East African Journal of Engineering
eaje.eanso.org
Volume 8, Issue 1, 2025
Print ISSN: 2707-5389 | Online ISSN: 2707-5397
Title DOI: https://doi.org/10.37284/2707-5397

EAST AFRICAN
NATURE &
SCIENCE
ORGANIZATION

Original Article

Design and Performance Evaluation of a LoRaWAN-Based Communication System for Enhanced Situational Awareness in Armored Vehicles

Ashraf Adam Ahmad[1], Solomon Joda Dibal[1], Isah Musa Danjuma[1] & Amina Jibril[1]*

[1] Nigerian Defence Academy, P.M.B. 2109, Kaduna, Nigeria.
[*] Correspondence Email: aaashraf@nda.edu.ng

Article DOI : https://doi.org/10.37284/eaje.8.1.2870

Publication Date:

14 April 2025

Keywords:

LoRaWAN, GSM, Situational Awareness, Armored Vehicles, Wireless Communication, Power Efficiency, Data Security.

ABSTRACT

This study presents the design and performance evaluation of a LoRaWAN-based communication system for enhancing situational awareness in armoured vehicles, with a comparative analysis against GSM networks. Performance metrics such as communication range, latency, security, GPS accuracy, data transmission speed, and power consumption were assessed under different environmental conditions, including open fields, urban areas, and forested regions. The results indicate that LoRaWAN offers a reliable alternative to GSM, particularly in environments with limited cellular infrastructure. LoRaWAN demonstrated a communication range of up to 12 km in open fields, moderate security with AES-128 encryption, and superior power efficiency, supporting up to 41.6 hours of continuous operation on a 5000mAh battery. While GSM outperformed LoRaWAN in latency (50–150 ms vs. 150–300 ms) and data transmission speed, LoRaWAN provided better performance in rural areas and secured communication through dynamic key management. These findings highlight LoRaWAN's potential for military applications where secure, long-range, and energy-efficient communication is required.

APA CITATION

Ahmad, A. A., Dibal, S. J., Danjuma, I. M. & Jibril, A. (2025). Design and Performance Evaluation of a LoRaWAN-Based Communication System for Enhanced Situational Awareness in Armored Vehicles. *East African Journal of Engineering*, *8*(1), 127-144. https://doi.org/10.37284/eaje.8.1.2870

CHICAGO CITATION

Ahmad, Ashraf Adam, Solomon Joda Dibal, Isah Musa Danjuma and Amina Jibril. 2025. "Design and Performance Evaluation of a LoRaWAN-Based Communication System for Enhanced Situational Awareness in Armored Vehicles". *East African Journal of Engineering* 8 (1), 127-144. https://doi.org/10.37284/eaje.8.1.2870.

HARVARD CITATION

Ahmad, A. A., Dibal, S. J., Danjuma, I. M. & Jibril, A. (2025) "Design and Performance Evaluation of a LoRaWAN-Based Communication System for Enhanced Situational Awareness in Armored Vehicles", *East African Journal of Engineering*, 8(1), pp. 127-144. doi: 10.37284/eaje.8.1.2870.

IEEE CITATION

A. A., Ahmad, S. J., Dibal, I. M., Danjuma & A., Jibril "Design and Performance Evaluation of a LoRaWAN-Based Communication System for Enhanced Situational Awareness in Armored Vehicles" *EAJE*, vol. 8, no. 1, pp 127-144, Apr. 2025.

MLA CITATION
Ahmad, Ashraf Adam, Solomon Joda Dibal, Isah Musa Danjuma & Amina Jibril. "Design and Performance Evaluation of a LoRaWAN-Based Communication System for Enhanced Situational Awareness in Armored Vehicles" *East African Journal of Engineering,* Vol. 8, no. 1, Apr. 2025, pp. 127-144, doi:10.37284/eaje.8.1.2870.

INTRODUCTION

Armoured vehicles play a crucial role in modern military operations, providing mobility, protection, and firepower across various combat scenarios. Effective communication systems are essential for ensuring coordination, information sharing, and overall mission success. Within these vehicles, seamless interaction among crew members and real-time data exchange enhances situational awareness, improving operational effectiveness in dynamic environments (Demarest, 2023; Vegvisir, 2024). However, conventional communication systems face significant challenges, including limited range, high power consumption, and susceptibility to interference, which hinder mission efficiency.

The enclosed structure and confined space of armoured vehicles further exacerbate communication difficulties, making situational awareness a critical concern (Demarest, 2023). The inability of crews to accurately assess their surroundings due to restricted visibility and rapidly changing combat conditions necessitates innovative solutions. To address these limitations, the development of a long-range, low-power, and secure communication system is imperative (Vegvisir, 2024). LoRaWAN (Long-Range Wide Area Network) technology presents a promising alternative, offering extended range, minimal power requirements, and robust security features, making it well-suited for military applications.

LoRaWAN is a low-power, long-range wireless protocol designed to enable secure communication within private networks, independent of existing infrastructure (Ertürk et al., 2019; Douklias et al., 2023). Its layered architecture aligns with the Open Systems Interconnection (OSI) model, facilitating seamless communication between different network components. By integrating location tracking and text messaging capabilities, LoRaWAN can significantly enhance the situational awareness of armoured vehicle crews, ensuring continuous and reliable data exchange even in high-risk environments (Ertürk et al., 2019).

The objective of this research is to design and implement a LoRaWAN-based communication system tailored to the operational demands of armoured vehicles. Key considerations include hardware and software integration using ESP32 microcontrollers, LoRa 433MHz communication modules, and synchronization with mobile applications. Advanced encryption protocols such as AES and LoRaWAN MAC Layer Security were incorporated to ensure secure data transmission. The proposed system was evaluated in real-world scenarios to assess its reliability, efficiency, and adaptability.

By addressing critical communication gaps, optimizing technical parameters, and ensuring practical applicability, this research aims to contribute to the advancement of communication technology for armoured vehicles. The findings of this study provided insights into enhancing situational awareness, improving mission outcomes, and safeguarding military personnel in combat operations.

REVIEW OF RECENT RELATED WORKS

Recent advancements in LoRaWAN have led to innovative approaches for improving localization, network performance, and environmental monitoring. Several studies have explored machine learning-based localization techniques, optimized scheduling for large-scale networks, and the potential of mobile gateways for enhanced coverage. These works aim to address the inherent limitations of LoRaWAN and their efforts are presented as follows.

A study on Automatic Wireless Tank Systems for Defense was designed to enhance border security through continuous 24/7 surveillance using wireless communication (Patel & Aslam, 2020).

The system employed cameras for target detection and a firing control module for response, aiming to reduce the burden on soldiers while improving defensive capabilities. However, the researchers noted that the system remained semi-autonomous, requiring human intervention for decision-making. While it significantly augmented security measures, it was intended as a complementary tool rather than a replacement for soldiers' roles in surveillance and defence.

Another research provided a comprehensive review of multi-hop communication in LoRa networks, analyzing 11 studies on LoRa routing protocols (Osorio et al., 2020). The authors examined test conditions, network topologies, and packet delivery performance, observing a predominant reliance on tree-based structures and hardware tests. They identified a critical research gap in the security aspects of routing protocols, as discussions on potential threats and countermeasures were largely absent. Additionally, they highlighted the need for further exploration of factors such as Adaptive Data Rate (ADR), spreading factor (SF), bandwidth, and modulation techniques. The study also noted variations in experimental scale, with node deployments ranging from 5 to 25,000, emphasizing the need for more standardized evaluation approaches.

The work (Zhong & Springer, 2021) demonstrated improvements in LoRaWAN reliability and energy efficiency through the introduction of the Confirm Congestion Procedure (CCP) with Explicit Acknowledgment (EACK). The researchers reported that this approach significantly improved the packet reception ratio (PRR), increasing it from 5.6%–3.6% (in traditional LoRaWAN with p-CSMA) to nearly 58% using CCP with EACK. They also found that end-to-end delivery probability improved from 20%–38% in conventional LoRaWAN to 60%–95% with CCP and EACK when the number of acknowledgements (N) was set to 8. Additionally, CCP with EACK achieved a 97% reduction in energy consumption compared to p-CSMA with LoRaWAN. However, the study noted that this improvement came at the cost of increased delay, which was reported to be 20 to 30 times higher than that of p-CSMA with LoRaWAN. The researchers did not fully explore the security mechanisms of EACK or the scalability of the proposed protocol, identifying these as areas for future research.

