TNE30009

Case Study

1. Introduction

In this case study you are to provide recommendations for securing the blasting system described in the attached paper.

The paper describes a prototype system for detonation of explosives used for hard-rock underground mining.

The process of obtaining approval for using electronic systems underground is slow and complex. An important part of that process is ensuring they are secure from intentional or accidental failure.

You are to consider how the product is to be secured and how it can be deployed in a secure manner. In particular you are to make recommendations as to what additional security features should be included in the product and how a mining company can deploy it in a secure manner.

The paper says the product currently has a PIN and streaming cipher as its only security features. This is probably inadequate.

Usually blasting systems are deployed as stand-alone systems. However there is interest in connecting the system to the underground WiFi network and initiating blasts from the surface. You are to consider security risks associated with both scenarios.

It is important to understand that the system described is not IP based. That may well have consequences for your recommendations.

2. Project requirements

You are required to:

1. Identify the key assets at risk from deployment of the system and the associated major security risks. You must identify and rank at least three risks. You must use the Delphi method discussed in class to rank the risks.
2. Write security policies that address the risks identified in the risk analysis.
3. Specify how each policy will be implemented. Explain what technologies and procedures will be deployed and how they will be used. Briefly outline the capabilities of the technologies to be implemented.

In preparing your report you will need to make a number of assumptions regarding the implementation. You are welcome to check your assumptions with the convenor. When you prepare your work you will need to document your assumptions.

3. Report

You must write the report using the standard IEEE conference template linked to on Canvas. Sections are to be numbered. Diagrams are to be labelled. Any references used are to be listed in a Reference section.

The report is to be no more than 2500 words excluding references. Below is the rubric for assessment. The report will be graded as Pass, Credit, Distinction, High Distinction or Not passed. Marking criteria are listed below. Referencing is to be IEEE.

The report is to have the following sections:

TNE30009

Case Study

1. Title including author name and email.
2. Executive summary.

   A short summary of the report including recommendations.
3. Introduction.

   Overview of the system and security issues it and similar systems face.
4. Risk analysis.

   Identify key assets in the system or affected by the system. Identify and rank the security risks associated with the assets using the method discussed in class.
5. Policy Formulation

   This is to consist of policy statements that address the risks identified in the previous section. At least three risks are to be addressed.
6. Implementation of security programme.

   Specify how each policy will be implemented. Specify what technologies are to be used and where and how they will be deployed. Outline any manual controls to be adopted.
7. Summary including recommendations.

   This will consist of a short bullet point list of recommendations.
8. References

   You must use IEEE.

In the above sections you MUST DOCUMENT ANY ASSUMPTIONS YOU MAKE.

4. Assessment

Assessment will be based on how thoroughly and clearly the risk analysis, the security programme and the implementation are described. The following rubric will be used:

	Pass	Credit	Distinction	High Distinction
Format (10%)	• The submitted report is formatted using the IEEE Conference template • Any figures/tables are appropriately labelled • The submitted report is in PDF format	Pass requirements plus • Paper includes at least two properly labelled figures and tables		Credit requirements plus • Formatting is clean with no words/tables wrapping beyond the edge of a column/page

TNE30009

Case Study

Structure (20%)	• The submitted report is properly structured with Executive Summary, Introduction, Risk Analysis, Policy Formulation, Implementation Outline and Summary • The report covers the main topics but some sections are lacking detail • A reference list is provided	Pass requirements plus: • Clear use of sub-sections as required to clearly delineate different aspects of the topic • The reference list is professionally structured and complete	Credit requirements plus: • All sections have a sufficient level of detail	Distinction requirements plus: • Suitable references have been located and used for all claims made in the paper
Analysis (50%)	• Risks have been identified based on assets of the system or assets related to the system. • The risks have been ranked. • Policies to address the risks have been formulated. • Technologies suitable for implementing the policies have been identified.	All Pass requirements plus: • The ranking of the risks has been justified. • An outline of how the policies address the risks is included. • How the technologies implement the policies has been explained.	All Credit requirements plus: • A discussion of the risk environment with a justification of the choice of risks and risk rankings is included. • Clear evidence is presented that all risks are addressed by the policies and an explanation of how they do so is included. • An evaluation of different technologies that can implement the policies is included.	All Distinction requirements plus: • An in-depth evaluation of the risk environment with citing of relevant literature justifying the choice of risks and risk rankings is included. • A thorough explanation of how the policies address the risks is included. • A detailed discussion of the relative strengths and weaknesses of different technologies that can be used to implement the policies with citing of relevant literature and a recommendation of appropriate technologies is included.
Language (20%)	• Basic language and grammatical skills	Pass requirements plus: • Good grammatical structure and flow of argument	Credit requirements plus: • A document suitable for reading by a professional audience	Distinction requirements plus: • An excellent report suitable for reading by an academic audience

