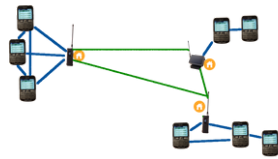


Clusters

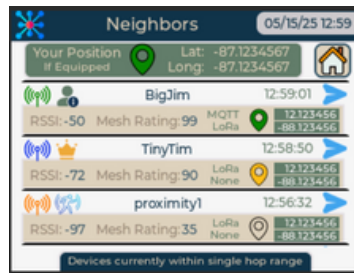


Clusters are (by design) private, closed, and secure. There is a fixed number of devices (although read-only links can be added infinitely). Clusters maintain a shared and evolving state.



Sending / Receiving Messages

- Smart path planning for direct messages
- Decentralized mesh cache helps deliver packets
- Direct Messages & Broadcasts
- Direct message delivery confirmation
- Broadcast confirmation of acceptance/rebroadcast
- Broadcasts can optionally be displayed on nodes

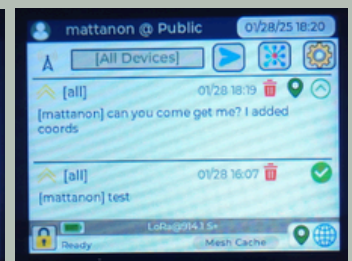
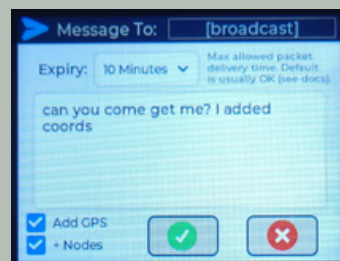


Channels



Channels are open to anyone possessing the channel ID, frequency passwords, and encryption passwords. Channels can be secure, if you keep the passwords secure.

- Decentralized mesh cache helps deliver packets
- All messages are broadcasts to the channel
- Broadcast confirmation of acceptance/rebroadcast
- Broadcasts can optionally be displayed on nodes



Location Awareness & Sharing

- Cluster-wide awareness of locations and connectivity
- Location is always being securely shared/propagated through cluster-wide "pings"
- View current or last-known location, speed, and heading of any device in your cluster - even those out of range

- Location can optionally be sent along with any broadcast
- The location marker (if sent) remains with that broadcast message as it carries forward to other devices
- View current or last-known location, speed, and heading included in any broadcast



Security

- New devices must be onboarded by the root device, where they are assigned a cluster address
- Direct messages are asymmetrically encrypted
- Broadcasts are symmetrically encrypted
- All transmissions are digitally signed

- Channel ID/creds can be manually entered into a communicator, or "pushed" from another communicator.
- Channel info must be pushed from communicators to nodes
- Broadcasts are symmetrically encrypted
- All transmissions are digitally signed using channel keys



Limitations

- New devices must be physically close enough to the root device in order to be onboarded, since keys are never viewable and devices must have a unique address in a cluster
- Max of 90 communicators and links
- Unlimited read-only links
- DM delivery attempts can continue for up to 24 hours
- Broadcast messages can continue to propagate for up to 2 hours

- Unlimited communicators and links
- DM delivery attempts can continue for up to 24 hours
- Broadcast messages can continue to propagate for up to 2 hours
- Your cluster's security is only as good as the weakest link in those who have/know the cluster credentials
- There is no neighbors screen