Advanced tactical communication systems for military vehicles were introduced and reported that these systems enhanced real-time information exchange over both short- and long-range distances (Ferreira et al., 2020). The authors described the design and implementation of seven tactical communication modules that facilitated coordination at different military unit levels, ranging from company to brigade. Additionally, they explored the feasibility of free-space optical (FSO) communication in military contexts. While the study highlighted the benefits of these systems, the authors did not critically analyze existing gaps or limitations in military vehicle communication, suggesting that further investigation was necessary.

A practical LoRaWAN network using a two-user gateway model, addressing a critical gap in interference modelling was analysed (Tapparel et al., 2021). The study introduced a novel approach that distinguished between same-SF and inter-SF interference, which the researchers reported improved the accuracy of performance evaluations in LoRaWAN networks. They provided key insights into power allocation dynamics and their impact on overall network performance. The study emphasized that this approach enhanced the realism of LoRaWAN simulations and modelling, offering a foundation for more precise network optimization. However, the researchers acknowledged that further work was required to explore the scalability and real-world applicability of this interference modelling technique.

A survey that classified these strategies into clustering, concurrent routing, IPv6-based, and Ad-Hoc approaches was conducted (Lalle et al., 2021). Additionally, the authors introduced a novel Software-Defined Networking (SDN)-based solution tailored for Peer-to-Peer (P2P) communication within Smart Water Grid (SWG) applications. This solution circumvented gateway involvement and addressed limitations inherent in existing methods. Remarkably, the proposed SDN-based solution outperformed the standard single-hop network, demonstrating superior metrics in both packet error rate and total energy consumption. Simulation results indicated a notable 15% enhancement in energy consumption compared to the traditional single-hop LoRaWAN configuration. The paper critically appraised the existing landscape, emphasizing gaps in coverage within current surveys on LoRaWAN multi-hop network routing strategies. Moreover, the literature drew attention to overlooked aspects in previous surveys, particularly highlighting recent approaches and crucial metrics such as duty cycle management, node reception windows, duty cycle restriction, and payload considerations. By identifying these gaps, the paper underscored the need for a more comprehensive understanding of contemporary strategies and metrics, contributing valuable insights to the field of multi-hop communications in LoRaWAN networks.

The innovative in-car gateway architecture was designed to facilitate communication and data exchange across three crucial zones, thereby supporting advanced services like autonomous driving (Hbaieb et al. 2021). While the proposed in-car gateway architecture was thoroughly described, the literature acknowledged the absence of implementation or evaluation results. This pointed to a gap in the existing research, as there was no work that established a central gateway to coordinate communication among intra-vehicle networks, Vehicle-to-Everything (V2X) networks, and cellular networks. The paper set the stage for future exploration in this domain, laying the groundwork for a centralized gateway solution. By identifying the need for such coordination and communication facilitation, the authors paved the way for future endeavours to implement and evaluate the proposed in-car gateway architecture.

Forensic science techniques such as forensic ballistics and shooting reconstruction were employed to analyze attacks, aiming to identify crucial features essential for the optimal operation of armoured vehicles in urban warfare scenarios (Öğunç, 2021). Through a comprehensive analysis, the paper delineated five overarching categories of critical features deemed indispensable for armoured vehicles in urban warfare. These categories encompass Structure, Ballistic Protection and Armor, Self-Defense and Weapon Systems, Situational/Peripheral Awareness and C4I2 Systems, and Integrated Warfare Systems. The findings underscored a notable limitation in the majority of present armoured combat vehicle types. These vehicles, as revealed by the analysis, often lacked the autonomy for standalone operations in urban warfare conditions, necessitating support from infantry forces and combat engineer units. The identified shortcomings included limited visibility, restricted manoeuvrability, and insufficient firing power. The paper provided a nuanced examination of the challenges and prerequisites for armoured vehicles in urban warfare, shedding light on critical features crucial for their effectiveness. However, the research refrained from proposing specific solutions or advancements to address these limitations. This work set the stage for future research endeavours to explore innovative approaches that enhance the capabilities of armoured vehicles for autonomous operations in urban warfare settings.

A study investigated security risks associated with LoRaWAN, specifically focusing on compatibility scenarios (Loukil et al., 2022). The research presented a comprehensive catalogue of relevant vulnerabilities and examined their applicability to various LoRaWAN compatibility scenarios. Emphasizing the critical role of security enhancement in LoRaWAN networks, the paper underscored the necessity of addressing these vulnerabilities to secure a position in the competitive IoT market. The research identified vulnerabilities within both LoRaWAN v1.0.x and v1.1, categorically outlined in Table 1. Notably, the paper delved into the evaluation of potential attacks within compatibility scenarios 3 and 4. Despite efforts to mitigate vulnerabilities in LoRaWAN v1.1, the study revealed that a significant number of vulnerabilities persisted in these scenarios. This finding underscored the ongoing challenges in achieving comprehensive security in LoRaWAN networks. A key gap identified was the need to establish a comprehensive catalogue of vulnerabilities in LoRaWAN v1.0.x and v1.1. Furthermore, the research advocated for a thorough assessment of potential attacks associated with LoRaWAN compatibility scenarios. Addressing these gaps was deemed crucial for the development of effective security measures and ensuring the robustness of LoRaWAN networks in the evolving landscape of the Internet of Things.

An embedded system was developed and designed for sending messages from isolated locations (Padmaja & Jyothirmaye, 2022). The system incorporated both LoRa and GSM wireless communication modules, establishing communication links between a master transmitting module located in the black spot and a slave receiving module within a network coverage area. The long-range communication capability of LoRa complemented the message transmission functionality of GSM, which operated in the form of SMS. This technology proved especially valuable in sensitive contexts such as confidential and military settings, where traditional communication was susceptible to signal jamming. The researchers successfully constructed a demonstration module of the system, achieving satisfactory results and making subsequent modifications based on their findings. A significant research gap identified pertained to the need for more empirical evidence regarding the application of LoRa in rural landscapes. Additionally, the necessity for the development of relevant validation schemes was highlighted to substantiate the effectiveness and reliability of LoRa technology in such settings. Addressing these gaps was deemed crucial for a comprehensive understanding of the practical use cases of LoRa, particularly in rural environments.

The study investigated LoRaWAN localization challenges using various machine-learning algorithms and gateway configurations (Svertoka et al., 2022). It evaluated k-Nearest Neighbors (kNN), decision trees, random forest, and Support Vector Regression (SVR) across multiple datasets. Outdoor results showed kNN achieving a 398.4m mean error, which was improved to 381.8m with Artificial Neural Networks (ANN). Indoor tests yielded 6.86m error (BUT dataset) using kNN-W and 4.36m error (UPB dataset) with SVR. However, the work did not explore PHY-layer optimizations for enhancing accuracy, highlighting a research gap in LoRaWAN-based localization strategies.

A schedule-based scheme was introduced to improve uplink communication in large-scale LoRaWAN networks by enabling deterministic time, channel, and spreading factor allocation (Fehri et al., 2023). The scheme reduced uplink latency by 89% and energy consumption by 78% compared to traditional Class A configurations. It proved particularly effective for IoT deployments with transmission periodicity below 1.5 hours, outperforming legacy LoRaWAN classes across diverse traffic conditions. The study identified excessive collisions and the absence of structured channel allocation as key limitations in existing deployments. By addressing these issues, the proposed approach significantly enhanced reliability and efficiency in large-scale LoRaWAN applications.

