Disaster-Resilient Telecommunication Infrastructure:

A Systematic Approach

[24-25J-049]

Final Report

24-25J-049

B.Sc. (Hons) in Information Technology Specializing in Computer Systems & Network Engineering

Department of Computer Systems Engineering

Sri Lanka Institute of Information Technology
Sri Lanka

April 2025

Disaster-Resilient Telecommunication Infrastructure:

A Systematic Approach

[24-25J-049]

Final Report

24-25J-049

B.Sc. (Hons) in Information Technology Specializing in Computer
Systems & Network Engineering

Department of Computer Systems Engineering

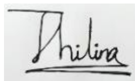
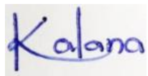
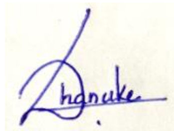
Sri Lanka Institute of Information Technology
Sri Lanka

April 2025

DECLARATION

We hereby declare that this is our own work, and this proposal does not incorporate without acknowledgment any material previously submitted for a degree or diploma in any other university or Institute of higher learning and to the best of our knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgment is made in the text. Also, I hereby grant to the Sri Lanka Institute of Information Technology, the nonexclusive right to reproduce and distribute my dissertation, in whole or in part in print, electronic or other mediums. I retain the right to use this content in whole or part in future works (such as articles or books).

GROUP MEMBER DETAILS

	STUDENT NAME	STUDENT NO.	EMAIL ADDRESS (SLIIT mail address)	SIGNATURE
1	Widanage W.T.N.	IT21377426	it21377426@my.sliit.lk	
2	Bandara H.K.K.T.	IT21176074	it21176074@my.sliit.lk	
3	Muhandiramge M.D.A.D	IT21383434	it21383434@my.sliit.lk	
4	S.M.T.S Senaratna	IT21337512	it21337512@my.sliit.lk	

ABSTRACT

In the wake of natural disasters, communication failures often prove to be one of the most critical barriers to effective emergency response. The collapse or unavailability of conventional cellular and internet infrastructures renders victims isolated and complicates the coordination efforts of rescue teams. This thesis presents the development of a self-adaptive, multi-functional communication and localization system designed to operate in post-disaster environments where traditional networks are compromised or unavailable. The proposed solution leverages commonly available technologies in mobile devices namely Bluetooth Low Energy (BLE), Wi-Fi Direct, and local wireless probing to construct a lightweight and reliable Mobile Ad-Hoc Network (MANET) that does not rely on external infrastructure.

At the core of the system lies a dual-network architecture. one based on BLE, optimized for energy-efficient short-range communication, and the other utilizing Wi-Fi Direct to extend the range and handle higher-bandwidth tasks. Devices within the network serve as both clients and servers, allowing them to exchange information directly. To enhance the resilience of the network, a self-healing mechanism was implemented that automatically reconfigures communication paths when nodes disconnect or move out of range. This mechanism ensures uninterrupted message flow and minimizes human intervention, enabling the network to adapt dynamically to changes in topology. Complementing the network layer is a secure SOS messaging system. This feature allows victims to broadcast urgent messages either to all devices in range or to specific nodes within the network. To ensure privacy and security, all messages are encrypted end-to-end, and communication prioritization is built in to reduce congestion during peak emergency periods. The system also includes a centralized dashboard that enables rescue coordinators to monitor the network, send mass alerts, and visualize communication activity in real time.

A key innovation in the project is the integration of a victim localization feature that operates independently of GPS. By deploying ESP32 microcontrollers configured to capture Wi-Fi probe requests, the system can estimate the location of nearby mobile devices using RSSI-based trilateration. This non-intrusive method allows emergency personnel to identify victim density in an area and optimize rescue routes accordingly, even in environments where GPS signals are weak or unavailable.

To support data persistence and scalability, a dual-database approach is employed. Mobile devices use SQLite for lightweight, offline storage, while a Raspberry Pi-based base station employs Apache Cassandra to store incoming data and perform long-term analytics. This combination ensures data reliability and enables synchronization when the central server becomes available. Comprehensive testing was conducted to assess the system's performance under simulated disaster conditions. Metrics such as connection stability, message delivery latency, reconnection time, power efficiency, and localization accuracy were analyzed. The system demonstrated consistent performance across varying environments, validating its potential for real-world deployment. By integrating communication, localization, data management, and network resilience into a single, decentralized platform, this project offers a comprehensive response to the challenges faced during emergency situations. The proposed system not only ensures the continuity of communication among victims and responders but also enhances situational awareness and supports more informed, timely decision-making in disaster response operations.

Keywords: Ad-hoc network, BLE, Wi-Fi Direct, self-healing network, disaster communication, SOS messaging, localization, probe request, SQLite, Cassandra

ACKNOWLEDGEMENT

I want to express my sincere appreciation to Miss Dinithi Pandithage for the invaluable guidance, expertise, and unwavering support, which were pivotal in the successful completion of this project. Your insightful feedback and encouragement have been vital throughout this endeavour. I also extend special thanks to Prof. Pradeep Abeygunawardhana and Dr Sanika Wijayasekara for the remarkable contributions and continuous assistance, providing me with a strong foundation and encouraging in overcoming numerous challenges.

I am deeply thankful to my diligent team members for their hard work, collaboration, and dedication. This project would not have been achievable without your combined efforts, creativity, and determination. My heartfelt gratitude goes to my family for their unwavering support and motivation. Your patience, understanding, and encouragement have been crucial during this demanding period.

Finally, I appreciate everyone who contributed to this project, whether directly or through words of encouragement. Your support has played a significant role in reaching this milestone.

Table of Contents

TABLE OF FIGURES

TABLE OF TABLES

LIST OF ABBREVIATIONS

Abbreviation	Full Form
BLE	Bluetooth Low Energy
Wi-Fi	Wireless Fidelity
Wi-Fi Direct	Wireless Fidelity Direct Connection (P2P)
MANET	Mobile Ad-Hoc Network
P2P	Peer-to-Peer
RSSI	Received Signal Strength Indicator
ESP32	Espressif Systems Microcontroller Unit (with integrated Wi-Fi and Bluetooth)
SOS	Save Our Souls (Emergency Distress Message)
E2EE	End-to-End Encryption
UI	User Interface
UX	User Experience
DB	Database
SQL	Structured Query Language
SQLite	SQL Lite (Lightweight Embedded Database for Local Storage)
NoSQL	Non-relational Structured Query Language
API	Application Programming Interface
MQTT	Message Queuing Telemetry Transport
LoRa	Long Range (Low-power wireless protocol)
MAC Address	Media Access Control Address
GPS	Global Positioning System
CPU	Central Processing Unit
RAM	Random Access Memory
OS	Operating System
IP	Internet Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
UN	United Nations
ICT	Information and Communication Technology
QoS	Quality of Service
EHR	Electronic Health Record
AI	Artificial Intelligence
GUI	Graphical User Interface
LAN	Local Area Network
JSON	JavaScript Object Notation
CSV	Comma-Separated Values
CAS	Cassandra (Distributed NoSQL Database System)
Flutter	UI Development Framework (Developed by Google)
Socket.IO	JavaScript Library for Real-Time Web Sockets Communication
Node-RED	Flow-based Development Tool for Visual Programming
Android SDK	Android Software Development Kit
WPA2	Wi-Fi Protected Access 2 (Security Protocol)
AES	Advanced Encryption Standard

FOV	Field of View
RTT	Round Trip Time
TTL	Time to Live
EESP	Emergency Event Signal Processing
FCC	Federal Communications Commission
UHF	Ultra-High Frequency
NFC	Near Field Communication
RTOS	Real-Time Operating System
CI/CD	Continuous Integration / Continuous Deployment
OTP	One-Time Password

1. INTRODUCTION

Communication is a foundational component of disaster response. When calamities strike be it earthquakes, floods, or other large-scale emergencies one of the first systems to fail is often the communication infrastructure. The breakdown of cellular towers, internet services, and power grids can leave entire communities isolated. In such moments, both victims and first responders find themselves in critical need of a resilient, decentralized communication solution that does not rely on traditional network infrastructure. Recognizing this urgent need, this project proposes a self-adaptive emergency communication and user localization system that operates independently of internet and mobile service providers.

The system is built on a multi-layered architecture that integrates five interdependent functions. At its core is an ad-hoc communication framework utilizing Bluetooth Low Energy (BLE) and Wi-Fi Direct. These technologies are embedded in nearly all modern smartphones and can form device-to-device connections without the need for a router or external network. By forming a Mobile Ad-Hoc Network (MANET), devices can transmit data across a mesh of nearby nodes. This framework is particularly useful in disaster-struck zones where infrastructure may be absent, allowing victims and rescuers to maintain contact even in isolated conditions. To ensure continuity and resilience in this decentralized network, a self-healing mechanism has been implemented. In rapidly evolving disaster environments, devices may frequently move out of range, lose power, or become otherwise unavailable. The self-healing algorithm detects such disconnections and dynamically reroutes communication paths through active devices, ensuring minimal downtime. This functionality is essential for maintaining stable communication over extended periods, especially in cases where manual intervention is impossible or inefficient. The self-healing feature distinguishes this network from basic mesh configurations by ensuring long-term adaptability and robustness.

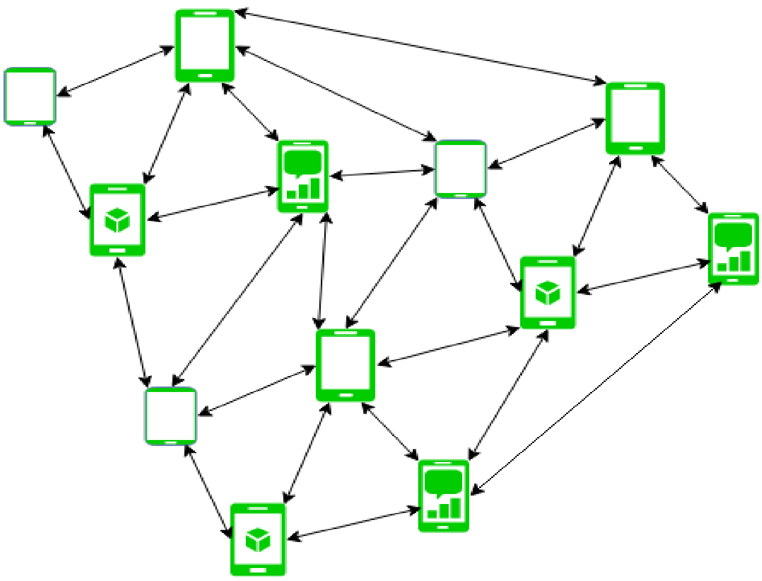


Figure 1-1 AD-Hoc network architecture diagram

Layered over the core network infrastructure is a secure SOS messaging system. During emergencies, the ability to send distress signals quickly and reliably can be lifesaving. The system supports both broadcast and targeted SOS messages that are end-to-end encrypted to ensure security and privacy. These messages can be shared over the BLE and Wi-Fi Direct networks, making them accessible even in complete network blackouts. A centralized dashboard adds another level of control, allowing rescue coordinators to monitor message flow, receive alerts from victims, and push out critical announcements to the entire network in real-time.

A unique component of this system is the victim localization feature, which allows responders to estimate the positions of individuals without the need for GPS. Many disaster zones suffer from poor GPS accuracy due to blocked satellite signals or device limitations. Instead, this project uses Wi-Fi probe requests emitted by smartphones as they search for nearby networks. ESP32 microcontrollers operating in promiscuous mode capture these signals. By analyzing the signal strength (RSSI) and applying trilateration techniques across multiple ESP32 nodes, the system can calculate the approximate location of a device. This technique enables non-intrusive, real-time tracking of people within the affected area, aiding rescue efforts and resource deployment.

To support the data operations of the system, a dual-database architecture is integrated. Each smartphone participating in the network stores messages and metadata locally using SQLite. This ensures that data remains accessible and consistent even if the device is offline. Meanwhile, base station used when available runs Apache Cassandra, a high-availability database that stores aggregated data for long-term analysis. This separation of edge and central storage guarantees that no critical data is lost during disconnections, and that synchronization can occur once connectivity is restored.

The combination of these five functions ad-hoc communication, self-healing, secure messaging, localization, and scalable data management forms a cohesive, self-reliant system. It is designed to be deployed quickly using existing mobile hardware, making it not only practical but also cost-effective. By taking advantage of low-energy communication protocols, modular components, and robust data handling, the system aims to empower disaster-affected communities with a reliable digital lifeline when they need it most. Through this research, the project explores the feasibility, performance, and scalability of such a solution in real-world scenarios. The subsequent chapters outline the technical underpinnings, development methodology, and testing results that validate the system’s functionality and impact. This initiative contributes not only to disaster communication technology but also lays a foundation for further innovations in decentralized and resilient network solutions for humanitarian purposes.

1.1. Background Literature

The increasing frequency and intensity of natural disasters have highlighted critical vulnerabilities in existing telecommunication systems. In many post-disaster scenarios, the immediate aftermath is characterized by a collapse in communication infrastructure due to damaged cellular towers, disrupted power lines, and overloaded networks. These disruptions isolate victims from emergency responders and severely hinder coordination among rescue teams. Conventional systems, which depend heavily on centralized infrastructures, often prove ineffective in such contexts. Consequently, there has been a growing emphasis in recent research on developing decentralized communication models that function independently of internet and mobile service providers. [1]

Mobile Ad-Hoc Networks (MANETs) have emerged as one of the most promising solutions for decentralized communication, especially in disaster-affected environments. MANETs enable direct device-to-device connectivity without relying on fixed base stations or network infrastructure. Multiple studies have validated the use of MANETs for emergency communication, showcasing their ability to maintain data exchange between mobile nodes even in the absence of conventional support systems. [2] However, the dynamic nature of disaster zones where nodes frequently move, become unreachable, or power down poses challenges to the stability and reliability of MANETs. These issues have prompted researchers to explore the integration of short-range wireless technologies such as Bluetooth Low Energy (BLE) and Wi-Fi Direct into MANET structures to improve their resilience and adaptability. [3]

BLE has gained attention due to its low power consumption, availability on most smartphones, and efficient short-burst communication model. BLE's characteristics make it an ideal fit for emergency networks where preserving device battery life is essential. In scenarios where victims are stranded without access to power for long durations, maintaining communication without draining device resources becomes critical. [4] Studies show that BLE-based communication is not only energy-efficient but also stable over time, enabling devices to remain active within a decentralized mesh network. BLE's advertising and scanning mechanism allows nearby devices to discover each other and establish connections automatically, providing a flexible method for creating spontaneous communication pathways. [5]

To overcome connectivity disruptions caused by node mobility or device failure, self-healing algorithms have been incorporated into BLE-based networks. These algorithms allow the network to reconfigure itself by detecting changes in node availability and rerouting data through active paths. This approach eliminates the need for manual re-establishment of connections and ensures that communication remains seamless even in unstable environments. Research indicates that self-healing mechanisms significantly enhance the robustness of mobile ad-hoc networks, allowing them to perform reliably in real-time disaster conditions. [6] The integration of self-healing into the system also reduces downtime, making it easier for both victims and rescue workers to remain connected throughout the rescue effort.

