Testing of a resilient community-driven communications network of LoRa devices in Wellington

Wellaveediyage Migada Menuwan Perera[1], Toby Connor-Kebbell[2], Teran Abeydeera[3], Mihir Ojas Rallapudi[4], Alex Vautier[5], Brian Ngan[6], and Raj Prasanna[7]

***Abstract*—Modern communications infrastructure such as mobile base stations, routing centres and servers are highly vulnerable to grid power loss and catastrophic damage that occur during natural disasters. Such failures render critical communications infrastructure inoperable exactly when they are needed. To address this, CRISiSLab has deployed and evaluated a Meshtastic LoRa mesh network across Wellington's varied terrain as a low-power, infrastructure independent communications solution. Testing demonstrated that while terrain was the primary limiting factor, effective city-scale communications is achievable with strategic device placement and appropriate preset selection. These findings suggest that Meshtastic is viable as an emergency backup communication network.**

I. INTRODUCTION

Our modern lives rely on communications systems that depend on large, fixed, and grid-dependent infrastructure (which includes Mobile Base stations, Routing/Switching centres, and servers). During natural disasters, large storms, or conflicts, grid power can be interrupted. Such disruptions would eventually render any communication system that relies on grid-powered infrastructure (Phones, Early warning systems, among others) inoperable [1]. While many of the services these systems provide are not essential (such as social media, food delivery services, and other conveniences), losing access to emergency services, communication with family members, and early warning systems can lead to tragic, life-threatening circumstances [1]. To maintain at least those essential services, a low-power resilient network that can run for extended periods of time on a battery backup and with minimal infrastructure is needed.

A. *Existing Low Power communications*

The existing LPWANs (Low Power Wide Area Networks) use standards developed for IoT (Internet of Things) [2]. These include LoRa (LoRaWan and Mesh networks), NB-IoT, DASH7, and MIoTy. All of these except NB-IoT use the unlicensed band in each region. NB-IoT instead uses a segment of the Mobile network [3]. Thus, NB-IoT is reliant on grid-powered infrastructure and can not be used during the previously described disaster scenarios. LoRaWan, DASH7 and MIoTy were not selected because existing firmware and systems are designed for sensor data collection and thus often use a star network topology with a central gateway that forwards collected data to servers over an internet connection [4], [5]. Due to their focus on data collection, the existing firmware and hardware systems lack the features that would enable city-scale communication without reliance on fixed grid-dependent infrastructure. While the existing software suite could be modified or a bespoke system could be made to gain the required functionality, LoRa already had options that met these requirements. The two existing LoRa Mesh systems, Meshtastic and Meshcore, were designed specifically for communication.

B. *Choosing firmware*

Meshtastic was released before MeshCore in 2020 [6]. When a device sends a message (either public or direct), the device will broadcast the message [7]. All devices in range of the initial broadcast will wait for their assigned contention window and rebroadcast [7]. If those devices hear a rebroadcast of the same message before their contention window has passed, then they will not rebroadcast [7]. In the case of a public message, this process will continue until all devices have heard it [7]. In the case of a private message, when the recipient receives the message, they will broadcast an ACK(acknowledgement). The broadcasted ACK will be flooded until the sender receives it. Along the way, all nodes that receive it will stop rebroadcasting the original message [7]. Device Roles such as CLIENT(the default), CLIENT_MUTE, ROUTER, and ROUTER_LATE modify both the length of the contention window before rebroadcasting [8] as well as other parameters. There are three main contention windows. Early, Normal,

[1]Perera is with JCDR, Massey University, 6021, Wellington, New Zealand, `wmmperera@tuta.io`.

[2]Connor-Kebbell is with JCDR Massey University, 6021, Wellington, New Zealand, `toby.connorkebbell@gmail.com`.

[3]Abeydeera is with JCDR, Massey University, 6021, Wellington, New Zealand, `abeydeeratc@gmail.com`.

[4]Rallapudi is with JCDR, Massey University, 6021, Wellington, New Zealand, `mihir.rallapudi@gmail.com`.

[5]Vautier is with JCDR, Massey University, 6021, Wellington, New Zealand, `vautier.a.8@gmail.com`.

[6]Ngan is with JCDR, Massey University, 6021, Wellington, New Zealand, `brianngan2406@gmail.com`.