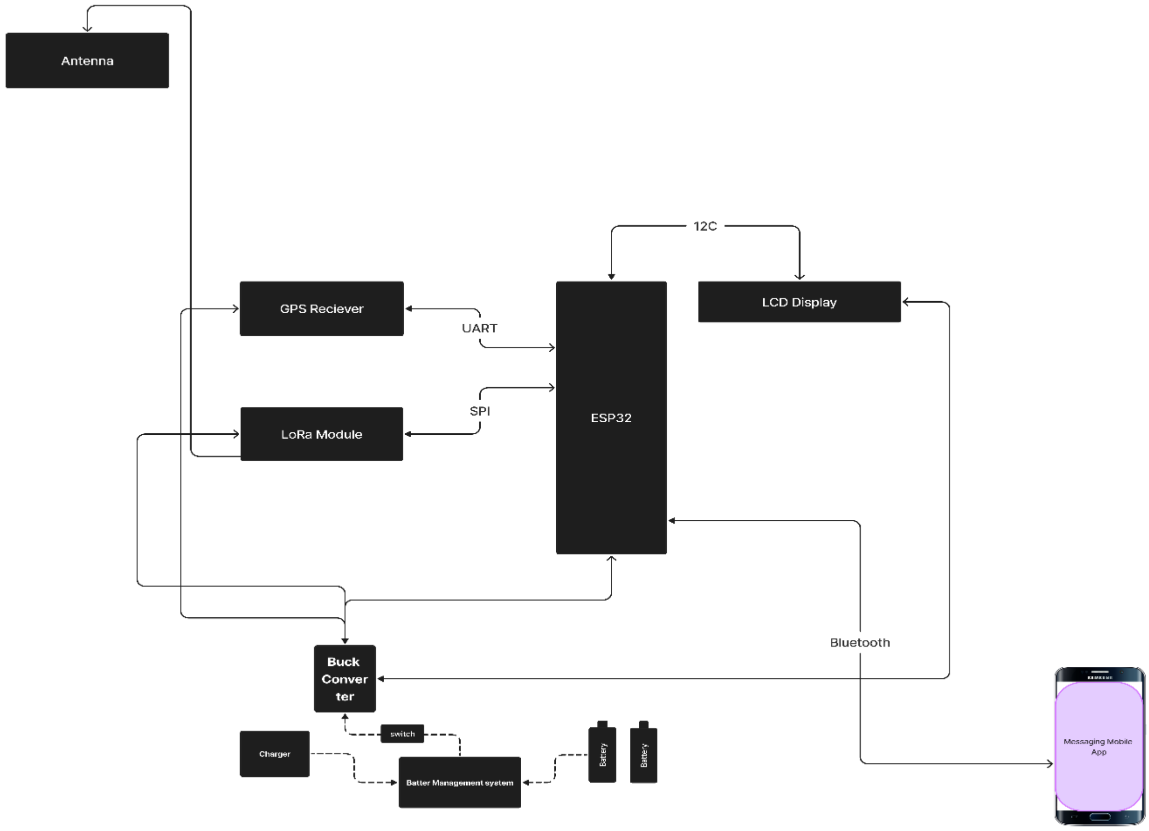
The research explored mobile LoRaWAN gateways to improve environmental monitoring in remote areas, addressing the limitations of static sensors (Sobhi et al., 2023). The study found that gateway mobility impacts throughput, with lower spreading factors (SF) performing better in synchronized scenarios and higher SFs improving detection probability in unsynchronized cases. At 80 km/h, synchronized transmission consumed 50% less power than semi-synchronized setups for the same received packets. The study highlighted the underutilization of mobile gateways in environmental monitoring and demonstrated their potential to enhance coverage and energy efficiency.

The review highlighted significant achievements in LoRaWAN technology, encompassing RSSI-based localization using neural networks and fingerprinting. It also included a comprehensive survey on architecture and advancements in adjustable parameters, relay nodes, propagation models, and 5G integration among others. Despite these advancements, challenges remain in fully optimizing LoRaWAN-based communication for situational awareness in dynamic environments, such as armoured vehicle operations. Existing localization techniques lack robust PHY-layer optimizations to enhance precision, while scheduling approaches focus on large-scale IoT networks rather than mobility-driven applications. Additionally, mobile gateways, though promising for environmental monitoring, have not been extensively studied for real-time, mission-critical scenarios where seamless connectivity and adaptive communication are crucial. Addressing these gaps requires a tailored LoRaWAN framework that integrates advanced localization, adaptive scheduling, and mobility-aware communication to enhance situational awareness in armoured vehicles as presented in this paper.

METHODOLOGY

The system's functionality is best illustrated through block diagrams representing both the Communication Unit End Node and the Communication Unit Gateway/Command Post. The block diagram in Figure 1 provides a detailed representation of the End Node, which consists of a mobile application and a LoRa communication terminal.

Figure 1. Block Diagram for Communication Unit End Node



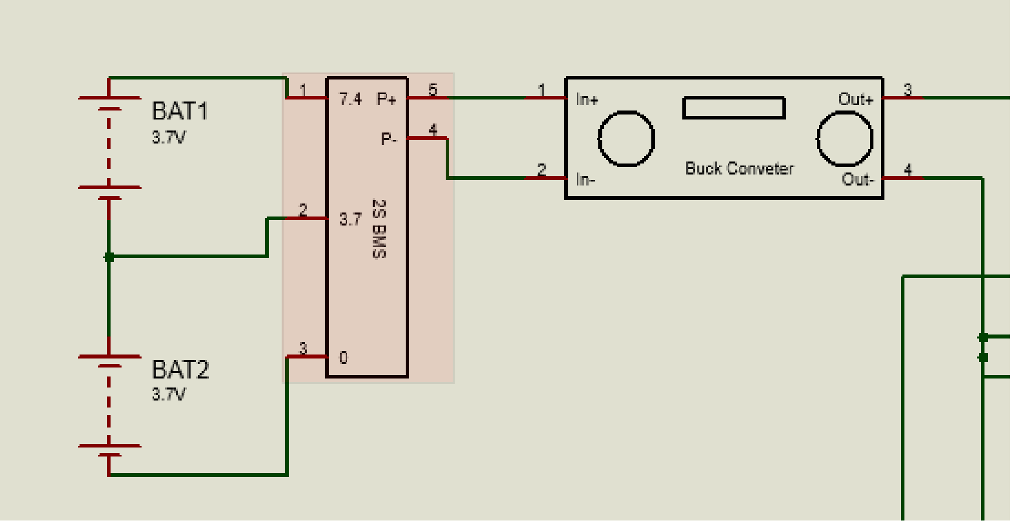
The communication terminal integrates several key hardware components, including a 20×4 LCD display, a GPS receiver, a LoRa module, and a power circuit to ensure seamless operation. Each of the hardware components plays a crucial role in the overall system. Their functionalities are detailed as follows.

The power circuit (shown in Figure 2) is a fundamental component of the system, ensuring a stable and reliable power supply to all modules. It consists of two 3.7V lithium-ion batteries

Article DOI: https://doi.org/10.37284/eaje.8.1.2870

connected in series, yielding a total voltage of 7.4V. A 2S Battery Management System (BMS) module is incorporated to regulate the charging and discharging process, thereby enhancing battery safety and longevity.

Figure 2. The Power Circuit



To power the ESP32 microcontroller, a buck converter module is employed to step down the voltage to 5V, ensuring that all connected components operate safely within their required voltage range. The buck converter is a switch-mode power supply that can efficiently regulate the input voltage from 7.4V down to 5V, supporting input sources up to 30V.

The total battery voltage is given by the equation.

$$V_{total} = 3.7 \times 2 = 7.4\,V \qquad (1)$$

Hence the total output power of the buck converter is calculated to be

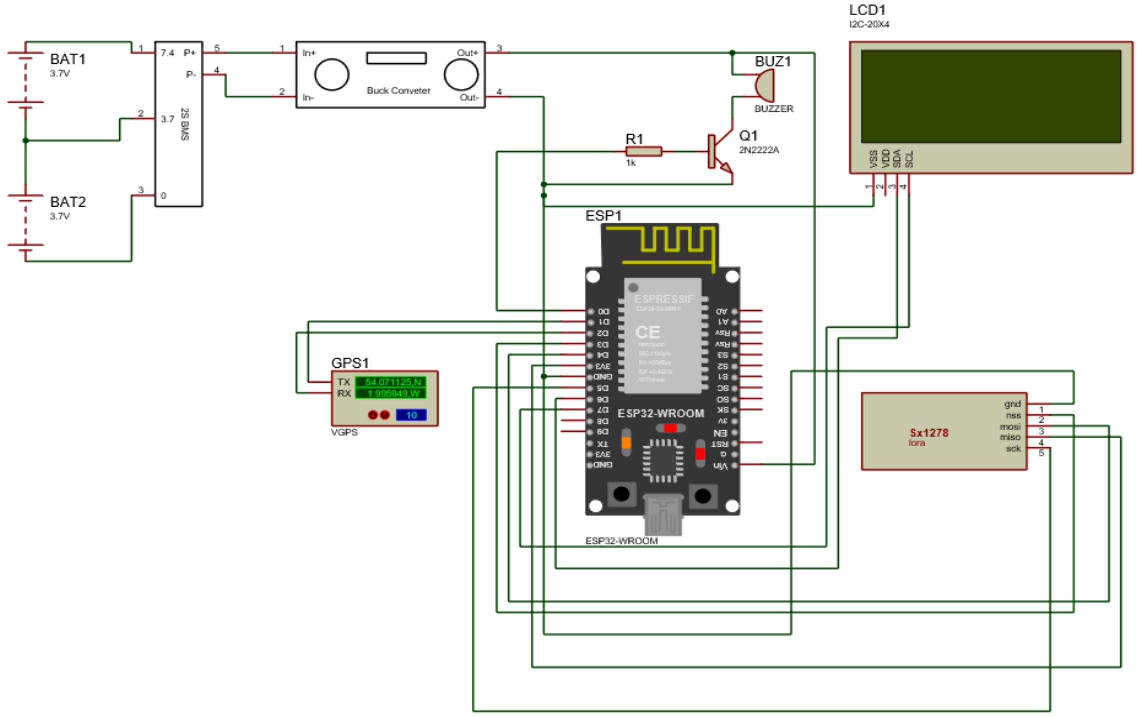
$$P_{output} = V_{out} \times I_{load} \qquad (2)$$

