adapts without top-down control

This transforms MAMAWMAIL into not just a messaging system—but a **self-organizing, self-optimizing communication swarm**, capable of evolving in real-world conditions.

6.4 Optional Aggregators for Private Meshes

While MAMAWMAIL is designed to operate fully peer-to-peer, certain use cases—especially **enterprise**, **military**, or **research networks**—may benefit from introducing **trusted aggregator devices** within a closed or semi-closed swarm.

These aggregators do **not control the network**, but they provide **routing intelligence enhancements** by collecting **anonymized learning data** (not messages) and optionally broadcasting optimized peer selections or swarm-wide routing strategies.

Example Applications:

- **Military Field Networks**:
  Forward units can deploy “smart relay boxes” that monitor which squad devices perform best and send back prioritized peer paths without requiring full internet or command network.
- **Enterprise Mesh Intranets**:
  In facilities without internet access, devices can learn peer layouts over

time and an aggregator (e.g. a local server) can suggest optimal message paths within a warehouse, ship, or compound.

- **University Research Swarms**:
  Used for deploying and analyzing self-healing communication in ad-hoc network simulations or communication blackouts.

Key Properties:

- Aggregators are **optional** and **non-authoritative**
- They only receive **peer score data**, never raw messages
- They output **routing optimization hints**, which nodes may choose to follow or ignore
- Aggregators can be **dynamic**, changing based on location, roles, or schedule

7. Deployment Use Cases & Scenarios

MAMAWMAIL's decentralized and self-healing nature makes it suitable for a wide range of environments where centralized communication is impossible, dangerous, or untrusted.

7.1 Disaster Response Networks (Corrected)

In areas where natural disasters or conflict destroy mobile towers and internet infrastructure, most messaging systems go offline. MAMAWMAIL offers a practical, infrastructure-free alternative.

It does not rely on store-carry-forward (where people must walk or move messages physically). Instead, MAMAWMAIL uses fractal propagation, where every device forwards messages to nearby peers immediately using local technologies like Bluetooth, Wi-Fi Direct, or LAN-based UDP.

As long as devices are discoverable and running the MAMAWMAIL daemon:

- Messages bounce through the mesh in real time
- Each successful hop deletes the previous copy
- Delivery is attempted from multiple paths
- Final recipients keep the message; all others erase it

This enables:

- Local emergency broadcasting without any mobile signal
- Survivor-to-rescuer communication by pure device-to-device chaining
- Search and rescue coordination across teams and zones with partial coverage

No user movement is required—just a mesh of awake, scanning devices within range of each other.

7.2 Censorship Resistance & Activism

In regions with suppressed connectivity or surveillance:

- Messages are fully encrypted and unlinkable to sender or recipient
- Paths are non-deterministic and change per hop
- The system deletes unused paths automatically
- Message logs are never stored unless the device is the intended recipient

This makes MAMAWMAIL suitable for:

- Activist messaging
- Anonymous organization
- Secure field updates

7.3 Tactical & Military Use

Military or field units in disconnected terrain (e.g. jungles, mountains, enemy territory) benefit from:

- Self-forming, zero-infrastructure networks
- Message propagation even across lost or destroyed devices
- Aggregators (base camps, command units) to enhance routing and analyze swarm behavior

MAMAWMAIL is ideal for:

- Battlefield updates
- Recon team messaging
- Autonomous field network routing without GPS or central commands

7.4 Enterprise or Industrial Intranets

Within large facilities like:

- Oil rigs
- Warehouses
- Hospitals
- Ships

Where Wi-Fi access may be limited or centrally controlled, MAMAWMAIL allows:

- Device-to-device messaging
- Maintenance report delivery
- Safety alerts via internal swarm

Optional aggregators (e.g., local servers) may optimize delivery, but are not required.

7.5 Educational & Research Platforms

MAMAWMAIL provides a real-world system for teaching:

- Swarm intelligence
- Network resilience
- Fractal propagation and feedback systems
- Federated learning via decentralized agents

Its lightweight footprint and open architecture make it perfect for university labs, hackathons, and AI field projects.