[7]Prasanna is with JCDR, Massey University, 6021, Wellington, New Zealand, `r.prasanna@massey.ac.nz`.

https://doi.org/10.54389/NEHG4452

and Late [8]. Routers and repeaters use the early contention window [8]. This means devices with those roles wait the least time before rebroadcasting, which will cause devices with longer contention windows to skip rebroadcasting. While this may save bandwidth, incorrectly placed ROUTERS and REPEATERS can cause rebroadcasts to stop prematurely, leading to areas where messages are not received. CLIENTs use the normal contention window [8]. ROUTER_LATE use the Late contention window, and so rebroadcast if Early and Normal contention window devices fail to propagate the message [8]. ROUTER_LATE is intended for locations where the only available ROUTER placement would destabilise the broader network, allowing that area to receive messages without disrupting others [8].

Meshcore firmware was released in 2025 [9] and is designed to provide the same messaging capabilities as Meshtastic while minimising bandwidth usage. [10]. Consequently, CLIENTs are unable to rebroadcast messages [10]. Rebroadcasting is instead exclusively handled by REPEATER nodes [10]. Unlike the REPEATER and ROUTER nodes in Meshtastic, each operator of a CLIENT node is encouraged to host a REPEATER node [10]. Flooding is only done for public channel messages, and as a last resort when a fixed path message fails [10]. By default messages between two CLIENT devices will be routed through REPEATERS if required [10]. Meshcore allows users to manually configure which repeaters messages should go through for each connection [10]. A user may choose to do this if a certain REPEATER is known to have good line of sight to both sender and recipient, or only some REPEATERS can be trusted [10]. Meshcore also has room server nodes which function as persistent group message channels, allowing nodes that connect later to retrieve previously sent messages [10].

C. Why use Meshtastic?

Meshtastic was initially chosen because Meshcore did not exist at the time the project commenced in November 2024. In addition, the use of a Meshtastic Network in Tai Rāwhiti during the floods that hit the Gisborne area in December of 2024 demonstrated that Meshtastic was already being used in real emergencies [11]. By the time Meshcore was released, a strong Meshtastic network had developed in Wellington. If this project were to switch to Meshcore it would require the creation of a new REPEATER network to provide coverage to the various suburbs already served by the Meshtastic Network .

D. CRISiSLab Experimental Meshtastic Network

CRISiSLab (Crisis Response and Integrated Simulation Science Laboratory) is a Research Laboratory within the Joint Centre for Disaster Research (JCDR) at Massey University, which conducts research on disruptive technologies with the potential to improve disaster management. This project addresses the operational continuity of communication systems in disaster scenarios in which grid power or physical infrastructure has been compromised, affecting emergency services, early warning systems, and interpersonal communications. The initial objective for this project is to deploy a Meshtastic network within Wellington's complex terrain to connect affected individuals, independent of grid-power or infrastructure vulnerable to disaster related damage. The secondary objective is to develop a backup network for other CRISiSLab projects that rely on internet connectivity to transmit critical data. To work towards these objectives, CRISiSLab has deployed Meshtastic devices across Wellington and its surrounding suburbs in collaboration with the public. The hosts of these devices were identified through a public expression of interest campaign. Additionally, CRISiSLab facilitates regular meetings with community groups already working to expand Meshtastic adoption within their respective areas. These meetings serve to assess network growth, identify opportunities for mutual support, and establish guidelines that ensure that the network expands in a stable and sustainable manner.

II. PRELIMINARY TESTING

A. Initial tests

To maximise the coverage achievable using the deployed 100 devices, tests were conducted to ascertain the reliability, range, and latency of the different channel options. While reliable, long range, and low-latency are all desirable properties, only two are achievable at once. The tests were conducted in Wellington and some surrounding suburbs. Wellington is located at the southern tip of New Zealand's North Island and has high terrain diversity. The central business district (CBD) and suburbs such as Newtown are predominantly flat, dense urban areas. Other suburbs such as Karori, Island Bay and Ngaio are situated within valleys. Testing was conducted across three representative environments: Makara Beach, a hilly rural environment; Island Bay, a suburban valley; and Cuba Street, a dense flat urban environment.

In each of the locations, the following procedure was performed on all different presets. A timer was initiated upon transmission of a 200-character message. The recipient would wait, prepared to respond immediately with a short message upon receipt of the initial message. The timer would be stopped on the receipt of the reply. This procedure was repeated 3 times per preset. If the 200-character message failed to send, the size was lowered, and the test was repeated.

