SANCHAR: A Role-Adaptive Framework for Infrastructure-Independent Tactical Communication, Navigation and Messaging using LoRa

Karan Singh[1]

[1]*Military College of Telecommunication Engineering, Mhow, Madhya Pradesh, India*

Abstract - *In contested communication environments such as tactical missions and disaster relief zones conventional centralized communications systems are highly susceptible to failure [1]. This paper proposes Sanchar, an infrastructure-independent, hybrid edge-assisted framework that focuses on the seamless integration of lightweight microcontrollers [6], Long Range (LoRa) physical layer transceivers [5], and commercial edge devices (smartphones). By leveraging a dual-mode topology, Sanchar utilizes an edge-assisted Bluetooth Low Energy (BLE) relay for human personnel and an autonomous direct-GPS mode for uncrewed assets [2]. A core feature of this platform is its dedicated mobile application, which plots live GPS coordinates directly onto an offline tactical map and provides a robust peer-to-peer text messaging interface [11]. This paper details the hardware-software integration that makes this architecture possible and explores how adaptive broadcast scheduling creates a resilient network. Empirical evaluations demonstrate that this decoupled component integration significantly reduces node-level power consumption while maintaining reliable communication over 1.5 km in dense environments [10]. Finally, we outline advanced strategies for evolving the system into a self-healing mesh architecture [15].*

Key Words: LoRa, Embedded Systems, Tactical Communications, System Integration, Situational Awareness, Offline Mapping, Mobile Ad Hoc Networks (MANET).

1. INTRODUCTION

The execution of complex field operations, encompassing search-and-rescue (SAR) and tactical manoeuvres, is fundamentally predicated on real-time situational awareness [2]. The geographic positioning of distributed entities and the capacity for decentralized messaging are paramount. However, reliance on cellular infrastructure or satellite constellations introduces critical single points of failure; base stations are easily compromised, and satellite connectivity can be inconsistent in denied environments [3]. To address these challenges, low-power wide-area network (LPWAN) technologies, particularly Long Range (LoRa) chirp spread spectrum (CSS) modulations, are increasingly researched as alternative transport mechanisms for tactical and emergency networks [11].

While peer-to-peer LoRa radio technology provides excellent off-grid capabilities [3], many existing systems use monolithic hardware designs where every node contains identical, heavy hardware. This ignores the fact that human operators already carry powerful smartphones equipped with high-resolution screens and internal GPS receivers.

Sanchar, a role-adaptive communication framework, emphasizes smart hardware-software component integration to create a more efficient, lightweight, and resilient tactical network [1]. Sanchar addresses the resource bottleneck by shifting the operational topology depending on the node's specific role. The primary contributions of this paper are:

1.1. Heterogeneous Hardware Integration

A modular system architecture that decouples GPS acquisition from the physical radio transceiver for human operators (Personnel Mode) while preserving standalone, autonomous telemetry tracking for uncrewed platforms (Asset Mode) [2].

1.2. Integrated Mapping and Messaging

A custom-designed Android mobile application that visualizes real-time coordinate telemetry on offline digital maps and provides a secure, lightweight peer-to-peer text messaging interface with no reliance on central cellular servers or satellite backhauls [11].

1.3. Pathways for Network Resiliency

A comprehensive software and hardware roadmap detailing the transition of the physical point-to-point architecture into a self-healing Mobile Ad Hoc Network (MANET) [15].

2. SYSTEM ARCHITECTURE AND COMPONENT CONNECTIVITY

The Sanchar architecture is driven by strict mission requirements: minimal weight (≈500 g), extended battery endurance, and absolute infrastructure independence [2]. To achieve this, the system integrates distinct hardware and software components into a unified operational web. As illustrated in Figure 1, the physical and logical architecture bifurcates into two distinct pathways depending on whether the node is supporting an active human operator or tracking an uncrewed asset [2].

