Emergency Messaging Network Feasibility Study

PADRAIG X. LAMONT (22494652), BRANDON KE (22731448), and ANDREW TAN (22614179)

1 INTRODUCTION AND BACKGROUND

In an emergency, reliable communication forms the bedrock of effective emergency response efforts [3]. Yet, prevailing methods, namely cellular networks and internet-based communication, demonstrate a marked susceptibility to failure during extreme weather conditions [5]. This can critically impede communication, potentially putting lives at risk [3].

This paper proposes a feasible solution to this quandary: A peer-to-peer communication protocol leveraging Long Range (LoRa) technology that could operate independently of the cellular or internet networks. LoRa, a low-power, long-range wireless communication technology, offers a resilient and decentralised alternative to traditional communication systems, particularly in the face of weather-induced network disruptions [2]. The intent is to employ a flooding protocol, a dissemination strategy where each node rebroadcasts received messages, to ensure effective message delivery across the entire University of Western Australia (UWA) campus.

Our vision is that a network of LoRa-enabled communication devices strategically dispersed across the UWA campus could form an effective backup emergency communication system. The devices could maintain consistent battery charge from a mains power outlet, ensuring they can operate during power outages (another example of an emergency). In the following sections, we will detail the design and results of an experimental study investigating the viability of the use of LoRa and a flooding protocol for this proposed network.

2 GOALS

This project aims to assess the practicality of using LoRa technology in conjunction with a flooding protocol for establishing a reliable backup communication system on the UWA campus. Given the expansive coverage required for UWA and the multitude of buildings and devices that could introduce interference, achieving this goal poses significant challenges.

A crucial part of this study involves quantifying network reliability and understanding the extent of building interference. This will be achieved through two primary metrics: Packet Delivery Rate (PDR), the ratio of successfully delivered messages to the total number of messages sent, and Packet Corruption Rate (PCR), the percentage of messages that get distorted during transmission. Both metrics will be measured under a variety of node setups and LoRa parameters, providing an in-depth understanding of the network performance.

Our goal is to not only explore the characteristics of LoRa communication at UWA but also to identify an optimal set of LoRa parameters that would maximize PDR and minimize PCR. These parameter choices will also be analysed in the context of transmitting from a battery-operated device where lowering power consumption is important to enhancing network longevity during power outages. The insights from this study may have broader implications, potentially informing the design of other communication systems in similar campus environments, such as sensor networks.

3 TECHNICAL IMPLEMENTATION

The flooding protocol was implemented on TTGO boards and was built upon the Arduino LoRa project by Sandeep Mistry [4]. Our setup involves sender nodes that broadcast packets on a scheduled basis and log the packets as they are transmitted. At the same time, receiver nodes are designed to listen for incoming packets, log them, and then re-broadcast them if they are neither duplicates nor corrupted.

To ensure efficient network performance, our system identifies and discards duplicate packets using a tracking table of the most recent 256 packet IDs received by the node. Corrupted packets are also detected via a hash verification process which matches a packet's included hash with the hash of the packet content. If the hashes do not align, the packet is marked as corrupt and the receipt of the corrupt packet is logged.

The transmitted packets include a hash, followed by a packet header and then additional node info sections that record routing information. The packet header and the node info sections follow specific structures detailed in tables 1 and 2 respectively. The packet header contains metadata about the packet, and each node info section contains additional information about each hop the packet has taken through the network. For example, the header contains a packet ID to disambiguate itself, and the node info sections contain node IDs, timestamps, and GPS coordinates.

Communication ID	Packet ID	Source Node ID	Destination Node ID	Hop Count

Table 1. The fields contained in the packet header.

Node ID	Timestamp (ms)	Packet RSSI	RSSI	Packet SNR	GPS Latitude	GPS Longitude

Table 2. The fields contained in the packet node info sections.

