



(10) Publication No: **IN202511130486 A1**
(22) Date of Filing: 23-12-2025

(43) Publication Date: 30-01-2026
Journal No: 05/2026

(19) Intellectual Property Office, India

(12) INDIAN PATENT APPLICATION

(54) Title: **Tiered communication protocol for resilient mobile connectivity**

(51) International Classification: H04L 69/14, H04W 88/06, H04W 4/14, H04L67/2869 (21) Application No: 202511130486 (31) Priority Document No: -- (32) Priority Date: -- (86) International Application No: -- Filing Date: -- (87) International Publication No: -- (61) Patent of Addition to Application No: -- Filing Date: -- (62) Divisional to Application No: -- Filing Date: --	(71) Name of Applicant(s): Dronacharya College Of Engineering, (72) Name of Inventor(s): 1. Adarsh Kumar 2. Ipshita Rawat 3. Rakashit Singh 4. Lalit Kumar 5. Prof. Vimmi Malhotra 6. Prof. Ashima Mehta
--	---

(57) Abstract:

Communication failures in rural or disaster-prone areas can have devastating effects. In the aftermath of a hurricane, for instance, essential information such as evacuation orders or medical supply needs may fail to reach affected populations due to reliance on a single, compromised communication channel. Similarly, rural populations often face delays in receiving critical services due to poor connectivity, which can worsen public health and safety outcomes. This project addresses the critical issue of communication failure in modern mobile applications caused by an over-reliance on a single, stable internet connection. This dependence creates a fundamental point of failure in low-connectivity zones, congested areas, or during disaster scenarios. Current mobile applications often rely on fall-back systems like SMS or email when high-speed internet fails. However, these systems are static, often failing to adapt to real-time network fluctuations. By incorporating a multi-layered, adaptive framework, our solution ensures that communication is never interrupted, intelligently adjusting to environmental changes like network congestion, geographical limitations, or device proximity. We propose the Tiered Communication Protocol, a novel, adaptive framework that guarantees data persistence and delivery by intelligently switching between multiple communication layers. The system operates on a hierarchy: Layer 1 (High-Speed Internet) is the default; it gracefully falls back to Layer 2 (SMS) for critical, low-bandwidth data when the internet fails; and finally utilizes Layer 3 (Wi-Fi Direct/Bluetooth) for peer-to-peer data relay in fully disconnected environments. The system leverages a scalable micro services architecture that allows for flexible, real-time synchronization across multiple devices and communication layers. In high-traffic disaster situations, the backend can efficiently handle large volumes of data and deliver it to the appropriate devices through adaptive load balancing and cloud-based processing. The expected outcome is a fully functional, field-validated product consisting of a cross-platform mobile application and a scalable micro services backend. The core innovation is the Intelligent Syncing Engine and the logic that dynamically selects the best available channel. The system's high relevance for disaster response and rural connectivity underscores its potential to fundamentally improve the reliability of mission-critical mobile communications. To ensure the highest standards of

data security and user privacy, the system employs end-to-end encryption for all communication layers, including SMS and peer-to-peer networks. Additionally, authentication protocols are integrated to prevent unauthorized access and ensure data integrity during transmission, even in high-risk environments.

TITLE: Tiered Communication Protocol for Resilient Mobile Connectivity

ABSTRACT:

Communication failures in rural or disaster-prone areas can have devastating effects. In the aftermath of a hurricane, for instance, essential information such as evacuation orders or medical supply needs may fail to reach affected populations due to reliance on a single, compromised communication channel. Similarly, rural populations often face delays in receiving critical services due to poor connectivity, which can worsen public health and safety outcomes.

This project addresses the critical issue of communication failure in modern mobile applications caused by an over-reliance on a single, stable internet connection. This dependence creates a fundamental point of failure in low-connectivity zones, congested areas, or during disaster scenarios.

Current mobile applications often rely on fall-back systems like SMS or email when high-speed internet fails. However, these systems are static, often failing to adapt to real-time network fluctuations. By incorporating a multi-layered, adaptive framework, our solution ensures that communication is never interrupted, intelligently adjusting to environmental changes like network congestion, geographical limitations, or device proximity. We propose the Tiered Communication Protocol, a novel, adaptive framework that guarantees data persistence and delivery by intelligently switching between multiple communication layers

The system operates on a hierarchy: Layer 1 (High-Speed Internet) is the default; it gracefully falls back to Layer 2 (SMS) for critical, low-bandwidth data when the internet fails; and finally utilizes Layer 3 (Wi-Fi Direct/Bluetooth) for peer-to-peer data relay in fully disconnected environments. The system leverages a scalable micro services architecture that allows for flexible, real-time synchronization across multiple devices and communication layers. In high-traffic disaster situations, the backend can efficiently handle large volumes of data and deliver it to the appropriate devices through adaptive load balancing and cloud-based processing.