A LoRa Relay Based System for Detonating Explosives in Underground Mines

Philip Branch*, Tony Cricenti†
Faculty of Science, Engineering and Technology
Swinburne University of Technology
Melbourne, Australia
*pbranch@swin.edu.au, †tcricenti@swin.edu.au

***Abstract*—In this paper we present our work on the use of LoRa as a network technology for detonation of low explosives in underground mining. Using explosives underground is a potentially hazardous activity that mining companies are keen to make safer by removing personnel from near the site of the detonation. Currently detonation is commonly carried out using lengths of copper cable or infrared transmission, both of which limit the distance between the initiator and the explosives. The wireless technology LoRa, is an attractive alternative. LoRa has a much longer transmission range than infrared transmission and other wireless technologies such as WiFi and ZigBee. We have developed and trialed in a working underground mine a prototype system for carrying out such detonations. The system makes use of LoRa as a multi-hop message passing system from an Initiator to a Detonator via a number of Relays. We describe the messages that are passed through the network. We also describe how we deal with contention, broadcast storms and duplicate messages. Our approach is robust, easy to deploy and gives deterministic delay. We also present measurements of signal strength taken underground. Our results indicates that underground LoRa wireless transmission suffers severe fading without line of sight but where this is a line of sight underground, we show that LoRa propagates considerable distances.**

***Index Terms*—LoRa, Industrial Internet**

I. Introduction

LoRa (from "Long Range") is a recently developed Low Power Wide Area wireless physical layer technology that is proving very popular in sensor and actuator networks [1]. LoRa operates in unlicensed bands, is easily installed, is low-cost, energy efficient and is able to transmit impressive distances. Distances of several kilometers in the open can be obtained with simple monopole antennae while ten or more kilometers have been reported with directional antennae.

LoRa is not a high bit rate technology but is ideal for sensor and actuator networks where bit rates are low. LoRa is a spread spectrum technology with a range of spreading factors that enables a trade-off between bit rate and distance. Bit rates of LoRa range from as low as 300 bps up to 50 kbps. The greater the spread, the further the distance the signal can propagate but at a lower bit rate [1].

LoRa is usually deployed as part of a networking technology called LoRaWAN [1]. In LoRaWAN a gateway mediates communications from LoRa enabled devices and forwards them on to the Internet using a protocol such as MQTT [2]. LoRaWAN networks are usually constructed as a star network or a star of stars with LoRa devices talking only to the LoRaWAN gateway.

However, LoRa has also attracted interest as a point to point or mesh technology where communication is between LoRa enabled end devices without using LoRaWAN [3]. We have adapted this approach in the work described in this paper.

Our interest in LoRa in an industrial setting has come about through our work with the mining industry. We have developed a proof-of-concept system that uses LoRa a link technology for a multi-hop network for the detonation of low explosives. Low explosives are more commonly used underground than high explosives [4]. Their purpose is to open up an ore body for extraction and to break up large boulders so that they are a suitable size for feeding into a crusher. Currently such explosives are usually detonated using a current transmitted over copper cable or via an actuator co-located with the explosives triggered using an infrared link. Both of these approaches limit the distance between the explosive and the person initiating the detonation. In the mining industry where safety is paramount, there is considerable interest in being able to increase this distance substantially so that detonation can be carried out well away from the detonation and also away from areas subject to air inrush caused by the explosion. We have developed a prototype that uses LoRa to transmit a detonation signal from a remote operator, to an actuator co-located with the explosives.

