Tackling the security concerns in a LoRa Relay-Based System for detonating explosives in underground mines: A Risk Analysis, Policy Formulation, and Implementation

1[a]Xuan Tuan Minh Nguyen
Dept. of Computer Science
Swinburne University of Technology
Hawthorn, VIC, Australia
103819212@student.swin.edu.au

I. Exclusive Summary

The report presents a comprehensive analysis of the LoRa Relay Based System for Detonating Explosives in Underground Mines to determine the security risks associated with the assets using the Delphi method. From the analysis, it is determined that the based System for Detonating Explosives in Underground Mines is vulnerable to threats of unauthorized access, physical security threats and the threat of message manipulation. To eliminate these threats Rule-based Access Control Policy, Multi-Factor Authentication (MFA) and Massage Authentication Codes (MACs) Policy are recommended alongside a brief outline of the Implementation of the security programme.

II. Introduction

LoRa is a Low Power Wide Area Wireless Physical Layer Technology developed recently showing efficiency in the actuator and sensor network. LoRa is a low-cost and energy-efficient technology to transmit at impressive distances. The LoRa Technology is developed as a part of the LoRaWAN networking technology which mediates communications from the devices that are LoRa-enabled and forwards them onto the Internet using the MQTT Protocol.

From the findings of Branch and Cricenti (2020), it is determined that the LoRa wireless transmission has experienced significant issues of fading without line of sight. However, when there is a line of sight underground LoRa propagates considerable distances. In addition to the above poor communication between the initiator, explosive and detonator creates the threat of reliability and timely response to incidents.

III. Risk Analysis

A. *Key Assets*

The LoRa Relay Based System for Detonating Explosives in Underground Mines is associated with multiple elements that includes Relay, Initiator, Detonator, and Communication medium.

In the following section the key assets of the LoRa Relay Based System for Detonating Explosives in Underground Mines are discussed: -

Relay- In the LoRa Relay Based System for Detonating Explosives in Underground Mines the relay forwards the message from the transmitter to the destination.

Initiator- In the LoRa Relay Based System for Detonating Explosives an Initiator is an interface that permits the operators to ensure strong connection to the explosive and to repair the network when such connectivity is not there.

Detonator- In the LoRa Relay Based System for Detonating Explosives a Detonate Message is sent to instruct the nodes.

Communication medium- the message passing system of LoRa is the communication medium used in this system.

B. *Risk Analysis*

In the following section a comprehensive risk analysis is performed to determine the risks associated with the LoRa and other relevant systems using Delphi Technique:

Myself & Imaginary Expert	**Malicious Attacks and Unauthorised access to the Nodes of LoRa**	**The threat of message manipulation**	**Breaching the physical vulnerability of the nodes**
Myself	4 * 3 * 12 = 144	3 * 3 * 9 = 81	4 * 3 * 12 = 144
Imaginary Expert 1	5 * 4 * 20 = 400	5 * 4 * 20 = 200	3 * 3 * 9 = 81
Imaginary Expert 2	3 * 3 * 9 = 81	4 * 3 * 12 = 144	5 * 4 * 20 = 400
Imaginary Expert 3	5 * 4 * 20 = 400	5 * 4 * 20 = 400	4 * 3 * 12 = 144
Imaginary Expert 4	4 * 3 * 12 = 144	3 * 3 * 9 = 81	4 * 3 * 12 = 144
Average	233.8	221.2	182.6

Table 1: Delphi Risk Analysis Table

C. *Risk Matrix*

Probability ratings	**Probability scale values**	**Ranking index values**				
Almost Certain	**5**	**Medium 5**	**Medium 10**	**Extreme 15**	**Extreme 20**	**Extreme 25**

Likely	4	Low 4	Medium 8	Medium 12	Extreme 16	Extreme 20
Possible	3	Low 3	Medium 6	Medium 9	Extreme 12	Extreme 15
Unlikely	2	Low 2	Low 4	Medium 6	Medium 8	Extreme 10
Rare	1	Low 1	Low 2	Low 3	Medium 4	Medium 5

Impact scale values	1	2	3	4	5
Impact ratings	Insignificant	Minor	Medium	Major	Severe

From the risk analysis using the Delphi Technique, it is found that the risk of malicious attacks and unauthorised access to the Nodes of LoRa has been determined as the high priority risk that needs to be mitigated with appropriate policy and mitigation strategy.

In addition to the above, the threat of manipulating the message can have a negative impact on the accuracy and effectiveness of the LoRa Relay Based System for Detonating Explosives in Underground Mines [1]. Lastly, the threat of physical vulnerability breach can increase a negative impact on the LoRa Relay Based System for Detonating Explosives in Underground Mines resulting inefficiency of the system.

IV. Policy Formulation

In order to eliminate the threat of the risks discussed above in the following section the best-suited policies are provided with policy statements:

A. Context-Based Access Control Policy

The Context-Based Access Control Policy is suggested for the multi-layered critical systems to ensure security threats are there. Within the dynamic infrastructure of the LoRa, there is a chance that the threat of unauthorised access to the nodes of the system may significantly impact the performance accuracy of the system operations. Furthermore, it can be stated that the application of a Context-Based Access Control Policy has the potential to restrict unauthorised access to the LoRa system to eliminate the chance of system inefficiency.

The key purpose of the Context-Based Access Control Policy is to bring an adaptive and dynamic approach to offer advanced security within the modern infrastructure [2]. Hence, it can be stated that within the system and nodes of LoRa, the use of a Rule-based Access Control Policy has the potential to protect the system from unauthorised access as the Rule-based Access Control Policy will only allow the authorized person to get access to the nodes and operations.