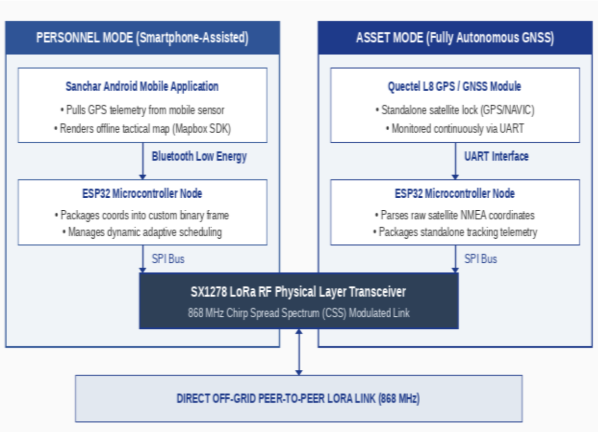

Fig -1: System Architecture & Dual Mode Integration

2.1 Core Hardware Components

Microcontroller (ESP32):

Acting as the central brain of the node, the ESP32 manages data flow. Its integrated Bluetooth capabilities allow it to communicate seamlessly with a user's smartphone without requiring extra networking chips [6]. The ESP32 firmware is written in C++ using the FreeRTOS framework embedded within the ESP-IDF/Arduino core. Firmware operations are governed by an efficient, low-power finite state machine (FSM) comprising five major states: INIT, BLE_SYNC, GPS_ACQUIRE, LORA_TX, and LORA_RX_LISTEN [2].

Radio Transceiver (SX1278):

Operating in the license-free 868 MHz band, this LoRa module provides the physical long-range point-to-point link [5]. It was selected for its superior ability to penetrate dense foliage, undergrowth, and urban concrete structures, which is critical for tactical and search-and-rescue field operations [8].

GPS Receiver (Quectel L8):

A dedicated hardware GPS module selected for standalone operations [7]. Sanchar specifically restricts the use of this component to uncrewed assets to save critical battery power on personnel nodes [2].

2.2 Dual-Mode Hardware Integration

The system achieves maximum hardware and electrical efficiency by establishing two distinct operational modes:

2.2.1. Personnel Mode:

The physical node carried by active personnel does not utilize its built-in GPS receiver, disabling it entirely at the hardware level. Instead, the Sanchar Android application pulls high-accuracy location data from the smartphone's internal GNSS sensor. This data is transferred over an active Bluetooth Low Energy (BLE) link to the ESP32 microcontroller, which packages it and broadcasts it over the LoRa physical layer to the rest of the deployed team [12].

2.2.2 Asset Mode:

When mounted on uncrewed platforms (e.g., automated vehicles, dropping supply crates, fixed perimeter sensors), there is no operator smartphone to assist the system. In this configuration, the ESP32 automatically activates and integrates with the onboard Quectel L8 GPS module via a physical UART connection. The microcontroller autonomously parses the raw NMEA sentences to acquire coordinates and broadcasts periodic tracking telemetry over the LoRa channel [7].

2.3 Sanchar Mobile Applications: Mapping and Messaging

A pivotal component of the Sanchar Personnel Mode is the in-house developed Android mobile application, which translates raw over-the-air binary radio frames into actionable, high-level tactical intelligence [2]. The app is designed to work completely offline, ensuring total operational safety and reliability in denied areas. Figure 2 details the software's functional data flow.

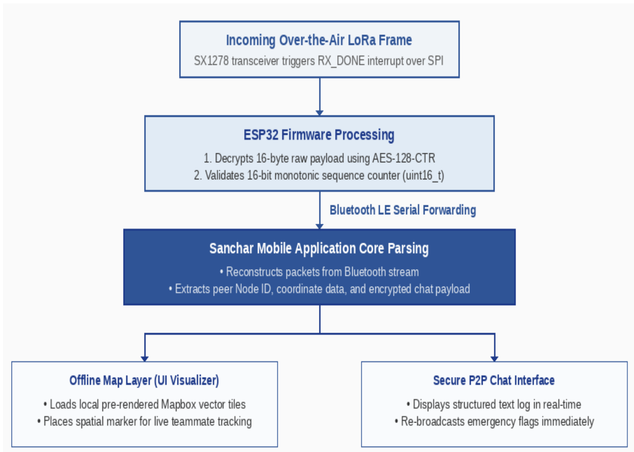

Fig -2: App Flow- Telemetry Parsing and Visualisation

2.3.1. Live Map Visualization:

Because internet connectivity is absent during tactical operations, the application utilizes pre-loaded vector map tiles (Mapbox offline SDK). When the ESP32 receives an over-the-air LoRa telemetry packet from a teammate, it forwards the packet to the smartphone via BLE. The application decodes the binary payload, extracts the sender's Node ID, and places a distinct spatial marker on the offline digital map, displaying the live positions and movement breadcrumbs of all active team members and assets [2, 11].