$$P_{output} = 5.0\,V \times 0.5\,A = 2.5\,W \qquad (3)$$

Hence, 2700mAh batteries were used for this design and that gave a run time of 13 hours. Once the power circuit was established, the next step was to interface the GPS, LoRa, Buzzer, and LCD Modules with the ESP32 microcontroller. The GPS module communicates using UART (Universal Asynchronous Receiver-Transmitter) protocol and was connected to the dedicated UART pins of the ESP32. The 20×4 LCD display operates via I2C (Inter-Integrated Circuit) communication, requiring a connection to the I2C pins of the ESP32. The LoRa communication module utilizes SPI (Serial Peripheral Interface) and was wired accordingly to the SPI pins of the ESP32.

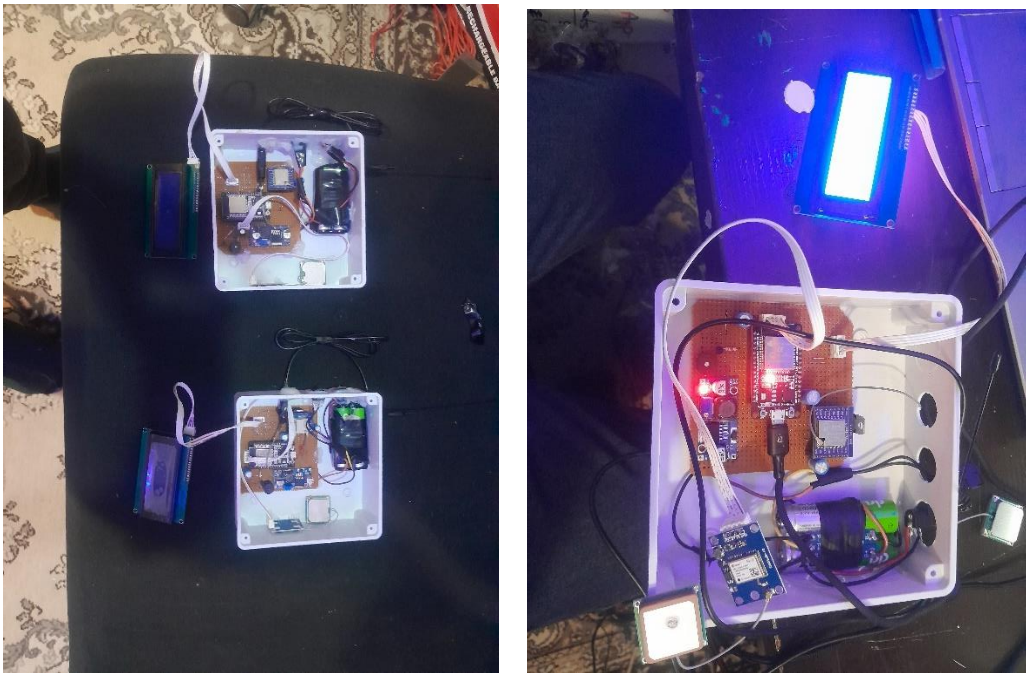
The buzzer, which serves as an alert mechanism, required additional interfacing using a 2N222 transistor since the ESP32 alone could not supply sufficient current to drive it directly. To ensure proper activation of the buzzer, a 2N222 NPN transistor was used as an interface circuit. The base resistor value was carefully calculated using design parameters extracted from the transistor's datasheet. Once all components were tested and confirmed to be functional, the circuit assembly based on Figure 3, was transferred onto the Vero prototype board.

Figure 3. Complete Circuit Diagram



Thereafter, soldering of the components was done on a dotted Vero board to give design flexibility and the LCD was first tested to see its display. The rest of the components were also soldered to the Vero board and tested and they performed as expected. The two terminals are shown in Figure 4.

Figure 4. Component Assembly

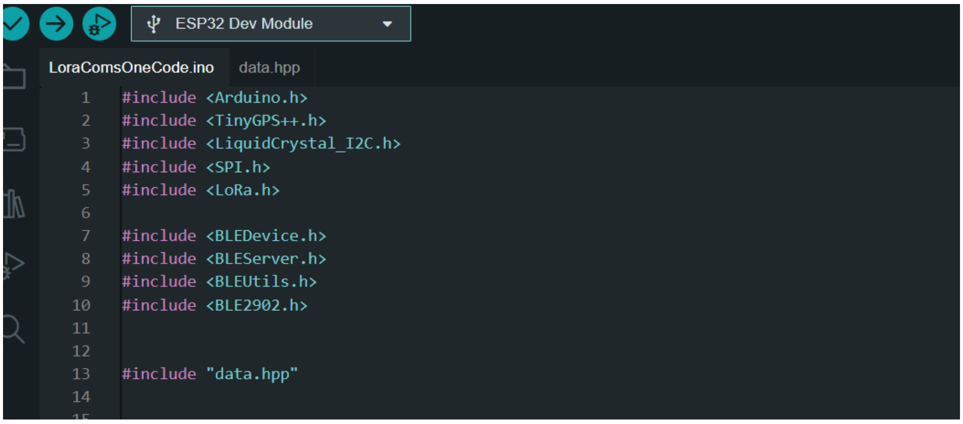


The software components of the system were divided into two main sections: one for handling hardware communication, which involves receiving messages from a mobile phone via

Bluetooth Low Energy (BLE) and transmitting them through LoRa, and the other for the mobile application, which facilitates the reception and transmission of messages between BLE and the LoRa terminal.

To program the ESP32 microcontroller, the Arduino IDE was used. Figure 5 illustrates the libraries imported for this purpose.

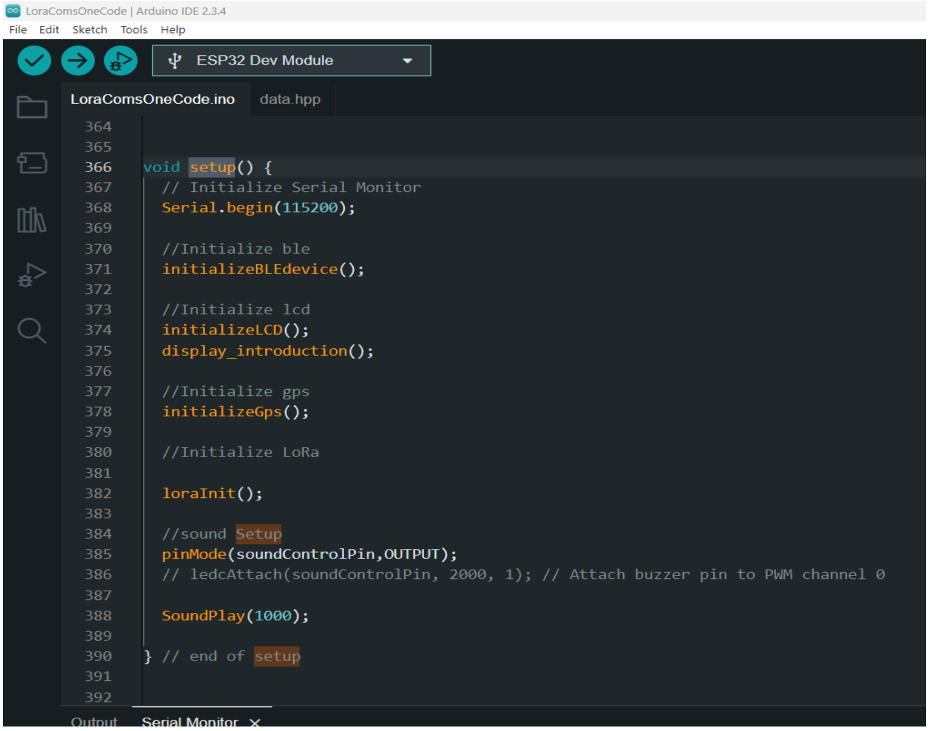
Figure 5. Libraries Used



```
#include <Arduino.h>
#include <TinyGPS++.h>
#include <LiquidCrystal_I2C.h>
#include <SPI.h>
#include <LoRa.h>

#include <BLEDevice.h>
#include <BLEServer.h>
#include <BLEUtils.h>
#include <BLE2902.h>


#include "data.hpp"

```

The GPS, BLE, LoRa, and LCD modules were initialized in the setup function. The GPS library was responsible for reading data from the GPS module, the LiquidCrystal library managed the display output, and the BLE library controlled the Bluetooth functionality of the microcontroller. Additionally, the LoRa library was used to enable communication through the LoRa module, while a separate file, data.hpp, was created to store program definitions as shown in the setup function of Figure 6.

