Bridging Technical Capability and User Accessibility: Off-grid Civilian Emergency Communication

Karim Khamaisi
University of St. Gallen
Dornbirn, Austria
karim.khamaisi@unisg.ch

Oliver Kamer
University of Zürich
Zürich, Switzerland
oliver@kamer.ch

Bruno Rodrigues
University of St. Gallen
Dornbirn, Austria
bruno.rodrigues@unisg.ch

Jan von der Assen
University of Zürich
Zürich, Switzerland
vonderassen@ifi.uzh.ch

Burkhard Stiller
University of Zürich
Zürich, Switzerland
stiller@ifi.uzh.ch

Abstract

During large-scale crises disrupting cellular and Internet infrastructure, civilians lack reliable methods for communication, aid coordination, and access to trustworthy information. This paper presents a unified emergency communication system integrating a low-power, long-range network with a crisis-oriented smartphone application, enabling decentralized and off-grid civilian communication. Unlike previous solutions separating physical layer resilience from user layer usability, our design merges these aspects into a cohesive crisis-tailored framework.

The system is evaluated in two dimensions: communication performance and application functionality. Field experiments in urban Zürich demonstrate that the 868 MHz band, using the LongFast configuration, achieves a communication range of up to 1.2 km with 92% Packet Delivery Ratio, validating network robustness under real-world infrastructure degraded conditions. In parallel, a purpose-built mobile application featuring peer-to-peer messaging, identity verification, and community moderation was evaluated through a requirements-based analysis.

CCS Concepts

• **Networks → Wireless access networks**; *Ad hoc networks*; *Network reliability*.

Keywords

LoRa MANET, Off-grid communication, Civilian networks, Emergency Communication, Resilience

ACM Reference Format:
Karim Khamaisi, Oliver Kamer, Bruno Rodrigues, Jan von der Assen, and Burkhard Stiller. 2025. Bridging Technical Capability and User Accessibility: Off-grid Civilian Emergency Communication. In . ACM, Vienna, Austria, 8 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

ACM IoT'25, Vienna, Austria

ACM ISBN 979-8-4007-1595-2/2025/11
https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 Introduction

Mobile applications are utilized for government-to-population crisis communication (*e.g.*, *AlertSwiss* in Switzerland [7]), relying heavily on centralized networks like Wi-Fi or cellular networks. However, centralized network infrastructure requires maintenance, planning, and operational management [9] and is susceptible to disruptions from natural disasters (earthquakes, hurricanes) and large-scale cyber-attacks, which can destabilize essential services [9].

Infrastructure failures (cell towers, power lines, Internet cables) can isolate populations from emergency services. Off-grid networks enable direct smartphone communication, bypassing centralized infrastructure. Decentralized systems facilitate sharing crucial information—survivor locations, medical assistance, relief updates—where both professional first responders and community volunteers become essential in managing the incident [29].

Volunteer-based civil response is necessary in large-scale emergencies for several reasons [12]: Emergency response teams are typically overwhelmed and may be partially affected by the disaster itself. Population connectivity remains essential for vital information distribution (*e.g.,* water contamination warnings during blackouts) and for providing information to optimize resource allocation.

Unlike previous work [3, 6, 15, 21] treating network resilience and user interaction separately, this work integrates physical-layer connectivity and application-layer functionality into a unified system for civilian use during infrastructure failure. The system combines a LoRa-based Mobile Ad-hoc Network (MANET) with a crisis-oriented smartphone application. The following contributions are outlined in this paper:

- Design characteristics of an emergency communication system integrating a MANET with smartphone application for resilient, off-grid civilian use during large-scale infrastructure failures.
- Real-world field experiments in urban Zürich with up to 10 LoRa nodes, evaluating performance under disaster-like conditions and measuring Packet Delivery Ratio (PDR), coverage range, and signal characteristics.
- Functional evaluation of the mobile application examining fulfillment of operational requirements critical for effective civilian emergency usage.

Real-world field experiments demonstrate that 868 MHz *LongFast* channel achieves optimal performance with 1.2 km range and

92% PDR, confirming suitability for dense urban disaster conditions. The mobile application integrating identity verification, community moderation, and resilient messaging achieved a System Usability Scale (SUS) score of 74/100, indicating strong acceptance for untrained civilian responders.

The remainder of this paper is structured as follows: Section 2 discusses related work and fundamental concepts. While Section 3 introduces the evaluation methodology, metrics, and scenarios, Section 4 presents the qualitative and quantitative evaluation. Conclusions and future work are outlined in Section 5.

2 Related Work

Radio. Although LoRa is excellent in line-of-sight (LOS) rural environments [3, 25], its application in urban emergency communications remains underexplored. Further, in a disaster scenario, both the mobility of nodes and a user-friendly mobile application are crucial. LOCATE, for example, uses LoRa-to-Bluetooth radios with delay-aware routing but lacks non-expert usability evaluation [21]. Disasteradio and Locha Mesh target solar-powered rooftops and censorship resistance respectively [6, 15], assuming fixed nodes with minimal mobile tooling for non-experts. In contrast, Meshtastic [16] offers cross-platform firmware and an active community, making it a practical base for mobile, volunteer-driven networks—the focus of our paper.

Non-LoRa alternatives for emergency systems include Wi-Fi MANET prototypes [27], and Automatic Packet Reporting System (APRS) amateur-radio links [26]. Wi-Fi MANETs suffer from short range and high power draw, while APRS requires licensed operators, hindering spontaneous civilian participation.