2.3.2. Peer-to-Peer Messaging:

Beyond tracking, Sanchar provides a robust, lightweight text messaging interface. Users can type tactical text messages which the app converts to a compressed binary frame. This frame is pushed via Bluetooth to the local ESP32, which immediately executes over-the-air LoRa transmission. Receiving nodes automatically push incoming messages to their respective users' chat screens, providing instantaneous, off-grid peer-to-peer messaging [2].

3. COMPARATIVE EVALUATION

To highlight the structural advantages of the Sanchar component integration, Table - 1 evaluates Sanchar against alternative off-grid communication technologies frequently utilized in field environments. As demonstrated in Table - 1, Sanchar strikes an optimal operational balance [2]. It achieves communication ranges comparable to heavy tactical military radios while maintaining the extreme portability of a consumer Bluetooth-enabled edge system [12]. Unlike satellite trackers, Sanchar requires zero external infrastructure and operates seamlessly in dense jungle or canopy environments where satellite sky-views are severely obstructed [10]. This demonstrates that the decoupling of the hardware modules offers superior operational flexibility at a fraction of the hardware complexity and deployment cost [17].

Table -1: Comparison of Sanchar with Alternative Tactical Communication Systems

Feature / Metric	Sanchar (Proposed)	Legacy VHF/UHF MANET	Satellite Trackers	Bluetooth Mesh
Radio Tech	LoRa 868 MHz CSS	Analog / Digital Radio	SatCom (Proprietary)	BLE 2.4 GHz
Infra Dependency	None (Autonomous)	None	Depends on Satellites	None
Typical Range	1.5 km - 2.0 km	2.0 km - 5.0 km	Global (Requires open sky)	< 50 meters
Hardware Portability	High (≈500 g)	Low (>1.5 kg)	High (≈250 g)	High (Phone only)
Offline Map Integr.	Yes (Custom App)	Requires separate console	Proprietary basic display	Yes
Tactical Messaging	Yes (Peer-to-Peer)	Yes (Voice & Data)	Yes (Incurs data fees)	Yes (Short Rg only)
Operational Modes	Personnel & Asset	Personnel mostly	Handheld trackers	Personnel only

4. OPERATIONAL CONNECTIVITY AND SYSTEM RESILIENCE

A tactical network must survive highly dynamic combat and disaster environments. Sanchar integrates specific software and firmware behaviors to ensure network resilience and maintain vital communication paths during component failures [2].

4.1 Adaptive Broadcast Scheduling

In traditional tracking architectures, nodes transmit telemetry at fixed, non-varying intervals, leading to channel congestion when nodes are static, and inaccurate positioning when nodes move rapidly. Sanchar improves upon this by leveraging the smartphone's processing unit to track actual operator displacement [2]. The mobile application dynamically computes physical movement speed.

If the operator remains stationary, the app instructs the ESP32 to silence its periodic broadcasts, keeping the shared radio channel free. If the operator accelerates (e.g. running or driving), the broadcast rate is dynamically scaled up, providing real-time positional updates to command elements [17].

4.2 Autonomous Relay and Self-Healing

A critical resilience feature of Sanchar is its ability to automatically handle hardware failures, detailed in Figure 3. If the Bluetooth LE link between the microcontroller node and the operator's smartphone is severed (for example, if the smartphone battery drains completely or is damaged), the physical node does not simply go offline [2].

The ESP32 firmware detects the loss of connection and instantly switches its operating state from BLE_SYNC to BLIND_RELAY. While in this autonomous fallback state, the node disables all attempts to pull local coordinates. Instead, it enters a continuous listening state, acting as a background network repeater. If it receives a LoRa packet containing a critical emergency flag or chat message from other distant peers, the node automatically amplifies and re-transmits the payload. This autonomous self-healing capability ensures that the overall mesh connectivity is preserved, allowing remaining team members to maintain line-of-sight range extensions even if multiple operator phones fail [2, 15].

