Securing a LoRa-Based Linear Sensor Network for Underground Mining Emergencies

TNE30009 Case Study Report

Dylan Rodwell
105341089
105341089@student.swin.edu.au

***Abstract*—Ensuring the safety and operational continuality of personnel and equipment in underground mining environments necessitates robust and reliable emergency communication systems. This report investigates the security challenges posed by a prototype LoRa-based linear sensor network designed for tracking the location of miners and equipment during emergencies. While LoRa technology offers long-range, cost-effective, and easily deployable communication suited to underground conditions, it lacks inherent security features and exposes critical networks to new risks. The report identifies key assets and vulnerabilities within the system, ranks security risks using a structured methodology, and formulates targeted security policies and implementation measures. By addressing a variety of security concerns, the proposed strategies aim to mitigate risks and enable secure deployment of LoRa-based emergency networks in underground mines.**

Keywords—LoRa, underground mining, sensor network emergency communications, security, risk analysis, policy

I. Introduction

When working in an underground mine, there are many challenges when protecting the security and safety of personnel and equipment. It is essential to have a backup communication network for emergencies where main communication systems are damaged or unavailable. The key characteristics of this type of system is to be robust, reliable and easy to deploy. The system explored in this report is a prototype LoRa-based linear sensor network designed to transmit location information of personnel and equipment in underground mines during emergencies.

LoRa (Long Range) technology offers various advantages for underground environments due to its long range, cost-effectiveness, and ease of deployment. The system uses a series of wireless relays, deployed as rescuers or repairers travel through the mine, to form a linear network. This linear network forwards location data from tags (source nodes) carried by personnel and equipment to a headend (destination node) on the surface. LoRa was also designed to work independently of Internet Protocol (IP) networks and utilises flooding rather than unicast for message forwarding, with collisions management based on a simplified Carrier Sense Multiple Access (CSMA) scheme [1].

However, along with all its advantages, LoRa also introduces significant security considerations. Unlike many conventional wireless technologies, such as IEEE 802.11, LoRa does not have any built-in security features, and the prototype system as described in the report, does not implement any additional security features either. Additionally, the fact the system has to connect to the mine's surface infrastructure via a gateway exposes the system to additional attack vectors, such as unauthorised access and potential disruption of critical communications.

This report analyses the security risks associated with deploying such a system in an underground mining operation. It identifies key assets and vulnerabilities, ranks the most significant risks, and formulates security policies and practical implementation measures to mitigate those risks. The goal is to ensure that any future deployment of this LoRa-based emergency network can be conducted in a secure manner, thereby safeguarding both personnel and operational assets during critical incidents.

II. Risk Analysis

The security of this LoRa-based network is critical for ensuring the safety and operational integrity of the underground mining operations, especially during emergencies. This section identifies the key assets at risk, assesses the major security threats and ranks these risks using the simplified Delphi method.

A. Key Assets

- **Personnel Safety:** The safety of miners and emergency responders relying on accurate, timely location data.
- **Location and Status Data:** Integrity and confidentiality of data transmitted through the network.
- **Relay and Tag Hardware:** Physical devices that enable communication.
- **Gateway/Headend:** The node connecting the underground network to the surface network.
- **Surface Network Connectivity:** The mine's border communication and control infrastructure.

B. Risk Identification and Assessment

Below are the primary risks identified, with justification for their impact and likelihood analysis.

Risk 1: ***Unauthorised Interception or Tampering of Data***

- **Description:** LoRa's lack of default encryption and open wireless medium allows adversaries to intercept or modify location data, endangering rescue operations or exposing sensitive information.
- **Impact: 5/5**

  Justification: Compromised or misleading location data can put lives at risk during emergencies.
- **Likelihood: 4/5**

Justification: LoRa transmissions are unencrypted and relatively easy to intercept or spoof with basic radio equipment.

- **Risk Score: 20/25**

Risk 2: ***Physical Compromise or Tampering with Relays/Tags***

- **Description:** Devices may be physically accessed and tampered with, destroyed, or replaced by unauthorised individuals.
- **Impact: 4/5**

  Justification: Unauthorised tampering could disable communications or introduce malicious devices, leading to data loss or decryption.
- **Likelihood: 3/5**

  Justification: Underground areas can be unmonitored, especially during emergencies, but access requires physical presence.
- **Risk Score: 12/25**

Risk 3: ***Compromise of Gateway/Headend***

- **Description:** The gateway links underground surface networks; compromise here could allow broad disruption or unauthorised access to critical systems.
- **Impact: 5/5**

  Justification: A compromised gateway could risk all emergency communication and potentially threaten the mine's IT infrastructure.
- **Likelihood: 2/5**

  Justification: The gateway is likely in a more secure area, making access less likely than other field devices.
- **Risk Score: 10/25**

Risk 4: ***Denial of Service (DoS) Attacks***

- **Description:** Attackers may flood the network, overwhelming relays and disrupting message delivery, especially in flood-based relay networks such as LoRa.
- **Impact: 3/5**

  Justification: Could delay or block critical information, increasing operational and safety risks.
- **Likelihood: 3/5**