Classic MANET efforts explore heterogeneous backbones for disasters. Luglio *et al.* combine a terrestrial MANET with satellite links but require specialized gateways and terminals [13]. Jang *et al.* build a Wi-Fi mesh ("P2Pnet") from rescue-volunteer laptops, assuming mains-powered notebooks and short-range radios [11]. Verma and Chauhan add an energy-aware overlay atop residual cellular coverage [28], while Dey *et al.* reduce broadcast storms with a counter-based scheme evaluated only in simulation [4]. None validate low-power long-range radio with modern mobile interfaces.

Mobile application. Several commercial apps provide infrastructure free messaging. AirChat uses Bluetooth only [5]. FireChat combined Bluetooth and Wi-Fi mesh and was widely adopted during the 2014 Hong Kong and 2019 Iraq protests before its removal from app stores [8, 23]. Bridgefy offers similar offline messaging, but independent audits show vulnerabilities to tracking, forgery, and plaintext recovery [2]. HypeSDK (HypeLabs) exposes a cross-radio API for developers [10]. Most of these solutions rely on Apple's Multipeer Connectivity framework [14], which restricts them to iOS only solutions and to short-range radios (<100 m). Successful MANETs like FireChat [8] and Bridgefy [2] remain closed-source, while many academic proposals [11, 13, 28] lack published implementations.

Table 1 shows off-grid communication project landscapes. Long-range systems (*e.g.,* LoRa or satellite) rarely support mobile, non-expert operation, while usability-oriented apps are confined to short-range Bluetooth/Wi-Fi with security or platform constraints. Our proposal addresses this gap by pairing Meshtastic-based LoRa networking with a crisis-oriented smartphone application, validated through field trials and human-centered testing in dense urban disaster scenarios.

Table 1: Representative off-grid communication projects and their key characteristics

System/Project	Radio/Backbone	Range†	Mobile Solution	Major limitation
LOCATE [21]	LoRa → Bluetooth	~1 km	✓	No non-expert evaluation
Disasteradio [6]	LoRa (solar nodes)	~1–2 km	✗	Fixed rooftop deployment
Locha Mesh [15]	LoRa (censorship focus)	~1–2 km	✗	Minimal mobile tooling
Meshtastic [16]	LoRa (open firmware)	~1–4 km	✓	Usability not formally tested
Wi-Fi MANET [27]	Wi-Fi ad hoc	<0.1 km	✓	Short range, high power
APRS [26]	VHF/UHF amateur	>10 km	✓	Requires radio licence
Luglio *et al.* [13]	MANET + satellite	multi-km	✓	Needs satellite terminals
Jang *et al.* [11]	Wi-Fi laptop mesh	<0.1 km	✓	Mains-powered notebooks
Verma & Chauhan [28]	Hybrid cellular / MANET	multi-km	✓	Relies on residual cellular
Dey *et al.* [4]	MANET (simulation)	n/a	✓	Simulation only
AirChat [5]	Bluetooth	<0.05 km	✓	Very short range
FireChat [8]	Bluetooth+Wi-Fi mesh	<0.1 km	✓	Discontinued, short range
Bridgefy [1]	Bluetooth mesh	<0.1 km	✓	Security vulnerabilities
HypeSDK [10]	Bluetooth/Wi-Fi API	<0.1 km	✓	iOS-centric, short range

†Indicative maximum one-hop range reported in literature or project documentation.

3 Design

The design comprises two major components—mobile application and radio—that create the mesh network (cf. Figure 2). Seven requirements drive the design are presented in Table 2: R1-R3 target physical constraints of large-scale emergencies, R4-R5 address human aspects (cross-platform usability, verifiable identities preventing misinformation), and R6-R7 handle temporal emergency dynamics (cellular fallback, easy bootstrapping). Figure 2 presents main design components, message structure, and user roles. The **identity** service manages certificate-based authentication, enabling message signing and community-moderator roles. The **messaging** service delivers location-scoped and peer-to-peer chat through the *BLE link* protobuf API [18]. The identity service binds users to verifiable certificates from government-ID checks, while the messaging service delivers signed, tamper-proof chat for specific locations (*e.g.,* postal code "8050").

Table 2: Requirements for Emergency Communication

ID	Requirement	Emergency need	Gap in prior work‡	Our approach
R1	Kilometre-scale, licence-free radio	Bridge blocked areas when networks fail	P2P apps < 100 m; Wi-Fi MANETs power-hungry [8, 27]	LoRa 868 MHz LongFast (1.2 km, 92 % PDR)
R2	Phone-enabled use, no radio skills	Civilians lack RF expertise/licences	APRS needs licences [26]; LOCATE skips user tests [21]	BLE bridge + Meshtastic
R3	24 h node on power-bank battery	Grid down; volunteers carry USB packs	Wi-Fi laptop meshes drain power [11]	ESP32-S3 + SX1262, < 0.4 W avg.
R4	Cross-platform app, *good usability*	Mixed device fleet; ease adoption	Few user studies & iOS-only tools [14]	Requirement-based analysis
R5	Verified identity + moderation	Limits misinformation, abuse	Bridgefy spoofing flaws [1]	PKI, role-based moderation
R6	Optional cellular fallback	Use LTE/5G to offload LoRa	LoRa projects lack switchover	Auto-select infrastructure in app
R7	Bootstrap in under 5 min	First hour is critical	Satellite hybrids need special kit [13]	Pre-flashed radios, QR key exchange

‡Citations indicate where the requirement is only partially met in earlier systems.