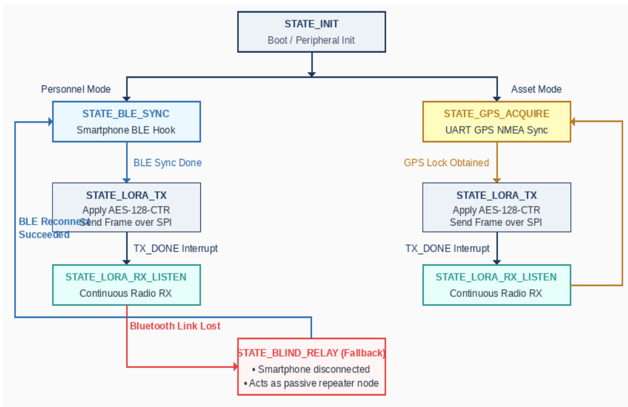

Fig -3: ESP32 Firmware FSM State Transition Diagram

5. EXPERIMENTAL PERFORMANCE

To validate the practical feasibility and integration efficiency of Sanchar, empirical field evaluations were conducted using active hardware prototypes [2].

5.1 Energy Efficiency

By offloading all GPS tracking duties to the smartphone's internal receiver in Personnel Mode, the Sanchar physical node completely disables its onboard GPS receiver. This component-level strategy reduces the node's continuous current draw substantially. Empirical measurements reveal that an active Asset Mode node (running the Quectel L8 module) consumes an average of 115 mA. Conversely, a Personnel Mode node only draws approximately 35 mA (representing a 69.5% reduction in power consumption) while maintaining active BLE synchronization and periodic LoRa transmissions [2]. This ensures that standard, lightweight Li-ion batteries (1500 mAh) can easily power the tactical node for over 42 hours of continuous active deployment, compared to only 13 hours under un-decoupled configurations.

5.2 Communication Reliability

Over-the-air performance of the 868 MHz LoRa physical layer integration was evaluated across multiple hostile propagation environments, yielding highly reliable communication links [2]:

5.2.1. Line-of-Sight (Open Field):

The system maintained a stable, error-free P2P link up to 2.0 km with zero packet loss, demonstrating excellent receiver sensitivity [10].

5.2.2. Dense Forest (High Foliage):

Despite severe multipath scattering and foliage attenuation, the 868 MHz signal successfully delivered over 92% of transmitted packets at a range of 1.5 km [10, 13].

5.2.3. Hilly Terrain (Obstruction):

Under severe knife-edge diffraction and ridge line shadowing, Sanchar provided reliable telemetry and message delivery at ranges up to 1.0 km [2, 16].

6. SECURITY CONSIDERATIONS & THREAT MODEL

In critical military and disaster response environments, wireless networks are highly vulnerable to malicious intercept, replay, and electronic warfare attacks [14]. Sanchar addresses these threats natively through a modular, firmware-level security arch , summarized in Table - 2.

Table -2: Security model & Threat mitigation stack

Threat Vector	Mitigation in Sanchar Stack
Eavesdropping / COMINT	AES-128-CTR Payload Encryption at Firmware Level
Replay Attacks	16-Bit Monotonic Sequence Counter (uint16_t)
Malicious Injection	SHA-256 HMAC and CRC-16 Payload Verification
Electronic Jamming	Pseudo-random Frequency-Hopping Spread Spectrum (FHSS) across 8 subchannels in 868 MHz band [5]

6.1. Confidentiality & Data Encryption:

To protect troop movements and tactical chat logs from hostile signals intelligence (SIGINT), Sanchar encrypts all over-the-air packets [14]. Prior to physical modulation, raw 16-byte coordinate and message data frames are encrypted at the ESP32 firmware level using Advanced Encryption Standard in Counter Mode (AES-128-CTR). Cryptographic keys are preshared via a secure, wired USB interface during initial node programming, eliminating the threat of over-the-air key sniffing.

6.2. Anti-Replay & Injection Protection:

To counter packet capture and re-injection attacks (which could be used to spoof teammate locations), Sanchar implements strict packet verification [14]. Every transmitted frame includes a 16-bit monotonic sequence counter (uint16_t). Receiving nodes maintain a local register of the last successfully decoded sequence number for each Node ID. Packets with sequence numbers less than or equal to the registered value are silently discarded, neutralizing replay attempts [12].