When using the Rule-based Access Control Policy the personnel will be able to access the system and nodes using the unique key identifiers and passwords so that the system can verify the identity of the system [3].

B. Multi-Factor Authentication (MFA) and Massage Authentication Codes (MACs)

In order to prevent the threat of messaging systems and message manipulation it is recommended to implement the authentication policy. From the analysis, it is determined that in the LoRa system, there is a threat that the messaging system to instruct the Relay Based System for Detonating Explosives in Underground Mines can be manipulated by the intruders having a significant negative impact on the accuracy and efficiency of the LoRa System [4]. Furthermore, it can be stated that the use of Multi-Factor Authentication (MFA) and Massage Authentication Codes (MACs) has the potential to ensure end-to-end protection of the LoRa Network.

Using the Multi-Factor Authentication (MFA) Policy for the Network of LoRa has the potential to offer comprehensive guidance to the users and operators of a system to reduce the threat of potential security exposures that can result from unauthorised access [5]. In addition, to the above the use of Massage Authentication Codes (MACs) Policy has the potential to eliminate the threat of message manipulation and ensure authentication of origin and the nature of the message. Hence, it can be stated that these two policies have the potential to eliminate the threat of messaging systems and message manipulation by preventing the system from receiving wrong instructions from the nodes.

C. Implementation of strong password-protected multi-factor authentication for physical security

To ensure the elimination of the threat of breaching the physical vulnerability of the nodes the use of strong password-protected multi-factor authentical can be helpful. A strong password-protected multi-factor authentication policy has the potential to protect the system from unauthorized physical access to the hardware elements of the network [5].

V. Implementation of Security Programme

A. Implementation of Rule-Based Access Control Policy

- Conduct Brainstorming and Gap Analysis.
- Identify the roles and assign the responsibilities to for appropriate execution of the policy.
- Train and Educate the staffs about the importance of Rule-Based Access Control Policy.
- Wireless Access Control Technology and Near Field Communication (NFC) Access Control Technology needs to be implemented to ensure effective Access Control [6].

B. Implementation of Multi-Factor Authentication (MFA) and Massage Authentication Codes (MACs) Policy

- Conduct Brainstorming and Gap Analysis.
- Identify the roles and assign the responsibilities to for appropriate execution of the policy.
- Train and Educate the staffs about the importance of Implementation of Multi-Factor

Authentication (MFA) and Massage Authentication Codes (MACs) Policy [6].
- Biometric Access Control Technology and Smart Card Access Control Technology is needed to implement the MFA.
- The use of HMAC and Cipher-Based Method Authentication Code (CMAC) is needed to implement the MACs [6].

C. Implementation of Physical Security
- Conduct Brainstorming and Gap Analysis.
- Identify the roles and assign the responsibilities to for appropriate execution of the policy.
- Train and Educate the staffs about the importance of Physical security system [7].
- Biometric Access Control Technology and Smart Card Access Control Technology is needed to implement the Physical Security [8].

VI. SUMMARY INCLUDING RECOMMENDATION

After completion of the above discussion it can be summarized that LoRa is a low-cost and energy-efficient technology to transmit at impressive distances as the Relay Based System for Detonating Explosives in Underground Mines.

- In this Relay Based System there are three key nodes that plays a significant role for effective execution of the system.
- The Relay Based System for Detonating Explosives in Underground Mines is vulnerable to threats of unauthorized access, physical security threat and the threat of message manipulation.
- The implementation of Rule-based Access Control Policy has the potential to prevent unauthorized access.
- The implementation of Multi-Factor Authentication (MFA) and Massage Authentication Codes (MACs) Policy has the potential to prevent the threat of message manipulation.
- The implementation of Biometric Access Control Technology and Smart Card Access Control Technology has the potential to prevent the system from physical security threat.

References

[1] P. Branch, and T. Cricenti, 2020, February. A LoRa relay based system for detonating explosives in underground mines. In 2020 IEEE International Conference on Industrial Technology (ICIT) (pp. 259-264). IEEE.

[2] F. Sifou, F. AlShahwan, A. Hammoud, M. Marwan and A. Hammouch, 2020. Implementing Policy Rules in Attributes Based Access Control with XACML within Cloud-Enabled IoT Environment. J. Commun., 15(1), pp.107-112.

[3] N. Boltz, M. Walter and R. Heinrich, 2020, August. Context-based confidentiality analysis for industrial iot. In 2020 46th Euromicro conference on software engineering and advanced applications (SEAA) (pp. 589-596). IEEE.

[4] Y.M. Abualkas, and D.L. Bhaskari, 2023, November. Secure Authentication and Authorization with MAC Address and Cryptography-Based Multi-Factor Algorithm. In 2023 Second International Conference on Informatics (ICI) (pp. 1-5). IEEE.

[5] F. Ramadhani, U. Ramadhani and L. Basit 2020. Combination of hybrid cryptography in one time pad (otp) algorithm and keyed-hash message authentication code (hmac) in securing the whatsapp communication application. Journal of Computer Science, Information Technology and Telecommunication Engineering, 1(1), pp.31-36.

[6] C.H. Liao, 2022. Message Authentication Codes On Ultra-Low SWaP Devices (Doctoral dissertation, Virginia Tech).

[7] O.A. Ayomide, S. Olayiwola Dare, M.Y. Olumoye, I.O. Emeka, F.K.S. Abiodun, J. Agboke Adeola and U.N. Virginus, 2021. Optimization Of An Identity Access control System Using Biometric Techniques. Int. J. Progress. Sci. Technol.(IJPSAT, 27(2), pp.647-653.

[8] B.B. Gupta and M. Quamara 2020. Attribute-based access control and authentication mechanism using smart cards for cloud-based IoT applications. International Journal of Embedded Systems, 13(1), pp.40-49.