3.1 Identity Service

Anonymity in digital platforms often leads to unwarranted behaviors [30]. Introducing a chat functionality that anchors users to their real-world identities can redefine online communication dynamics. Therefore, we provide an identity service based on a lightweight Public Key Infrastructure (PKI) that encompasses the creation of the digital identity and its application later to sign messages. Once a user submits a government-ID scan, the back-end

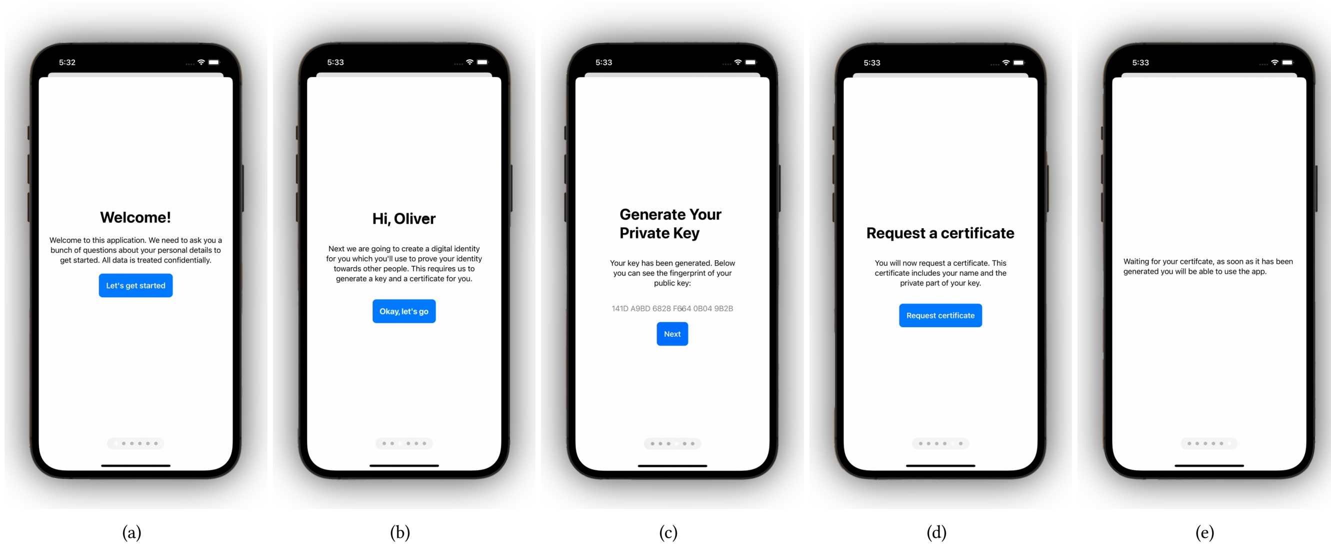


Figure 1: Identity service during the signup process-flow: (a) Welcome Screen, (b) Digital Identity, (c) Private Key, (d) Certificate Request, (e) Confirmation

returns a personal X.509-style certificate. Every message is signed with the corresponding private key, so provenance is verifiable on any device and revocation is immediate. This allows for both reducing misinformation/spamming and enables to create user roles:

- Unauthenticated: does not have certificates. May read but not post messages.
- Authenticated: holds a personal certificate. Can post signed messages to their location or directly to nearby peers.
- Community moderators: authenticated users that carry an additional "moderator" flag. They can flag, hide, or rate-limit content within their zip-code community (*i.e.,* location).
- Administrator: can approve or revoke identities, assign moderators, broadcast alerts, and delete messages.

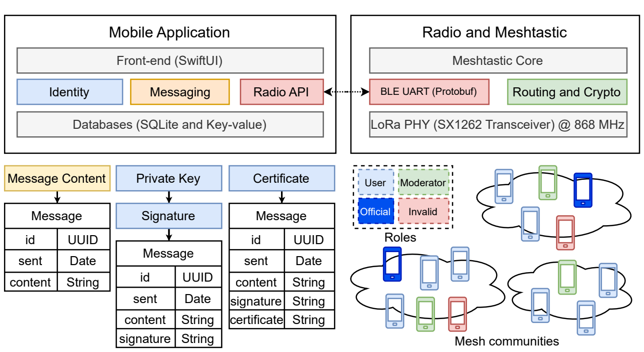


Figure 2: Component-view: mobile app and radio. Message object (bottom left) and mesh network including user roles (bottom right)

Figure 1 shows the user sign-up process. The user opens the application to a welcome screen, where a private key is securely generated and stored in the keychain. The keychain provides secure storage without requiring custom implementation and enables easy application access. A certificate signing request is created using a third-party package through a simple button press, then transmitted to the backend identity application for system administrator approval.

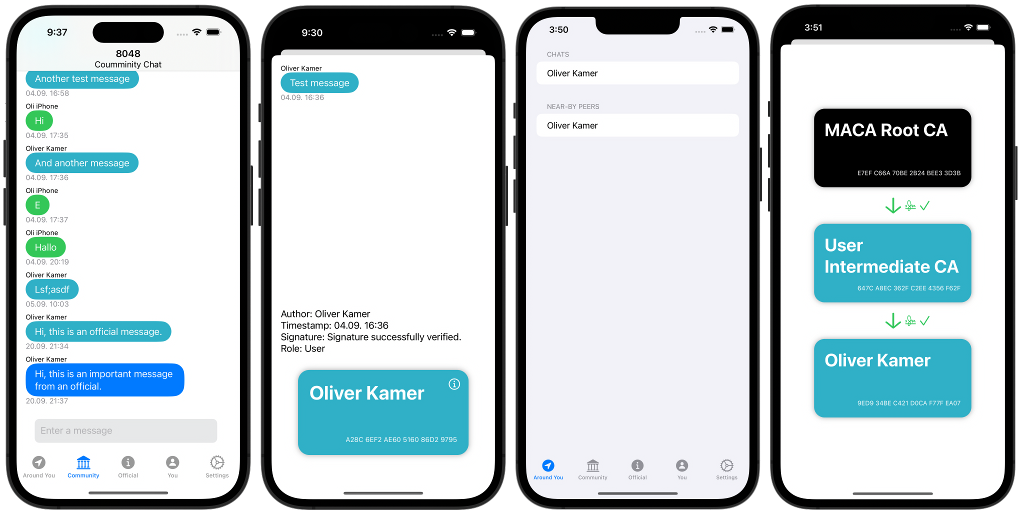
3.2 Messaging Service

After identity creation, the messaging service enables communication using certificates and private/public keys to sign messages. While messaging and identity components are detached (cf. Figure 2), the mobile application requires only messaging functionality once identity setup completes. Users communicate through peer-to-peer messaging (cf. Figure 3 - a) and location-grouped community chat addressed by zip code (cf. Figure 3 - c), supporting both radio and cellular transmission when available. Each message includes date, ID, content, signature, and sender's certificate, as illustrated in Figure 2 bottom left.