4 EXPERIMENT

To validate the proposed protocol, we conducted extensive testing on the UWA campus using three LoRa nodes and 12 unique sets of LoRa parameters, resulting in 24 different testing configurations. The parameters, detailed in table 3, were selected based on preliminary testing which determined a baseline parameter set that could reliably transmit packets at a distance of 250 meters outdoors with minimal power consumption. This baseline is represented as parameter set "B" in table 3. Other parameter sets were then generated by altering a single parameter from the baseline set, enabling us to assess the impact of each LoRa parameter individually.

Each node was assigned a specific role: node 1 served as the source node, broadcasting messages at a minimum rate of one packet per second, and nodes 2 and 3 functioned as receiver nodes that listened to and forwarded messages. Two distinct setups, labelled 'Inside' and 'Outside', dictated whether node 2 was placed inside or outside the engineering building, as shown in figure 1. For both setups, node 1 was placed outside the Computer Science building, and node 3 was situated on the Reid Library balcony.

The node positions, illustrated in figure 1, were chosen as they displayed the most variance in performance between the highest and lowest power LoRa parameter sets. This was important for illustrating changes in performance as each LoRa parameter was changed.

We ensured the nodes remained static during the testing of different parameter sets and collected data for at least 50 transmitted packets for each test configuration. The tests were conducted within a three-hour period on the same day to control for any potential time-varying link quality effects.

LoRa Parameter Set ID	Transmit Power	Bandwidth	Spreading Factor	Coding Rate	Frequency
A	0	250 KHz	8	5	915 MHz
B	4	250 KHz	8	5	915 MHz
C	8	250 KHz	8	5	915 MHz
D	12	250 KHz	8	5	915 MHz
E	16	250 KHz	8	5	915 MHz
F	20	250 KHz	8	5	915 MHz
G	4	500 KHz	8	5	915 MHz
I	4	100 KHz	8	5	915 MHz
J	4	50 KHz	8	5	915 MHz
K	4	250 KHz	7	5	915 MHz
M	4	250 KHz	9	5	915 MHz
N	4	250 KHz	10	5	915 MHz

Table 3. The sets of LoRa parameters that were tested.