  Justification: DoS is possible with radio jamming or by flooding with rogue devices, but would require proximity and effort. [3]
- **Risk Score: 9/25**

Risk 5: ***Unauthorised Surface Network Access via Gateway***

- **Description:** Insufficient gateway controls could allow attackers to bridge from the LoRa network to the mine's border IT network.
- **Impact: 4/5**

  Justification: Could result in escalated attacks, data breaches, or operational sabotage.
- **Likelihood: 2/5**

  Justification: Requires both access to the gateway and weaknesses in the surface network defences.
- **Risk Score: 8/25**

Risk 6: ***Loss or Faliure of Devices (Accidental or Environmental)***

- **Description:** Relays or tags may be lost, damaged, or fail due to harsh underground environmental conditions (e.g., dust, moisture, impact).
- **Impact: 3/5**

  Justification: Device loss may reduce coverage or create data blind spots, affecting response effectiveness.
- **Likelihood: 4/5**

  Justification: The underground setting is harsh and devices are portable, so failure or loss is likely over time.
- **Risk Score: 12/25**

Risk 7: ***Insider Threats or Malicious Actors***

- **Description:** Personnel with legitimate access might act maliciously, disabling, reprogramming, or misusing devices.
- **Impact: 4/5**

  Justification: Insiders can bypass some physical and procedural controls, potentially causing significant disruption.
- **Likelihood: 2/5**

  Justification: While possible, the likelihood is lower due to trust and oversight, but cannot be ignored.
- **Risk Score: 8/25**

Risk 8: ***Privacy Breach of Personnel Location Data***

- **Description:** Unauthorised parties could access location data, leading to privacy violations.
- **Impact: 3/5**

  Justification: Could expose sensitive movement patterns or personal information.
- **Likelihood: 3/5**

  Justification: Unencrypted transmissions are susceptible, but only valuable in specific attack scenarios.
- **Risk Score: 9/25**

C. Risk Ranking Table

Risk	Impact	Likelihood	Risk Score	Rank
Data Interception/Tampering	5	4	20	1
Physical Compromise of Relays/Tags	4	3	12	2
Device Loss/Failure (Accidental/Environment)	3	4	12	2
Compromise of Gateway/Headend	5	2	10	3
Denial of Service (DoS)	3	3	9	4
Privacy Breach of Personnel Location Data	3	3	9	4
Unauthorised Surface Networks Access via Gateway	4	2	8	5
Insider Threats	4	2	8	5

Figure 1. Risk Analysis Ranking Table.

(Note: Ties in score are given equal rank; prioritisation may depend further on context.)

D. Assumptions

- Physical access to underground devices is possible during emergencies or due to supervision gaps.
- Attackers may include external adversaries, disgruntled staff, or insiders.
- The gateway/headend is assumed to be in a relatively secure area.
- The LoRa network is not IP-based, lacks LoRaWAN security features, and devices are deployed rapidly with minimal configuration.
- Underground environmental hazards (moisture, dust, impact) increase the risk of device loss or failure.

III. Policy Formulation

Based on the previous risk analysis, the following security policies are proposed to mitigate the highest-priority risks associated with the deployment of a LoRa-based linear sensor network in underground mining operations.

Policy 1: ***Ensure Confidentiality and Integrity of Data Transmission***

Policy Statement: All data transmitted between tags, relays, and the headend must be encrypted and authenticated to prevent unauthorised interception, tempering, or spoofing of messages.

Risks Assessed:

- Unauthorised interception or tampering of data.
- Privacy breach of personnel location data.

Policy 2: ***Protect Physical Security of Network Devices***

Policy Statement: Physical access to all tags, relays, and headend devices must be restricted, monitored, and protected against tampering, unauthorised removal, or destruction. All devices must include tamper-evident features.

Risks Assessed:

- Physical compromise or tampering with relay/tags.
- Device loss or failure (accidental/environmental).
- Insider threats.

Policy 3: ***Enforce Secure Gateway Operations***

Policy Statement: The gateway (headend) connecting the underground network to the surface infrastructure must enforce strict access controls, logging, and network segmentation to prevent unauthorised access and lateral movement into the surface network.

Risks Assessed:

- Compromise of gateway/headend.
- Unauthorised surface network access via gateway.

Policy 4: ***Maintain Network Availability and Resilience***

Policy Statement: Appropriate anti-jamming, redundancy, and failover measures must be implemented to minimise the impact of denial-of-service (DoS) attacks and device failures, to ensure continuous availability of emergency communications.

Risks Assessed:

- Denial of Service (DoS) attacks.
- Device loss or failure.

Policy 5: ***Protect Sensitive Information***

Policy Statement: Access to personnel location data must be limited to authorised users only, and all access must be logged. Data retention sharing must comply with applicable privacy regulations and company policy.

Risks Assessed:

- Privacy breach of personnel location data.

Policy 6: ***Investigate Potential Insider Threats***

Policy Statement: All personnel with access to network devices or sensitive data must undergo background checks, regular training, and must be subject to the principle of least privilege and robust auditing.