Message authenticity requires three validations: valid signature, valid certificate with intermediary certificate, and valid certificate resolving through the certificate chain to root certificate. Official messages are protected through two mechanisms: only system administrators can create official message objects, and only messages signed by the official intermediary certificate are valid.

3.3 Radio Module and Meshtastic

The physical layer foundation to achieve an off-grid communication. To meet requirements R1 and R2, the system allows nodes to communicate directly without reliance on pre-existing base stations or gateways. In contrast to Narrowband-IoT (NB-IoT) that



(a) (b) (c) (d)

Figure 3: Messaging service: (a) Community Chat, (b) Message Details, (c) Nearby Users, (d) Certificate Chain

operates within a licensed cellular spectrum, LoRa operates on ISM frequency bands (*e.g.*, 868 MHz in Europe) being available for spontaneous use [22].

The system leverages the Meshtastic open-source firmware [17], which provides a complete protocol stack for building a LoRa-based MANET. In addition, it provides the crucial link between the radio hardware and the mobile application via a protobuf-based API over a BLE link [18], as shown in Figure 2. Meshtastic organizes physical layer settings into "modem presets," which are pre-defined combinations of LoRa parameters that balance the trade-off between data rate and range. Logical communication occurs over "channels," which are encrypted groups for messages.

3.4 Field Testing

The system's performance was evaluated by performing field tests in urband Zürich with nodes deployed at varying distances (100 meters apart, cf. Figure 4), recording PDR, latency, and signal strength metrics. Two test groups were designed and conducted using identical scenarios, locations, and methodology, differing only in utilized radio devices and corresponding frequency range: 868 MHz and 433 MHz.

Each group conducted two field tests using the same frequency. Within each group, two communication channels were tested to determine optimal emergency communication channels. Channel configuration involves different LoRa parameters (Spreading Factor, Coding Rate, Bandwidth), creating trade-offs between data rates, range, and link budget.

- The **Short Range Fast Channel** provides the highest data rate possible. However, it also has the smallest link budget and, thus, a shorter range.
- The **Long Range Fast Channel** consists of the most balanced LoRa configuration parameters, allowing for a longer range while maintaining a fast data rate.

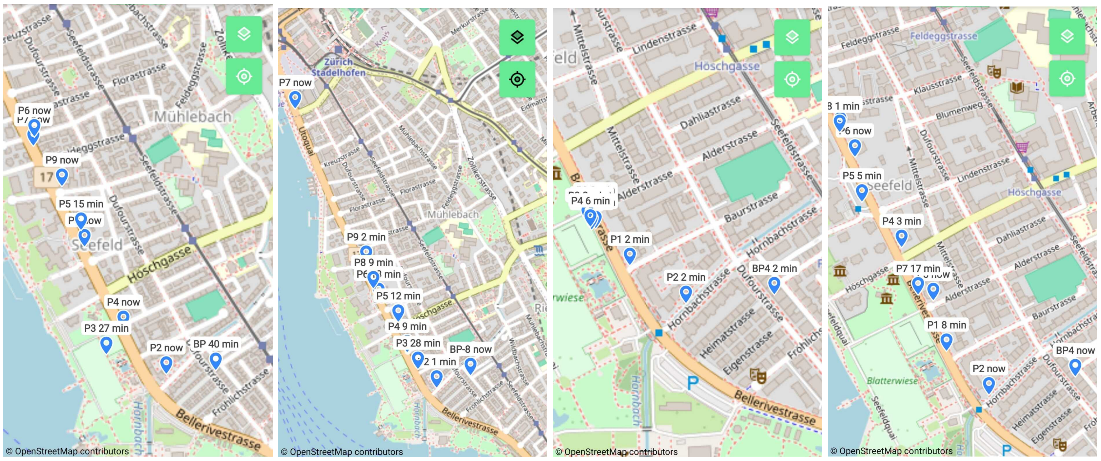
Ten nodes were employed in each field test and split into two groups: sending and receiving nodes. The first node, a central non-moving node that sends packets to other nodes, while the rest are moving nodes that receive messages from the central node. This setup simulates a central contact point for volunteers or community members coordinating rescue operations.

Field tests utilized the *Range Test* module of Meshtastic, which transmits numbered messages at configurable intervals for performance evaluation. Testing methodology comprised three stages:

(1) **Device configuration**: Receiving devices (moving nodes) were configured for continuous monitoring (time interval set to zero). Sending devices (central node) used transmission intervals following Meshtastic recommendations [19]: 30 seconds for LongFast channel, 15 seconds for ShortFast channel.
(2) **Data collection**: Range tests began after all receiving nodes passed sanity checks and received the first sequence. Distance between sending and receiving nodes increased in 50-meter increments. At 100 meters, one receiving node was fixed to relay messages to further nodes. Testing continued until the farthest receiving node stopped receiving messages. Receiving nodes transmitted only telemetry data to the network.
(3) **Data extraction and analysis**: Range test results, including message types, telemetry, and location data, were exported from mobile devices in `.csv` format. To avoid memory limitations (50 kB) and ensure data completeness, only the farthest receiving node and sending node were connected to mobile devices for complete data capture.