In addition to BLE, Wi-Fi Direct plays a vital role in extending the functionality of emergency networks. While BLE is well-suited for low-energy, short-distance messaging, Wi-Fi Direct offers higher data throughput and broader communication range, which is beneficial in transferring larger files such as images or location data. Unlike traditional Wi-Fi, Wi-Fi Direct enables two or more devices to communicate directly without requiring an access point, making it particularly useful when internet connectivity is completely unavailable. [7] Studies have shown that incorporating both BLE and Wi-Fi Direct into disaster communication networks results in a hybrid system that balances efficiency and performance, ensuring that the network can scale according to communication demands.

Legacy Wireless Networks	Ad Hoc Wireless Networks
Infrastructure based wireless networks requires proper planning for setup	Usually unplanned, no planning is generally required.
Thus it requires high setup time	Requires minimal setup time
It demands fixed backbone network for extended connectivity	No fixed backbone connectivity is required
High infrastructure cost	Virtually no infrastructure cost
All nodes operate under centralized administration	No centralized administration, loosy networks.

Figure 1-2Comparison between Ad Hoc and Legacy Wireless Networks

Another critical function of disaster communication systems is the ability to transmit distress signals efficiently and securely. In high-risk situations, the timely delivery of SOS messages can mean the difference between life and death. Traditional SMS or app-based messaging systems often fail due to signal congestion or server downtime. Therefore, researchers have developed peer-to-peer SOS messaging protocols that operate within ad-hoc networks. These systems ensure that messages are transmitted without delay by bypassing congested infrastructure. Moreover, to protect sensitive information such as victim location or health status, encryption protocols are applied to all outgoing and incoming messages. [8] This protects users from data breaches while maintaining the integrity of the communication network. Some studies have further enhanced these systems by enabling message prioritization, ensuring that emergency messages take precedence in transmission queues and reach the intended recipients swiftly. [9]

Localization is another vital component of disaster management. When victims are trapped or unable to communicate, their detection and identification become a top priority for responders. In environments where GPS signals are blocked or weak such as in collapsed buildings or underground spaces alternative methods for location tracking become necessary. One widely researched technique involves the use of Wi-Fi probe requests emitted by smartphones. When devices search for known networks, they emit signals containing metadata like MAC addresses and signal strength. These can be captured by microcontrollers such as ESP32 operating in promiscuous mode. By deploying multiple ESP32 units across a location, signal strength can be measured from different angles, and trilateration techniques can be applied to approximate the position of the device. [10] Studies have demonstrated the viability of this approach for accurate indoor localization, making it a valuable asset for identifying victim locations when visual contact or verbal communication is not possible.

Data management plays an essential role in ensuring that information gathered during a disaster response is stored, retrieved, and analyzed effectively. To address this, a hybrid storage architecture has been proposed combining local and centralized databases. On mobile devices, SQLite is used as a lightweight solution for temporary and offline data storage, such as message logs and connection states. SQLite offers low resource consumption and fast data access, which is particularly useful for mobile applications running under constrained conditions. [11] At the base station or rescue command center, Apache Cassandra serves as the central storage platform. Cassandra is a distributed NoSQL database that supports horizontal scaling and high availability, making it suitable for handling large volumes of data from multiple field devices. [12] This dual-database system ensures that data is not lost during connection interruptions and can be synchronized once the network stabilizes.

To bring all components together, a centralized management dashboard is used to provide real-time control and visibility over the entire network. This dashboard enables rescue coordinators to view active devices, monitor victim density through localization inputs, and receive incoming SOS alerts. The dashboard also supports outbound communication, allowing central commands to send mass notifications to all connected devices. The visualization features assist in making quick decisions, coordinating field efforts, and ensuring that information flows remain uninterrupted. [13]

The integration of these technologies BLE, Wi-Fi Direct, self-healing mesh algorithms, encrypted messaging, Wi-Fi-based localization, and hybrid database architecture results in a comprehensive emergency communication platform that is both scalable and autonomous. Unlike conventional systems that collapse under stress, this model adapts to the changing landscape of a disaster zone, keeping victims and responders continuously connected. By unifying connectivity, messaging, location awareness, and data persistence into one framework, the system offers a robust solution for post-disaster communication where it’s needed the most.

1.2. Research Gap

In recent years, numerous studies have explored the potential of wireless communication technologies to support emergency response in disaster-prone areas. While mobile ad-hoc networks (MANETs), Bluetooth Low Energy (BLE), Wi-Fi Direct, and mesh communication models have all been proposed as solutions to overcome the limitations of centralized infrastructure, these studies often fall short when it comes to offering an all-in-one, scalable, and energy-efficient solution that can function autonomously in dynamic and infrastructure-deficient environments. Despite the proliferation of research in isolated domains, a cohesive model that integrates reliable connectivity, robust message delivery, accurate victim tracking, and resilient data management remains largely undeveloped.

One of the critical limitations observed in existing research is the over-reliance on single-technology communication protocols. While BLE has been recognized for its low energy consumption and growing presence in smartphones, most BLE-based systems are optimized for static environments and do not effectively address real-world challenges such as node mobility, sudden device disconnections, or environmental interference. On the other hand, Wi-Fi Direct, although faster and more suitable for high-bandwidth communication, is often treated in isolation without being paired with other protocols for redundancy or fallback. Few studies have attempted to merge BLE and Wi-Fi Direct into a unified system capable of adapting to bandwidth needs, power constraints, and shifting network topologies, especially in highly unstable disaster zones.

The concept of network resilience is often limited to theoretical models or basic redundancy principles. While some frameworks explore static mesh formations or single-point rerouting in the event of node failure, they lack dynamic self-healing capabilities that can automatically reconfigure communication paths when nodes disconnect unexpectedly. In disaster scenarios, where devices may move out of range or be physically damaged, the absence of a real-time self-healing mechanism significantly hinders continuous communication. Very few systems implement and evaluate a practical self-healing strategy tailored for mobile ad-hoc networks formed by smartphones and embedded microcontrollers operating under resource limitations.

SOS messaging has been a cornerstone of emergency communication systems, yet current implementations are often tied to the availability of mobile data, SMS services, or internet infrastructure. Many existing applications assume at least intermittent access to traditional networks, which is an unrealistic expectation in post-disaster environments. Even when offline messaging systems are introduced, they tend to lack encryption, prioritization, and the ability to send messages to both specific nodes and as mass broadcasts. There is a gap in developing a lightweight yet secure messaging system that can deliver urgent distress signals reliably, even in congested or partitioned networks, without compromising user privacy.

Victim localization has typically relied on GPS-based technologies or external positioning systems. However, GPS accuracy diminishes significantly in enclosed spaces such as buildings, tunnels, or dense urban areas. Research on alternative methods such as Wi-Fi probe request analysis using RSSI values exists, but implementations are often constrained to theoretical simulations or controlled laboratory environments. There is minimal research that applies this methodology in a field-ready format using widely available hardware like ESP32 devices for passive localization. Moreover, existing models do not adequately address the use of trilateration techniques to refine position accuracy in real-time, especially in dynamic and noisy signal conditions.

Data management presents another notable gap in the research. While some systems propose centralized databases or rely on server synchronization once internet access is restored, few offer robust hybrid models that combine edge-based local storage with centralized servers that can operate under intermittent connectivity. SQLite is often used in standalone mobile applications for local data persistence, but its integration with a distributed system like Apache Cassandra for disaster-focused use cases remains largely unexplored. This gap leads to inconsistencies in data availability, synchronization errors, and challenges in maintaining data integrity when switching between online and offline modes in unpredictable environments.

Another overlooked area is the integration of a real-time centralized dashboard for network management and situational awareness. While some research papers mention monitoring tools or control interfaces, most fail to provide a comprehensive solution that ties together communication logs, location data, device health, and SOS message routing. The absence of such a tool creates a disconnect between what victim's experience on the ground and what rescue coordinators can oversee and act upon. A centralized yet offline-accessible dashboard that bridges this gap would significantly improve disaster management efforts and operational efficiency.

In summary, although each of the core technologies BLE, Wi-Fi Direct, SOS messaging, probe-based localization, and distributed databases has individually been explored in past research, there exists a significant gap in developing a holistic system that integrates these components into a single, scalable, disaster-resilient framework. Most existing solutions are fragmented, untested in real-world scenarios, or overly reliant on external infrastructure. This thesis addresses these shortcomings by proposing and evaluating a unified, infrastructure-free, energy-efficient communication and localization model that functions effectively in both isolated and high-stress environments. The project's innovation lies not in inventing new technologies, but in combining and adapting existing ones into a resilient system that can save lives when traditional networks fail.

2. RESEARCH PROBLEM

Natural disasters such as earthquakes, floods, and wildfires can devastate communities in a matter of moments, often destroying critical infrastructure and severing lines of communication at the very time they are most needed. In such scenarios, victims may be unable to contact emergency services, share their locations, or even signal for help. Likewise, rescue teams may face major challenges coordinating responses, locating survivors, and sharing real-time updates across scattered and disconnected regions. Despite significant technological advancements in recent decades, modern disaster response strategies continue to rely heavily on centralized systems mobile networks, internet access, and cloud-based services that are extremely vulnerable during crisis events. When these systems fail, so too does the ability to provide life-saving support.

This reality raises an urgent question: **How can we create a reliable system that detects and relays the presence of people in disaster areas, while also transmitting SOS alerts and instructions when traditional networks fail?** The need for such a solution is clear, but current technologies fall short in several critical ways. Most emergency communication systems are dependent on the very infrastructure that disasters tend to destroy. Systems that offer offline capabilities are often limited in range, energy-inefficient, or unable to scale in high-density victim scenarios. Others lack the security and adaptability necessary for real-time use in chaotic environments.

The fundamental challenge lies in building a communication and localization system that operates autonomously in the absence of external infrastructure, is accessible via devices already in people's hands namely smartphones and is capable of real-time communication, location estimation, and data management. Furthermore, the system must be resilient to device disconnections and adaptable to constantly changing network topologies common in mobile environments. It should also support secure, direct peer-to-peer communication and provide a centralized overview of the network and active users to aid rescue teams in managing ongoing operations.

Another layer to this challenge involves locating individuals who may be unconscious, trapped, or unable to communicate. While GPS offers a common method for location detection, it is often unreliable indoors or underground. Therefore, a solution must be developed that can passively detect nearby devices through existing signals and estimate positions without user input. Such a system would allow emergency personnel to identify areas with a high presence of potential survivors and optimize their response strategies accordingly. Equally important is the ability to transmit distress signals both to nearby peers and central coordinators without relying on mobile carriers or internet connectivity. A simple, intuitive messaging system that can operate entirely offline while maintaining encryption and delivery reliability is essential. Without it, even survivors who are equipped with functioning devices may be unable to request help in a timely manner. Most existing offline messaging tools are either proprietary, hardware-specific, or dependent on physical proximity, making them impractical for large-scale deployments in unpredictable environments.

From a system design perspective, yet another research challenge emerges how to ensure the continuous availability and synchronization of critical data. When using mobile devices as temporary communication nodes, the risk of data loss due to battery depletion, software crashes, or signal interruption becomes a major concern. This calls for a hybrid data management model where local storage ensures operational continuity and central databases (if available) provide redundancy and longer-term data preservation. The system should also offer the ability to monitor its own health in real time, automatically detect faults, and recover from unexpected disconnections without manual intervention.

Lastly, any system designed for real-world disaster use must be low-cost, easily deployable, and compatible with existing hardware. Introducing specialized or proprietary devices would not only increase the cost of deployment but also limit the reach and inclusivity of the solution. Leveraging widely available technologies such as Bluetooth Low Energy (BLE), Wi-Fi Direct, and affordable microcontrollers (e.g., ESP32) makes it possible to build a solution that is scalable and sustainable. The research problem, therefore, is multi-dimensional. It involves developing a fully decentralized, infrastructure-free communication and localization system that is reliable, power-efficient, secure, and scalable capable of functioning independently in disconnected environments to assist both victims and emergency responders. This project seeks to address that gap by designing and implementing a self-adaptive model that integrates multiple wireless technologies, real-time messaging protocols, user localization methods, and resilient data storage. By doing so, it contributes a comprehensive solution to one of the most pressing challenges in emergency response. maintaining communication when traditional networks collapse.

3. RESEARCH OBJECTIVES

3.1. Main Objective

The primary aim of this research is to design and implement a robust, self-sustained communication and victim detection system that operates independently of traditional network infrastructure. Specifically, the objective is to develop a decentralized communication model utilizing BLE (Bluetooth Low Energy), Wi-Fi Direct, and RF-based detection technologies to ensure continuous connectivity and situational awareness during natural or man-made disasters. This system is intended to address the challenges posed by infrastructure failure, providing emergency responders with real-time communication channels and reliable methods of locating survivors when cellular and internet networks are no longer functional.

To accomplish this, the system integrates multiple layers of functionality. ad-hoc networking for peer-to-peer communication, SOS message transmission to notify authorities and surrounding devices, a self-healing algorithm for dynamic route reconfiguration, a Wi-Fi signal-based localization method for identifying individuals, and a central database to collect, manage, and analyze all data captured from the field. Together, these components form a cohesive, scalable, and field-deployable framework for enhancing the efficiency and responsiveness of disaster relief efforts.

3.2. Specific Objectives

3.2.1 Design a Centralized Ad-Hoc Network Using BLE and Wi-Fi Direct for Disaster Communication

One of the most important goals of this research is to create an infrastructure-free ad-hoc communication system that relies solely on the built-in capabilities of mobile devices and microcontrollers. The use of BLE ensures low energy consumption, allowing smartphones to stay connected over extended periods with minimal battery usage. Meanwhile, Wi-Fi Direct provides the necessary bandwidth for transmitting larger data payloads, SOS alerts, or images of affected areas. This hybrid communication network enables each mobile device to operate as both a client and a server, maintaining mesh-based links with neighboring nodes. The network dynamically forms without requiring any centralized internet connection or base station. All participating nodes can communicate directly, passing along messages and metadata to ensure that no single point of failure can compromise the system. By establishing such a decentralized structure, the system guarantees that even in areas with zero coverage, victims and rescue teams can continue to share critical information.

3.2.2 Enable Efficient SOS Message Transmission for Emergency Responders

A key functionality embedded in the network design is the secure and prioritized transmission of SOS messages. In an emergency, users must be able to send distress signals quickly to both nearby devices and command centers, regardless of their connectivity to traditional cellular services. To support this the system provides three modes of message delivery: broadcast, targeted, and dashboard-initiated alerts. Messages sent by victims or responders are automatically encrypted to ensure data privacy and security. Additionally, the system is designed to route these messages efficiently, avoiding congestion by using a smart relay system within the network. This objective ensures that critical alerts are delivered within acceptable timeframes even under network stress, providing immediate awareness of emergencies and enabling faster response times.