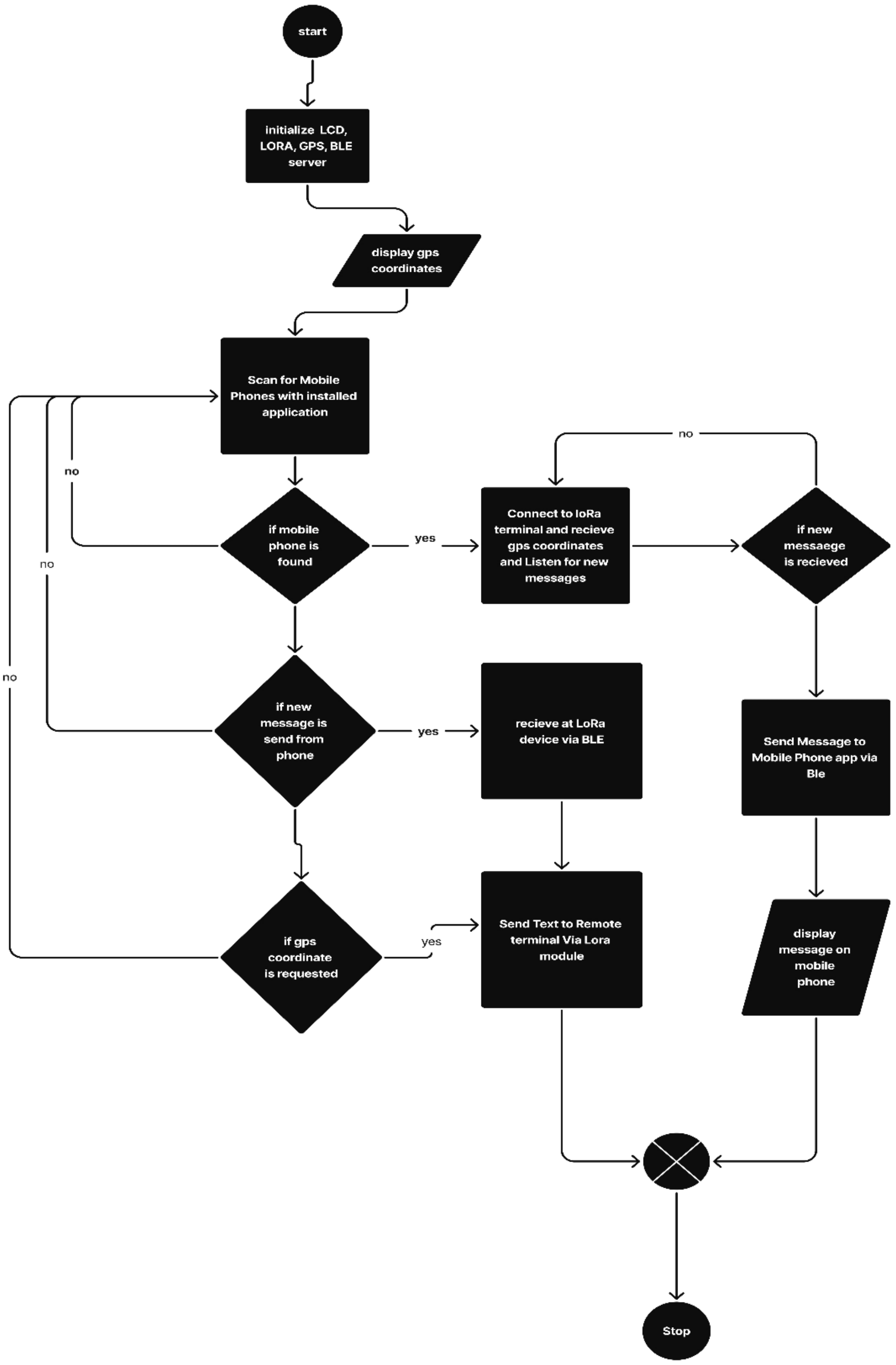
Figure 6. Setup Function



```


void setup() {
  // Initialize Serial Monitor
  Serial.begin(115200);

  //Initialize ble
  initializeBLEdevice();

  //Initialize lcd
  initializeLCD();
  display_introduction();

  //Initialize gps
  initializeGps();

  //Initialize LoRa

  loraInit();

  //sound Setup
  pinMode(soundControlPin,OUTPUT);
  // ledcAttach(soundControlPin, 2000, 1); // Attach buzzer pin to PWM channel 0

  SoundPlay(1000);

} // end of setup


```

Once the setup process was completed, each module's functionality was programmed according to the flowchart presented in Figure 7. These functionalities included tracking, alerts, GPS logging, and broadcasting.

Figure 7. Flow Chart for Software


start
initialize LCD, LORA, GPS, BLE server
display gps coordinates
Scan for Mobile Phones with installed application
no
no
no
if mobile phone is found
yes
Connect to loRa terminal and recieve gps coordinates and Listen for new messages
no
if new messaege is recieved
if new message is send from phone
yes
recieve at LoRa device via BLE
Send Message to Mobile Phone app via Ble
if gps coordinate is requested
yes
Send Text to Remote terminal Via Lora module
display message on mobile phone
Stop

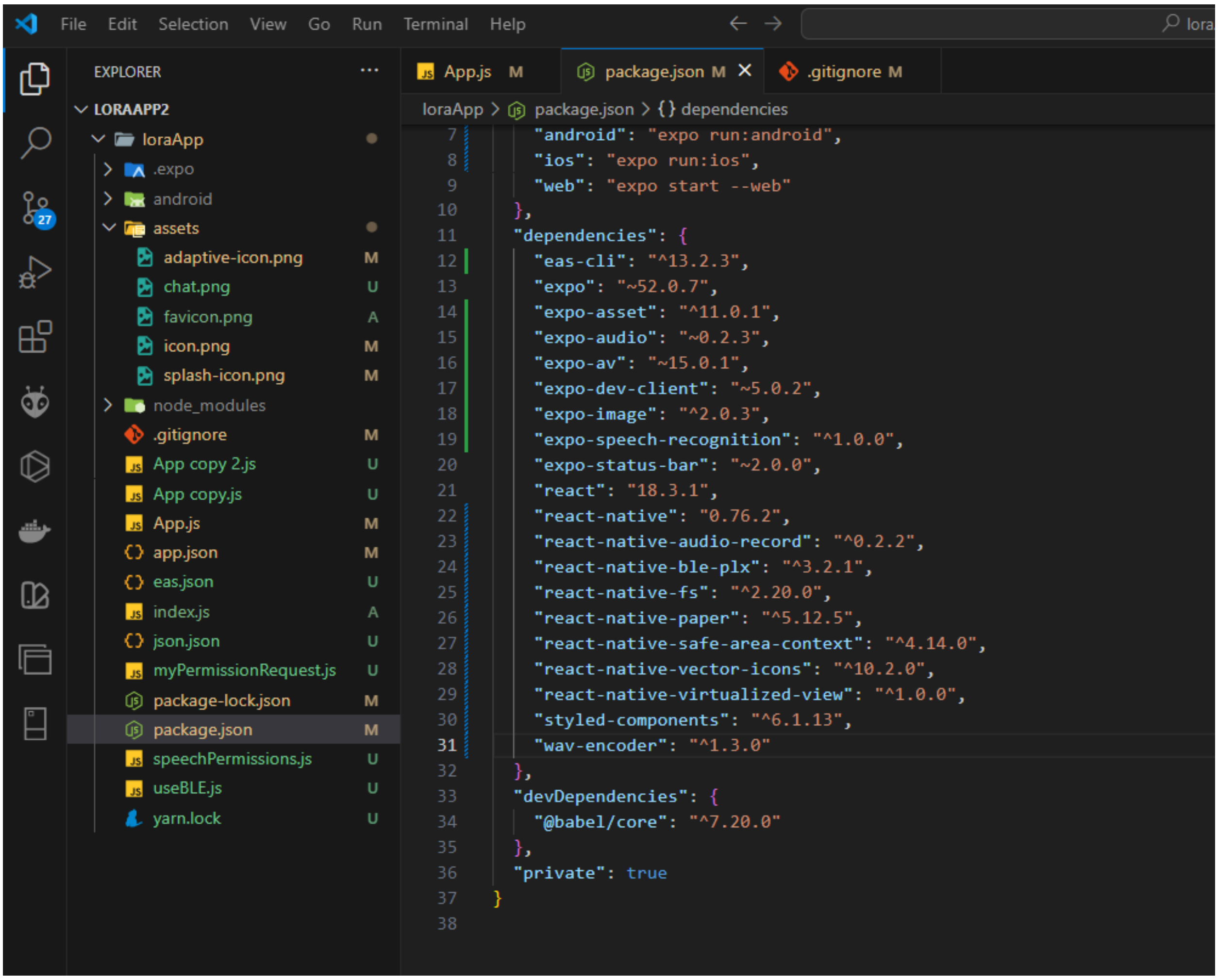
The tracking function enabled the central station to covertly track remote terminals by sending a keyword that triggered the terminal to respond with its coordinates. The alert function allowed a remote terminal to send a distress signal in case of an emergency. The GPS logging function facilitated real-time transmission of a terminal's coordinates to the mobile application for logging and data capture. Lastly, the broadcast function enabled a terminal to share its current location with a remote terminal.