B. Initial findings

All test results are measured in seconds.

As shown in Table I, all long presets took longer than 10 seconds. The marginal increase in reliability improvements of the long presets did not warrant the increased latency. ShortTurbo failed to send messages of 200 characters. Therefore, only the Medium, ShortFast , and ShortSlow presets were deemed suitable for further consideration.

Table I. Cuba St results

Channel Preset	Payload size (characters)	Run 1	Run 2	Run 3
Long Fast	140	33	21	16
Long Moderate	140	24	25	41
Long Moderate	200	25	33	27
Long Slow	140	40	50	36
Long Slow	200	74	90	99
Medium Fast	200	4.36	4.16	4.57
Medium Slow	200	6.35	5.77	6.1
Short Turbo	90	11.1	8.58	13
Short Fast	200	4.42	3.16	3.99
Short Slow	200	4.77	3.86	3.86

Table II. Island Bay Results

Channel Preset	Payload Length (Characters)	Run 1	Run 2	Run 3
Long Fast	140	27	8.58	37
Long Moderate	200	30	31.45	26.69
Long Slow	200	48	66	56
Medium Fast	200	5	5.12	4.73
Medium Slow	200	14	5.1	5.19
Short Turbo	150	3.68	2.83	2.81
Short Fast	200	2.96	3.3	2.63
Short Slow	200	9.31	Fail	20.79

Table III. Makara Beach Test 1 Results

Channel Preset	Payload Length (Characters)	Run 1	Run 2	Run 3
Long Fast	150	25	36.78	9.93
Long Moderate	200	30	30.81	31
Long Slow	200	59.3	50.15	55.73
Medium Fast	200	5.50	5.11	5.1
Medium Slow	200	5.68	5.12	58.59
Short Turbo	200	DNS	DNS	N/A
Short Turbo	150	DNS	N/A	N/A
Short Fast	200	3.54	3.86	3.02
Short Slow	200	3.61	3.2	3.26

This test was conducted using three devices with one as a hop Fig. 2. This configuration was used to evaluate the effect of a single hop on latency. The results were broadly consistent with those obtained at Cuba St. Table II shows there is an increase in latency in most of the runs. Additionally, the results indicated that loss of line of sight, even in the absence of large obstructions, was sufficient to degrade connectivity significantly.

Table IV. Makara Beach Test 2 Results

Channel Preset	Payload Length (Character)	Run 1	Run 2	Run 3
Long Fast	150	DNS	DNS	N/A
Long Fast	140	DNR	24.17	24.27
Long Moderate	200	28.17	32.8	DNR
Long Slow	200	1.08.52	41.6	33.04
Medium Fast	200	7	30	8.64
Medium Slow	200	7.47	9.07	9.32
Short Turbo	200	N/A	N/A	N/A
Short Fast	200	DNR	5.05	6.35
Short Slow	200	7.14	6.5	6.63

This first part of the Makara Beach testing was a direct connection test between the orange marker and the blue marker in figure Fig. 3. The results indicated that in rural areas, Medium, ShortFast, and ShortSlow presets had the least latency while maintaining reliability.

Table IV shows the results for the second part of the tests. Test messages were transmitted from the orange marker, relayed through the blue marker to the red marker Fig. 3. The results demonstrated that when a hop is added, the reliability of the network decreased across all presets. The medium presets transmitted the messages reliably with low latency, whilst the short presets lacked reliability.

Based on the results of the three tests, the MediumFast preset was selected for the CRISiSLab network as it consistently transmitted data reliably with latencies consistently below ten seconds. Additionally, the test results demonstrated the importance of placing nodes in elevated locations to relay messages to distant areas. Consequently, nodes were deployed at a multi-storey building in Victoria University as well as Massey University.

III. THE CRISISLAB NETWORK AND THE TESTING OF IT

The coverage of the CRISiSLab network shown in Fig. 4 was found by identifying which devices could successfully communicate with one another and whether any messages were missing. The ideal outcome was full mesh coverage with no missing messages. The test procedure was as follows. On the day of the test, each host would send a message in the CRISiSLab Meshtastic channel before commencing their day. At the end of the day, each host would send back screenshots of the CRISiSLab channel showing all the messages they received that day. These screenshots were used to identify coverage gaps.