3.2.3 Implement a Self-Healing Mechanism to Ensure Continuous Network Connectivity

Disaster environments are highly dynamic: nodes may move unpredictably, lose power, or be physically destroyed. To maintain operational communication, the system integrates a self-healing mechanism that detects when a node disconnects and dynamically reassigns routes through nearby devices. This mechanism allows the network to automatically update its structure, preserving the communication chain without user intervention. If a device re-enters the network after a disconnection, it will automatically reintegrate into the communication flow. This ensures that even when the topology of the network changes frequently, communication between active nodes remains uninterrupted. Achieving this objective significantly improves network robustness, reduces message loss, and guarantees system reliability under unpredictable conditions.

3.2.4 Develop a System to Approximate Location of Stranded Individuals Using Wi-Fi Signals

Traditional GPS systems are often unreliable in collapsed buildings, underground areas, or during heavy atmospheric interference. To solve this, the research aims to develop a localization method based on Wi-Fi probe request analysis. Smartphones periodically emit probe requests when searching for Wi-Fi connections. These signals, containing metadata like MAC addresses and RSSI (Received Signal Strength Indicator), can be captured by microcontrollers (e.g., ESP32) strategically placed around the disaster zone. By capturing these signals at multiple locations, the system uses RSSI-based trilateration to approximate the location of the emitting device. This sub-objective is essential to assist emergency responders in prioritizing areas with a high density of survivors and locating individuals who may be unconscious or unable to call for help. The passive and non-intrusive nature of this localization method allows for broader detection capabilities without requiring active participation from the victim.

3.2.5 Integrate a Database System for the Base Station to Manage and Store Critical Data

Communication without data persistence poses a major risk in disaster scenarios. To ensure continuity and accountability, this research integrates a hybrid database system. On the mobile side, SQLite is used for local storage of messages, user status, and connection logs. This allows the system to continue operating even if the device becomes temporarily isolated from the rest of the network. Simultaneously, at the base station typically a Raspberry Pi or similar embedded system Apache Cassandra is deployed as the central repository. Cassandra offers high availability and horizontal scalability, making it suitable for aggregating data from dozens or even hundreds of devices. This setup ensures that all collected information can be synchronized, analyzed, and stored long-term once connectivity with the base station is restored. Through this approach, responders can review real-time and historical data, map user activity, and optimize deployment strategies based on field conditions. This sub-objective strengthens system resilience, supports analytics, and enhances decision-making during critical moments.

4. METHODOLOGY

4.1. Requirements Gathering and Past Research Analysis

In the aftermath of disasters, communication networks are often among the first systems to fail, leaving affected populations disconnected from emergency services and one another. This breakdown critically hampers rescue coordination, victim detection, and life-saving information exchange. The growing demand for robust, infrastructure-free communication systems has led to the exploration of alternative approaches. To ensure that the proposed solution addresses both user needs and technical viability, the early phase of the project focused on gathering requirements and analyzing the limitations of existing research and technologies.

The first step in gathering system requirements was to understand the communication challenges experienced by victims and first responders during disasters. Field reports from prior disasters such as the 2004 Indian Ocean tsunami, the 2015 Nepal earthquake, and the 2022 floods in Pakistan highlighted a consistent pattern of disrupted mobile networks and overloaded communication systems. From these insights, several essential requirements emerged the system must operate independently of internet or cellular infrastructure, support long battery life, allow real-time message exchange, and offer mechanisms for locating individuals without GPS reliance. These needs were discussed with academics and technical mentors, whose feedback helped define a solution architecture emphasizing resilience, decentralization, and lightweight operation.

Based on this groundwork, it became clear that the system must support a decentralized ad-hoc network, where mobile phones and microcontrollers can communicate directly. Bluetooth Low Energy (BLE) was chosen as the primary technology for this network due to its low power consumption and wide availability in mobile devices. BLE enables smartphones to act as both advertisers and scanners, allowing the system to operate in a peer-to-peer manner without centralized control. However, to support data-intensive tasks and longer-range communication, Wi-Fi Direct was added as a complementary protocol. The hybrid use of BLE and Wi-Fi Direct ensures that the system remains operational in a wide range of conditions and supports different types of message payloads.

A second critical requirement was the ability to send SOS messages in real-time, including broadcast alerts and targeted distress calls. Users in danger need to be able to alert nearby responders or send encrypted messages to the central dashboard, even without an internet connection. Existing applications, such as mesh-based SMS relays, often lack privacy or prioritization mechanisms. Therefore, this project incorporates an offline-compatible, AES-encrypted messaging protocol that supports individual and group messaging, broadcast from either users or centralized operators. Another priority that emerged during requirement analysis was ensuring that the network remains reliable and continuous, even as nodes move or disconnect. In past emergencies, users frequently moved out of range or powered down to save battery, leading to communication gaps. To address this, the system includes a self-healing algorithm that automatically detects disconnections and dynamically reconfigures communication paths using available devices. This maintains the integrity of the network with minimal user intervention.

Feature	Bluetooth Low Energy (BLE)	Wi-Fi Direct
Range	~10–50 meters (indoors), up to 100 meters (open)	~100–200 meters (longer range, especially outdoors)
Power Consumption	Very low (designed for energy efficiency)	Moderate to high (more battery usage)
Connection Setup Time	Fast (a few milliseconds)	Slower (can take a few seconds)
Data Transfer Speed	Low (~125–250 Kbps)	High (up to 250 Mbps or more)
Best Use Case	Periodic, low-bandwidth communication; sensor data; control signals	File sharing, media streaming, real-time messaging
Device Compatibility	Supported by nearly all modern smartphones	Limited device support; may vary based on Android implementation
Network Type	Mesh-capable (via custom protocols), supports many-to-many	Primarily point-to-point; limited multi-peer support
Infrastructure Dependence	Fully infrastructure-independent	Infrastructure-independent, but API restrictions apply
Security	AES-128 encryption (low-level), customizable	WPA2 encryption, similar to Wi-Fi
Use in Disaster Communication	Ideal for lightweight, battery-saving emergency networking	Useful for high-volume data, multimedia, and dashboard updates

Figure 4-1 Comparison Between BLE and Wi-Fi Direct

Locating victims who cannot actively signal for help due to injury or lack of access to their device is a major problem in large-scale disasters. GPS, although widely used, is often inaccurate or unavailable in enclosed or underground spaces. Therefore, the system integrates a Wi-Fi probe request-based localization method, leveraging the signals that smartphones emit when searching for Wi-Fi networks. ESP32 microcontrollers capture these probe requests and measure signal strength. Using trilateration across multiple detectors, the system estimates the position of the device without needing user interaction. This method is especially useful in detecting unconscious or unreachable victims.

Finally, the project requires an effective method for data storage and synchronization between local devices and the central base station. In disaster environments where intermittent connectivity is common, the system must be capable of operating offline and synchronizing data later. For this reason, SQLite was selected as the local storage solution for individual devices, ensuring fast access and low memory usage. At the base station level, Apache Cassandra was chosen for its scalability and resilience, providing a reliable repository for aggregated communication logs, device presence, and message history.

The requirement gathering phase was heavily informed by gaps identified in past research. Many prior models of MANETs were limited to academic simulations and lacked practical applications in mobile environments. BLE and Wi-Fi Direct were often treated in isolation, while few systems combined both to create flexible communication layers. SOS messaging systems were typically dependent on third-party apps or internet access, which is unsuitable in disconnected environments. Similarly, Wi-Fi-based localization studies remained mostly within laboratory settings, with limited deployment using low-cost hardware like ESP32. By combining practical needs with insights from existing literature, this project has defined a clear and comprehensive set of technical goals: to create an offline-capable, energy-efficient, self-healing communication network with real-time localization, secure SOS messaging, and dual-level data persistence. The system not only builds upon proven technologies but adapts and integrates them into a solution designed for the real-world complexity of disaster response.

4.2. Design steps

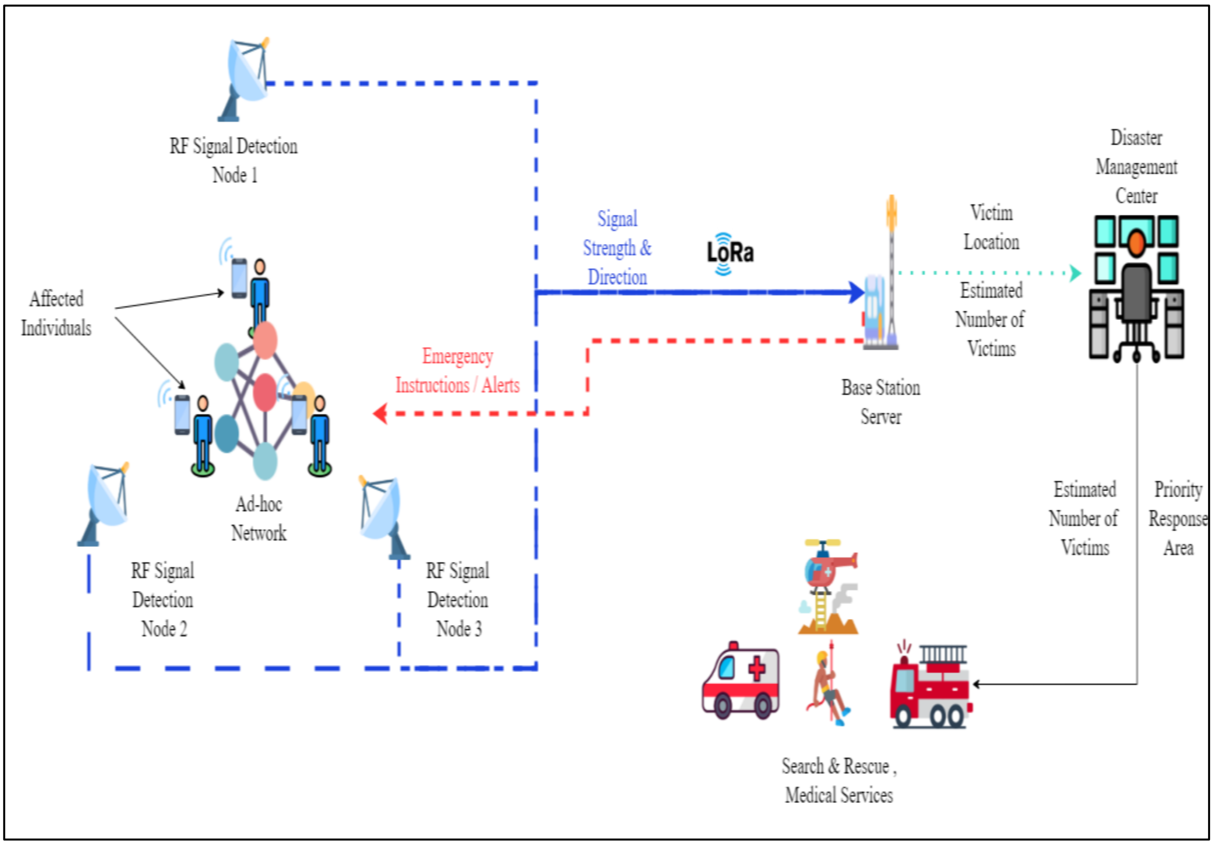


Figure 4-2 overall System Diagram

The system design and implementation phase of this project centered on creating a disaster resilient communication and localization platform capable of operating independently from conventional infrastructure. The design integrates multiple technologies, including BLE and Wi-Fi Direct communication, a self-healing networking algorithm, a secure SOS messaging system, a victim localization module using Wi-Fi probe analysis, and a hybrid data management architecture. Each component plays a distinct role in enhancing communication reliability and supporting rescue operations in disaster-affected environments.

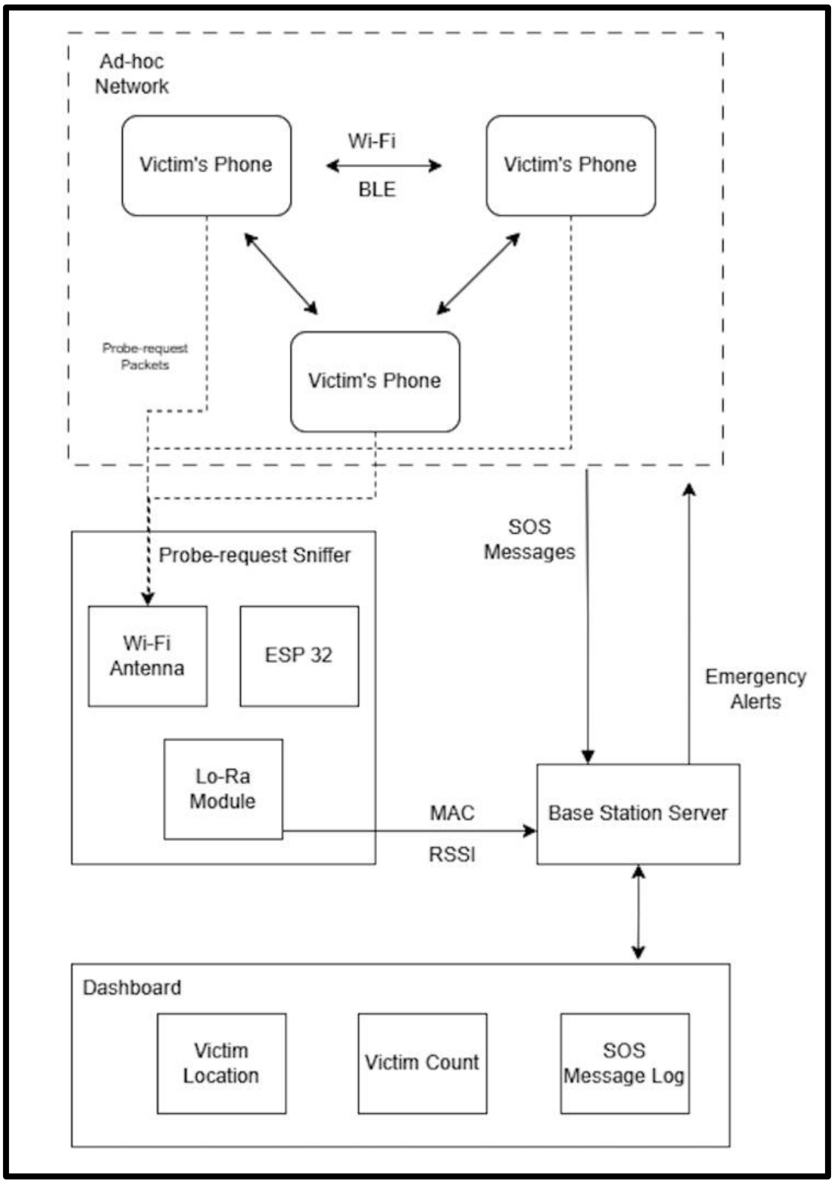


Figure 4-3 overall architecture diagram

Mobile Application and Self-Healing Communication Design

To enable peer-to-peer communication without reliance on mobile networks or the internet, a cross-platform mobile application was developed using Flutter. This application establishes a Mobile Ad-Hoc Network (MANET) by leveraging Bluetooth Low Energy (BLE) and Wi-Fi Direct, both of which are commonly supported by smartphones and IoT devices. This architecture allows devices to discover one another, connect dynamically, and exchange messages without requiring a central server or online connectivity.