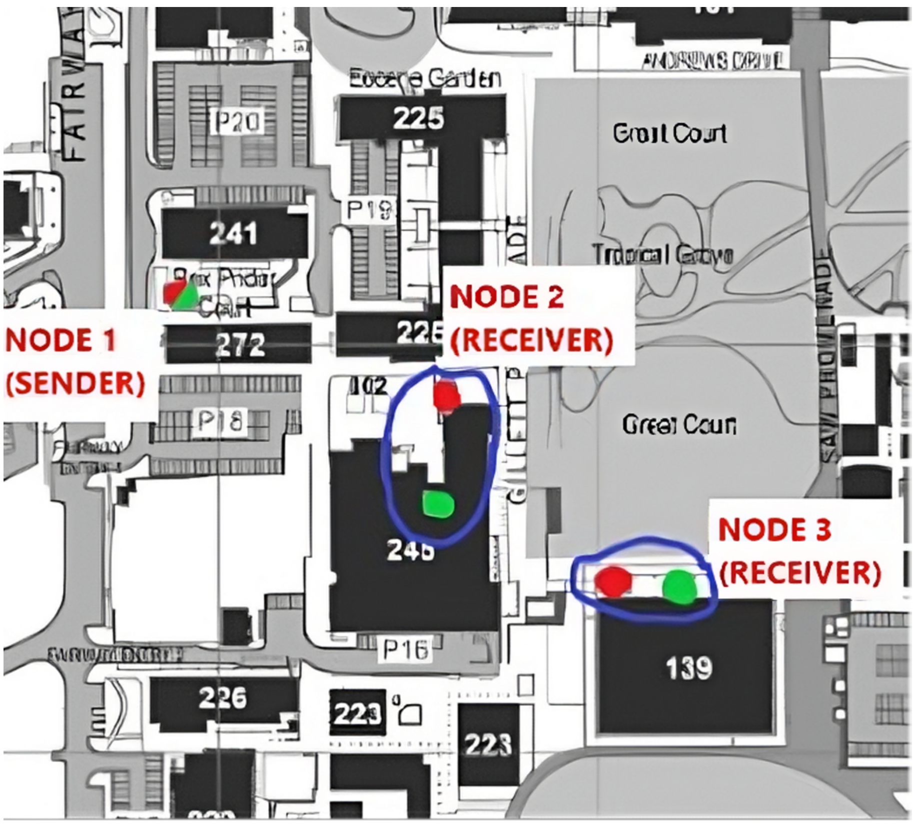

Fig. 1. The position of test nodes on the UWA campus. The green nodes represent node positions under the 'Inside' setup, while the red nodes represent node positions under the 'Outside' setup.

5 EXPERIMENTAL PROCEDURE

In this section, the procedure undertaken in our experiment is broken down into the following steps:

(1) Establish a connection between each TTGO board and a laptop. The laptop serves as a host for uploading the protocol code to the TTGO board and for collecting log data.
(2) Relocate each laptop and the corresponding TTGO board to their predetermined positions on the campus.
(3) Open the experiment.h file on each laptop. This file contains configuration details for the experiment.
(4) In the experiment.h file, uncomment the line corresponding to the desired LoRa parameter set. This action will apply the parameter set to the subsequent test.
(5) Update the COMM_ID value in the experiment.h file. This unique identifier represents the current setup of the nodes and the chosen LoRa parameter set.
(6) Upload the appropriate sender or receiver code to the TTGO board. The code, stored in .imo files, instructs the TTGO board to act as either a sender or receiver in the network.
(7) Initiate the serial monitor on each laptop to start logging the TTGO board's output.
(8) Repeat steps 2 to 7 for all combinations of node setups and LoRa parameter sets.

6 EXPERIMENTAL RESULTS

This section contains the outcomes of our experiment, and details how we calculated the metrics that are discussed. Our experiment was primarily designed to measure two primary metrics: Packet Delivery Rate (PDR) and Packet Corruption Rate (PCR). However, additional graphs were also generated to visualise how packets propagated through the network, and how long the packets took to transmit.

The PDR is the ratio of messages that were successfully delivered from node 1 to nodes 2 and 3. Conversely, the PCR is the ratio of packets received by nodes 2 or 3 that were found to be corrupt. Figures 2 and 3 show how PDR and PCR, respectively, varied with changes to each LoRa parameter. No data was received by any nodes with a bandwidth of 500 KHz for the 'Inside' node setup, and therefore, the PCR could not be calculated. The 'Inside' and 'Outside' node results are delineated in green and blue respectively, with solid and dashed lines portraying values measured at nodes 2 and 3.

Further, we explored the propagation pattern of messages across the network by tracking whether nodes 2 or 3 most commonly received packets directly from the source node (node 1), or whether they more commonly received re-broadcast packets. Whether node 2 or 3 received packets directly from the source node is shown for different testing configurations in figure 4.

The amount of time required to transmit each packet was also measured from our logs from the source node. This was possible as we delayed for a fixed amount of time between transmitting each packet. Therefore, the actual interval of time between each packet transmission was the sum of the fixed delay and the time spent transmitting the packet. So, by subtracting the fixed delay, we can calculate the time taken to transmit packets under different LoRa parameters, as is shown in figure 5.