Fig. 5, created from the screenshots gathered, shows the connected nodes. As shown in the image, the nodes in the Wellington CBD and Newtown were able to communicate with each other. These nodes are shown within the blue line in figure Fig. 5. This is attributed to line-of-sight connectivity between these devices and the CRISiSLab nodes in Massey or Victoria University's multi-storey building. In-person surveys of the areas surrounding the disconnected devices identified the following limitations. The lack of coverage in Hataitai and Kilbernie was attributed to signal obstruction by Mt Victoria. Devices in Karori lacked coverage due to obstruction by Wrights Hill. The other large area that lacked coverage was the suburbs of Berhampore and Island Bay. Preliminary surveys of the area through online map services suggested no obvious terrain to obstruct signals. However, an in-person survey of the area revealed that the peak of Adelaide St was sufficient to obstruct signals going to and leaving the two suburbs. As the network did not meet CRISiSLab's requirements in its current state, efforts to find additional device hosts continued. During the search, CRISiSLab was contacted by Steve Gilberd from the Wellington Meshtastic Facebook group, who informed CRISiSLab about the existing ShortFast Network. Upon determining the scale and coverage of this existing network, the CRISiSLab network migrated to the ShortFast preset.

IV. TESTING THE NEW NETWORK

Following the migration to the ShortFast preset, the same testing procedure was repeated. Analysis of the submitted screenshots revealed a significant improvement in coverage. The suburbs that lacked coverage due to geography (Island Bay, Berhampore, Karori, and suburbs east of Mt Victoria) were able to send messages to other nodes in the network. The public Mt Albert Infill and Hawkins Hill Routers provided coverage to Island Bay, Berhampore, Karori, and Kilbernie. However, several locations experienced inconsistent coverage, most notably Island Bay. During this round of testing, the device hosted there was able to receive messages from many people, including those in Karori, Churton Park and the Wellington CBD. However, no other nodes successfully received messages transmitted from Island Bay. Two factors likely contributed to this issue. The first factor is that these devices transmit at low power and require sufficient receiver sensitivity to decode signals below the environmental noise floor. Consequently, transmitted messages may have been too weak to be decoded by nearby routers. The second factor is the insufficient device density within Island Bay. As the CRISiSLab device in Island Bay lies within the RF shadow of Mt Albert, the router placed there may not be able to receive messages from the device at all. If there were another device in Island Bay, either at the valley floor or on the other slope, then such a device could relay the message to the Mt Albert ROUTER.

V. CONCLUSIONS

From the tests discussed in Section II, Section III, and Section IV the results indicate that the main impeding factor when creating a Meshtastic Network was the terrain of the deployment site. Not only did it eliminate coverage from entire suburbs, as seen in Section III, but it also produced asymmetric connectivity, where certain devices could receive messages but not successfully transmit, and others experienced the inverse. While the network in Wellington does have some issues, especially in places with complicated terrain such as Ngaio and Khandallah, the majority of devices within the Wellington CBD and surrounding cities, towns, and suburbs, such as Lower Hutt and Maungaraki, and Island Bay, can communicate with one another without significant packet loss. The remaining areas without coverage or with low-quality coverage are expected to improve as the number of hosts in the CRISiSLab network increases. This is demonstrated by the coverage improvements observed following the migration of the CRISiSLab network to the ShortFast preset, which connected once-isolated suburbs such as Karori, Kilbernie and Island Bay to the rest of the CRISiSLab network.

Overall, Meshtastic has the potential to be used as a backup communication method during emergencies. However, as discussed in Section I.B, Meshtastic is vulnerable to excess rebroadcasting and improperly placed ROUTERs. To mitigate the issue of excess rebroadcasting, the device profile named CLIENT_MUTE should be used for most personal carry or even some stationary home devices. They retain full send and receive functionality while refraining from rebroadcasting other messages. Thus preserving bandwidth. To mitigate the improper use of the ROUTER role, users should be advised of the potential for network impact of improper ROUTER deployment. To this end, guidelines should be provided to prevent network bandwidth exhaustion. To address this, pages have been added to the CRISiSLab website to serve as an information centre for the Wellington Regional Network. It can be found at https://www.crisislab.org.nz/wellingtoncommunitymeshnetwork. It contains information on the various communities and projects comprising the Wellington Network. It also provides guidance on joining the network or establishing a separate network without disrupting existing coverage. Detailed technical explanations are planned for future iterations of the website.