The expected outcome is a fully functional, field-validated product consisting of a cross-platform mobile application and a scalable micro services backend. The core innovation is the Intelligent Syncing Engine and the logic that dynamically selects the best available channel. The system's high relevance for disaster response and rural connectivity underscores its potential to fundamentally improve the reliability of mission-critical mobile communications. To ensure the highest standards of data security and user privacy, the system employs end-to-end encryption for all communication layers, including SMS and peer-to-peer networks. Additionally, authentication protocols are integrated to prevent unauthorized access and ensure data integrity during transmission, even in high-risk environments.

PROBLEM STATEMENTS:

- **Communication Failure in Low-Connectivity Areas:** Solving the complete breakdown of app functionality when mobile data or Wi-Fi coverage is poor or non-existent (rural/remote areas).
- **Single Point of Failure:** Eliminating the current system's reliance on a singular high-speed internet connection for all functions.
- **Inadequate Disaster Response Communication:** Providing a reliable communication channel for critical alerts and data transfer when cellular infrastructure is damaged or overwhelmed.
- **Network Congestion Overload:** Ensuring message delivery during high-traffic events (e.g., festivals, public gatherings) when the internet layer becomes unusable.
- **Data Persistence in Offline Mode:** Overcoming the challenge of building an application with a robust offline-first capability that queues and manages data locally.
- **Data Inconsistency/Duplication:** Resolving the issue of data being submitted multiple times via different channels (e.g., Internet then SMS) by implementing a backend de-duplication algorithm.
- **Integration of Disparate Technologies:** Solving the complexity of merging three distinct communication paradigms (Internet, SMS, P2P) into a single, unified, and intelligently managed protocol.
- **SMS Data Limitations:** Overcoming the limitations of traditional SMS systems by integrating a rich-media fall-back logic, reserving SMS strictly for critical text-based data only.
- **Low-Power P2P Signalling:** Addressing the need for minimal data exchange and basic signalling over short distances using low-power Bluetooth.
- **User Intervention Requirement:** Eliminating the need for users to manually switch modes or settings based on their current connection status.
- **Scalability Under Duress:** Providing a communication architecture that can scale down gracefully under stress (loss of network) while still guaranteeing delivery of critical data.

SUMMARY OF INVENTION / PROTOTYPED SYSTEM:

The core invention is an Intelligent, Multi-Modal Tiered Communication Protocol embedded within an Offline-First Mobile Application and supported by a robust backend. The system's purpose is to ensure continuous data delivery by automatically selecting the most resilient communication layer based on real-time network availability.

1. The Tiered Protocol Model

LAYER	TECHNOLOGY	PRIORITY / FUNCTION
Layer 1 (Primary)	High-Speed Internet	Default mode for full, rich-data functionality, real-time sync, and media transfer.
Layer 2 (Fall-back)	SMS Gateway	Activated when the internet fails, reserved strictly for low-bandwidth, critical text data (e.g., alerts, status reports).
Layer 3 (Decentralized)	Wi-Fi Direct & Bluetooth	● Wi-Fi Direct handles peer-to-peer data relay for large files. ● Bluetooth handles short-range signalling and minimal data exchange in zero-infrastructure environments.

2. Prototype Components

- **Mobile App (Cross-Platform):** This is the user-facing prototype, containing the core **Connection Manager** Module that handles the dynamic switching logic. It employs an **Offline-First Architecture** to locally queue all data.
- **Intelligent Syncing Engine:** A module responsible for automatically and reliably uploading queued offline data once any communication path (Internet, SMS, or P2P data relay) is detected as available.
- **Micro services Backend:** A scalable, cloud-hosted server architecture that integrates with a commercial **SMS Gateway** and features a **Backend De-duplication Algorithm** to ensure data consistency, regardless of the channel used for submission.