4 Results and Evaluation

Two testing group sets were designed, with two subtests in each group. The testing scenario and location are the same for all field



(a) (b) (c) (d)

Figure 4: Nodes on the Map: (a) 868 MHz ShortFast, (b) 868 MHz LongFast, (c) 433 MHz ShortFast, (d) 433 MHz LongFast

tests. The major difference between the two main field tests is the frequency utilized, *i.e*, 868 MHz and 433 MHz frequencies.

Table 3 summarizes the results of the acquired metrics from the various field tests, showing the communication channel's mean Received Signal Strength Indication (RSSI) and Signal-to-Noise Ratio (SNR), the achieved maximum distance from the base point, and the overall PDR.

Table 3: Performance Metrics by Frequency and Channel

Frequency	Channel	Mean SNR (dB)	Mean RSSI (dBm)	Max Distance (m)	PDR (%)
868 MHz	LongFast	-3.68	-113.95	1274	92.00
868 MHz	ShortFast	2.99	-121.45	786	58.57
433 MHz	LongFast	-1.90	-104.42	576	40.98
433 MHz	ShortFast	0.92	-84.27	281	51.06

The SNR with the corresponding location data was visualized using the base point data export, while PDR was calculated from the most distant node's data. The distance and payload columns from the data export were used for PDR calculations. The distance column indicated the distance between the sending and receiving nodes, and the payload column contained sequenced messages.

PDR was calculated for distance ranges increasing in 50-meter increments. For example, in the 0–50 m range, all messages within this distance were considered. For each range, PDR was calculated by dividing received messages by total sent messages, where the highest sequence number indicates the total sent. For instance, receiving sequence numbers 1 and 5 from 5 total sent messages (sequences 1-5) yields a PDR of 40%.

RSSI values were primarily extracted from the base point node, but when packets started hopping (*e.g.* with the 868 MHz LongFast channel at greater distances), RSSI values from other receiving nodes were utilized.

Figure 5 and 6 present the RSSI and SNR metrics for field tests on the 868 MHz frequency, comparing the ShortFast (left) and LongFast (right) channels. The first two plots in Figure 5 show RSSI and corresponding SNR values over distance. While the LongFast channel achieved greater range, RSSI recordings were limited to approximately 850 m due to the multi-hopping mechanism of the routing protocol, which drops certain information when no direct link exists. Although RSSI is captured within SNR calculations, the two metrics provide distinct insights. Signal strength diminishes beyond 200 m on both channels, with RSSI values generally ranging between -120 dBm and -140 dBm, indicative of weak signals. Up to 800 m, both channels exhibit similar RSSI values.

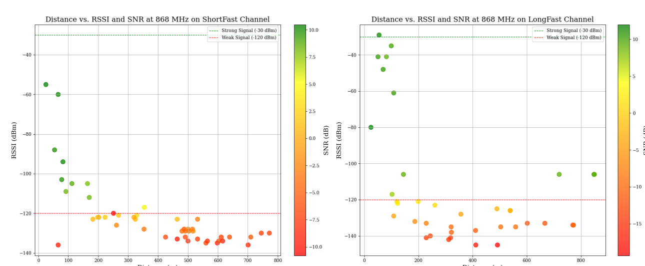


Figure 5: Distance vs. RSSI and SNR for 868 MHz on ShortFast and LongFast Channels

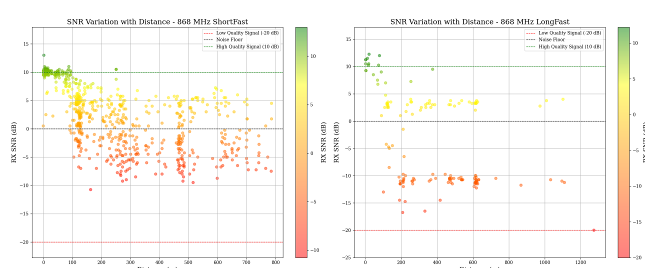


Figure 6: SNR Variation with Distance for ShortFast and LongFast Channels at 868 MHz

Figure 6 compares SNR values for both channels. The ShortFast channel shows better signal quality with most values above -10 dB, while the LongFast channel records several values near -20 dB, even at 200 m. This difference results from higher external node density on the LongFast channel (30+ devices) versus ShortFast (10 devices).

The ShortFast channel's 15-s transmission interval produced twice as many messages as LongFast, explaining its higher data record count. Lower ShortFast PDR delayed distance increments until successful message reception, enabling telemetry logging to the base point

4.1 Radio Frequency: 868 vs. 433 MHz

Figure 7 and 8 present the RSSI and SNR values over distance for the 433 MHz frequency on both ShortFast channel (left) and LongFast channel (right). Figure 7 compares RSSI values for the ShortFast and LongFast channels. All recorded signals on the ShortFast channel remained above the weak signal threshold, exhibiting stronger signals than those on the LongFast channel. However, the ShortFast channel achieved a shorter maximum distance.