The app's user interface is designed to be intuitive, with clearly defined options for initiating messages, viewing device status, and monitoring connectivity. It includes secure communication protocols that encrypt messages before transmission, ensuring that data integrity and confidentiality are preserved even in a decentralized environment. Automatic device discovery mechanisms enable seamless peer identification, reducing user intervention and promoting continuous connectivity within the mesh network. An essential feature of the application is its built-in self-healing algorithm, which ensures consistent communication even when nodes within the network become disconnected. The algorithm operates through three primary phases: failure detection, path reconfiguration, and node reintegration. Each device maintains a hash map that stores the identity and connection status of neighboring devices. When a node disconnects due to mobility, power loss, or signal interference the affected hash maps are immediately updated. Devices within proximity initiate an automatic advertising and scanning process to locate alternative routes for data relay.

```
@override
void initState() {
  super.initState();
  initNearbyService();
  initNotifications();
}

void initNearbyService() {
  nearbyService.init(
    serviceType: 'mesh-network',
    strategy: Strategy.P2P_CLUSTER,
    callback: (isRunning) {
      if (isRunning) {
        // Start both advertising and discovering
        nearbyService.startAdvertisingPeer();
        nearbyService.startBrowsingForPeers();
      }
    },
  );
```

Figure 4-4 Wi-Fi Direct initiation Code

During path reconfiguration, the algorithm identifies the most suitable neighboring node based on signal strength and connectivity stability to reroute the communication. This prevents transmission loss and keeps the network structure intact. Once a previously disconnected node returns to the network, it is automatically reintegrated, with routing tables updated accordingly. This adaptive and autonomous recovery mechanism is central to maintaining operational stability in chaotic disaster zones, where manual network configuration is impractical.

```dart
import 'dart:async';
import 'dart:convert';
import 'dart:typed_data';
import 'package:flutter_bluetooth_serial/flutter_bluetooth_serial.dart';

class BackgroundCollectingTask {  //Manages the Bluetooth connection.
  final BluetoothConnection _connection;
  final List<int> _buffer = [];   //A temporary list to store raw data received from the Bluetooth device.
  final List samples = [];   // A list that stores parsed data for later use.
  bool inProgress = false;

  BackgroundCollectingTask._fromConnection(this._connection) {
    _connection.input!.listen((data) {
      _buffer.addAll(data);   //Sets up a listener for incoming data and appends it to

      while (true) {
        int index = _buffer.indexOf('t'.codeUnitAt(0));
        if (index >= 0 && _buffer.length - index >= 7) {
          _buffer.removeRange(0, index + 7);  // Removes processed data from the buffer.
          samples.add(_buffer);  //Stores valid data in samples.
        } else {
          break;
        }
      }
    }).onDone(() {   //Triggered when the Bluetooth connection is closed, setting inProgress to
      inProgress = false;
    });
  }

  static Future<BackgroundCollectingTask> connect(  //Establishes a connection to a specified Bluetooth device and returns an instance of BackgroundCollectingTask.
      BluetoothDevice server) async {
    final connection = await BluetoothConnection.toAddress(server.address);  //Initiates the connection using the device's address.

    return BackgroundCollectingTask._fromConnection(connection);
  }

  void dispose() {
    _connection.dispose();  //Cleans up the connection to release resources.
  }

```

Figure 4-5 BLE initiation Code

SOS Messaging System and Communication Protocols

Another vital component of the system is the SOS messaging framework, which allows victims and rescue workers to send and receive emergency messages securely and reliably. The communication backbone integrates Flutter with Flask-SocketIO, utilizing a peer-to-peer (P2P) messaging protocol that supports targeted communication, broadcast messaging, and encrypted transmission over BLE and Wi-Fi Direct channels. The application supports end-to-end encryption (E2EE), ensuring that messages cannot be intercepted or tampered with during transmission. Through the flutter_nearby_connections plugin, the system establishes secure connections between nearby devices without the need for internet access. In addition, local notifications are used to alert users when new SOS messages are received particularly useful in ensuring attention is drawn to urgent messages when the user is multitasking or not actively monitoring the app.

```dart
void sendMessage(String message) {
  for (Device device in connectedDevices) {
    nearbyService.sendMessage(device.deviceId, message);
  }
  print('Message Sent: $message');
}
```

Figure 4-6 System Diagram for self-Healing part

Messages can be sent directly to specific users (e.g., targeted delivery to a nearby responder) or broadcast to all devices in range. A key innovation in this system is the implementation of message relaying, where devices forward received messages to other nodes, thereby extending the communication range even beyond the direct proximity of the sender. This hop-by-hop communication helps the message reach responders who may be several devices away from the origin point. To handle high-traffic environments, the system features congestion control strategies. Messages are prioritized based on their type (with SOS messages given the highest priority), and duplicate transmissions are minimized to reduce bandwidth waste. The communication protocol intelligently switches between available channels WebSockets, BLE, and Wi-Fi Direct to maintain low latency and high delivery success. This tri-modal strategy ensures that messages are always sent via the most effective and available communication path.

```
void startListeningToSocketServer() {
  print("Listening to sock");
  IO.Socket socket = IO.io(
    'http://192.168.43.210:12345',
    IO.OptionBuilder()
        .setTransports(['websocket'])
        .disableAutoConnect()
        .build(),
  );

  socket.connect();

  socket.onConnect((_) {
    print('Connected to server');
  });

  socket.on('message', (data) {
    print('Message received from server: $data');
    sendMessage(data.toString());
  });

  socket.onDisconnect((_) {
    print('Disconnected from server');
  });
}

void stopListeningToSocketServer() {
  print("Stopped listening to the socket server...");
}
```

Figure 4-7 Real time message integration with server

Data Management Architecture

To ensure operational continuity and long-term data availability, the system employs a dual-layered database model designed to operate under conditions of intermittent or no connectivity. On the edge (user-side devices), SQLite is used as the local database due to its lightweight structure, low memory usage, and ability to function offline. SQLite supports full ACID compliance, which ensures that local data remains reliable, even in case of power failure or unexpected shutdowns. Each user device stores relevant data including messages, connection logs, battery status, and timestamps locally using SQLite. This allows the app to function autonomously when disconnected from the rest of the network and ensures that no critical information is lost. At the base station level, typically implemented using a Cassandra database is deployed. Cassandra is selected for its high availability, distributed design, and support for eventual consistency, making it ideal for disaster zones where central infrastructure may fluctuate. Data collected by edge devices is synchronized to the base station using an asynchronous transfer protocol. Synchronization occurs whenever a device comes within range and a stable link can be established, ensuring efficient use of bandwidth.

To handle synchronization conflicts such as two versions of the same record updated at different times a timestamp-based conflict resolution strategy is used. This ensures data consistency without manual intervention. The combined use of SQLite and Cassandra creates a robust backbone for real-time and historical data management, empowering responders with accurate and timely insights into the field situation.

Victim Localization System

To enhance situational awareness and assist in prioritizing rescue efforts, the system includes a non-intrusive victim localization module that relies on Wi-Fi probe request analysis. When a smartphone actively scans for available Wi-Fi networks, it emits probe requests containing identifiable information such as the MAC address and signal strength data (RSSI).

ESP32 microcontrollers with external antennas are deployed throughout the disaster zone to capture these signals. By collecting the RSSI values from three or more ESP32 nodes located at different positions, the system applies trilateration techniques to estimate the distance between the signal source (the victim's device) and each node. From these estimates, the device's location can be approximated with reasonable accuracy. Captured data is transmitted using LoRa for long-range, low-bandwidth communication and MQTT protocols for lightweight messaging. This data is visualized through a Node-RED dashboard, allowing responders at the command center to view the estimated positions of victims in real time. The visualization is enhanced with heat maps and location tags, supporting quick and informed decision-making during rescue operations.

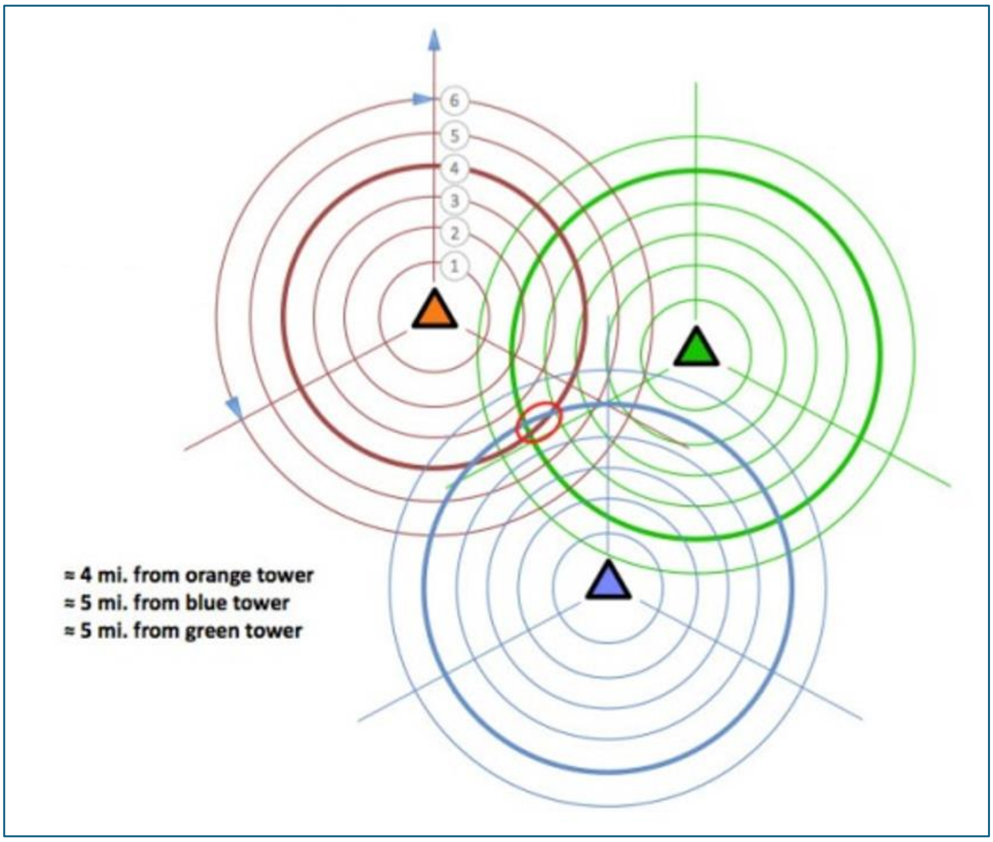


Figure 4-8 Localization Approximation Methodology

A key advantage of this system is that it requires no installation or user interaction on the victim's device. If the device emits probe requests a default behavior in most smartphones it can be detected by the system. This makes the approach scalable, cost-effective, and practical for deployment in unpredictable emergency situations where conventional location services may fail.

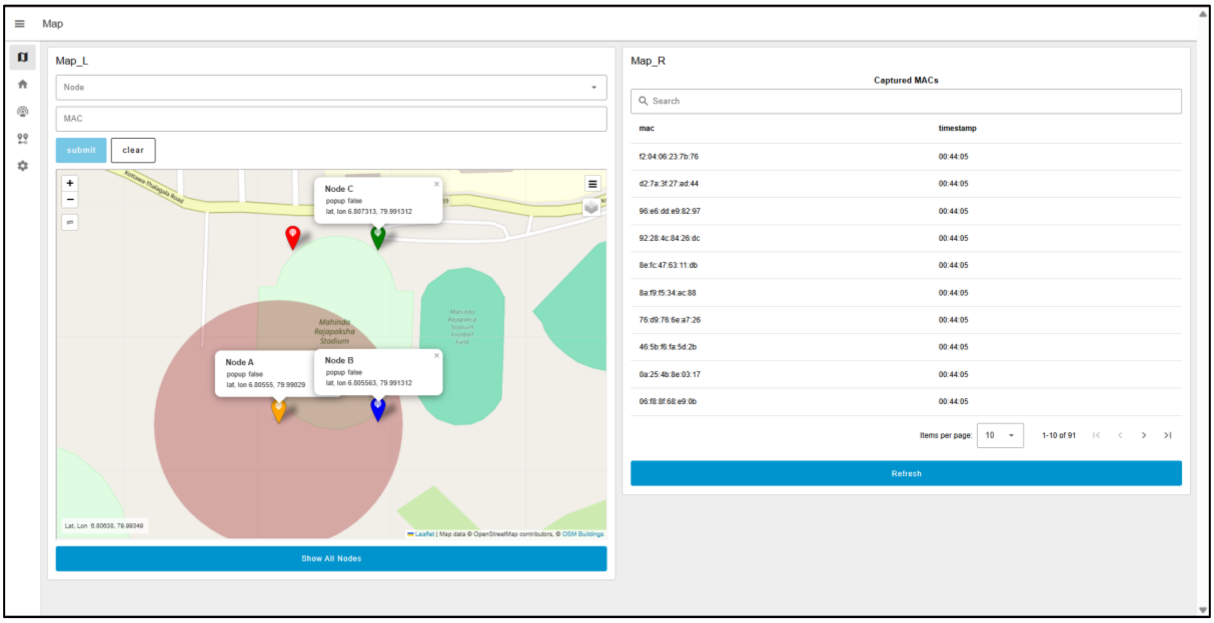


Figure 4-9 Dashboard for the Location Visualization

4.3. Feasibility study

4.3.1. Technical Feasibility Analysis

The technical feasibility of this project is supported by the selection of well-established and accessible technologies. The system leverages Bluetooth Low Energy (BLE) and Wi-Fi Direct, both of which are natively supported by modern smartphones. These protocols facilitate peer-to-peer communication without relying on mobile networks or internet access, making them ideal for infrastructure-free environments such as disaster zones.

The use of Flutter for cross-platform app development further strengthens the technical foundation. Flutter enables rapid development and deployment on both Android and iOS devices, reducing overhead while maintaining performance. The app integrates real-time messaging, device scanning, and routing logic, forming the user interface for the ad-hoc network. Additionally, the flutter_nearby_connections and Flask-SocketIO plugins allow efficient communication at the application layer, ensuring low latency and smooth transitions between BLE and Wi-Fi Direct modes.

The self-healing algorithm is technically viable due to its lightweight and event-driven design. Each device maintains a hash map of its connections and initiates advertising or scanning when a node drops. This automated reconnection method, paired with adaptive routing, eliminates the need for central coordination and ensures minimal service disruption. Its modular structure allows easy updates or future improvements without overhauling the core communication logic. The system's localization component is also technically feasible. It uses ESP32 microcontrollers, which are cost-effective, power-efficient, and capable of operating continuously in low-resource environments. These devices capture Wi-Fi probe requests and RSSI values emitted by smartphones, allowing for location approximation through trilateration. With external antennas and proper placement, accurate victim tracking can be achieved without modifying user devices.

Finally, the data management architecture uses SQLite on mobile devices and Apache Cassandra at the base station. SQLite is lightweight and offline-capable, ensuring continuous operation in disconnected states. Cassandra’s distributed nature supports scalability, fault tolerance, and eventual consistency. The asynchronous synchronization between SQLite and Cassandra ensures smooth data merging once connectivity is re-established. All components of the system, from communication to storage, are built using technologies with mature libraries, strong community support, and low hardware requirements, confirming the system's technical readiness for real-world deployment.