SYSTEM REQUIREMENTS:

1. Functional Requirements

Requirement Category	Specific Requirement	Protocol Layer
Data Synchronization	The system must automatically queue and persist all user-submitted data locally when disconnected (Offline-First).	All Layers

Dynamic Fall-back	The system must dynamically detect connection failure in Layer 1 (Internet) and gracefully switch to Layer 2 (SMS) within a defined timeout period.	Layer 1
Core Delivery Guarantee	The system must use Layer 2 (SMS) to ensure critical, text-based data (alerts, status updates) is delivered even without the internet.	Layer 2
Peer-to-Peer Relay	The system must allow nearby devices to establish a Wi-Fi Direct connection to relay large data packets (e.g., photos/videos) in zero-infrastructure environments.	Layer 3 (Wi-Fi Direct)
Minimal P2P Signalling	The system must allow for low-power, short-range signalling and minimal data exchange via Bluetooth Low Energy (BLE).	Layer 3 (Bluetooth)
Data Integrity	The backend must execute a de-duplication algorithm to ensure only one instance of any data item is recorded, regardless of the submission channel.	Backend
Real-Time Data	The system must use Layer 1 (Internet) to enable real-time streaming and data visualization (e.g., map updates).	Layer 1

2. Non - Functional Requirements

Requirement Category	Specific Requirement	Metric / Standard
Reliability	The system must maintain an up-time of 99.9% for critical message delivery across all communication modes.	Measured in Field Trials
Scalability	The backend must be able to handle a 5x increase in concurrent users and data submissions via Layer 1 without significant latency.	Micro services Architecture
Usability	The mobile application's UI/UX must ensure the communication channel switching is seamless and transparent to the end-user.	Documentation/Field Testing
Performance	The failover time from Layer 1 (Internet failure) to Layer 2 (SMS activation) must be less than 10 seconds.	Stress Testing
Security	All data transmitted via Layer 1 and stored in the backend must be secured using standard encryption protocols (TLS/SSL).	Encryption Standards

3. Hardware and Technology Requirements

Component	Requirement	Justification
Mobile App	Compatibility with Android (v9+) and iOS (latest version).	Ensures broad cross-platform reach and utilization of current native APIs.

Backend	Cloud Hosting platform (AWS/GCP/Azure) capable of hosting a micro services architecture.	Required for scalability and the ability to integrate external services like the SMS Gateway.
Database	A hybrid approach: Relational (PostgreSQL/MySQL) for structured data and NoSQL (MongoDB) for unstructured, quickly syncing data.	Supports both transactional integrity and flexible data handling.
Integration	Access to a commercial SMS Gateway API for sending and receiving Layer 2 data.	The project relies on an existing service for reliable SMS integration (Out-of-Scope: building a new gateway).

CLAIMS:

- **A Unified, Adaptive Hybrid Model:** The project claims to be the first to successfully integrate Internet, SMS, and peer-to-peer (P2P) communication (Wi-Fi Direct/Bluetooth) into a single, unified, and intelligently managed protocol.
- **Tiered System for Graceful Degradation:** It claims to guarantee graceful degradation of service by seamlessly falling back through three distinct layers, eliminating catastrophic failure associated with single-channel apps.
- **Core Intellectual Contribution:** The project claims the Tiered Communication Protocol Logic itself is the primary intellectual contribution, providing a blueprint for resilient systems.
- **Intelligent Channel Selection:** The system claims to dynamically select the best available communication channel in real-time, based on network status and data requirements, without user intervention.
- **Guaranteed Message Persistence:** The system claims to ensure 100% data persistence through an offline-first mobile architecture, queuing data locally until any connection is restored.
- **Guaranteed Data Delivery:** It claims to guarantee delivery of critical messages by using the most robust available channel (SMS) when higher layers fail.
- **Resolution of Data Duplication:** The system claims its backend de-duplication algorithm effectively resolves data integrity issues arising from messages submitted concurrently via multiple channels (e.g., Internet and SMS).
- **Elimination of Single Point of Failure:** The architecture fundamentally claims to remove the single point of failure that plagues existing mobile applications.
- **Functionality in Zero-Infrastructure Environments:** The project claims to enable functional data relay and communication even in areas completely devoid of external communication infrastructure (cell towers, Wi-Fi).
- **High-Bandwidth P2P Transfer:** It claims the system can facilitate the fast, high-bandwidth transfer of large files between nearby devices using Wi-Fi Direct when the internet is unavailable.
- **Cost-Effective Critical Communication:** The system claims to reserve the more expensive Layer 2 (SMS Gateway) strictly for critical, low-bandwidth data, making emergency communication more cost-effective.
- **Foundation for Advanced Features:** The architecture claims to provide the necessary reliable data stream to enable future advanced features, such as AI/NLP engines and dynamic hotspot detection.
- **Paradigm Shift in Mobile Communication:** The project claims its framework represents a paradigm shift in the design of resilient mobile applications, moving beyond traditional models.
- **High Relevance for Critical Scenarios:** It claims the solution has high importance and direct relevance for real-world critical scenarios, including disaster response and rural connectivity.
- **Field-Validated Reliability:** The final outcome claims the system will be a field-validated product, with its reliability and efficiency proven through comprehensive controlled experiments and field trials.