A limitation of LoRa in an underground mine is that despite the considerable distance it can transmit where there is a line of sight, when there is no line of sight, LoRa suffers substantial signal loss. In underground mining this occurs often. As shown in Fig. 1 underground mines are constructed as a hierarchy of access tunnels, extraction tunnels and extraction zones. Extraction tunnels branch off access tunnels. Extraction zones are small galleries that branch off extraction tunnels. Extraction tunnels are separated from access tunnels by large steel doors. In our experiments we found that although LoRa is able to successfully transmit the full length of a typical extraction tunnel of up to 190 metres or more, the signal rapidly declines once line of sight is lost. Consequently, in order to use LoRa in underground mining it is necessary to forward a message from the initiator to the recipient via one or more relays while maintaining line of sight between individual

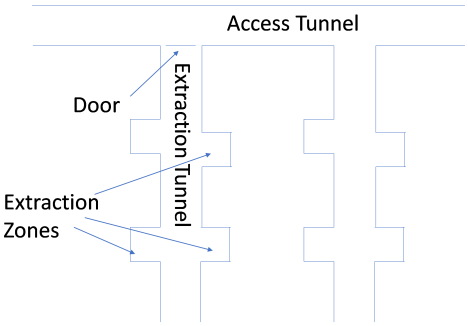

Fig. 1. Tunnel Structure

relays.

In a relay network, relays do not initiate communications. They forward messages from a transmitter to a destination. A relay network can be based on broadcast or unicast communication. With broadcast, relays that are within range receive the message and forward it. With unicast messages are addressed to a neighbouring node. Only the node to which the message is addressed processes the message. Other nodes ignore it.

The system needs to manage contention and provide reliable delivery in a severe fading environment on resource constrained devices. To meet these challenges we have developed a novel approach to Medium Access Control that avoids collisions, is simple to deploy, robust and provides predictable delay.

We make a number of contributions in this paper. First is the design of a LoRa based system for controlling underground detonations. Second is a design of a robust, low complexity LoRa relay. Third are underground measurements of LoRa signal propagation.

The remainder of the paper is structured as follows. Section II provides a brief overview of related work. Section III describes the messages that are exchanged across the network to control and carry out the detonation. Section IV discusses the design constraints in implementing this system. Section V discusses the relay algorithm, hardware and software. Section VI describes the results of system testing. In particular we present measurements of signal strength against distance in an extraction tunnel. Finally in Section VII we summarise the paper and discuss future work.

II. Related work

Related work falls into the following categories: the role of wireless communications in underground mining, radio signal propagation underground, the use of LoRa as a relay technology, and contention management in wireless networks.

In recent years the broad area of wireless communications in underground mining has attracted quite a lot of interest [2], [5], [6], [7]. The need to know where equipment and personnel are located and the ability to control potentially dangerous industrial processes at a distance means wireless communications is an increasingly important part of mining infrastructure. However, balanced against this is the extreme environment of underground mining. An underground mine is a dynamic environment with new tunnels being created, old ones subsided and with mining equipment regularly being moved. Wireless components need to operate in a physical environment which is often hot, humid and dusty. Equipment needs to be reliable, easy to install, use, move and remove.

Underground mines may well be serviced by a substantial wired network. Access tunnels are typically very long lived and contain much infrastructure such as power, lighting and monitoring. Communications are often based on IEEE 802.11 Access Points connected by Ethernet [8]. Occasionally, LTE infrastructure is deployed in underground mines [9].

There has been considerable research on underground radio signal propagation, notably by Zhou et al. where they carried out an extensive series of measurements at frequencies ranging from 455 MHz to 5800 MHz [7]. They examined the effect on propagation of polarization and antennae position in mines and tunnels of different types, dimensions and shapes. They found an extraordinary diversity in attenuation ranging from as high as 107.79 dB to as low as 1.49 dB per hundred meters. Interestingly, lower frequencies were attenuated more severely than higher frequencies, which was most likely related to the dimensions of the tunnel. Conversely Hakem et al. looked at frequencies of 2.4, 5.8 and 60 GHz and found that path loss increased as frequency increased [2]. Measurements of LoRa propagation in tunnels are rare. Abrardo and Pozzebon found that attenuation in the underground aqueducts they were interested in was very severe [3]. As well as taking signal strength measurements they explored the use of LoRa as a multi-hop relay technology. Their main concern was energy use minimization. They developed an approach of synchronizing transmission times which they claimed reduced energy consumption by up to 50%.