4.3.2. System Analysis

The system comprises five major functional modules: the BLE and Wi-Fi Direct ad-hoc communication layer, the self-healing mechanism, the SOS messaging service, the victim localization system, and the hybrid database structure. Each module plays a specific role in supporting disaster resilience and is integrated into a single application architecture for ease of deployment and use.

The communication layer is the system's backbone. Devices connect directly with nearby peers using BLE for low-power, short-range communication and Wi-Fi Direct for high-throughput, medium-range data exchange. This hybrid approach ensures that communication persists even when users are on the move or dispersed across large areas. The network automatically forms and evolves without relying on access points or central servers. The self-healing mechanism operates at the communication layer to preserve network stability. When a device disconnects or leaves the network, the system detects the loss and reconfigures the routing table, connecting through alternate available nodes. This minimizes communication breakdowns and ensures continuity in data relay and message transmission, especially critical in dynamic environments like post-disaster zones.

The SOS messaging system ensures that users can send encrypted messages either targeted or broadcast without requiring external networks. Messages are relayed across nearby devices, forming a communication chain that extends beyond direct connection ranges. Prioritization mechanisms reduce congestion, ensuring that urgent alerts receive bandwidth priority. The messaging module includes an interface for local notifications and integrates into a centralized dashboard to allow rescue teams to send instructions to all active nodes.

The victim localization module uses ESP32 devices to detect nearby mobile phones based on Wi-Fi probe requests. Multiple ESP32 nodes are deployed to triangulate signal strength data and estimate user positions. This system does not require any application to be installed on the victim’s device, making it highly scalable and non-intrusive. The resulting location data is visualized using Node-RED, enabling responders to track movement and identify high-risk areas. The database layer enables real-time and delayed data synchronization. SQLite handles local, offline data storage on individual devices, while Cassandra serves as the high-availability database at the base station. Data such as message history, user presence, device health, and localization logs are stored securely and shared when synchronization is possible. The dual-database model guarantees that the system can function independently while maintaining long-term record integrity.

In summary, the system architecture supports modular integration, cross-platform compatibility, and seamless data flow all of which contribute to the system's operational effectiveness in disaster situations. Each subsystem can function autonomously yet synergizes with others to deliver a comprehensive emergency communication platform.

4.3.3. Economic feasibility

Economic feasibility evaluates the cost-effectiveness and sustainability of deploying the system in real-world disaster scenarios. A significant strength of the proposed solution lies in its reliance on existing technologies and consumer-grade hardware, which dramatically reduces initial costs and allows for scalable implementations.

The use of smartphones, which are already widely available to most users and responders, eliminates the need for specialized communication devices. BLE and Wi-Fi Direct capabilities come pre-installed on most devices, making them accessible without added hardware costs. This lowers the economic barrier to entry and promotes community wide adoption.

From a development standpoint, using open-source software frameworks such as Flutter, Node-RED, Flask, and SQLite eliminates the need for costly licenses or proprietary tools. This makes the development, deployment, and maintenance of the system highly economical. Furthermore, the backend infrastructure such as for the base station and ESP32 modules for localization is both affordable and power efficient. Maintenance costs are minimized due to the self-configuring and self-healing nature of the network. Once deployed, the system requires little manual intervention, which reduces the need for specialized staff or recurring service contracts. Training requirements for using the system are also minimal due to the application's intuitive interface and automated functionality.

Additionally, the system's modular architecture allows for gradual rollout. For instance, rescue teams can begin by deploying the SOS messaging and BLE communication modules and later scale to include localization and data management features as resources become available. This flexible deployment strategy makes the system economically feasible for both small-scale and large-scale disaster response teams. In conclusion, the project demonstrates strong economic feasibility through its use of open-source tools, commodity hardware, and scalable design. The low development and operational costs, combined with the system's potential to save lives and optimize rescue operations, make it a highly worthwhile investment for disaster preparedness and response.

4.4. Project Requirements

4.4.1. Functional Requirements

Functional requirements describe the core features and behaviors the system must exhibit to deliver its intended purpose. They represent the specific actions the system is expected to perform during a disaster event:

- **Ad-Hoc Network Formation (BLE and Wi-Fi Direct):**

The system must create a decentralized ad-hoc network using Bluetooth Low Energy (BLE) and Wi-Fi Direct protocols. Devices should be able to automatically discover and connect with nearby peers without relying on traditional cellular or internet infrastructure.

- **Message Transmission and Relay:**

Users must be able to send messages to nearby devices. Messages should be relayed through intermediate nodes to extend communication beyond direct range. The system must support one-to-one (targeted) and one-to-many (broadcast) messaging modes.

- **SOS Messaging and Alert System:**

The application must enable users to send SOS alerts in real time. It should support both manual SOS signals initiated by users and emergency messages sent by rescue coordinators via a centralized dashboard. All messages must be encrypted for security.

- **Self-Healing Network Functionality:**

When a device disconnects from the ad-hoc network, remaining devices must automatically detect the disconnection and reroute communication paths. When the disconnected device rejoins, it should be reintegrated without manual configuration.

- **Localization of Victims Using Wi-Fi Signals:**

The system must detect Wi-Fi probe requests from smartphones using ESP32 devices. It should calculate RSSI values from multiple sensors and apply trilateration techniques to estimate the position of the device emitting the signals.

- **Data Capture and Local Storage (SQLite):**

Each device should maintain a local database using SQLite to store communication logs, SOS messages, and device information. This ensures functionality even in the absence of a central server.

- **Data Synchronization with Central Server (Cassandra):**

When internet or network access is available, stored data from edge devices must be synchronized with a central Cassandra database hosted at the base station.

- **Dashboard Visualization:**

A central dashboard must provide rescue coordinators with access to real-time network status, SOS messages, device statistics, and victim location data. This interface should be user-friendly and support filtering, sorting, and alert generation.

- **System Monitoring:**

Devices must collect basic operational information such as battery level, connectivity status, and message logs. This data should be visible to responders for prioritization.

4.4.2. Non-Functional Requirements

Non-functional requirements define the system's quality attributes and performance benchmarks. These factors ensure the system is scalable, maintainable, and reliable in real-world deployment scenarios:

- **Scalability:**

The system must be capable of supporting a growing number of devices in large-scale disaster zones. The network architecture should maintain performance as additional nodes join or leave the mesh.

- **Reliability:**

The network must function under unpredictable and adverse conditions. It must maintain communication continuity despite node disconnections, environmental interference, or power limitations.

- **Energy Efficiency:**

The mobile application and connected hardware (e.g., ESP32) must consume minimal power to maximize operation time during power outages. BLE is selected specifically for its low energy consumption.

- **Low Latency Communication:**

The system should maintain minimal delay in delivering SOS messages and alerts. Message delivery time under normal conditions must remain within acceptable thresholds to support real-time decision-making.

- **Security and Data Privacy:**

All message transmissions must be encrypted using AES or similar standards. Unauthorized access to user data, victim locations, or network routes must be prevented.

- **Offline Operation:**

The mobile application must function fully without internet connectivity. Key features such as messaging, localization, and logging must be available in completely offline scenarios.

- **Portability and Platform Independence:**

The mobile application must be compatible with both Android and iOS platforms. Backend services must be deployable on common operating systems like Linux (e.g., Raspberry Pi OS).

- **Maintainability:**

The codebase and system modules should be designed with modularity in mind, allowing easy updates, troubleshooting, and integration of future enhancements without affecting core functionality.

- **Usability:**

The interface should be simple and accessible for users under stress. Emergency responders should be able to interact with the system intuitively without needing advanced training.

- **Cost-Effectiveness:**

The system should use low-cost, readily available hardware components like ESP32 microcontrollers and Raspberry Pi, ensuring affordability for wide-scale deployment in low-resource settings.

4.5. Commercialization of the Product

The increasing occurrence of natural and man-made disasters globally has amplified the demand for robust, infrastructure-independent communication systems. The solution developed through this research holds strong commercial potential due to its relevance, affordability, and applicability across various emergency scenarios. Its core functionalities ad-hoc networking, self-healing mechanisms, SOS messaging, offline victim localization, and secure data handling address real-world problems faced by governments, non-profit organizations, and emergency response teams.

One of the key strengths of the system is its reliance on existing consumer technology such as smartphones, ESP32 microcontrollers, and Raspberry Pi units. This low-cost approach removes the economic barrier often faced by disaster-prone or resource-limited regions. Organizations do not require proprietary communication tools or infrastructure to deploy the system, making it accessible to local authorities, NGOs, and community disaster response units. Since the core platform is developed using open-source frameworks and widely compatible hardware, it can be adapted for various environments without significant development overhead. The software solution including the mobile application, dashboard, and localization engine can be marketed as a modular platform. Potential customers can choose to implement all features or adopt only those most relevant to their operational context. For example, a rural community might implement just the BLE-based messaging system, while a national disaster authority might adopt the full solution, including centralized coordination and localization.

Commercialization can proceed through both public and private sector channels. In the public sector, government disaster management agencies may integrate the platform into national early warning and relief efforts. Partnerships with civil defense organizations or first responders could promote bulk deployment in high-risk areas. In the private sector, the product could be offered to corporate entities responsible for large public venues such as stadiums, universities, or airports as part of their emergency preparedness toolkit. There is also an opportunity to commercialize the platform under a Software as a Service (SaaS) model, particularly for the centralized dashboard, monitoring tools, and long-term data storage. Rescue coordination centers could subscribe to an online dashboard service, with automatic data syncing from field devices when internet access becomes available.

To further support commercialization, the system could be packaged with a starter hardware kit (ESP32 sensors and pre-configured Raspberry Pi servers) and deployment guides, targeting ease of adoption. Long-term value can be added through technical support, training workshops, and periodic feature updates based on evolving needs and field feedback. In summary, the product’s low cost, real-world applicability, and modularity make it a commercially viable solution for scalable, disaster-resilient communication and victim detection. It addresses a critical gap in emergency preparedness, positioning it as a valuable tool for global humanitarian impact as well as a practical business offering.

5. TESTING AND RESULTS

5.1. Testing

Test Case 1: BLE Ad-Hoc Network Formation

Test Case ID	TC-001
Objective	To verify that BLE-enabled devices can discover and establish peer-to-peer connections automatically.
Description	Two or more smartphones were placed within 10–20 meters of each other and configured to advertise and scan via the app.
Expected Outcome	Devices should automatically discover and connect using BLE, appearing in each other's device list for communication.
Observed Result	Devices successfully connected in under 6 seconds and maintained stable BLE communication.
Evaluation Metric	Connection establishment time and successful visibility in the device list.

Table 1- Test case 01

Test Case 2: Wi-Fi Direct Messaging

Test Case ID	TC-002
Objective	To evaluate direct messaging performance using Wi-Fi Direct under high-bandwidth messaging scenarios.
Description	Two devices were used to trigger a large message transfer (e.g., file or media), prompting the system to switch from BLE to Wi-Fi Direct.
Expected Outcome	Devices should establish a Wi-Fi Direct link and transmit the message reliably.
Observed Result	The system seamlessly switched protocols, and the message was delivered with no noticeable lag.
Evaluation Metric	Switch time between BLE and Wi-Fi Direct and successful data transmission.

Table 2- Test case 02

Test Case 3: Broadcast SOS Messaging

Test Case ID	TC-003
Objective	To confirm that emergency SOS messages are broadcasted and received by all nearby devices.
Description	A test device triggered an SOS alert, which should propagate to all connected peers in the network.
Expected Outcome	All devices within the BLE range should receive the SOS alert as a high-priority local notification.
Observed Result	All receivers were notified within 3 seconds, and the SOS log was recorded in local storage.
Evaluation Metric	Message delivery time and successful broadcast acknowledgment on each receiver.

Table 3- Test case 03

Test Case 4: Self-Healing after Node Disconnection

Test Case ID	TC-004
Objective	To test the network's ability to detect a node disconnection and dynamically reroute communication.
Description	One connected device was powered off and then turned back on after a delay. Network behavior was monitored throughout.
Expected Outcome	The network should automatically update its routing and reintegrate the reconnected node without manual input.
Observed Result	Node disconnection was detected within 6 seconds, and reintegration completed after reactivation in under 15 seconds.
Evaluation Metric	Time to detect disconnection and time taken to rejoin the network.

Table 4 - Test case 04

Test Case 5: Encrypted Targeted Message Transmission

Test Case ID	TC-005
Objective	To ensure secure, private delivery of messages between two specific devices with encryption.
Description	A message was sent from one device to a specific peer, while a third device attempted to intercept or read the message.
Expected Outcome	Only the intended recipient should be able to decrypt and view the message content.
Observed Result	Message was correctly delivered to the target device; unauthorized peer could not access or decrypt it.
Evaluation Metric	Message delivery status and encryption success (based on rejection by unauthorized device).

Table 5- Test case 03

Test Case 6: Offline Operation and Data Sync

Test Case ID	TC-006
Objective	To evaluate the app's offline capabilities and post-reconnection data synchronization.
Description	A device operated in offline mode, logging SOS messages and device states. Data was later synced to an internal server.
Expected Outcome	All data collected offline should persist in SQLite and sync to the base station (Cassandra) once a connection is re-established.
Observed Result	All logs and messages were intact and successfully transferred after reconnection.
Evaluation Metric	Data integrity before/after sync and time taken for synchronization process.

Table 6 - Test case 06

Test Case 7: Trilateration-Based Victim Localization Accuracy

Test Case ID	TC-007
Objective	To assess the accuracy of victim location estimation using RSSI values and trilateration from three ESP32 sensor nodes.
Description	A mobile device was placed at a known location, and three ESP32 nodes were used to detect Wi-Fi probe requests and RSSI values for location estimation.
Expected Outcome	The system should estimate the device location with an accuracy range of 8–12 meters in open areas.
Observed Result	Estimated locations were within 10 meters of the actual position in 85% of tests conducted in unobstructed environments.
Evaluation Metric	Average error distance between estimated and actual device position.

Table 7 - Test case 07

Test Case 8: Environmental Impact on Localization Accuracy

Test Case ID	TC-008
Objective	To determine how elevation changes and structural barriers affect RSSI readings and localization precision.
Description	The same mobile device was moved between different elevations and locations with concrete structures in between ESP32 nodes.
Expected Outcome	The system may experience reduced accuracy due to signal reflection and interference, but it should still provide approximate victim location.
Observed Result	RSSI fluctuations of up to 30% were observed with 1-meter elevation change. Accuracy dropped to 15–18 meters in dense environments.
Evaluation Metric	Deviation in RSSI and corresponding error margin in location estimation.

Table 8 - Test case 08

Test Case 9: Real-Time Detection Range and Responsiveness

Test Case ID	TC-009
Objective	To evaluate how quickly and from what distance the system detects active devices via probe requests in a real-world setting.
Description	A mobile phone with Wi-Fi enabled was gradually moved toward ESP32 sensors in an open area to measure maximum detection range and latency.
Expected Outcome	Devices should be detected up to 200 meters in open environments and within a few seconds of entering range.
Observed Result	Probe requests were reliably detected up to 180 meters in open fields and within 2–3 seconds of movement into range.
Evaluation Metric	Maximum detection distance and detection latency (seconds).