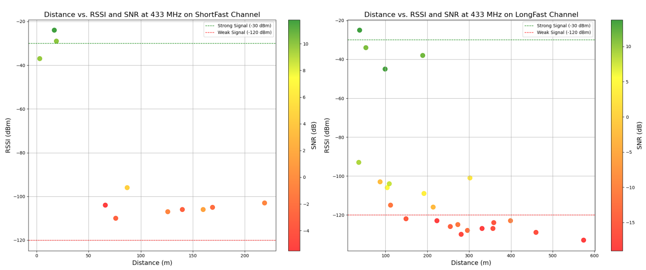


Figure 7: Distance vs. RSSI and SNR for 433 MHz on ShortFast and LongFast Channels

Figure 8 highlights SNR variations over distance for both channels. Similar to RSSI, SNR values on the ShortFast channel were generally far from the low-quality threshold, while the LongFast channel recorded several signals exceeding the -20 dB level. As expected, the LongFast channel achieved a greater range but at the cost of weaker signal quality. The ShortFast channel provided better signal strength and quality, while the LongFast channel excelled in distance, achieving nearly double the range of the ShortFast channel.

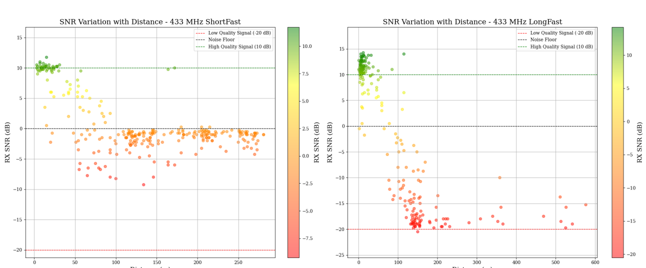


Figure 8: SNR Variation with Distance for ShortFast and LongFast Channels at 433 MHz

Figure 9 compares PDR values and achieved distances for both frequency ranges (868 MHz in red and 433 MHz in blue). The results highlight the superior performance of the 868 MHz frequency, which achieves both higher PDR values and greater range. Notably, the 868 MHz ShortFast channel outperforms the 433 MHz LongFast channel, even though the latter is designed for extended range.

All channels exhibit an abrupt drop in PDR to zero at their maximum range rather than a gradual decline. For example, the 868 MHz LongFast channel maintains a PDR of approximately 85 up to 1,250 m before dropping to zero. To ensure accuracy, each test allowed sufficient time for 10 messages to be sent before concluding. For example, on the LongFast channel with a 30-second message interval, tests were terminated after five minutes of no message reception, and the maximum attainable distance was recorded.

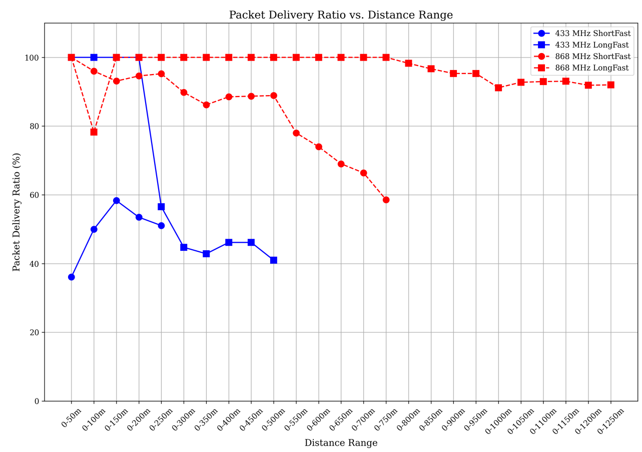


Figure 9: Packet Delivery Ratio vs. Distance Range

4.2 Mobile Application

To evaluate the effectiveness of the mobile application component for civilian emergency communication, a requirement-based analysis was conducted. The evaluation seen in Table 4 focused on requirements R2, R4, R5, R6, and R7, which target user accessibility and interface design challenges.

The 868 MHz LongFast channel, achieving a 1.2 km range with 92% PDR, provides a reliable physical layer (R1). This contrasts with other off-grid solutions [3, 6, 15, 21], which are often limited by a shorter range and higher power consumption. Also, most related work lack an authentication and role system and, as such, are open systems for anyone to join and, therefore, not suitable for a volunteer chat application, as this means that anyone can participate and bad actors have no responsibility through their identity that is linked with them [24].

The mobile application bridges R2 by enabling users to access LoRa mesh capabilities without requiring an understanding of the underlying radio protocols. The BLE bridge implementation allows civilians to connect mobile phones to radio boards using familiar smartphone interactions for mesh network communication. Cross-platform usability (R4) was validated through system-wide communication across various mobile platforms utilizing a shared LoRa

Table 4: Mobile Application of Requirements

ID	Eval.	Description
R1	✓	Achieved 1.2 km range and 92% PDR in urban field tests.
R2	✓	BLE bridge abstracts radio complexity for phone use.
R3	◐	Low-power hardware used, but 24h endurance was not tested.
R4	◐	High usability validated, but prototype was iOS-only.
R5	✓	Implemented a full PKI system with verified identity and roles.
R6	✓	System design supports automatic switching between local P2P and cellular.
R7	◐	Streamlined setup, but requires manual admin approval for identity.

● = property ; ◐ = property partially provided; ✗ = property not provided

infrastructure. Messages transmitted through the LoRa mesh network are received and processed regardless of mobile platform. The application interface utilizes established messaging conventions to ensure intuitive operation during emergency scenarios.

For verified identity and moderation requirement (R5), the application's integrated PKI system enables cryptographic verification in a user-friendly format, allowing users to verify message authenticity through signature validation. Furthermore, the role-based moderation system enables community moderators to maintain communication quality. The cellular fallback capability (R6) serves as an intelligent switching mechanism within the application. The application automatically selects the most suitable communication path based on availability, eliminating the need for user intervention.

Finally, the rapid bootstrap requirement (R7) was validated through simplified emergency deployment. Once users complete the initial identity verification, the system becomes immediately operable after establishing Bluetooth connectivity with the LoRa device. Unauthenticated users access the system in read-only mode, receiving critical emergency information without setup requirements.