The deployment of LoRa as a mesh or multi-hop network rather than the more common LoRaWAN star network has also attracted some attention. Lundell et al. developed a routing protocol based on the Hybrid Wireless Mesh Protocol (HWMP) and the Ad-hoc On Demand Distance Vector Routing (AoDV) [10]. Lee et al. developed a similar mesh network protocol to act as a concentrator for LoRaWAN [11]. Liao et al. proposed using LoRa in association with a novel contention control mechanism called ‘Concurrent Transmission’ [12].

Relay networks are a particular type of mesh network where the topology is long and thin. Its purpose is to provide connectivity over a considerable distance. As such they are a natural fit for networks in tunnels. The design of relay networks (sometimes referred to as linear Wireless Sensor Networks) has attracted some interest over the past few years, mostly related to maximizing battery life of the nodes through coordinated scheduling of listening and transmission. Chen et al. give a useful overview as well as proposing a novel scheduling algorithm [13].

The final topic related to our work is the issue of managing contention in wireless networks where two nodes wish to transmit at the same time. This topic has a very long

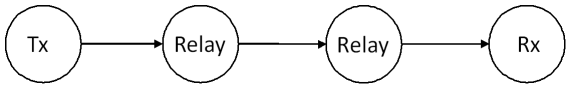

Fig. 2. Relay Network

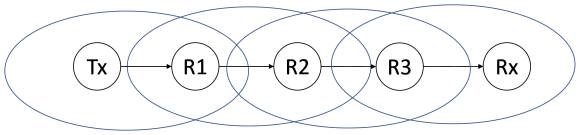

Fig. 3. Ideal Node Coverage in a Relay network

history [14]. The early Aloha wireless network made no attempt to prevent collisions but resolved contention through acknowledgments and timeouts. Since then WiFi, ZigBee and Bluetooth have all adopted strategies for dealing with contention. Some of the strategies include requesting and obtaining permission from the network to transmit through a Request to Send / Clear to Send (RTS/CTS) exchange. Others, such as Bluetooth take a centralized master / slave approach where a master node mediates which slave nodes can transmit.

Our work differs from much of that in the literature in that ours is an Actuator network rather than a Sensor network. In our system the typical concerns of sensor networks such as long battery life of months or longer are less important than reliable message delivery and deterministic delay.

III. System Overview

The system we have developed is a message passing system based on LoRa relays. The system is comprised of three node types. These are the Initiator, Relay and the Detonator. There is only one Initiator and one Detonator but there may be multiple Relays.

As well as initiating the detonation, the Initiator includes an interface that allows the operator to ensure there is connectivity to the explosive and to debug the network when such connectivity is not present.

We have defined a number of messages that are exchanged in preparing for and carrying out the detonation. All messages are numbered and contain a Time-To-Live (TTL) field. We discuss the significance of these fields in the next section.

Table I summarises the messages and their purpose. Trace Request and Response are used to debug the network. They provide the operator with information as to the number of hops between each relay and the Initiator. The Test Request and Response messages test connectivity from the Initiator to the Detonator. The Detonate Message is used to detonate the explosive. The Reset Message is sent to instruct all nodes to reset their record of the highest message value they have encountered to zero.

IV. Design Constraints

A relay used in the way described in this paper confronts some quite challenging design constraints. The relay needs to be simple to deploy, be small and compact, be lightweight in terms of resource requirements, have small predictable delay, and be reliable.