Future network testing will be conducted as the network continues to expand. As device density increases across underserved suburbs, subsequent rounds of the testing procedure described in Section III and Section IV are expected to demonstrate improvements in coverage and reliability. Additionally, a network-wide stress test is planned to evaluate the network's failure modes under high message load, reflecting worst-case communication demand scenarios that are highly likely to occur during an actual disaster.

This paper has presented the preliminary testing, deployment, and evaluation of the CRISiSLab Meshtastic network. Concurrent with the continued deployment efforts, CRISiSLab has commenced development of a network monitoring and management system. This system serves two objectives. The first objective is to centralise the monitoring and management of community-hosted CRISiSLab nodes. Second, the system is intended to support the use of Meshtastic devices in rural areas alongside other CRISiSLab projects to maintain data flow from critical sensors such as Earthquake Early Warning devices. While the system's initial design has been implemented, Node management functionality remains to be implemented. The system is currently undergoing testing and debugging prior to a small-scale deployment within the CRISiSLab network.

VI. FIGURES AND TABLES

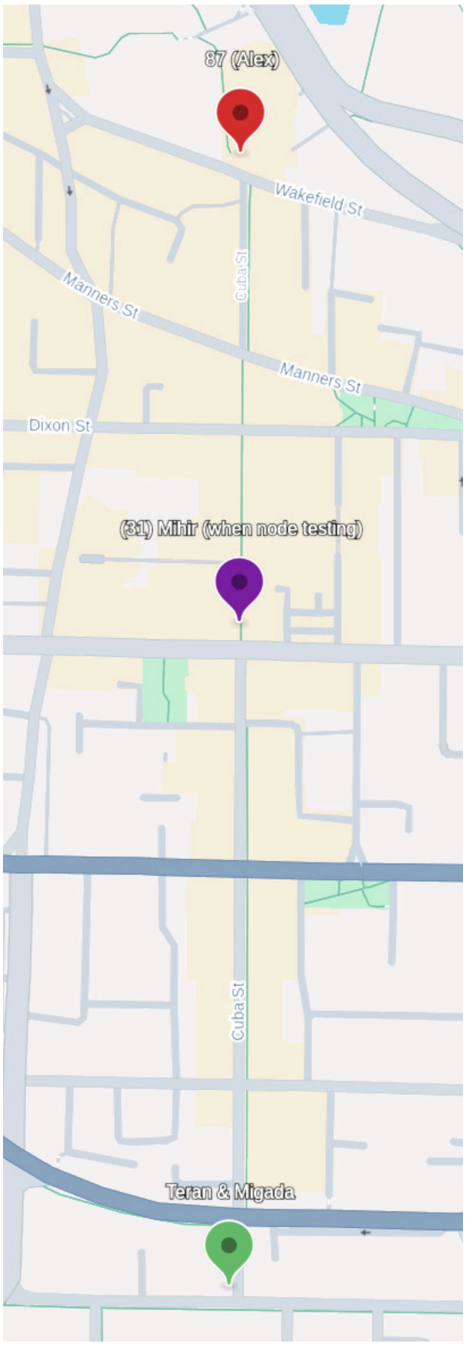

Fig. 1. Cuba St test locations

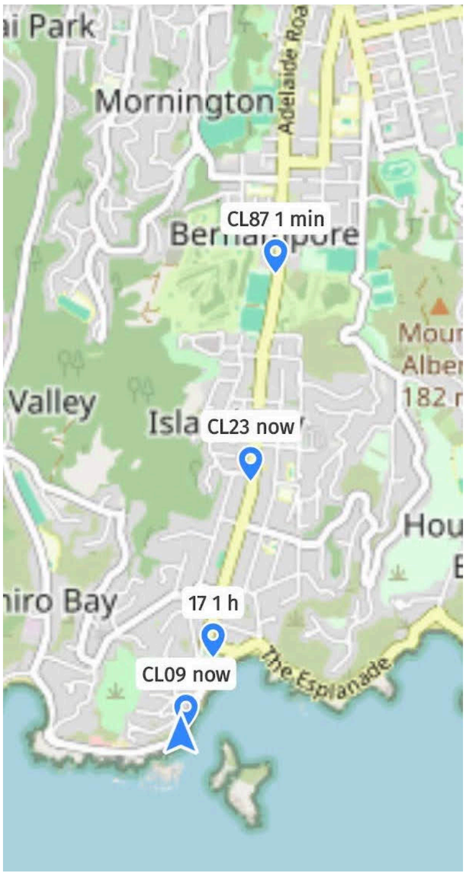

Fig. 2. Island Bay test locations

Fig. 3. Makara Beach test locations

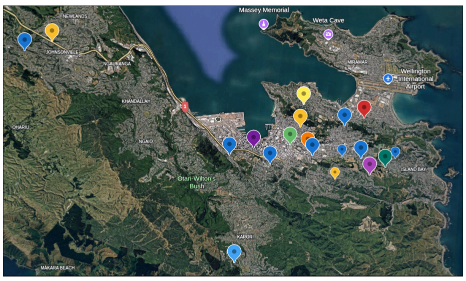

Fig. 4. Initial CRISiSLab Network

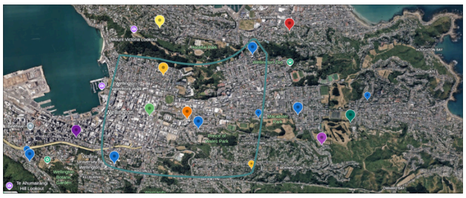

Fig. 5. Nodes that were connected to each other

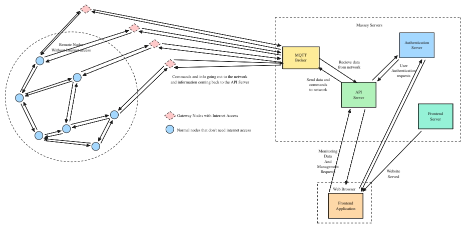

Fig. 6. Mesh Network Monitoring and Management System Topology

REFERENCES

