



Meshtrike

WHITEPAPER · BUILD V1.1 · OCTOBER 2026

Meshtrike: a voice that can't be switched off

An offline, end-to-end encrypted messenger for the moments when networks fail or are shut down. Phones talk directly to each other and carry sealed messages for one another, so people can keep speaking, and be heard, when it matters most.

WHY WE BUILT THIS

Meshtrike began as an act of solidarity with the people of India, built by one of them: a young citizen of India.

When citizens come together peacefully around a common cause, switching off the internet and silencing their voices is not an answer. We stand united in India's unity and diversity, and we will not accept silence imposed from above. People's voices, their photos, and the truth of what they witness deserve to reach the public.

The voices of young people cannot be ignored or brushed aside. We are the future of India, and our concerns matter as much as anyone else's. We stand firmly with the democratic values and fundamental rights that belong to every one of our people.

We built Meshtrike so that everyone can still be heard when those in power cut the lines people depend on. It was born in India, but it belongs to anyone, anywhere, who faces oppression or the loss of their right to communicate.

Use it wisely and with good intentions. It exists to protect people and the truth, never to harm them.

1. The problem

Almost every messenger people rely on depends on two things they don't control: cell towers and company servers. Both can be overloaded, damaged or ordered offline. When that happens during a protest, a disaster or a crackdown, people lose the ability to coordinate, check on each other and document what is happening, at exactly the moment they need it most.

Existing offline tools each solve part of this. Some need special radio hardware for every person. Some only sync between people who are already contacts. Some have had serious, publicly reported security flaws. Meshtrike aims to work on the phone people already carry, reach beyond their immediate contacts, and stay honest about what it can and cannot protect.

2. Design principles

- **Offline first.** Phones talk directly over Bluetooth, Wi-Fi Direct and LoRa. The internet is an optional extra, never a requirement.
- **No accounts, no servers.** No phone number, no email, no Meshtrike server. Identity is a key pair created on the phone.
- **The app never touches the internet.** A separate, optional add-on, MeshGRID, handles Wi-Fi Direct and the private internet route.
- **Honest states.** The app never implies a message was sent while it is still on the phone, and every wait comes with a one-line reason.
- **Nothing reveals who talks to whom.** The app does not know or store message paths or hop counts.
- **Private by design.** Notifications carry no names or content, screenshots are blocked, and received media is never shown from the original file.

3. How it works

Identity and trust

Keys are generated on the phone and never leave it. The local database is sealed with a 6-digit PIN, which is deliberately stretched so guessing is slow. An optional duress PIN silently wipes everything and shows a fresh install.

Contacts are added in person by scanning each other's QR code, which expires after two minutes. Every contact carries a trust state shown with an icon and words, never color alone:

State	Meaning
Verified	Met in person and scanned each other's code.
Not verified	Met through a public channel. Photos are hidden until tapped.
Key changed	A new key appeared under a known name. Sending pauses until you re-pair in person.

Each conversation also has a 30-digit safety number, shown in groups of five so two people can read it aloud and confirm nobody sits between them.

Routes

Under every contact's name, a live "route pill" shows how the next message will travel. When several routes work, the higher row wins.

Route	Range and speed	When it's used
Nearby · Bluetooth	10–30 m · text instant, photos in seconds	You are close to each other
Nearby · Wi-Fi Direct	50–100 m · 10–50× Bluetooth	Large photos and files between nearby phones
Long range · LoRa	Kilometres · short text only	A small LoRa radio is paired to the phone
Internet · private route	Worldwide · text in seconds, files in minutes	Both people have the route on, through the Nym mixnet
Carried by the mesh	Grows as people move · minutes to hours	Other phones are nearby, but not theirs
Camera handoff	Arm's length · about 1 MB in 2–3 minutes	Radio is jammed; phones exchange moving QR codes

Store and forward

When the recipient isn't in range, nearby Meshtrike phones carry the message for them. Relays hold only sealed data they can't read and can't attribute. Carried messages expire after 24 hours (72 at most) or when delivered, and each phone carries at most 2,000 messages or 50 MB for others.

Delivery states

A clock means the message is still on your phone. One tick means it left. Two ticks mean the other phone confirmed it, and a stronger double tick means it was read, if they share read receipts. Messages that expire before arriving are marked “Not delivered” with a Retry option. A delivery timeline shows each step.

The internet route and MeshGRID

Meshtrike itself never connects to the internet. The optional MeshGRID add-on provides Wi-Fi Direct and a route through the Nym mixnet, which hides who talks to whom and when. Anyone watching the network can see that the mixnet is in use, but not who is talking. Bridges can disguise the connection as ordinary web traffic. MeshGRID only ever receives messages that Meshtrike has already sealed.

4. What people can do with it

- One-to-one chats, groups of up to 50, and public channels where each person posts under a different random name.
- Photos (resized, metadata stripped) and files up to 5 MB, saved but never opened inside the app.
- Voice notes of up to 5 minutes, at about 120 KB per minute so they travel well over Bluetooth and the mesh.
- Nearby voice calls over Bluetooth or Wi-Fi Direct, with fresh keys for every call.
- Swipe to reply, with the quote sealed inside the message.
- Disappearing messages from 5 minutes to 4 weeks, and “send later” or “hold until I release it”.

5. Security model

Protection is layered so that one failure doesn’t expose everything: on the phone (sealed database, duress PIN, panic wipe, blocked screenshots), in the message (sealed end to end, fresh call keys, disappearing timers), on the network (opaque relays, no stored paths, optional mixnet) and in identity (in-person verification, safety numbers, key-change blocking).