TABLE I
Message Types and Description

Message	Description
Trace Request	Message sent by initiator to relays and detonator for debugging network connectivity problems
Trace Response	Message sent by relay and detonator with node identifier and TTL value
Test Request	Message sent by initiator via relays to detonator to verify path to detonator configured correctly
Test Response	Message sent by detonator via relays to initiator to confirm that the detonator can receive messages
Detonate Request	Message sent by initiator via relays to detonator to request detonation
Detonate Failed	Message sent by detonator after initiating the explosion. If the detonator is still active then the explosion failed and this message is sent back to the Initiator
Reset	Message sent by any node that restarts. All nodes, upon receipt, set their "highest sequence number received" to zero

Simplicity of deployment is the most important requirement. The relays need to be placed in potentially awkward locations, in dim lighting, by people who most likely have little or no networking knowledge. Deployment needs to be fast and simple. Any delay in underground operations is expensive. Consequently, no configuration at the time of deployment is possible.

Traditional approaches to routing are unsuitable in this environment. The nodes have limited processing capabilities and memory in which to store routing tables. LoRa is a low capacity network so exchange of routing information as occurs in traditional networks is undesirable. Complex and potentially slow to converge protocols such as AoDV or Spanning Tree are unsuitable for this environment.

Reliability is also important. Algorithms such as Aloha where collisions are resolved by retransmission introduce variable delay and increase complexity. Detonations are often carried out as a cascading sequence of explosions where delay has to be predictable. Algorithms that introduce variable delay are unacceptable.

Given these constraints we made the design decision to base message propagation on broadcast rather than unicast. That is, a node will listen for a message and, subject to the few constraints described below, broadcast it.

This approach removes the need for complex routing protocols and makes deployment very simple. However, it creates additional problems. In particular broadcast storms can occur. To illustrate this, consider the network in Fig. 3.

R1 receives a message from Tx. It then broadcasts it. R2 sees the message and it too broadcasts it. Unfortunately, R1 sees the message again and broadcasts it again leading to an unending sequence of broadcasts. The solution is to make use of message sequence numbers and TTL.

Each relay keeps track of the highest message number it has seen and will not forward messages with message numbers less than or equal to this value. This prevents a

broadcast storm where two or more nodes continually receive and broadcast the same message. Unfortunately, the solution is not quite that simple. When a node restarts the value of the highest message it has seen will be lost. This will result in the node ignoring messages from the restarted node. To deal with this problem, when a node restarts it sends an Initialise message. Upon receipt of this message, each node resets its counter to zero and retransmits the message. But this again brings us back to the broadcast storm problem. To prevent that we make use of the TTL field. The TTL specifies the maximum number of times a message can be transmitted. It is initialised with this value (5 in our system) and is decremented by each relay when it retransmits it. Once the TTL reaches zero the message is dropped.

Sequential message numbering and TTL can address the problems of duplicates and broadcast storms but there is still the issue of contention. It is quite possible that coverage of one node will span more than just its immediate neighbours. Where nodes in a wireless network share the same spectrum with many other devices there needs to be some way of dealing with contention. That is, there needs to be a Medium Access Control (MAC) algorithm [14].

MAC algorithms attempt to deal with access to a shared medium. If more than one node wishes to transmit at the same time, then collisions may occur. In a wireless environment, collisions cannot be guaranteed to be detected because of the hidden terminal problem where two nodes beyond the range of each other transmit at the same time causing a collision at a third node. Consequently, in wireless networks the approach has usually been to deal with collisions through retransmits after a delay in receiving an acknowledgment (Aloha networks), or to avoid them occurring through Request To Send / Clear To Send (RTS/CTS) exchanges or through scheduling of transmissions. The MAC may be to simply transmit when it has a message (Aloha network for example) or may use Carrier Sensing (WiFi for example) where the node waits until the medium goes silent and then transmits. Depending on the algorithm there may be a delay before transmission and possibly multiple retransmissions.

The challenges of easy deployment, minimal configuration, hidden terminals, duplicates and broadcast storms are particularly problematic when dealing with devices that are resource constrained and are communicating over a low speed network.

Taking these factors into consideration has led us to a particular relay design which is described in the next section.