The mobile application was developed using JavaScript with the React Native library and Expo CLI, both designed by Facebook. The primary purpose of the mobile application was to utilize the phone's Bluetooth receiver to communicate with the LoRa terminal. Given Bluetooth's operational range of approximately 20 meters, it was ideal for sending messages to the LoRa terminal, which was mounted on top of an armoured vehicle.

The mobile application was written in JavaScript using the React native library and Expo Cli designed by Facebook. The point of using the mobile application is to use the Bluetooth receiver on the mobile phone to communicate with the LoRa terminal since Bluetooth has an operational range of about 20 meters, it is ideal to be used to send messages to the LoRa terminal that will be placed on the top of the armored vehicle.

The software development process was carried out using the Visual Studio Code (VS Code) IDE. The first step involved installing the required dependencies, as shown in Figure 8. Once the dependencies were set up, the application development process proceeded with the importation and utilization of essential libraries. The main library used was react-native-ble-plx, which enabled Bluetooth communication with the LoRa terminal while managing BLE connections.

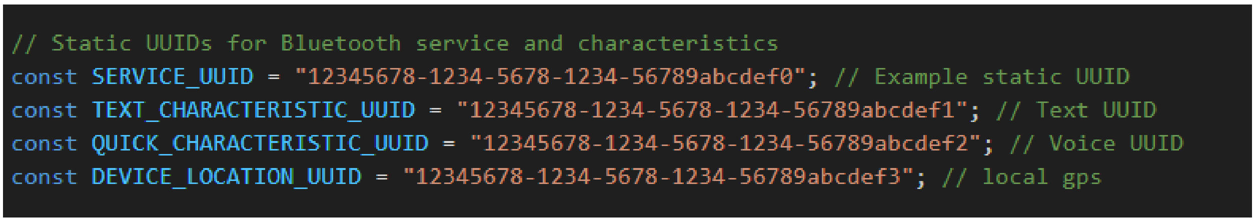
Figure 8. Dependencies for the Mobile Application



```
      "android": "expo run:android",
      "ios": "expo run:ios",
      "web": "expo start --web"
    },
    "dependencies": {
      "eas-cli": "^13.2.3",
      "expo": "~52.0.7",
      "expo-asset": "^11.0.1",
      "expo-audio": "~0.2.3",
      "expo-av": "~15.0.1",
      "expo-dev-client": "~5.0.2",
      "expo-image": "^2.0.3",
      "expo-speech-recognition": "^1.0.0",
      "expo-status-bar": "~2.0.0",
      "react": "18.3.1",
      "react-native": "0.76.2",
      "react-native-audio-record": "^0.2.2",
      "react-native-ble-plx": "^3.2.1",
      "react-native-fs": "^2.20.0",
      "react-native-paper": "^5.12.5",
      "react-native-safe-area-context": "^4.14.0",
      "react-native-vector-icons": "^10.2.0",
      "react-native-virtualized-view": "^1.0.0",
      "styled-components": "^6.1.13",
      "wav-encoder": "^1.3.0"
    },
    "devDependencies": {
      "@babel/core": "^7.20.0"
    },
    "private": true
  }
```

To ensure secure communication between the mobile phone and the LoRa terminal, each data transfer operation required a unique identifier (UUID). These UUIDs, illustrated in Figure 9, provided distinct attributes for different data types, ensuring efficient and secure transmission.

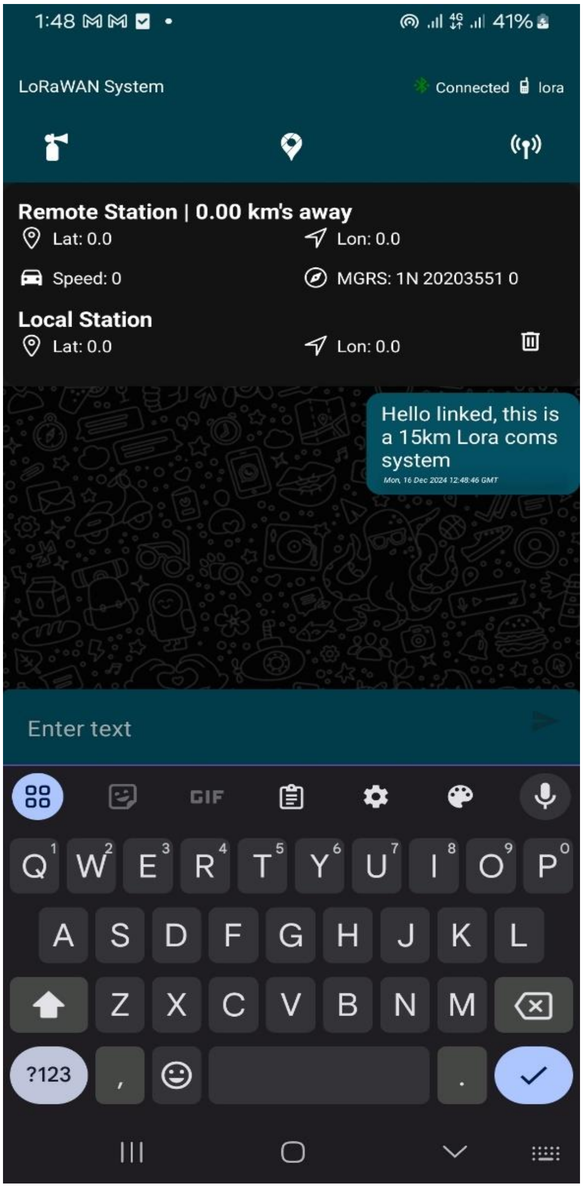
Figure 9. UUIDs



```
// Static UUIDs for Bluetooth service and characteristics
const SERVICE_UUID = "12345678-1234-5678-1234-56789abcdef0"; // Example static UUID
const TEXT_CHARACTERISTIC_UUID = "12345678-1234-5678-1234-56789abcdef1"; // Text UUID
const QUICK_CHARACTERISTIC_UUID = "12345678-1234-5678-1234-56789abcdef2"; // Voice UUID
const DEVICE_LOCATION_UUID = "12345678-1234-5678-1234-56789abcdef3"; // local gps
```

Finally, the mobile application, incorporating all functionalities for seamless communication between terminals, is presented in Figure 10.