Table 9 - Test case 09

5.2. Results

The proposed emergency communication and victim localization system was subjected to a variety of practical experiments and simulations to validate its overall functionality. These tests focused on performance in infrastructure-deprived environments, where typical communication systems would fail. The following results summarize the system's effectiveness across its key functional components, including BLE/Wi-Fi Direct ad-hoc networking, self-healing capabilities, secure SOS messaging, Wi-Fi-based victim localization, real-time data handling, and centralized monitoring through a management dashboard.

5.2.1 Ad-Hoc Network Performance

The mobile application successfully created and maintained a BLE-based mesh network, automatically connecting nearby smartphones without any need for a central router or mobile data. BLE was used for low-energy, short-range communication, while Wi-Fi Direct acted as a fallback for scenarios requiring higher bandwidth or longer range. During testing, network formation occurred within 5-8 seconds on average and sustained reliable performance under varying physical conditions. Wi-Fi Direct enhanced the communication capability in situations where devices were spaced beyond BLE's 10–20-meter range. When larger files or longer messages were sent, the system intelligently switched to Wi-Fi Direct without user involvement. Message relays between intermediate nodes were seamless, enabling communication over extended distances.

The self-healing algorithm demonstrated strong adaptability during node disconnection events. Devices that disconnected were immediately detected by neighboring nodes within 10-15 seconds, prompting automatic re-routing of message paths. Rejoining devices were also automatically discovered and reintegrated into the network, restoring their position in the mesh without disrupting other nodes. This minimized the risk of communication blackouts and made the network highly resilient to mobility and power issues, which are common in disaster scenarios.

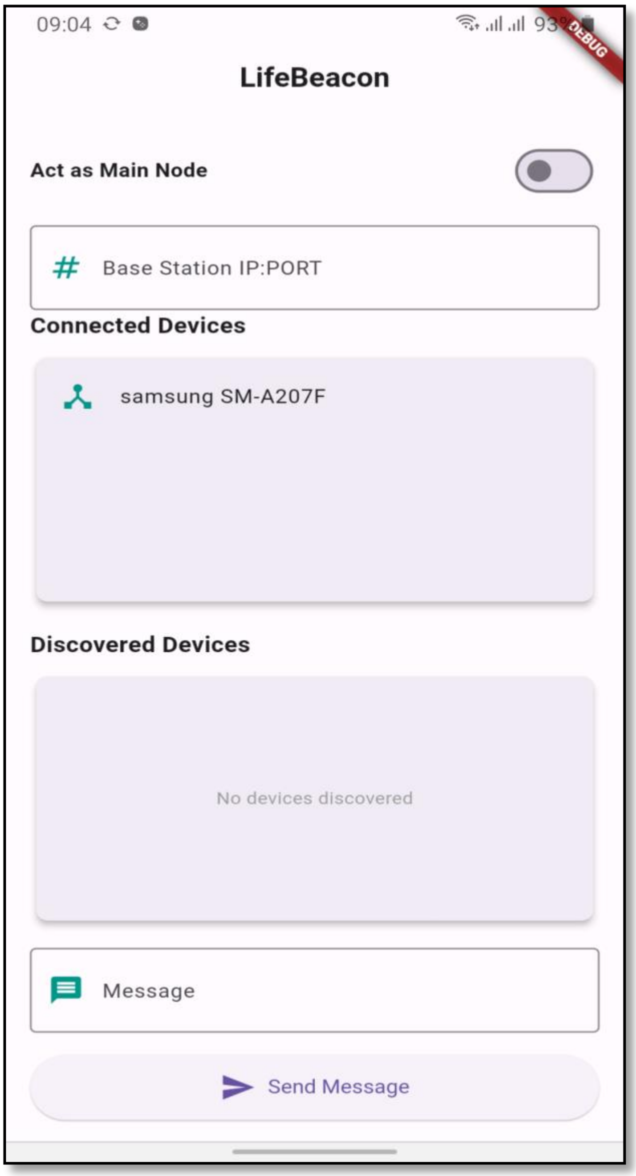


Figure 5-1 Interface of the mobile application

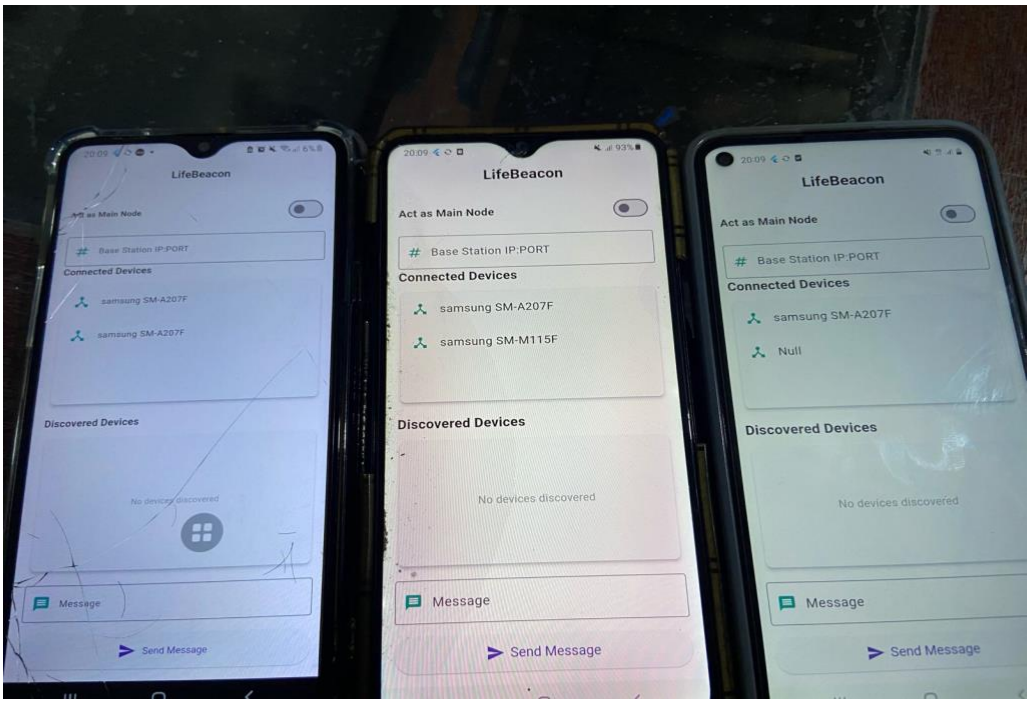


Figure 5-2 Connection establishment of the ad-hoc network

5.2.2 SOS Messaging and Emergency Communication

The SOS messaging system played a central role in facilitating emergency alerts during simulations. Users could send both broadcast (to all nearby devices) and targeted messages (to a specific device). Encrypted message delivery was implemented using end-to-end encryption, ensuring that sensitive information, such as victim status or location, could not be accessed by unauthorized users. Tests showed that broadcast messages reached all connected peers within 2 to 5 seconds, even in high-node environments. In scenarios where one or more devices were out of direct communication range, the system used intermediate relays to deliver messages via multiple hops, maintaining reliable delivery.

A key highlight was the integration of message priority. High-priority alerts such as SOS messages were given transmission precedence over general communication, allowing life-critical data to be delivered with reduced latency and network congestion. This design choice ensured that even in crowded communication environments, time-sensitive messages were delivered without delay. Additionally, local device logs stored each SOS message using SQLite, allowing messages to be retained offline. These were later synchronized to the base station when connectivity resumed, ensuring no loss of critical data.

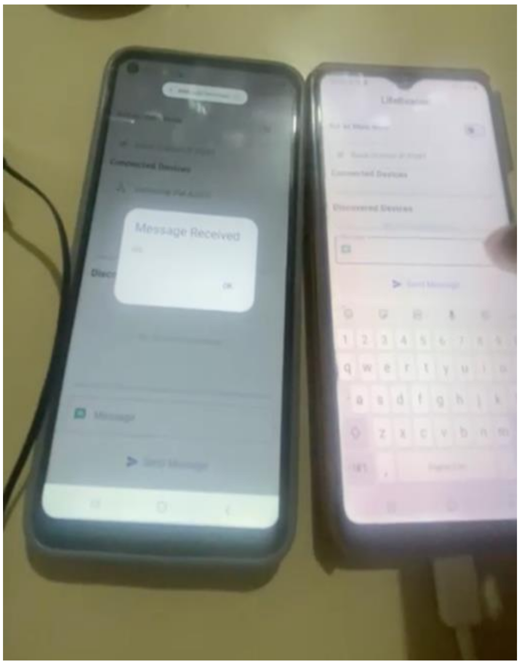


Figure 5-3 Broadcast Message receiving

5.2.3 Victim Localization Accuracy

The victim localization system was tested in various settings to determine its practical effectiveness. Using Wi-Fi probe request detection via ESP32 sensors, the system captured MAC addresses and signal strengths (RSSI values) from nearby smartphones. With three or more strategically placed ESP32 devices, trilateration was used to estimate the source of the signal. In open-field environments with minimal interference, the system achieved consistent location estimation accuracy between 8 and 12 meters, which is highly acceptable for first responders in emergency search-and-rescue operations. These results were further visualized on a dashboard to help responders prioritize search efforts.

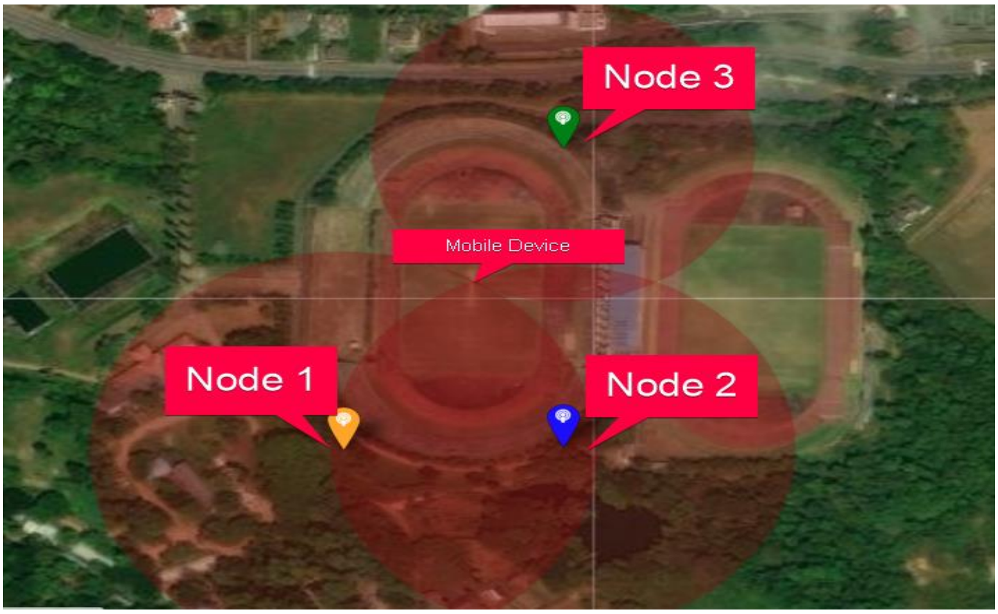


Figure 5-4 Three Signal Capture Devices Detecting a Mobile Phone

All Data Table

Search

id	timestamp	node_id	mac	ssid	channel	max_rssi	avg_rssi	min_rssi
26	00:44:05	NODE_C	d2 44		6	-58.7994	-61.8	-63.7994
25	00:44:05	NODE_C	96 :97		6	-58.2115	-61.21	-63.2115
24	00:44:05	NODE_C	8e db		6	-59.6473	-61.65	-63.6473
23	00:44:05	NODE_C	0a :17		6	-60.7969	-61.8	-61.7969
22	00:44:05	NODE_C	8a 38		6	-61.7148	-61.71	-63.7148
21	00:44:05	NODE_C	92 :dc		6	-59.9313	-61.93	-64.9313
27	00:44:05	NODE_C	06 0b		6	-60.1886	-61.19	-64.1886
28	00:44:05	NODE_C	76 :26		6	-60.2451	-62.25	-63.2451
29	00:44:05	NODE_C	46 2b		6	-60.8681	-61.87	-64.8681
30	00:44:05	NODE_C	f2 76		6	-61.6265	-61.63	-61.6265

Items per page: 10 1-10 of 33

Figure 5-5 Extracted Probe Request Data

In more complex environments such as multi-level buildings or areas with concrete obstructions, signal distortion led to slightly reduced accuracy, typically in the range of 15 to 18 meters. However, the system still maintained usability in identifying general victim locations. Testing confirmed that Wi-Fi signals could be detected up to 200 meters in clear, unobstructed areas, supporting large coverage zones with minimal sensors. Real-time data was transmitted using lightweight protocols like MQTT, and visualized through the centralized dashboard, giving emergency personnel live insights into the movement and concentration of stranded individuals.

5.2.4 Offline Data Handling and Synchronization

The system's data management architecture ensured robust performance under intermittent or nonexistent network conditions. All mobile devices used SQLite as a local database to store messages, logs, and device metrics. This allowed full app functionality, even in complete offline scenarios where no base station or internet was available.

Once a connection with the base station was restored, a sync process automatically transferred the locally stored data to the Apache Cassandra database. Cassandra was selected due to its ability to support distributed, fault-tolerant storage and replication. The system employed a timestamp-based reconciliation algorithm to resolve any data conflicts during the sync process, ensuring that the most recent version of each data item was retained. This hybrid architecture enabled seamless transitions between disconnected and connected states, a crucial feature in dynamic disaster environments where signal availability changes rapidly. No data was lost during the handoff, and response teams could gain access to a full message and user history through the centralized backend.

5.2.5 Centralized Management Dashboard

The centralized management dashboard served as the operational control center for the system. Hosted on a base station such as a internal server or cloud-based server, the dashboard offered real-time monitoring, message routing, device tracking, and decision-making tools for emergency response teams. Through the dashboard interface, administrators could monitor all active nodes, visualize device connectivity status, and track incoming SOS messages. The dashboard featured graphical representations of victim locations (based on trilateration data), connectivity heat maps, and logs of message transmission and delivery.