V. LoRa Relay Design

A. Overview

The approach we have adopted is based on distributed scheduling using different slot times. Transmission intervals are divided into slots, each of which is approximately equal to the maximum time it takes to transmit a message. Upon receipt of a message, each relay waits a specific number of slot times before transmitting. The number of slot times is different for each relay. In our approach there are no unicast transmissions, only broadcasts. Each relay, upon receipt of a message, waits its allotted number of slots before retransmitting. We discuss the algorithm, contention management and implementation in the following subsections.

B. Algorithm

The algorithm implemented by each node is as follows. Each relay goes through an initialization process, then goes into a loop where it listens to the medium and waits for a message. Upon receipt it then decides whether or not to transmit the message. If it does decide to transmit, it waits a predetermined number of slot times and then transmits it. The number of slot times to wait is different for each relay and is discussed in the next section.

Pseudocode for the algorithm is as follows:

```
begin
Initialise NumberOfSlots;
HighestMessageNumber := 0;
Transmit Initialise Message;
While true do
   wait(receive.message);
   if Message.TTL < 0 then
     drop message
   else
  begin
      Case message of
      "Initialise":
       Delay NumberOfSlots;
          HighestMessageNumber := 0;
          Broadcast Message;
      "Trace":
           Message.TTL := Message.TTL - 1;
           Message.relayNumber := relayNumber;
           Delay NumberOfSlots;
           Broadcast Message
       "Other":
       If Message.Sequence >
            HighestMessageNumber
          HighestMessageNumber =
              Message.SequenceNumber;
          Delay NumberOfSlots;
          Broadcast Message;
          end-if;
      end-case;
   end-while
end
```

C. contention

In a wireless network it is difficult to judge the exact coverage of each transmitter and receiver. Also, given the challenging environment of an underground mine environment it is impractical to carry out signal strength studies each time a detonation is to be done. Consequently, the relay must deal with situations where coverage of relays may overlap. This can give rise to some quite complex situations that cause collisions at the receiver.

To illustrate the nature of the problem consider Fig. 4.

In this network, coverage of the transmitter Tx includes both R1 and R2. Also, coverage of R1, R2 and R3 includes the receiver Rx. Even if the slot times are different for each relay, there are values of slot delays that will cause contention.

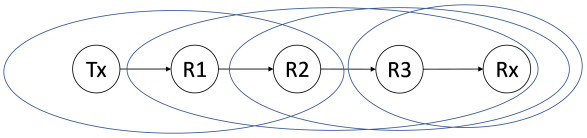

Fig. 4. Relay Network with Contention

For example, suppose R1 receives the message at time t = 0 and waits one slot time before transmitting. R2 also receives the message but waits 3 slot times before transmitting. R3 receives the message from R1 and waits 2 slot times before transmitting. Unfortunately, both R2 and R3 will transmit at time t = 3, causing a collision at Rx.

For robust transmission, slot times need to be chosen such that no arrangement of relays and slot times can cause any transmission times to coincide. This condition is met if each slot delay is not a sum of other slot delays. So for example, slot delays of 0, 1, 2 and 4 are acceptable, but 0, 1, 2 and 3 is not since relays could be arranged as described in the above example.

It is worth noting that in real deployments it is unlikely that more than three or four relays will be needed.

D. Implementation

We have implemented this system using the LoRa Modtronix inair4 which operate in the 415 MHz range and a microcontroller based on the ATmega328P. Programming was done using the Arduino IDE. The transceiver and microcontroller were connected using the SPI interface. The LoRa transceiver was controlled using the RadioHead Packet Radio libraries for embedded microprocessors [15].

We have implemented access security using a PIN. We have also implemented a simple stream cipher for encryption of messages.

VI. System Testing

A. Underground and Surface Testing

The system was tested underground in Newcrest's Cadia mine in New South Wales. In that test we used two relays. We also took measurements of signal strength which demonstrate that where there is line of sight a usable signal spans more than the full length of a 170 meter extraction tunnel, although without line of sight, signal strength decreases rapidly.

We have also successfully tested the system on the surface with three and four relays with various levels of overlap.