4.3 Discussion

The primary goal of the field experiments was to evaluate whether a **LoRa-based MANET** can effectively function in emergencies and determine the most suitable frequency (868 MHz vs. 433 MHz) and channel configuration parameters in Zürich.

LoRa configuration parameters were grouped by channels, balancing range, data rate, and link budget. While LoRa excels in long-range communication, achieving high values for all three metrics is challenging, particularly in urban environments with significant signal-blocking objects. Nonetheless, LoRa's affordability, high link budget, and ability to handle low-quality signals make it a viable alternative in emergencies.

The 868 MHz frequency was superior in the Zürich urban setting, outperforming 433 MHz in range, PDR, and signal quality. For instance, the 868 MHz LongFast channel maintained nearly 10 dB better signal quality at twice the distance (600 m vs. 300 m) compared to the 433 MHz LongFast channel. This superiority is partly due to higher transmission power (25 mW vs. 10 mW) and reduced interference from other devices, which are more common on the 433 MHz frequency. While both frequencies adhered to duty cycle limits, no significant issues arose during the tests. Messages' size was small (*e.g.,* `"seq 5"`), and the ShortFast channel maintained 15-second intervals without exceeding utilization limits. Power consumption was moderate, with nodes consuming 2–10% battery during one-hour tests, depending on Bluetooth connectivity. Devices on 868 MHz, despite higher power output, showed no notable difference in power usage compared to 433 MHz.

The **mobile application** evaluation shows that cryptographic operations can be integrated into civilian-accessible interfaces, according to best practices listed in [20]. The requirement-based analysis demonstrates that technical resilience and user accessibility can coexist within emergency communication systems. The PKI implementation enables message authenticity verification while maintaining intuitive operation, addressing the critical challenge of preventing misinformation during crisis scenarios. Additionally, cross-platform compatibility through shared LoRa infrastructure validates the system's deployment flexibility across diverse device ecosystems. This approach eliminates platform-specific constraints that have limited previous emergency communication solutions. The cellular fallback mechanism enables intelligent adaptation to varying infrastructure conditions, ensuring continuous communication as network availability fluctuates during emergencies.

The unified approach of combining validated LoRa mesh performance with accessible smartphone interfaces addresses the gap in emergency communications between technical capability and civilian adoption. Unlike previous work that treats these dimensions separately, our system demonstrates that both requirements can be satisfied simultaneously without compromising either technical performance or user accessibility.

4.4 Limitations

First, real-world conditions and logistical challenges constrained the field tests. Weather dependency limited testing to favorable conditions, potentially overlooking performance degradation during adverse weather scenarios typical in emergencies. Coordinating participants within short timeframes was difficult, resulting in device placement at fixed locations rather than the intended mobile mesh network simulation, where users carry the devices.

Second, the mobile application evaluation was conducted as a separate component study, rather than as part of integrated system testing. While requirement-based analysis validates component compatibility, actual integration performance remains to be validated through comprehensive end-to-end testing. Furthermore, the identity verification process assumes the availability of government ID validation infrastructure, which may not be present in all deployment contexts. Alternative verification processes are therefore necessary to maintain security while ensuring broader accessibility.

Third, the network scalability assessment was limited to 10 nodes, which may not accurately reflect the performance characteristics of larger emergency networks communicating over the same LoRa channel. Additionally, while the field tests were conducted in urban Zürich, other urban testing environments with different geographic or demographic characteristics may show different results in terms of performance. Building densities, terrain topography, and electromagnetic interference patterns can all impact the signal and network reliability.

Finally, the mobile application dependency on pre-emergency identity setup creates barriers for spontaneous network participation. While unauthenticated users can receive messages, the inability to send messages without prior verification may limit the effectiveness of community-driven emergency responses.

5 Summary and Future Work

This paper presented a unified emergency communication system integrating LoRa-based MANET infrastructure with a civilian accessible mobile application. Field experiments in urban Zürich validated the performance of the LoRa mesh network. The 868 MHz frequency, using the LongFast configuration, achieved optimal performance (1.2 km range and 92% PDR), significantly outperforming the 433 MHz frequency. These results establish the viability of LoRa for urban emergency communications as a potential network infrastructure. The mobile application component demonstrated that emergency communication features can be made accessible to civilian users. Requirement-based evaluation confirmed the mobile application achieves cross-platform usability, PKI-based identity verification, and rapid deployment without compromising technical capabilities.

Future work will explore additional LoRa configuration parameters (like power consumption and channel utilization) through expanded field tests with larger node counts (50+ nodes) and diverse geographic environments (rural and urban areas). Comparisons with alternative communication systems and comprehensive end-to-end validation remain crucial for practical deployment. Lastly, exploring integration possibilities with existing emergency response infrastructures is important. This, for example, will explore how to make the system more interoperable and directly coordinate and sync the civilian network with professional emergency services.

Acknowledgments

This work builds upon Karim's Master Thesis submitted at UZH, contributing to the CYREN Project, while extending gratitude to Melanie Knieps for her invaluable support during the field tests and usability questionnaires.