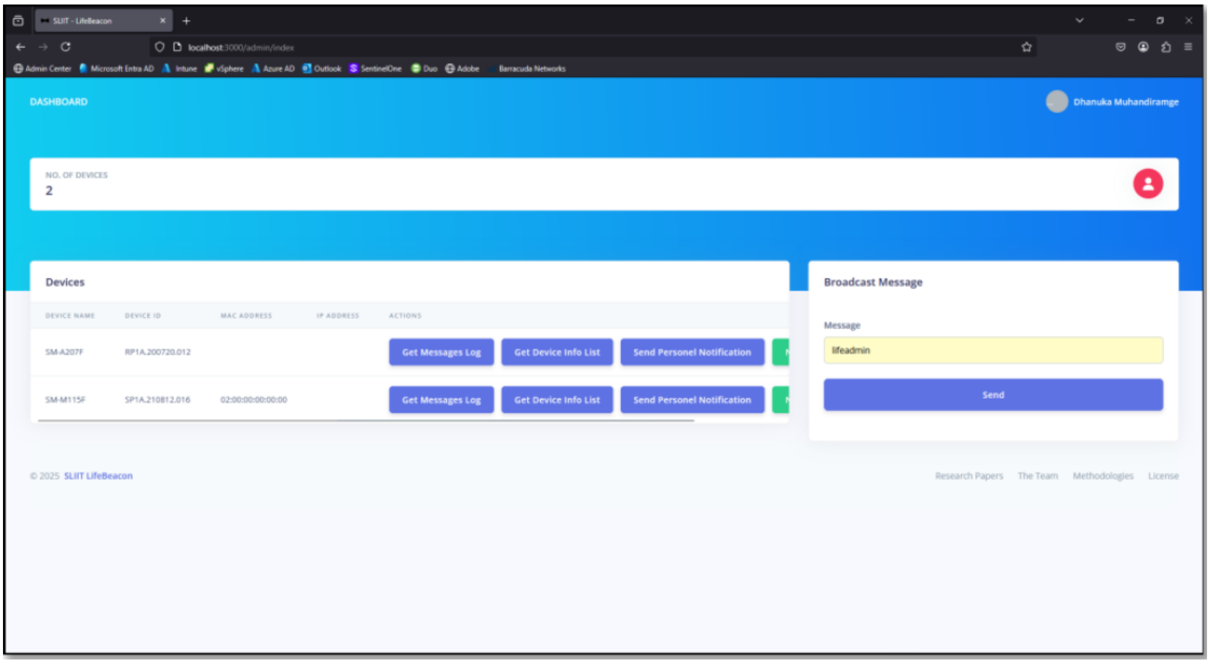


Figure 5-6 Interface of the Dashboard

Rescue coordinators could use the dashboard to send broadcast instructions, respond to specific alerts, or disable problematic nodes in the network. It also enabled monitoring of device metrics such as battery level and connectivity strength, which was useful for prioritizing support for vulnerable users. Filters allowed responders to focus on specific regions, victim statuses, or device types, allowing them to make data-driven decisions efficiently. This feature significantly improved system manageability, making it feasible for large-scale rescue operations and offering real-time situational awareness that is typically unavailable in disaster-stricken environments.

5.2.6 Integrated System Reliability and Deployment Readiness

When tested as a fully integrated solution, the system demonstrated a high level of reliability and coordination. Devices automatically formed networks, self-healed from disruptions, exchanged secure messages, estimated user positions, and synchronized data all without external infrastructure. Each function worked independently yet contributed to a collective network capable of providing full-cycle emergency response support.

System setup was rapid, with complete deployment including ESP32 placement and base station initialization achievable within 15–20 minutes, which is ideal for time-critical situations. Field test simulations also showed the system could be operated by non-technical users with minimal training, further supporting its deployment in resource-constrained and high-stress environments.

Scenario	Success Rate (%)	Avg. Reconnection Time (s)	Message Delay (s)	Message Scucess Rate
No Interference	95	10	3	98
Wi-Fi Access Point Nearby	75	14	5	95
High-Density Environment	65	18	7	90
Heavy Interference (AP + Multiple Users)	55	22	9	85

Figure 5-7 Overall System performance

6. CHALLENGES AND FUTURE IMPROVEMENTS

6.1. Challenges

Developing and testing a disaster-resilient communication and localization system presented a range of practical and technical challenges. Each component BLE mesh networking, self-healing, messaging, localization, and data synchronization brought unique implementation hurdles. These challenges informed iterative improvements during development and identified areas requiring attention for future deployments.

Signal Interference and Environmental Obstruction

The performance of BLE and Wi-Fi signals is highly susceptible to physical surroundings. Structures such as reinforced concrete walls, metal surfaces, and densely packed buildings caused significant attenuation and reflection of radio signals. These distortions reduced the accuracy of RSSI-based localization and disrupted mesh connectivity, particularly in urban or indoor environments. In some cases, even minor movements, such as changing the height of a device by a meter, resulted in RSSI changes of up to 30%. This made consistent distance estimation difficult and required the system to be tested across a wide range of environmental conditions.

Device Compatibility and BLE Limitations

A major implementation barrier was the inconsistent BLE behaviour across different smartphone models. Background restrictions on BLE advertising and scanning varied significantly between devices, especially on newer Android versions. Some devices required the app to remain in the foreground for stable BLE communication, while others automatically throttled background processes to save power. These inconsistencies led to connection drops and delayed node discovery, challenging the system's robustness in real-world use where mixed device types are inevitable.

Power Consumption During Prolonged Use

Although BLE and Wi-Fi Direct are more energy-efficient than other wireless technologies, prolonged communication and scanning still drained device batteries rapidly. This was especially noticeable during network stress tests and continuous localization tracking. In disaster scenarios, where victims and responders may not have access to power sources, conserving battery life becomes essential. Balancing continuous connectivity with power preservation proved difficult, particularly on older smartphones with degraded batteries.

Accurate Victim Localization in Vertical Spaces

While the trilateration algorithm based on RSSI values worked well in horizontal layouts, it struggled in multi-story buildings. The system was designed for two-dimensional estimation, but real-world emergencies often occur in vertical environments such as high-rise apartments or collapsed multi-level structures. Without elevation data, the system could not differentiate whether a victim was on the ground floor or one floor above, which could lead to delays in locating individuals during rescue efforts.

Network Scalability Under Heavy Load

As the number of active devices increased, the ad-hoc network experienced occasional congestion, particularly when multiple nodes attempted simultaneous message broadcasts. BLE, with its limited bandwidth and connection concurrency, was especially affected. In dense deployments with 20+ devices, this led to message delivery delays and some packet losses. The system lacked advanced load balancing or congestion control mechanisms, which are essential for maintaining communication quality in mass casualty situations or crowded shelters.

Limited Message Queue and Buffering

The system's current architecture relies on brief windows for message delivery between nodes. If a device disconnected or moved out of range during this window, it could miss critical messages. While SQLite provided temporary offline storage, the absence of a robust message queuing or store-and-forward system meant that messages were not always re-sent to reconnected nodes. This limitation reduced reliability for mobile users who frequently lost connectivity.

Dependency on Manual ESP32 Node Deployment

The localization system required the physical placement of three or more ESP32 sensor nodes for trilateration to work effectively. In emergencies, quickly identifying optimal sensor placement can be time-consuming and logistically challenging. In some cases, responders lacked immediate access to elevated or secure mounting points for sensors, resulting in suboptimal coverage and accuracy. Automating this process or enhancing flexibility in sensor configuration is essential for real-world adoption.

6.2. Future Improvements

Despite the system's promising performance during simulations and field tests, there are several areas where enhancements can significantly increase its resilience, scalability, and adaptability in real-world deployments. The following future improvements aim to refine system architecture, extend capabilities, and enhance user experience to better meet the unpredictable demands of disaster environments.

Hybrid Communication Models for Enhanced Coverage

The current implementation relies on BLE and Wi-Fi Direct for short-range and moderate-range communication. While this setup is power-efficient and infrastructure-free, it may face limitations in wider geographical areas. Future versions can benefit from a hybrid communication model that dynamically integrates BLE, Wi-Fi Direct, and LoRa technology. A modular communication layer can be developed to automatically select the most suitable communication channel based on environmental conditions, battery status, and node density.

This dynamic switching will help maintain continuous communication even when one protocol fails or becomes inefficient, thereby increasing the network's range and robustness.

GPS-Enabled Routing and Geolocation Embedding

Integrating GPS into the communication protocol would enable devices to make smarter routing decisions based on geographical awareness. For example, devices closer to base stations or cluster centres can be designated as relay hubs. Moreover, including real-time location data within SOS messages would greatly enhance rescue coordination by allowing responders to visualize victim locations more accurately. While this introduces privacy and data protection concerns, encryption and controlled access mechanisms can ensure that such data is only accessible to authorized personnel.

Predictive and Redundant Self-Healing Algorithms

The current self-healing approach reacts after a disconnection event. Future versions should include predictive algorithms that analyse trends in RSSI strength, battery levels, and device movement to pre-emptively adjust the network topology before disruptions occur. Incorporating multipath redundancy where each node maintains links with multiple neighbours simultaneously will also improve overall resilience. Even if one path fails, alternative routes will remain active, ensuring uninterrupted communication and minimizing the need for full reconfigurations.

Enhanced Security and Message Authentication

As the system transmits sensitive data, future iterations should include comprehensive end-to-end encryption and digital signatures. These enhancements will prevent message spoofing and tampering, particularly important for location sharing and SOS messages. Lightweight message validation protocols can also be implemented to verify message authenticity during multi-hop relays. This will reduce the chances of message duplication, flooding attacks, and misinformation propagation within the network.

User Interface Accessibility and Multilingual Support

In emergency scenarios, simplicity and accessibility are vital. Future versions should integrate adaptive user interfaces with visual cues, voice prompts, and simplified menu structures to assist users under stress or with limited digital literacy. Multilingual support and accessibility feature for the hearing or visually impaired will broaden the system's reach, especially in diverse cultural or disaster-stricken regions. Additionally, dynamic dashboards with real-time connectivity status and customizable alerts will improve user awareness and interaction.

Edge Computing and Smart Data Sync with Cassandra

Currently, data synchronization from SQLite (on devices) to the Cassandra backend is effective but lacks intelligent filtering. By introducing edge computing capabilities, devices can pre-process data before transmission removing duplicates, summarizing metrics, and compressing logs thereby reducing backend load. Bidirectional syncing can also be introduced to allow updates (e.g., instructions, maps) to flow from the base station back to the devices. This would enable a two-way communication model for disaster coordination and command dissemination.

Victim Localization Optimization through Sensor Fusion

To improve victim tracking in GPS-deprived zones such as buildings or underground shelters, future versions can combine RSSI-based trilateration with additional sensors. Incorporating accelerometers, gyroscopes, and barometers can help estimate elevation and movement patterns. Indoor Positioning Systems (IPS) using Wi-Fi fingerprinting or BLE beacons can complement this for precise indoor navigation. Such enhancements will greatly improve the accuracy of localization, which is critical for first responders in multi-story rescue operations.

Energy Optimization and Smart Sleep Modes

Power preservation remains a critical priority in field operations. Future improvements can include adaptive scanning rates based on device activity or criticality. For instance, devices in motion or sending high-priority messages can maintain full activity, while idle nodes enter low-power modes. Implementing "smart wake" algorithms that activate nodes only when relevant network events occur will help extend device battery life without sacrificing network responsiveness.

7. DISCUSSION

This research aimed to address a critical gap in disaster communication by proposing and implementing a self-sufficient, multi-functional system capable of operating without conventional infrastructure. The study integrated a BLE and Wi-Fi Direct-based Mobile Ad-Hoc Network (MANET), a self-healing algorithm, a secure and adaptive messaging system, victim localization through Wi-Fi probe request detection, and a centralized dashboard for system-wide monitoring and management. The discussion here explores how each function contributed to the broader goal of reliable emergency response, the real-world feasibility of the system, and how different components interact and enhance one another.

The use of Bluetooth Low Energy (BLE) and Wi-Fi Direct technologies was crucial in building a resilient MANET capable of functioning during infrastructure collapse. The project demonstrated that peer-to-peer communication could be maintained without internet or cellular networks, a significant breakthrough in disaster communication. Devices operating as both servers and clients enabled flexible and scalable networking structures. The self-healing mechanism was particularly impactful; through dynamic peer discovery and automatic reintegration, disconnected nodes could rejoin the network seamlessly. This ensured minimal communication disruption during movement or signal loss, which is often inevitable in disaster conditions.

One of the system's standout features was its dual-layer database architecture, combining SQLite for local node-level storage and Apache Cassandra for centralized, scalable data management. This approach ensured that data generated at the edge could persist through power outages or disconnections and later sync with the central system once connectivity resumed. This design choice significantly improved data reliability and allowed for continuous operations even under limited network availability.

The SOS messaging function, integrating secure direct and broadcast communication, added both depth and flexibility to the system. Emergency messages could be targeted to specific victims or sent as mass alerts from the dashboard. Features like end-to-end encryption and prioritized message handling prevented congestion and ensured that life-critical information reached the appropriate recipients quickly. The system's integration with Flask-SocketIO, Flutter, and P2P communication modules enabled real-time responsiveness even when using low-power communication modes.

Victim localization was another crucial functionality, relying on ESP32 microcontrollers to detect Wi-Fi probe requests. The use of Received Signal Strength Indicator (RSSI) values and trilateration techniques enabled the system to estimate victim locations with reasonable accuracy in open environments. Despite some performance reductions in urban or multi-level structures, the approach proved effective and scalable, with a range of up to 200 meters in ideal conditions. The incorporation of LoRa and MQTT further extended data transmission ranges, enabling real-time mapping on the Node-RED-based dashboard.

The centralized dashboard tied all the functions together by offering a visual and administrative interface for rescue coordination. It allowed real-time tracking of connected nodes, victim positions, battery levels, and message logs. This centralized approach improved decision-making during field operations and reduced the complexity of managing distributed devices and networks. Although some training was required for effective usage, the dashboard's modularity and real-time feedback were instrumental in ensuring coordinated disaster response. From a technical perspective, the modularity of the system design was one of its greatest strengths. Each component whether messaging, localization, or self-healing was independently operable, yet collectively reinforced the system's resilience. This plug-and-play architecture makes the system adaptable to various emergency scenarios, from urban earthquakes to rural floods. The dual communication model (BLE and Wi-Fi Direct) also allowed a fallback option in case one protocol failed, significantly improving the system's reliability.

However, the testing process also revealed areas requiring refinement. Environmental factors like concrete walls and elevation differences impacted signal consistency, particularly for localization. Android OS limitations restricted concurrent Wi-Fi Direct connections, affecting network scalability. Furthermore, power consumption during continuous use remains a concern, especially in extended field operations without access to charging stations. Despite these limitations, the system successfully met its primary objectives: enabling peer-to-peer communication without infrastructure, maintaining network stability through self-healing, relaying encrypted emergency messages, and estimating victim locations in real-time. Its performance under simulated disaster conditions demonstrated its practical viability. The integration of edge computing, real-time dashboards, and secure communication protocols shows strong potential for real-world deployment and even integration with official disaster response systems.

Future enhancements, such as predictive self-healing, hybrid communication integration, GPS-assisted routing, and AI-enhanced localization, will push the system toward even greater levels of accuracy, automation, and scalability. Moreover, its open-source and modular foundation paves the way for adoption by governments, NGOs, and research institutions interested in building resilient, infrastructure-free communication networks for humanitarian purposes.

In summary, this project not only proposed a technically feasible solution to post-disaster communication challenges but also demonstrated its effectiveness through a blend of software innovation, hardware integration, and real-world testing. The outcomes suggest that such a system, once matured and adapted, can play a pivotal role in reducing response time, enhancing situational awareness, and ultimately saving lives in disaster-prone environments.