B. LoRa Signal Propagation Underground

As part of the investigation we took measurements of signal strength in an extraction tunnel with both line of sight and without line of sight. These are preliminary results and further research is needed. Nevertheless, they give some interesting insight into LoRa signal propagation in an underground mine.

Tunnels in an underground mine are arranged as a series of access tunnels off which extraction tunnels branch, usually perpendicularly. Perpendicular to extraction tunnels are

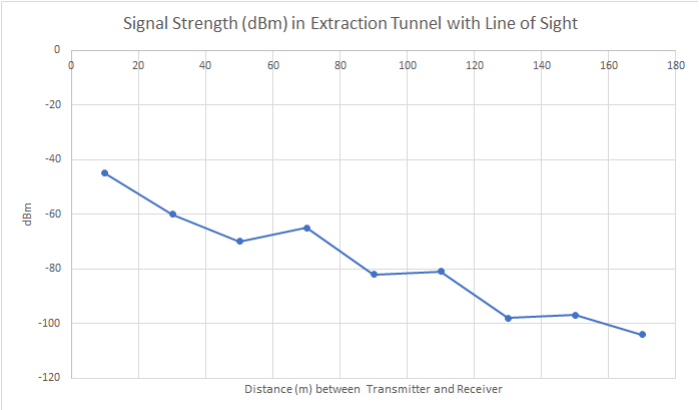

Fig. 5. Signal Strength with Line of Sight

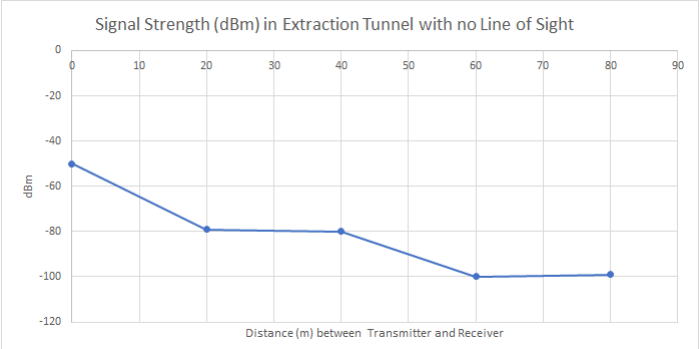

Fig. 6. Signal Strength with No Line of Sight

extraction zones. This is illustrated in Fig. 1. In the mine in which we tested our system in, the extraction tunnel was separated from the Access tunnel by a large steel door but with a large glass window.

We carried out signal strength measurements with line of sight for one hundred and seventy meters. We were able to obtain a usable signal for the full length of the tunnel even beyond the steel door. Underground mines are lined with steel mesh to reduce the risk of collapse. Steel mesh may have some waveguide properties. There was perhaps some indication of waveguide behaviour that we will explore in future research.

Even beyond the steel door we had a usable signal so long as we had line of sight (via the glass window in the door). However, once line of sight was lost signal strength declined rapidly.

Fig. 5 shows the signal strength as the distance between the transmitter and receiver was increased. The drop in signal strength at distance 120 meters of approximately 10 dB corresponds to the location of the steel door. We were able to obtain a usable signal beyond the steel door for the maximum tunnel length in which we could take measurements of approximately 170 meters.

Fig. 6 shows signal strength without a line of sight. In this case the transmitter was placed approximately five meters within the extraction chamber. In this case we lost a usable

signal after 80 meters.

Perhaps the most interesting result is the distance that the signal propagates with a line of sight. We were able to obtain a usable signal, even beyond a steel door, for the full length of the tunnel provided we had line of sight.

VII. Conclusion

In this paper we make a number of contributions. The first is that we describe a LoRa based system that can make a potentially dangerous industrial process simpler and safer than it currently is. The second is that we have developed a simple, robust approach to using LoRa as a link technology in a multi-hop relay network. The approach is robust, easy to deploy and gives deterministic delay. The third contribution is that we have presented some results on the propagation of LoRa in steel mesh lined underground tunnels. Underground tunnels are regarded as being severe fading environments and certainly our data shows that without line of sight LoRa signals decrease significantly over quite short distances. However, contrary to other research we demonstrate that in this particular instance where there is line of sight, the signal propagates considerable distances.