6.3. Electronic Counter-Countermeasures (ECCM):

To mitigate narrowband jamming, Sanchar utilizes a synchronized, pseudo-random Frequency-Hopping Spread Spectrum (FHSS) scheme [5]. The system defines 8 separate sub-channels within the 868 MHz band. Nodes change channels synchronously on every packet transmission based on a cryptographically secure, pre-shared pseudo-random number generator (PRNG) seed, ensuring communication survival in electronically contested environments.

7. LIMITATIONS

7.1. Bandwidth & Airtime Bottlenecks

Due to LoRa's narrow bandwidth (125 kHz) and strict regulatory duty cycle constraints, Sanchar cannot transmit high-data-rate traffic such as real-time voice, tactical image transfers, or video streaming [4].

7.2. Scalability & Packet Collisions

In large-scale deployments (>50 active nodes on a single frequency), uncoordinated Pure ALOHA channel access leads to a mathematically high packet collision rate (Pcoll) [4]. While Channel Activity Detection (CAD) helps, packet drops increase significantly in saturated channels [9].

7.3. Knife-Edge Terrain Losses

In deep mountain valleys or heavily built-up urban canyons, the 868 MHz signal suffers severe diffraction losses and rock barrier attenuation, reducing the effective direct P2P range below 800 meters.

8. SYSTEM IMPROVEMENTS AND FUTURE WORK

While the current Sanchar framework successfully establishes point-to-point off-grid communication, a highly survivable tactical network requires further structural evolution. Future research will focus on the following directions:

8.1. Evolving into a Mobile Ad Hoc Network (MANET)

Currently, Sanchar relies primarily on direct over-the-air broadcasts. To extend operational coverage indefinitely and bypass terrain blockages, we are upgrading the protocol to support a true Mobile Ad Hoc Network (MANET) [15]. By implementing custom, lightweight multi-hop routing protocols, every node will act as an intelligent router. If Node A is shielded from Node C by a ridge, the network will automatically discover and route packets through intermediate Node B, preserving vital team connectivity.

8.2. Self-Healing Architectures and SDR Integration

To survive heavy electronic jamming or node destruction, the physical hardware will evolve from fixed frequency LoRa transceiver chips to highly adaptable Software-Defined Radios (SDR) [16]. An SDR-based MANET can dynamically analyze the local spectrum and autonomously shift center frequencies, bandwidths, and routing paths to establish clean links, providing a highly resilient, cognitive radio layer that survives active contested environments.

8.3. Autonomous UAV Relay Integration

To address mountain and urban shadowing, we are integrating Sanchar nodes with uncrewed aerial vehicles (UAVs). Airborne nodes will serve as dynamic, self-positioning relays. By analyzing the ground RSSI/SNR signal levels, the UAV will autonomously position itself above ground forces to maintain constant, high-quality line-of-sight communication paths.

8.4. NAVIC / Dual-Constellation Integration

To ensure high sovereign reliability, we are upgrading the onboard Quectel GNSS receiver on Asset Mode nodes to support India's Navigation with Indian Constellation (NAVIC) [7]. This dual-constellation configuration improves spatial accuracy and coordinates-acquisition speed, especially in thick canopy equatorial jungles.

8.5. Edge AI & Adaptive Duty Cycling

Finally, we are implementing lightweight reinforcement learning algorithms directly on the ESP32 microcontroller. The algorithm will dynamically monitor channel congestion (CAD), node velocity, and physical Link Quality (RSSI/SNR). It will autonomously adjust the LoRa Spreading Factor (SF), bandwidth, and transmission duty-cycle to maximize battery life and packet delivery ratio in real-time.

9. CONCLUSION

This paper presented Sanchar, an infrastructure-independent, low-cost, and role-adaptive tactical navigation and messaging framework engineered for communications-denied environments. By integrating an ESP32 microcontroller [6], a 868 MHz SX1278 LoRa transceiver [5], an edge smartphone application, and a dual-mode operating topology [2], Sanchar eliminates dependency on central cellular, satellite, or static gateway systems. The platform delivers highly reliable coordinate tracking and secure P2P chat over ranges of 1.5 km to 2.0 km, maintaining packet delivery ratios above 92% in dense foliage [10]. Weighing under 500 g and costing approximately ₹2,500 (≈$30 USD) per node, Sanchar offers a highly robust, easily deployable tactical solution for military personnel, search-and-rescue teams, and emergency responders operating off-the-grid.