Risks Assessed:

- Insider Threats.

IV. Implementation of Security Programme

This section details the practical steps, processes, and controls required to implement each security policy for the LoRa-based linear sensor network in underground mining operations.

Policy 1: ***Ensure Confidentiality and Integrity of Data Transmission***

Technical Implementation:

- Integrate AES-128/256 encryption and message authorisation code (MAC) functionality into the firmware of all tags, relays, and headend devices.
- Use pre-shared cryptographic keys, securely provisioned before deployment. Keys must be rotated at scheduled intervals or upon suspected compromise.

- Device firmware should block unauthenticated messages and log suspicious communication attempts.

Manual Controls:

- Maintain a key management procedure, including secure key storage authorised key rotation, and emergency key revocation.
- Train technical staff to recognise signs of data tampering, such as repeated communication failures or verification errors.
- Regularly audit cryptographic settings and update firmware as needed for security patches.

Policy 2: ***Protect Physical Security of Network Devices***

Technical Implementation:

- Equip all devices (tags, relays, headend) with tamper-evident seals and casings.
- Attach RFID tags or barcodes to each device for asset tracking.
- Place relays in hard-to-reach or monitored locations to reduce the risk of physical tampering or theft.

Manual Controls:

- Conduct scheduled inspections and audits of device integrity and locations.
- Log all device deployments, movements, and retrievals in an asset management system.
- Establish a clear incident response plan for lost, missing, or tampered devices, including prompt investigation and device replacement.

Policy 3: ***Enforce Secure Gateway Operations***

Technical Implementation:

- Install firewalls and VLANs to segment the LoRa emergency network from other mine IT systems.
- Require multi-factor authentication (MFA) for all administrative access to the gateway/headend.
- Enable centralised logging for all access attempts and configuration changes, with automated alerts on suspicious activities.
- Physically secure the gateway in a locked, access-controlled room.

Manual Controls:

- Restrict physical and administrative access to the gateway to authorised personnel only.
- Review access and activity logs regularly, investigating anomalies.
- Document all changes to gateway configurations and maintain an up-to-date access roster.

Policy 4: ***Maintain Network Availability and Resilience***

Technical Implementation:

- Implement frequency hopping or channel switching on LoRa devices to reduce jamming risk.
- Install redundant relays and establish alternative communication paths, especially in critical areas of the mine.
- Equip all relays and tags with spare batteries or backup power supplies.
- Deploy network monitoring tools to continuously check device and link status.

Manual Controls:

- Perform regular functional testing of network paths, device status, and backup power.
- Maintain an inventory of spare relays, tags, and batteries for rapid replacement.
- Develop and rehearse emergency procedures for communication failures and DoS scenarios.

Policy 5: ***Protect Sensitive Information***

Technical Implementation:

- Enforce role-based access controls (RBAC) on all systems storing or displaying personnel location data.
- Enable automated logging and audit trails for all accesses, queries, and exports of sensitive data.
- Require user authentication on all monitoring stations and data terminals.

Manual Controls:

- Schedule periodic and data protection training to detect unauthorised use or data breaches.
- Provide privacy and data protection training to all staff with access to sensitive information.
- Establish and follow procedures for timely data deletion and for responding to potential privacy breaches in accordance with the laws and company policy.

Policy 6: ***Investigate Potential Insider Threats***

Technical Implementation:

- Deploy privileged access management (PAM) software to enforce least-privilege principles and monitor administrator actions.
- Enable automated audit logging and real-time monitoring for unusual or unauthorised activity.

Manual Controls:

- Conduct background checks for all personnel with system or data access responsibilities.
- Require regular completion of security awareness training and re-certification.
- Perform periodic reviews of user permissions and audit logs to ensure compliance and detect suspicious patterns.

V. SUMMRAY

This report outlined the main security risks and recommended policies for deploying a LoRa-based emergency sensor network in underground mines. Implementing these measures will help protect personnel, data, and operations during critical situations.

Key Recommendations:

- Encrypt and authenticate all network communications.
- Secure and track all physical devices with tamper-evident measures.
- Protect the gateway with strong access controls and monitoring.
- Build network resilience with redundancy and regular testing.
- Limit and log access to sensitive location data.
- Mitigate insider threats through training, auditing, and least-privilege access.

REFERENCES

[1] P. Branch, B. Li, and K. Zhao, "A LoRa-Based Linear Sensor Network for Location Data in Underground Mining," *Canvas Swinburne*, May 28, 2020. https://swinburne.instructure.com/courses/66714/files/37649206?module_item_id=4974335

[2] S. Dudek, "Low Powered and High Risk: Possible Attacks on LoRaWAN Devices," Trend Micro, Jan. 26, 2021. https://www.trendmicro.com/en_au/research/21/a/Low-Powered-but-High-Risk-Evaluating-Possible-Attacks-on-LoRaWAN-Devices.html

[3] A. Haque and A. Saifullah, "Handling Jamming Attacks in a LoRa Network." Available: https://saifullah.eng.wayne.edu/iotdi2024.pdf