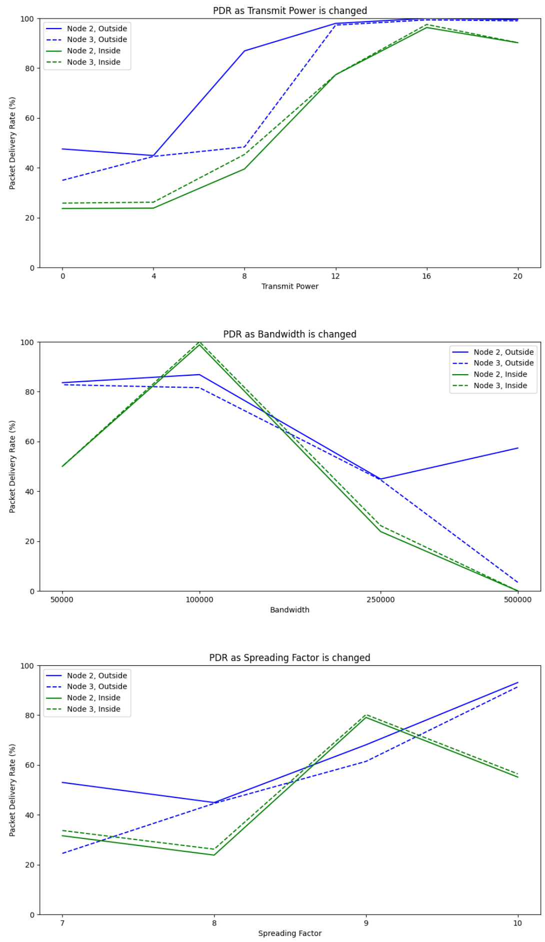

Fig. 2. Packet delivery rate as the following LoRa parameters are changed: Transmit Power (top), Bandwidth (middle), and Spreading Factor (bottom). The results are provided for the 'Inside' node setup in green and the 'Outside' node setup in blue.

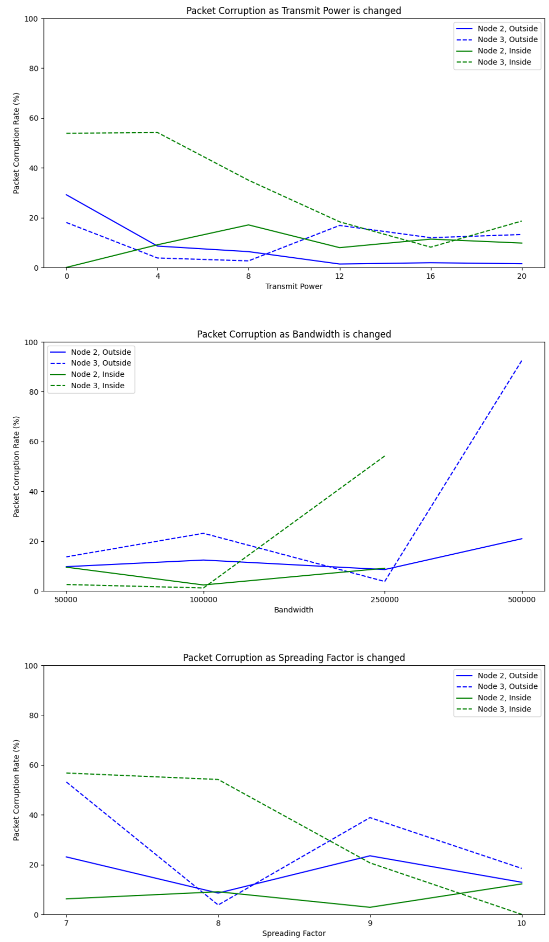

Fig. 3. Packet corruption rates as the following LoRa parameters are changed: Transmit Power (top), Bandwidth (middle), and Spreading Factor (bottom). The results are provided for the 'Inside' node setup in green and the 'Outside' node setup in blue.