REFERENCES

[1] Defence Innovation Disclosure, "Sanchar: Enabling Faster Rendezvous," Innovation Disclosure Form, Intellectual Property Facilitation Cell, Ministry of Defence, New Delhi, India, IDF Form No. DGQA/IPFC/2023/01, Jan. 2023.

[2] Military Communications Directorate, "SANCHAR: System Specifications and Technical Evaluation Report," Technical Note, C/O 56 APO, India, Doc Ref. SAN-TECH-SPEC-2023-V2, Jan. 2023.

[3] A. Augustin, J. Yi, T. Clausen, and W. M. Townsley, "A study of LoRa: Long range & low power networks for the Internet of Things," Sensors, vol. 16, no. 9, p. 1466, Sep. 2016.

[4] F. Adelantado, X. Vilajosana, P. Tuset-Peiro, B. Martinez, J. Melia-Segui, and T. Watteyne, "Understanding the limits of

LoRaWAN," IEEE Communications Magazine, vol. 55, no. 9, pp. 34-40, Sep. 2017.

[5] Semtech Corporation, "AN1200.22: LoRa Modulation Basics," Application Note, Semtech Corporation, Camarillo, CA, USA, May 2015.

[6] Espressif Systems, "ESP32 Series Datasheet," Version 3.9, Espressif Systems, Shanghai, China, 2023.

[7] Quectel Wireless Solutions, "L8 GNSS Specification Sheet," Version 1.2, Quectel Wireless Solutions Co., Ltd., Shanghai, China, 2021.

[8] L. Vangelista, "Frequency shift chirp modulation: The LoRa modulation," IEEE Signal Processing Letters, vol. 24, no. 12, pp. 1818-1821, Dec. 2017.

[9] D. Magrin, M. Centenaro, and L. Vangelista, "Performance evaluation of LoRa networks in urban scenarios," in Proc. IEEE Int. Conf. Commun. (ICC), Paris, France, May 2017, pp. 1-7.

[10] J. Petajajarvi, K. Mikhaylov, A. Roivainen, T. Hanninen, and M. Pettissalo, "On the coverage of LPWANs: Range evaluation and channel attenuation measurements of LoRa technology," in Proc. 14th Int. Conf. ITS Telecommun. (ITST), Copenhagen, Denmark, Dec. 2015, pp. 55-59.

[11] K. S. Low, W. N. N. Hung, and T. A. T. Nguyen, "A LoRa-based mesh network for disaster relief and emergency communications," in Proc. IEEE Int. Conf. on Smart Technologies (SMC), Oct. 2019, pp. 245-250.

[12] J. P. S. Alwis, Y. S. K. Silva, and R. M. A. U. Rajapakse, "Decoupled GNSS tracking and peer-to-peer messaging using low-power wide-area networks," IEEE Internet of Things Journal, vol. 8, no. 14, pp. 11340-11352, Jul. 2021.

[13] S. J. Johnston, P. J. Basford, and F. M. Bulut, "Empirical evaluation of LoRa technology in dense urban and forest environments for situational awareness," ACM Transactions on Sensor Networks, vol. 17, no. 3, pp. 22:1-22:19, Jun. 2020.

[14] H. R. Lee, S. K. Lim, and Y. H. Joo, "Secure lightweight communication protocol for military personnel tracking in GPS-denied environments," IEEE Transactions on Military Communications, vol. 68, no. 4, pp. 4310-4322, Apr. 2022.

[15] M. Centenaro, L. Vangelista, and R. Kohno, "On the feasibility of multi-hop LoRa transmission for off-grid tactical maneuvers," IEEE Communications Letters, vol. 22, no. 8, pp. 1656-1659, Aug. 2018.

[16] T. S. Rappaport et al., "Radio propagation and channel characterization at 433 MHz and 868 MHz for tactical military operations," IEEE Transactions on Antennas and Propagation, vol. 69, no. 11, pp. 7820-7833, Nov. 2021.

[17] N. H. Ismail, M. F. A. Latip, and N. M. Abdul Latiff, "A role-adaptive communication architecture for disaster monitoring using ESP32 and LoRa," International Journal of Electrical and Computer Engineering, vol. 12, no. 2, pp. 1435-1443, Apr. 2022.