References

[1] Martin R. Albrecht, Jorge Blasco, Rikke Bjerg Jensen, and Lenka Mareková. 2021. Mesh Messaging in Large-Scale Protests: Breaking Bridgefy. In *Topics in Cryptology – CT-RSA 2021*, Kenneth G. Paterson (Ed.). Vol. 12704. Springer International Publishing, Cham, 375–398. doi:10.1007/978-3-030-75539-3_16 Series Title: Lecture Notes in Computer Science.
[2] Bridgefy, Inc. 2023. Bridgefy – Offline Messages App & SDK. https://bridgefy.me/
[3] Angelica Moreno Cardenas, Miguel Kiyoshy Nakamura Pinto, Ermanno Pietrosemoli, Marco Zennaro, Marco Rainone, and Pietro Manzoni. 2020. A low-cost and low-power messaging system based on the LoRa wireless technology. *Mobile networks and applications* 25 (2020), 961–968.
[4] Manjusha Deshmukh and Sangeeta Kakarwal. 2019. 1. Adaptive routing for emergency communication via MANET. In *The Internet of Everything*, Nilanjan Dey, Gitanjali Shinde, Parikshit Mahalle, and Henning Olesen (Eds.). De Gruyter, 5–28. doi:10.1515/9783110628517-002
[5] Mark DiFranco. 2023. AirChat: Peer-to-Peer Chat. https://apps.apple.com/us/app/airchat-peer-to-peer-chat/id1606916296
[6] Disasteradio. 2024. A disaster-resilient communications network powered by the sun. https://disaster.radio/
[7] Federal Office for Civil Protection FOCP. 2024. AlertSwiss. https://www.alert.swiss/
[8] Alex Hern. 2014. Firechat updates as 40,000 Iraqis download 'mesh' chat app in censored Baghdad. *The Guardian* (June 2014). https://www.theguardian.com/technology/2014/jun/24/firechat-updates-as-40000-iraqis-download-mesh-chat-app-to-get-online-in-censored-baghdad
[9] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt, and Piet Demeester. 2004. An overview of mobile ad hoc networks: applications and challenges. *Journal-Communications Network* 3, 3 (2004), 60–66.
[10] HypeLabs Inc. 2020. HypeLabs. https://hypelabs.io/
[11] Hung-Chin Jang, Yao-Nan Lien, and Tzu-Chieh Tsai. 2009. Rescue information system for earthquake disasters based on MANET emergency communication platform. In *Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly*. ACM, Leipzig Germany, 623–627. doi:10.1145/1582379.1582514
[12] Yao-Nan Lien, Hung-Chin Jang, and Tzu-Chieh Tsai. 2009. A MANET based emergency communication and information system for catastrophic natural disasters. In *2009 29th IEEE international conference on distributed computing systems workshops*. IEEE, 412–417.
[13] Michele Luglio, Cristiano Monti, Cesare Roseti, Antonio Saitto, and Michael Segal. 2007. Interworking between MANET and satellite systems for emergency applications. *International Journal of Satellite Communications and Networking* 25, 5 (Sept. 2007), 551–558. doi:10.1002/sat.890
[14] Mattt. 2013. Multipeer Connectivity. https://nshipster.com/multipeer-connectivity/
[15] Locha Mesh. 2024. Locha Mesh - The resilient network. https://locha.io/
[16] Meshtastic. 2024. Meshtastic device firmware. https://github.com/meshtastic/firmware
[17] Meshtastic. 2024. An open source, off-grid, decentralized, mesh network built to run on affordable, low-power devices. https://meshtastic.org/
[18] Meshtastic. 2024. Radio Settings. https://meshtastic.org/docs/overview/radio-settings/
[19] Meshtastic. 2024. Range Test Module Configuration. https://meshtastic.org/docs/configuration/module/range-test/
[20] Bart Preneel. 2011. Cryptography Best Practices.
[21] Luca Sciullo, Angelo Trotta, and Marco Di Felice. 2020. Design and performance evaluation of a LoRa-based mobile emergency management system (LOCATE). *Ad Hoc Networks* 96 (2020), 101993.
[22] Semtech. 2024. LoRa and LoRaWAN. https://web.archive.org/web/20240328053451/https://lora-developers.semtech.com/documentation/tech-papers-and-guides/lora-and-lorawan/
[23] Peter Shadbolt. 2014. FireChat in Hong Kong: How an app tapped its way into the protests. https://edition.cnn.com/2014/10/16/tech/mobile/tomorrow-transformed-firechat/index.html
[24] Filipo Sharevski, Paige Treebridge, Peter Jachim, Audrey Li, Adam Babin, and Jessica Westbrook. 2020. Beyond Trolling: Malware-Induced Misperception Attacks on Polarized Facebook Discourse. http://arxiv.org/abs/2002.03885 arXiv:2002.03885 [cs].
[25] Deeksha Rai Sharma, Rohini Ravindrasingh Raghuwanshi, Tanvi Chandak, and Dipali Ramdasi. 2023. LoRa-based IoT system for emergency assistance and safety in mountaineering. *International Journal of Safety & Security Engineering* 13, 3 (2023).
[26] Sok Oeun Un, Kimtho Po, Kosorl Thourn, Rathna Pec, Channareth Srun, and Seven Siren. [n. d.]. Design of Emergency Position Reporting System for Disasters Using Amateur Radio and Automatic Packet Reporting System (APRS) as a Mobile Station Operator for Educational Purposes. *Indonesian Journal of Educational Research and Technology* 3, 3 ([n. d.]), 257–264.
[27] Himanshu Verma and Naveen Chauhan. 2015. MANET based emergency communication system for natural disasters. In *International Conference on Computing, Communication & Automation*. IEEE, 480–485.
[28] Himanshu Verma and Naveen Chauhan. 2015. MANET based emergency communication system for natural disasters. In *International Conference on Computing, Communication & Automation*. IEEE, Greater Noida, India, 480–485. doi:10.1109/CCAA.2015.7148424
[29] CYREN ZH. 2022. CYREN ZH: Cyber Resilience Network For The Canton Of Zurich. https://dizh.ch/en/2022/07/07/cyren-zh-cyber-resilience-network-for-the-canton-of-zurich-2/
[30] Adam G. Zimmerman and Gabriel J. Ybarra. 2016. Online aggression: The influences of anonymity and social modeling. *Psychology of Popular Media Culture* 5, 2 (April 2016), 181–193. doi:10.1037/ppm0000038