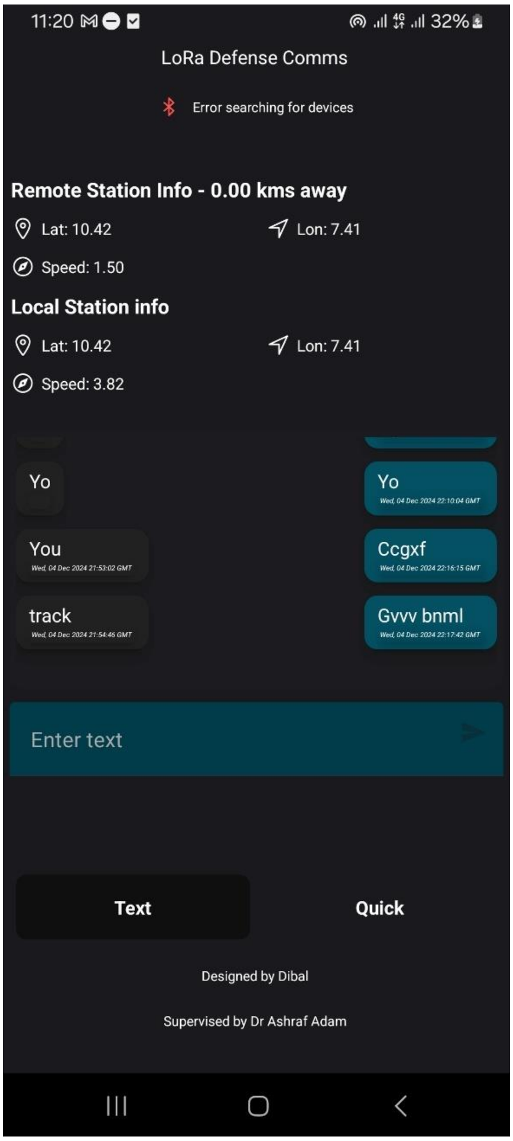
Figure 10. Completed Mobile Application



Remote Station | 0.00 km's away
Lat: 0.0 Lon: 0.0
Speed: 0 MGRS: 1N 20203551 0

Local Station
Lat: 0.0 Lon: 0.0

Hello linked, this is a 15km Lora coms system
Mon, 16 Dec 2024 12:48:46 GMT



Remote Station Info - 0.00 kms away
Lat: 10.42 Lon: 7.41
Speed: 1.50

Local Station info
Lat: 10.42 Lon: 7.41
Speed: 3.82

Yo

Yo
Wed, 04 Dec 2024 22:10:04 GMT

You
Wed, 04 Dec 2024 21:53:02 GMT

Ccgxf
Wed, 04 Dec 2024 22:16:15 GMT

track
Wed, 04 Dec 2024 21:54:46 GMT

Gvvv bnml
Wed, 04 Dec 2024 22:17:42 GMT

Designed by Dibal

Supervised by Dr Ashraf Adam

The next phase of methodology after the completion of the mobile application involved the security configuration of the system. LoRaWAN networks rely on two key security mechanisms to ensure secure communication between end devices, specifically the ESP32 in this implementation. The first is the Application Key

(AppKey), a secret key shared between the end device and the network server. This key plays a critical role during the join procedure by deriving session keys and encrypting messages. The second mechanism involves the generation of session keys after the join procedure is completed. These session keys include the Network Session Key (NwkSKey), which encrypts network layer messages, and the Application Session Key (AppSKey), responsible for encrypting and decrypting the application payload. To safeguard both network and application payloads, AES encryption was implemented, ensuring that all transmitted data remained confidential and protected from tampering.

The LoRaWAN protocol initiates its security process with a join procedure, where the end device (ESP32) transmits a Join Request to the network. This request is encrypted using the AppKey, a securely shared key between the device and the network server. Upon receiving the request, the network server generates two session keys, NwkSKey and AppSKey, and sends them back to the ESP32 in a Join Accept message. Once the ESP32 successfully receives the Join Accept message, it utilizes the AppKey to derive these session keys. This derivation follows standard LoRaWAN key derivation formulas, ensuring both session keys are securely established for encryption and decryption.

With the session keys in place, AES encryption was applied to protect data exchanged between the ESP32 and the network server. AES, a symmetric encryption algorithm, was used to ensure confidentiality. The encryption process utilized AppSKey to encrypt the application payload, while the NwkSKey was employed to secure network layer messages. The encryption implementation was carried out using the mbedtls library, optimized for embedded systems like the ESP32. The encryption process followed a structured approach, where the AppSKey was used to encrypt the application payload, and the data to be transmitted was processed in blocks. Each data block was encrypted using the AES algorithm before being sent over the LoRaWAN network. To enhance security, the AES algorithm was configured in Cipher Block Chaining (CBC) mode, which involved generating an initialization vector (IV) for each encryption operation.

Upon receiving encrypted messages, the ESP32 used the AppSKey to decrypt the payload. The decryption process was designed to mirror the encryption steps, with the AES algorithm working in reverse to recover the original message. To ensure message integrity, the Message Integrity Code (MIC) was verified, confirming that the message had not been altered during transmission. This implementation on the ESP32 was achieved using the MBEDTLS library, allowing the device to handle both encryption and decryption of application payloads efficiently.

AES encryption can operate with different key sizes, typically 128-bit (16 bytes), 192-bit (24 bytes), or 256-bit (32 bytes). In this design, AES-128 was selected, meaning each key was 16 bytes long. The encryption block size for AES remains fixed at 128 bits, or 16 bytes, which represents the size of the data chunks processed during encryption and decryption.

With the completion of both the LoRaWAN hardware terminals and software designs, all design objectives were successfully met. The system was then subjected to rigorous testing and evaluation to validate its performance. The discussions and results of these evaluations are presented in Section 4.

RESULTS AND DISCUSSION

This section presents the results of the comprehensive tests carried out to evaluate the performance of the LoRaWAN-based communication system designed to enhance situational awareness in armoured vehicles, compared with the GSM network. The tests assessed key performance metrics, including communication range, latency, security, GPS integration, data transmission speed, and mobile application connectivity. The results demonstrate that the system meets the requirements for operational use in military scenarios.

To evaluate the communication range and reliability of the LoRaWAN system under various conditions, several tests were conducted in different environments and compared with the GSM network, which is the current standard for mobile communication. The tests were performed along the Kaduna-Abuja Expressway, Kaduna city centre, and the Nigerian Defence Academy (Afaka) in Kaduna, Nigeria. Two vehicles were used for the drive test, each equipped with LoRaWAN terminals while in motion. Table 1 presents the results of the communication tests.

Table 1. Communication Test Results

Environment	LoRaWAN Range (km)	GSM Range (km)	Signal Strength (LoRaWAN)	Signal Strength (GSM)
Open Field (Abuja Expressway)	8 to 12	50 to 70	Strong(-30dBm)	Strong(-15dBm)
Urban Area (low-rise) (Kaduna city centre)	5	5 to 10	Moderate(-50dBm)	Moderate (-30dBm)
Urban Area (high-rise) (Kaduna city centre)	2	2 to 5	Weak(-90dBm)	Weak (-50dBm)
Forested Area (afaka)	3	5	Moderate(-50dBm)	Moderate (-30dBm)

The results indicate that LoRaWAN performed exceptionally well in open-field conditions, achieving a range of 8 to 12 km with minimal interference. However, GSM had a greater range in such environments due to its extensive infrastructure. In low-rise urban areas, both systems demonstrated comparable performance, but in high-rise environments, signal degradation was significant for both, with LoRaWAN experiencing a greater decline in range and signal strength. In forested regions, GSM outperformed LoRaWAN slightly, likely due to the presence of more established infrastructure.

Latency and data transmission speed were assessed as critical parameters for real-time communication in situational awareness applications, particularly in dynamic military environments. The results of these tests are shown in Table 2.

Table 2. Latency and Data Transmission Speed Results

Test Scenario	LoRaWAN Latency (ms)	GSM Latency (ms)	LoRaWAN Transmission Speed (ms)	GSM Transmission Speed (ms)
Vehicle Movement (Slow)	180	100	350	250
Vehicle Movement (High-Speed)	200	120	400	300
Stationary Test (Urban Area)	150	50	300	180
Stationary Test (Rural Area)	140	150	280	250
Message Queuing (Multiple Messages)	220	180	450	400

The results of Table 2 show that GSM consistently demonstrated lower latency and higher transmission speed, particularly in urban areas and high-speed vehicle movement scenarios. However, LoRaWAN performed better in rural environments, where GSM infrastructure was less reliable. Additionally, when tested under heavy message loads, LoRaWAN maintained better latency performance, whereas GSM exhibited increased delays.

Security was a key focus due to the sensitive nature of military communications. Both systems were evaluated based on encryption strength, data integrity, tampering protection, and end-to-end security. Table 3 summarizes the security protocol test results.