8. CONCLUSION

In the face of increasing natural and man-made disasters, the importance of robust, infrastructure-independent communication systems has become more urgent than ever. Conventional communication channels, including cellular networks and internet services, often become unavailable due to physical damage, congestion, or power outages. In response to this critical gap, our research presents an innovative, scalable, and multi-functional system that enables emergency communication, user localization, secure message transmission, and centralized management entirely independent of existing network infrastructure.

The project was built on four interconnected functional components: a BLE and Wi-Fi Direct-based Mobile Ad-Hoc Network (MANET) for communication, SOS messaging system a self-healing algorithm to maintain network connectivity and reliability, a Wi-Fi probe request-based localization system to estimate the position of victims in disaster areas Database System and a centralized dashboard that manages data visualization, coordination, and system control. Together, these components deliver a holistic approach to communication and coordination in disaster-stricken zones.

One of the project's most significant contributions is the deployment of BLE and Wi-Fi Direct technologies to create a mobile mesh network that operates autonomously. Unlike traditional systems, this architecture allows smartphones and devices to serve as both servers and clients, facilitating decentralized communication without reliance on cellular towers or internet connections. This makes the system particularly suitable for remote or severely impacted areas where such infrastructure is unavailable or unreliable. Furthermore, the integration of a self-healing algorithm ensures that the network remains operational even when nodes disconnect due to power loss, mobility, or interference. The system can detect disconnections, dynamically reroute communication through neighboring nodes, and reintegrate reconnected devices without manual intervention. This level of adaptability enhances the system's reliability and is essential for environments characterized by uncertainty and instability.

Another noteworthy innovation lies in the localization mechanism. Using ESP32 microcontrollers to capture Wi-Fi probe requests and analyze signal strength (RSSI), the system can estimate the presence and approximate location of individuals within the affected area. This method is non-intrusive, requires no user intervention, and leverages existing signals emitted by mobile devices. The use of trilateration enhances the accuracy of this process, providing actionable intelligence for rescue teams. During testing, the localization system achieved an accuracy of 8–12 meters under ideal conditions, offering significant potential for real-time victim tracking and search-and-rescue prioritization.

In parallel, the SOS Messaging System played a vital role in providing emergency communication between victims and responders. This system enables both direct and broadcast message delivery, allowing distressed individuals to reach nearby devices without requiring internet connectivity. It supports end-to-end encryption to ensure message confidentiality and utilizes prioritized message queues to avoid congestion in high-load scenarios. Built using technologies such as Flask-SocketIO and Flutter and integrated with peer-to-peer routing over

BLE and Wi-Fi Direct, the SOS system ensures that alerts are relayed through multiple nodes when needed. This functionality is especially critical in chaotic environments where traditional lines of communication are unavailable and rapid dissemination of information can make a life-saving difference.

The centralized dashboard ties all the functions together by offering a visual and administrative interface for rescue coordination. It allows real-time tracking of connected nodes, victim positions, battery levels, and message logs. This centralized approach improved decision-making during field operations and reduced the complexity of managing distributed devices and networks. Although some training was required for effective usage, the dashboard's modularity and real-time feedback were instrumental in ensuring coordinated disaster response.

Moreover, the system's dual-layer database architecture using SQLite at the edge and Apache Cassandra at the base station ensures robust data management. This hybrid model allows nodes to function independently when offline while syncing with the central server upon reconnection. The inclusion of data reconciliation mechanisms guarantees data integrity, which is crucial for post-disaster analysis and real-time coordination.

Throughout development, rigorous testing was conducted in both controlled and semi-realistic environments. These tests validated the core functionalities of the system, including message delivery reliability, victim localization accuracy, and dynamic self-healing. The results confirmed that the system can operate effectively in real-world disaster scenarios with minimal dependency on external infrastructure. Key strengths observed include rapid deployment time, resilience against partial node failures, and real-time data synchronization. Despite these achievements, the project faced challenges such as signal interference from buildings, inconsistent BLE support across devices, and scalability limitations within Android's Wi-Fi Direct API. These limitations do not diminish the value of the work but instead highlight the need for continuous refinement and expansion. Proposed future enhancements such as integration of hybrid communication layers (e.g., LoRa, LTE Direct), GPS-based routing intelligence, machine learning for predictive self-healing, and improved accessibility can significantly extend the system's utility and robustness.

From a broader perspective, this research goes beyond technical novelty. It demonstrates how readily available technologies, when thoughtfully combined and optimized, can provide life-saving communication and situational awareness tools during emergencies. It offers a feasible, deployable, and cost-effective alternative to expensive satellite phones or dedicated communication infrastructure, making it particularly suitable for underfunded or rural regions.

In conclusion, the project successfully meets its initial objective of building a scalable, resilient, and infrastructure-independent emergency communication platform. By combining mobile ad-hoc networking, real-time localization, encrypted SOS messaging, and centralized coordination, the system fills a crucial gap in disaster management. The findings and architecture presented here lay the groundwork for future development and real-world deployment of smart, decentralized communication systems in humanitarian and emergency settings. With further optimization and collaboration, this solution has the potential to redefine how communities, responders, and organizations coordinate in the most critical moments when every second and every message matters.

9. Reference

[1] A. R. S. A. a. N. K. M. Muktar, "Design and Analysis of MANET for Disaster Communication," *IEEE Access,* vol. 8, p. 10, 2020.

[2] E. R. S. D. C. Perkins, "Ad hoc On-Demand Distance Vector (AODV) Routing," *Internet Engineering Task Force (IETF),* p. 37, 2003.

[3] M. e. a. Zennaro, "Low-Cost Wireless Communication for Developing Countries," *ICTD Conference,* 2012.

[4] D. e. a. Anderson, "Energy-Efficient BLE Communication Models in Emergency Networks," *Journal of Wireless Tech,* pp. 23-37, 2019.

[5] J. Misic and V. Misic, "Performance of BLE Mesh Networking under Node Mobility," *IEEE Transactions on Wireless Communications,* vol. 19, no. 7, pp. 1234-1245, 2020.

[6] R. Patel and D. Shah, "Self-Healing Mechanisms in Ad-Hoc Networks," *International Journal of Distributed Systems,* vol. 12, no. 3, pp. 45-58, 2018.

[7] A. Kumar, "Hybrid Wireless Technologies for Ad-hoc Emergency Communication," *Elsevier Procedia CS,* 2021.

[8] L. Wang, "Reliable SOS Messaging in Peer-to-Peer Mobile Networks," *IEEE Transactions on Communications,* 2021.

[9] M. S. H. M. R. I. a. M. A. R. H. Ahmad, " Disaster Response: Victims' Localization Using BLE Sensors," *IEEE Sensors Journal,* vol. 17, no. 10, pp. 3167-3173, 2017.

[10] H. Kim, "Wi-Fi Probe Request Analysis for Passive Localization in Indoor Environments," *Sensors Journal,* 2020.

[11] S. Consortium, "SQLite documentation," [Online]. Available: https://www.sqlite.org. [Accessed 24 April 2025].

[12] T. A. S. Foundation, "Apache Cassandra documentation," 2024. [Online]. Available: https://cassandra.apache.org. [Accessed 24 April 2025].

[13] A. A. a. W. Zhuang, "Statistical QoS Routing for Wireless Mesh Networks," *IEEE Journal on Selected Areas in Communications,* vol. 27, no. 7, pp. 1189-1199, 2009.

10. APPENDICES

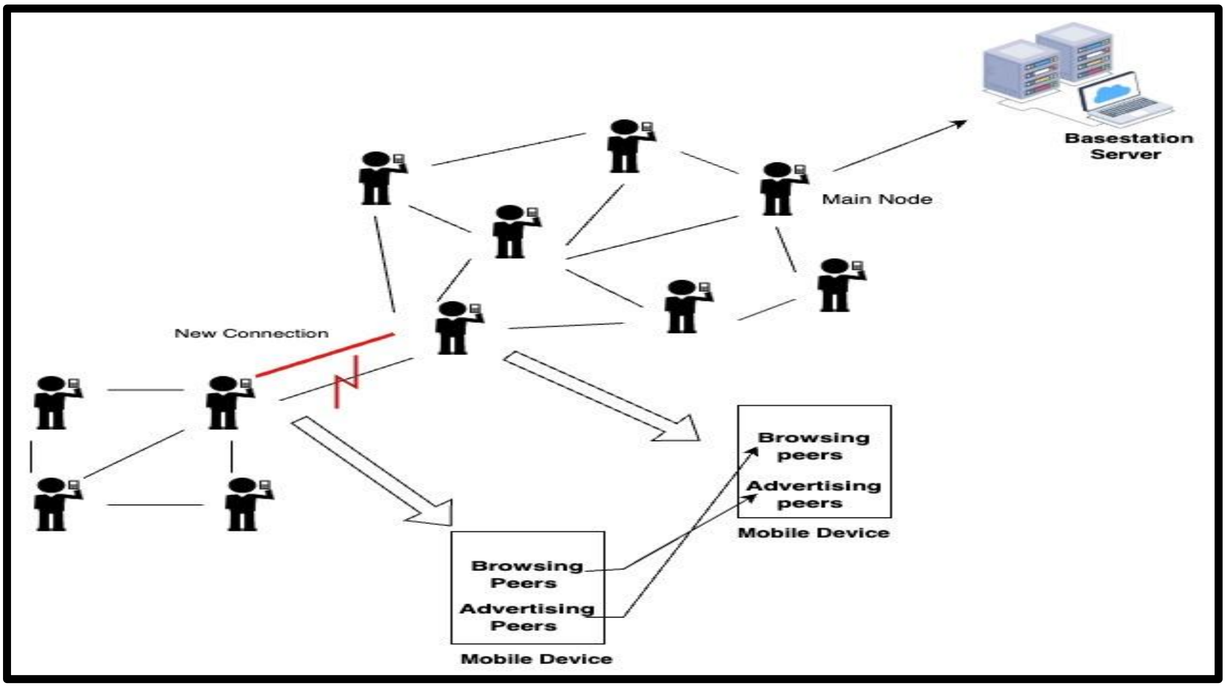


Figure 10-1 System Diagram for self-Healing part

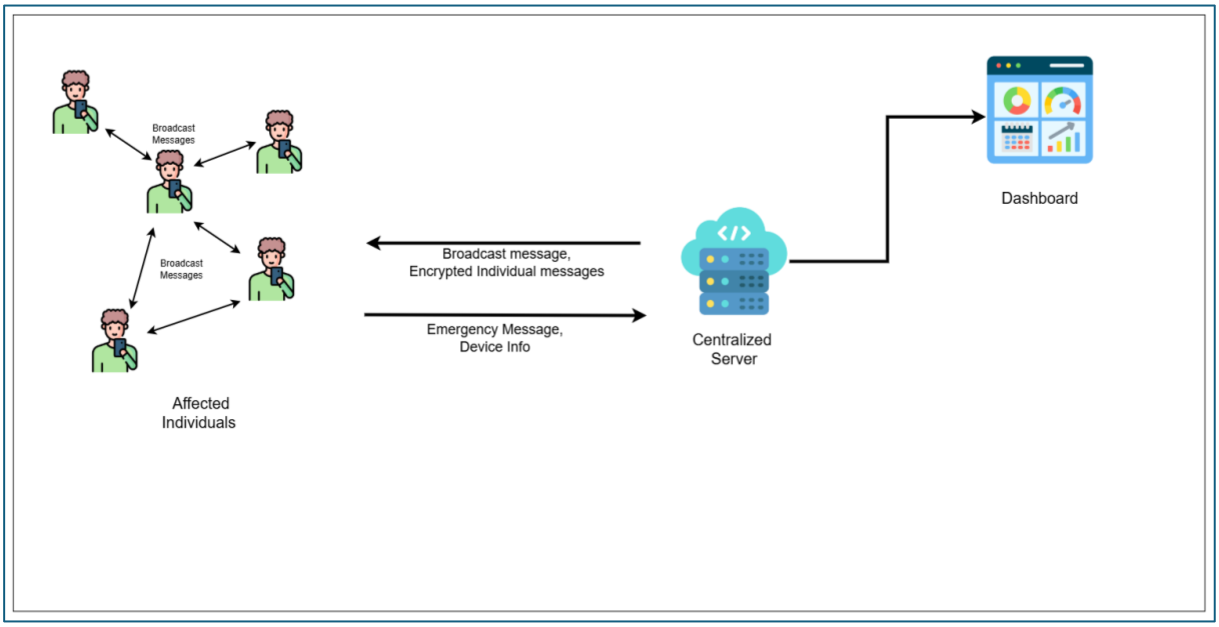


Figure 10-2 System Diagram for Messaging function

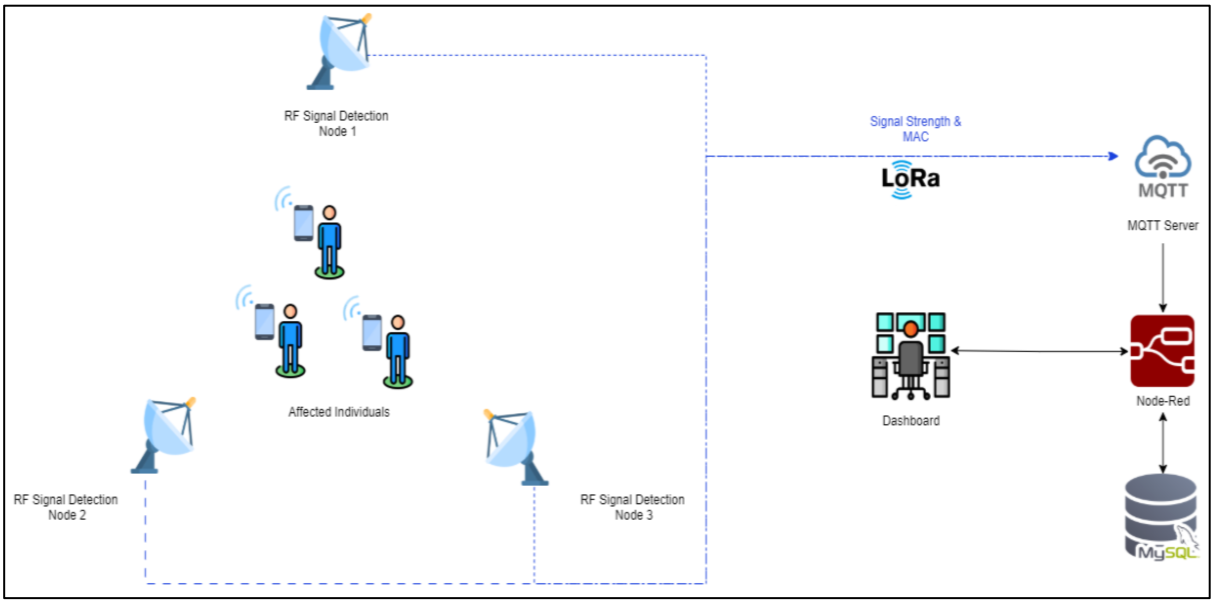


Figure 10-3 System Diagram for Localization Function

Figure 10-4 Hardware Design for the Localization Nodes

Figure 10-5 Gantt Chart for the project