[1] A. M. Townsend, ‘Telecommunications Infrastructures in Disasters: Preparing Cities for Crisis Communications’, 2006. [Online]. Available: https://reliefweb.int/report/world/telecommunications-infrastructures-disasters-preparing-cities-crisis-communications

[2] W. Ayoub, A. E. Samhat, F. Nouvel, M. Mroue, and J.-C. Prévotet, ‘Internet of Mobile Things: Overview of LoRaWAN, DASH7, and NB-IoT in LPWANs Standards and Supported Mobility’, *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1561–1581, 2019, doi: 10.1109/COMST.2018.2877382.

[3] H. A. H. Alobaidy, M. J. Singh, R. Nordin, N. F. Abdullah, C. Gze Wei, and M. L. Siang Soon, ‘Real-World Evaluation of Power Consumption and Performance of NB-IoT in Malaysia’, *IEEE Internet of Things Journal*, vol. 9, no. 13, pp. 11614–11632, 2022, doi: 10.1109/JIOT.2021.3131160.

[4] W. Koch and N. Q. N. Ho, ‘MIOTY™ – Physical Layer Technology: Telegram Splitting as a Game Changing Technology for the Future of LPWAN’, Erlangen, Germany, Dec. 2018.

[5] M. Weyn, G. Ergeerts, R. Berkvens, B. Wojciechowski, and Y. Tabakov, *DASH7 Alliance Protocol 1.0: Low-Power, Mid-Range Sensor and Actuator Communication*. in 2015 IEEE Conference on Standards for Communications and Networking (CSCN). IEEE, 2015, pp. 54–59. doi: 10.1109/CSCN.2015.7390420.

[6] K. Hester, ‘Meshtastic Firmware Release 0.0.3 Alpha’. [Online]. Available: https://github.com/meshtastic/firmware/releases/tag/0.0.3

[7] ‘Overview’. [Online]. Available: https://meshtastic.org/docs/overview/

[8] S. Gilberd, ‘Demystifying ROUTER_LATE’. [Online]. Available: https://meshtastic.org/blog/demystifying-router-late/

[9] ‘MeshCore Companion Firmware v1.0.0c’. [Online]. Available: https://github.com/meshcore-dev/MeshCore/releases/tag/companion-v1.0.0c

[10] ‘MeshCore FAQ’. [Online]. Available: https://github.com/meshcore-dev/MeshCore/blob/main/docs/faq.md

[11] A. Cook, ‘New technology could keep communications going during disasters’. [Online]. Available: https://www.rnz.co.nz/news/national/535819/new-technology-could-keep-communications-going-during-disasters