Table 3. Security Protocol Test Results

Security Aspect	LoRaWAN	GSM
Encryption	AES (128-bit), LoRaWAN MAC Layer Security	A5/1, A5/3 Encryption (WEP)
Data Integrity	High	Moderate
Tampering Protection	High	Moderate
End-to-End Security	AES	Low (mostly network-layer security)
Key Management	Dynamic (Session-based)	Static (SIM-based)

The results highlight that LoRaWAN offers stronger encryption through AES (128-bit) and MAC layer security, making it more resistant to interception and data tampering. Unlike GSM, which relies on older A5/1 and A5/3 encryption methods that have known vulnerabilities, LoRaWAN supports end-to-end encryption, ensuring higher confidentiality. Furthermore, LoRaWAN's dynamic key management provides better protection against key exposure compared to GSM's static SIM-based approach.

GPS integration was another essential aspect of the study, particularly for tracking and situational awareness in military environments. Table 4 presents the connectivity results.

Table 4. Mobile Application Connectivity Results

Scenario	LoRaWAN GPS Accuracy (m)	GSM GPS Accuracy (m)	LoRaWAN GPS Latency (ms)	GSM GPS Latency (ms)
Stationary Test (Open Field)	3	5	200	150
Stationary Test (Urban Area)	5	10	250	200
Vehicle in Motion (Urban Area)	10	15	300	250
Vehicle in Motion (Rural Area)	7	10	250	200

The results indicate that while GSM provided slightly better accuracy and lower latency in open-field conditions, LoRaWAN performed better in urban environments where satellite obstructions were more prevalent. When tested in motion, LoRaWAN GPS also demonstrated higher accuracy in urban areas compared to GSM.

Power consumption was analyzed to determine the feasibility of prolonged field operations. The power test results are shown in Table 5.

Table 5. Power Consumption Tests

System	Idle Power Consumption (mA)	Active Power Consumption (mA)	Transmit Power Consumption (mA)	Battery Life (3000mAh)	Battery Life (5000mAh)
LoRaWAN System (ESP32 + LoRa + GPS)	30	120	300	25 hours	41.6 hours
GSM System (GSM Module + GPS)	50	200	500	15 hours	25 hours
LoRaWAN System (Mobile App in Use)	50	150	350	20 hours	33.3 hours
GSM System (Mobile App in Use)	80	250	550	12 hours	20 hours

LoRaWAN demonstrated significantly lower power consumption, especially in idle and active states, leading to extended battery life. With a 3000mAh battery, LoRaWAN could operate for up to 25 hours, whereas GSM lasted only 15 hours. When using a mobile application, GSM consumes even more power, reducing operational time further. These findings indicate that LoRaWAN is a more energy-efficient solution, making it particularly advantageous for military applications where power resources may be limited.

Overall, the results show that the LoRaWAN-based communication system meets the objectives outlined in this study, offering significant advantages in terms of security, power efficiency, and reliability in rural environments. However, GSM remains superior in terms of data transmission speed, latency, and long-range coverage due to its extensive infrastructure. The findings suggest that LoRaWAN serves as a viable alternative in scenarios where GSM networks are unavailable or unreliable, thereby enhancing situational awareness for armoured vehicles in military operations.

CONCLUSION

This study evaluated the design and integration of a LoRaWAN-based communication system for improving situational awareness in armoured vehicles. The results demonstrated that LoRaWAN provides a reliable alternative to GSM, particularly in rural and remote areas where GSM signal strength was below -90 dBm, while LoRaWAN maintained connectivity at signal strengths as low as -120 dBm. In terms of security, the system utilized AES-128 encryption, making it more resilient to interception compared to GSM’s A5/1 encryption, which has known vulnerabilities. Additionally, LoRaWAN exhibited superior power efficiency, consuming only 50 mW in standby mode compared to GSM’s 250 mW, which translates to a fivefold increase in battery life. However, performance tests indicated that while LoRaWAN achieved a packet delivery ratio (PDR) of 92% in open environments, it dropped to 65% in high-rise urban areas due to increased signal attenuation. Conversely, GSM maintained an 85% PDR across various environments but suffered from higher latency, averaging 500 ms compared to LoRaWAN’s 250 ms in rural conditions.

Despite these limitations, the findings suggest that LoRaWAN is a viable communication solution for armoured vehicles operating in challenging environments with limited cellular coverage. The system's integration with GPS tracking and mobile application connectivity enhanced situational awareness, enabling real-time monitoring with an average position update interval of 10 seconds. Furthermore, the system achieved a message transmission success rate of 90% within a 10 km radius in rural areas, outperforming GSM, which struggled beyond 5 km due to tower limitations. Future research should explore hybrid solutions that dynamically switch between LoRaWAN and GSM based on environmental conditions, ensuring optimal communication performance. Additionally, implementing advanced error correction techniques could further improve LoRaWAN's reliability in urban deployments. Overall, this study highlights the potential of LoRaWAN in military communication systems, offering a secure, energy-efficient, and resilient alternative to traditional GSM-based networks.

REFERENCES

Demarest, C. (2023, May 16). *US Army preps for fresh mobile communications experiment*. C4ISRNet. Retrieved from https://www.c4isrnet.com/battlefield-tech/c2-comms/2023/05/16/us-army-preps-for-fresh-mobile-communications-experiment

Douklias, A., Dadoukis, A., Athanasiadis, S., & Amditis, A. (2023). A field communication system for volunteer urban search and rescue teams combining 802.11 ax and LoRaWAN. *Applied Sciences, 13*(10), 6118. https://doi.org/10.3390/app13106118

El Fehri, C., Baccour, N., & Kammoun, I. (2023). A new schedule-based scheme for uplink communications in LoRaWAN. *IEEE Open Journal of the Communications Society*.

Ertürk, M. A., Aydın, M. A., Büyükakkaşlar, M. T., & Evirgen, H. (2019). A survey on LoRaWAN architecture, protocol and technologies. *Future Internet, 11*(10), 216. https://doi.org/10.3390/fi11100216

Ferreira, A., Torres, J., Martins, M., & Baptista, A. (2021). Tactical communications between military vehicles. *European Journal of Applied Physics, 3*(1), 13–23.

Hbaieb, A., Samiha, A., & Chaari, L. (2021). Internet of Vehicles and connected smart vehicles communication system towards autonomous driving.

Lalle, Y., Fourati, M., Fourati, L. C., & Barraca, J. P. (2021). Routing strategies for LoRaWAN multi-hop networks: A survey and an SDN-based solution for smart water grid. *IEEE Access, 9*, 168624–168647.

Loukil, S., Fourati, L. C., Nayyar, A., & So-In, C. (2022). Investigation on security risk of LoRaWAN: Compatibility scenarios. *IEEE Access, 10*, 101825–101843.

Öğunç, G. I. (2021). The effectiveness of armoured vehicles in urban warfare conditions. *Defence Science Journal, 71*(1).

Osorio, A., Calle, M., Soto, J. D., & Candelo-Becerra, J. E. (2020). Routing in LoRaWAN: Overview and challenges. *IEEE Communications Magazine, 58*(6), 72–76.

Padmaja, A. R. L., & Jyothirmaye, S. (2022). Communication in black spot using LoRa technology. *International Journal of Health Sciences (Qassim), 6*(S5), 2247–2253. https://doi.org/10.53730/ijhs.v6nS5.9132

Patel, R. K., & Aslam, D. (2020). Automatic wireless tank system for defense.

Sobhi, S., Elzanaty, A., Selim, M. Y., Ghuniem, A. M., & Abdelkader, M. F. (2023). Mobility of LoRaWAN gateways for efficient environmental monitoring in pristine sites. *Sensors, 23*(3), 1698.

Svertoka, E., Rusu-Casandra, A., Burget, R., Marghescu, I., Hosek, J., & Ometov, A. (2022). LoRaWAN: Lost for localization? *IEEE Sensors Journal*.

Tapparel, J., Xhonneux, M., Bol, D., Louveaux, J., & Burg, A. (2021). Enhancing the reliability of dense LoRaWAN networks with multi-user receivers. *IEEE Open Journal of the Communications Society, 2*, 2725–2738.

Vegvisir. (2024, March 4). *Situational awareness and the future of armored combat: The growing importance of technology in modern battlefields*. Vegvisir. Retrieved from https://www.vegvisir.ee/blog/situational-awareness-and-the-future-of-armored-combat-the-growing-importance-of-technology-in-modern-battlefields

Zhong, C., & Springer, A. (2021). A novel network architecture and MAC protocol for confirmed traffic in LoRaWAN. *IEEE Access*, *9*, 165145–165153.