GhostWire Project Overview

Contents

GhostWire Project Overview

Executive Summary

GhostWire is a modular, privacy-focused mesh networking and messaging platform designed for everyone—from activists and disaster responders to rural communities and tech enthusiasts. It enables secure, decentralized communication even when the internet is down or censored.

What is GhostWire?

GhostWire lets people connect and communicate directly, forming a mesh network using whatever technology is available: Bluetooth, WiFi, LoRa, WebRTC, or even standard internet. It bridges different protocols (like Briar, Meshtastic, Matrix) and puts privacy and security first.

- **For non-technical readers:** Think of GhostWire as a walkie-talkie for the digital age, but smarter, more private, and able to connect across cities, rural areas, or even during disasters—no cell towers needed.

- **For technical readers:** GhostWire is a modular Rust-based backend with a modern React/Tailwind web UI, supporting pluggable transports, protocol adapters, and advanced security modules (E2EE, Sybil defense, quotas, blacklists, traffic obfuscation, etc.).

Who is GhostWire For? (Real-World Scenarios)

- **Activists & Journalists:** Communicate securely in areas with censorship or surveillance. Example: Protesters in a city use GhostWire over Bluetooth and WiFi to coordinate without relying on the internet.
- **Disaster Relief:** When hurricanes or earthquakes knock out infrastructure, GhostWire lets first responders and communities relay messages using LoRa radios and mesh phones.
- **Rural & Off-Grid:** Farmers and rural communities use GhostWire to stay connected over long distances with LoRa, even where there's no cell coverage.
- **Everyday Privacy:** Anyone can use GhostWire to chat securely, knowing their messages are encrypted and not stored on central servers.

Key Features

- **Mesh Networking:** Devices connect directly, relaying messages across the network.
- **Multi-Transport:** Bluetooth, WiFi, LoRa, WebRTC, TCP/IP, Stealth TCP.
- **Protocol Adapters:** Bridge to Briar, Meshtastic, Matrix, and more.
- **Security:** End-to-end encryption, Sybil defense, quotas, blacklists, disaster triggers, reputation, federation, traffic obfuscation.
- **Store & Forward:** Messages are cached and relayed when possible, so you don't have to be online at the same time.
- **Modern Web UI & CLI:** Easy to use for everyone, with advanced tools for power users.

How Does It Work? (Plain & Technical)

- **Plain:** GhostWire turns your phone or computer into a node in a network. Each node can talk to others nearby, and messages hop from device to device until they reach their destination.
- **Technical:** The Rust backend manages a registry of active transports and protocol adapters, routing messages over the best available path. Security modules enforce encryption, quotas, and trust. The web UI and CLI interact with the backend via REST and WebSocket APIs.

Why GhostWire?

- **Resilience:** Works when the internet is down or censored.
- **Privacy:** No central servers, strong encryption, and privacy by design.
- **Community:** Open-source, extensible, and built for real-world needs.

Quick Start (for Everyone)

- Try the web demo (if available) or join a local mesh event.
- For developers: See the Getting Started chapter for setup instructions.

Further Reading

- Getting Started
- Architecture Deep Dive
- Transports & Protocols
- Security & Privacy
- Protocol Adapters
- FAQ
- Contributing

GhostWire: Communication for everyone, everywhere, every time.