It is built to protect against

Network shutdowns and overloaded towers · relays and strangers reading messages · a server being hacked or subpoenaed, because none exists · impersonation of a contact verified in person · being forced to unlock, through the duress PIN.

What it cannot do

It cannot stop malware already on a phone, someone photographing an unlocked screen with another camera, or contacts who choose to share what they receive. Above all, a phone that is transmitting can be located by someone nearby with the right radio equipment. In high-risk situations, plan with that in mind.

High-Risk mode tightens everything with one switch: constant cover traffic, text only, LoRa and Wi-Fi off, no internet route, 24-hour disappearing messages and an instant lock. Calls are disabled in this mode, because a call keeps the radio transmitting the whole time.

6. Getting the real app

Meshtrike is meant to spread from phone to phone, often when there is no internet to check anything. That makes fake copies a real risk, so every release can be verified the way Tor Browser's can, with several independent checks:

- **One signing key.** Meshtrike and MeshGRID are signed with a single private release key that never leaves the team and is never stored online. Android refuses any update not signed with it, and Meshtrike refuses a MeshGRID signed with anything else.
- **A published fingerprint.** The key's SHA-256 fingerprint is printed below, on the website, in every release and in the source repository. Any genuine copy, however it reached you, shows the same value. The verify page checks an APK right in the browser, on a phone or a computer, without uploading it: it re-checks the signature the way Android does and compares the fingerprint.
- **Signed checksums.** Each release lists the SHA-256 hash of every APK in a file signed twice, with an OpenPGP key (the format Tor uses) and with an independent minisign key. Forging a release would mean stealing both.
- **Open code.** The source is public under the Apache-2.0 license, so anyone can check what the app does. Reproducible builds, where anyone can rebuild an identical APK from that code, are planned next.

Official fingerprints

APK signing certificate (SHA-256): AB:09:7B:F4:3C:9B:63:0F:06:67:02:E0:61:9A:60:43:05:13:6A:D2:D6:4B:AA:38:E7:62:2F:AF:17:09:AD:3E

OpenPGP release key: 79E2 783E D581 74B7 3393 FE0F 79A5 F1F0 4F2D EA99

minisign public key: RWSC18AkPYb719TWSVy8CzBHwL/ZqkM7aXeAqeL1LHhsKDeoAaiZ463t

To check a copy, open meshtrike0.github.io/verify.html and pick the APK; it answers REAL or NOT REAL. On a computer, `sh verify.sh meshtrike.apk` does the same in one command. If anything does not match, do not install the app, and do not pass it on.

7. RESPONSIBLE USE

Meshtrike is a tool for protecting people and the truth.

Because there are no servers and no accounts, no one, including us, can read, moderate or remove what people send. That freedom comes with responsibility. Use Meshtrike to stay safe, to stay together and to bear witness.

Do not use it to harm, harass, deceive or incite violence against anyone.

8. Status and roadmap

Stage	Includes
Shipped - v1.0.0	Mesh messaging, routes and route pill, delivery states, groups, public channels, photos and files, photo viewer, QR handoff, internet route via MeshGRID, High-Risk mode
Built, in field testing	Swipe to reply, voice notes, nearby voice calls over Bluetooth and Wi-Fi Direct
Next	First signed public release, verification in the browser, reproducible builds, F-Droid
Then	Community servers run by volunteers (below); offline maps with satellite positioning (below); independent security audit
Later	iPhone app, group calls, disguise bridges

Roadmap: community servers run by volunteers

Meshtrike needs no servers, and it always will. But when any phone in a mesh reaches the internet, servers run by volunteers, the way Tor relies on relays run by its community, can carry sealed messages much further: as **mailboxes** that hold messages for phones that are offline, as **bridges** between separate meshes in different towns or countries, and later as **disguise bridges** where the private internet route is blocked. They only ever handle sealed envelopes, so they learn no contents, no contacts and nothing about who talks to whom, and no phone depends on any one server. Running one will take a single small program, with a public list of servers signed by the team.

Roadmap: maps that keep working through a shutdown

When the internet is cut, online maps stop working with it: Google Maps and similar apps need servers to draw the map, search places and plan routes. People are left without a way to find each other, a meeting point, a hospital or a safe way out. Meshtrike plans a map that needs none of that.

- **Position straight from the satellites.** Phones carry a satellite-navigation receiver that listens directly to several constellations at once: GPS, Galileo, GLONASS, BeiDou and, in India, NavIC. Reception needs no internet, no cell tower and no account. The receiver only listens; it sends nothing. Working out your own position therefore reveals nothing to anyone.
- **Open maps, stored on the phone.** Map data comes from OpenStreetMap, the open, community-made map of the world. Compact regional extracts are saved on the phone ahead of time and drawn on the device with open-source map rendering. Nothing about where you look is ever requested from a server.
- **Maps that travel like messages.** A region can be downloaded through MeshGRID while the internet works, or passed from phone to phone over Wi-Fi Direct when it doesn't, so one prepared phone can equip a whole group.
- **Share a place, not a trail.** A pin or a meeting point is sent as an ordinary sealed message, with the same disappearing timers. Live location is opt-in, limited in time, and shown to the people you choose. In High-Risk mode, location sharing is off.

Honest limits

Satellite signals can be jammed or faked in some conflict areas. Meshtrike will compare constellations and show how certain a position is, and warn when signals look wrong. Without internet assistance, the first fix can take a few minutes, and maps must be on the phone before they are needed. A position is also only as private as what you choose to send: sharing it hands it to the people you send it to.

9. Closing

A shutdown can switch off a network. It cannot switch off people standing next to each other. Meshtrike turns that simple fact into a way to keep talking, keep each other safe and keep the record of what happened, wherever voices are being silenced.

From India, for everyone.