Although LoRa is usually deployed with LoRaWAN it has considerable potential as a relay technology. Exploring the design of LoRa as a relay technology is a topic of future research we intend to explore further. LoRa also has potential in other applications in underground mining which we also intend to investigate.

Acknowledgment

Support from Newcrest Mining Ltd in the preparation of this paper is gratefully acknowledged.

References

[1] LoRa Alliance, "What is the LoRaWAN specification?" vol. 2019, no. 1 April 2019. [Online]. Available: https://lora-alliance.org/about-lorawan

[2] N. H. G. D. Y. Coulibaly, "Radio-wave propagation into an underground mine environment at 2.4 ghz, 5.8 ghz and 60 ghz," in *The 8th European Conference on Antennas and Propagation (EuCAP 2014)*, Conference Proceedings.

[3] A. Abrardo and A. Pozzebon, "A multi-hop LoRa linear sensor network for the monitoring of underground environments: The case of the medieval aqueducts in siena, italy," *Sensors (Basel)*, vol. 19, no. 2, 2019. [Online]. Available: https://www.ncbi.nlm.nih.gov/pubmed/30669487

[4] Bradbury Science Museum, "What is a high explosive," vol. 2019, no. 02/04/2019, 2017. [Online]. Available: https://www.lanl.gov/museum/news/newsletter/2017/2017-04/high-explosives.php

[5] A. E. Forooshani, S. Bashir, D. G. Michelson, and S. Noghanian, "A survey of wireless communications and propagation modeling in underground mines," *IEEE Communications Surveys and Tutorials*, vol. 15, no. 4, pp. 1524–1545, 2013.

[6] H. Kunsei, K. S. Bialkowski, M. S. Alam, and A. M. Abbosh, "Improved communications in underground mines using reconfigurable antennas," *IEEE Transactions on Antennas and Propagation*, vol. 66, no. 12, 2018.

[7] C. Zhou, T. Plass, R. Jacksha, and J. A. Waynert, "RF propagation in mines and tunnels: Extensive measurements for vertically, horizontally, and cross-polarized signals in mines and tunnels," *IEEE Antennas and Propagation Magazine*, vol. 57, no. 4, pp. 88–102, 2015.

[8] S. Yarkan, S. Guzelgoz, H. Arslan, and R. R. Murphy, "Underground mine communications: A survey," *IEEE Communications Surveys and Tutorials*, vol. 11, no. 3, pp. 125–142, 2009.

[9] R. Zhohov, D. Minovski, P. Johansson, and K. Andersson, "Real-time performance evaluation of LTE for IIoT," in *IEEE 43rd Conference on Local Computer Networks (LCN)*, 2018, Conference Proceedings.

[10] D. Lundell, A. Hedberg, C. Nyberg, and E. Fitzgerald, "A routing protocol for LoRa mesh networks," in *2018 IEEE 19th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)*, Conference Proceedings, pp. 14–19.

[11] H. C. Lee and K. H. Ke, "Monitoring of large-area iot sensors using a LoRa wireless mesh network system: Design and evaluation," *IEEE Transactions on Instrumentation and Measurement*, vol. 67, no. 9, pp. 2177–2187, 2018.

[12] C.-H. Liao, G. Zhu, D. Kuwabara, M. Suzuki, and H. Morikawa, "Multi-hop LoRa networks enabled by concurrent transmission," *IEEE Access*, vol. 5, pp. 21 430–21 446, 2017.

[13] G. Z. Chen, Q. C. Meng, and L. Zhang, "Chain-type wireless sensor network node scheduling strategy," *Journal of Systems Engineering and Electronics*, vol. 25, no. 2, pp. 203–210, 2014.

[14] D. Zucchetto and A. Zanella, "Uncoordinated access schemes for the iot: Approaches, regulations, and performance," *IEEE Communications Magazine*, vol. 55, no. 9, pp. 48–54, 2017.

[15] M. McCauley, "Radiohead packet radio library for embedded microprocessors," vol. 2019, no. 02/04/2019. [Online]. Available: https://www.airspayce.com/mikem/arduino/RadioHead/index.html