8. Future Support for Group Messaging (Multicast Routing)

While MAMAWMAIL is designed around unicast delivery (one sender → one recipient), future expansions can support multicast routing to enable use cases like group chat, team alerts, or broadcast-only channels.

8.1 Concept: Multicast in a Decentralized, Hop-Based Network

Group messaging in MAMAWMAIL is not achieved via a central server or message hub. Instead, it will rely on multicast-aware propagation headers, allowing:

- A single message to propagate toward multiple intended recipients
- Recipient verification before message decryption (via key exchange or group membership hash)
- Individual message receipt confirmation to stop unnecessary propagation
- Propagation pruning once all recipients have confirmed receipt

8.2 Implementation Strategy (Minimal Overhead)

Step	Function
1	Sender constructs a packet with multiple public recipient identifiers (e.g., public key hashes)
2	The message is encrypted once, but locked using a group key
3	Devices that match one of the group identifiers can decrypt and store the message
4	Once all intended recipients acknowledge, delete signals remove remaining branches
5	Learning updates still apply (routing stats by recipient success rate)

8.3 Use Cases for Multicast in MAMAWMAIL

Use Case	Benefit
Field team coordination	Single command reaches all squad members simultaneously
Factory or facility alerts	Maintenance or hazard alerts to all relevant personnel
Community broadcasting	Community messages, emergency alerts, school announcements
Study groups or classes	Class-wide communication even without internet
Secret cells or task forces	Encrypted multicast without exposing identities

8.4 Optional Enhancements (Future AI)

- AI models could predict which nodes are most likely to deliver messages to multiple recipients (multicast-optimal peers).
- Federated learning can further train delivery paths that are topologically efficient for repeating group interactions.
- Smart grouping: if certain recipients frequently appear together in multicast lists, the system can learn and optimize those as a dynamic group node.

Summary

Group communication in MAMAWMAIL will follow the same principles as individual messaging: encrypted, decentralized, hop-based, and self-cleaning. Group messages will not rely on any permanent infrastructure and will instead use intelligent propagation with per-device validation.

9. Funding, Grants, and Pitch-Ready Roadmap

9.1 Strategic Objectives

MAMAWMAIL offers a unique value proposition at the intersection of decentralized networks, privacy-first communication, and AI-assisted routing. To maximize impact and accelerate development, the following roadmap is structured around achievable phases that align with funding opportunities, open-source credibility, and long-term sustainability.

9.2 Pitch for Grant Applications

Title: MAMAWMAIL: A Fractal, Serverless, Self-Optimizing Communication Protocol for Infrastructure-Free Messaging

Summary Paragraph: In disaster zones, suppressed regions, and offline industrial environments, the need for serverless, censorship-resistant, and autonomous communication is urgent. MAMAWMAIL is a fully decentralized messaging system that uses encrypted fractal propagation, swarm intelligence, and optional federated learning to deliver and manage messages without mobile signal, Wi-Fi, or internet. Every device becomes a node in a self-cleaning, self-organizing swarm that adapts in real time. Designed for civilians, researchers, enterprises, and military users alike, MAMAWMAIL is not just a tool—it's a communication ecosystem that evolves to fit its network.

Use of Funds:

- Prototype development (Android/Linux): messaging core, daemon runner, P2P relay
- Swarm routing optimization, statistics system, and learning hooks
- Secure multicast group messaging expansion
- Open-source developer toolkit and test net
- Field trials (with community groups, responders, NGOs)
- Documentation, whitepaper refinement, and academic submission

Impact Goals:

- Restore local communication in internet/cell-dead areas
- Support safe messaging under surveillance
- Demonstrate a viable, AI-extendable communication protocol
- Train a new wave of decentralized engineers and field agents

Closing Pitch

MAMAWMAIL isn’t just a workaround for failed networks—it’s a new paradigm for how messages move, adapt, and survive. Designed to serve where the cloud cannot reach, it enables resilient messaging for people, places, and missions that traditional systems leave behind.