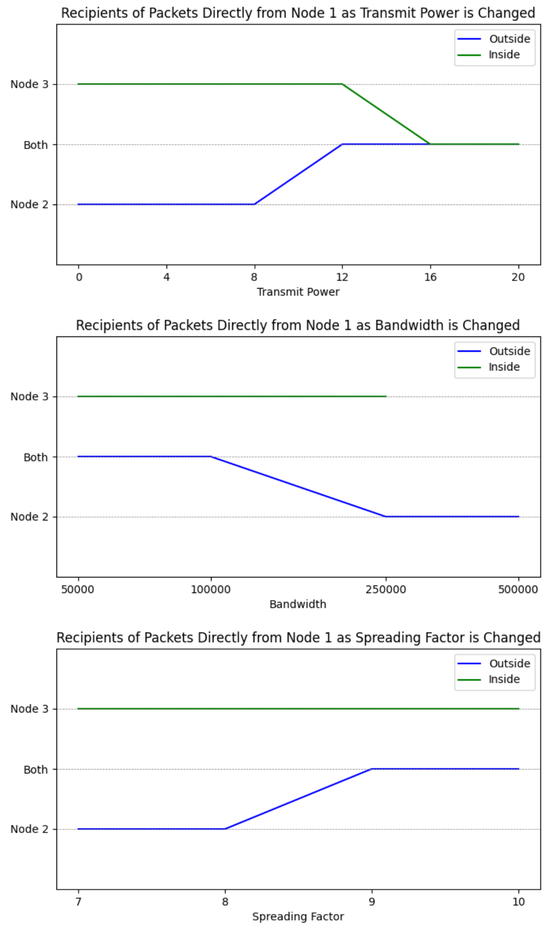

Fig. 4. The first recipient of packets from the source node as the following LoRa parameters are changed: Transmit Power (top), Bandwidth (middle), and Spreading Factor (bottom). The results are provided for the 'Inside' node setup in green and the 'Outside' node setup in blue.

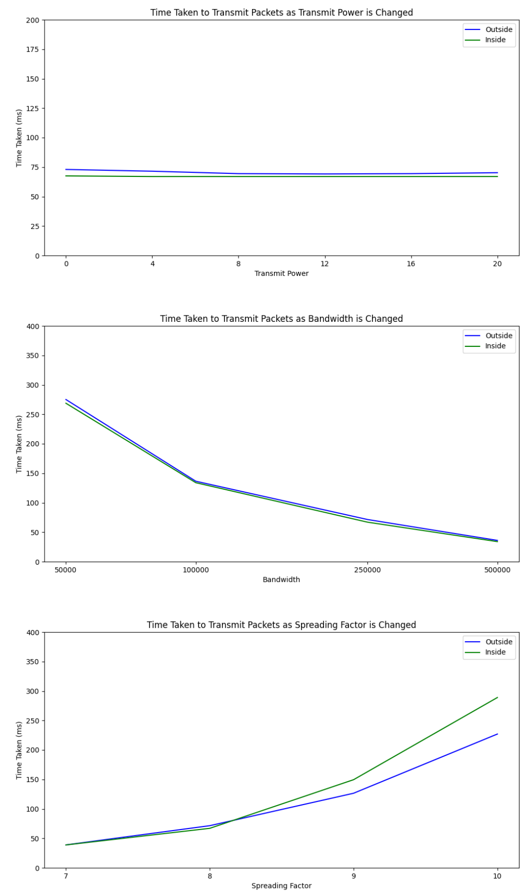

Fig. 5. The time required to transmit packets as the following LoRa parameters are changed: Transmit Power (top), Bandwidth (middle), and Spreading Factor (bottom). The results are provided for the 'Inside' node setup in green and the 'Outside' node setup in blue.

7 DISCUSSION

7.1 Impact of Transmit Power

Increasing the transmit power consistently improved network performance. Our experiment shows that both the packet delivery rate (PDR) and packet corruption rate (PCR) improve significantly as transmit power is increased, as seen in figures 2 and 3, respectively. However, a transmit power of 0 demonstrated similar results to a transmit power of 4, which we believe may be due to a physical minimum limit on the transmit power of TTGO boards.

There is also a noticeable shift in the nodes' routing behaviour as the transmit power is increased, as seen in figure 4. As transmit power increases, nodes are more likely to receive messages directly from the source node, which suggests that with lower transmit powers the nodes are more likely to receive re-broadcast messages. This demonstrates how the routing is able to improve the performance of the network in cases where the nodes can't receive all messages from the source node.

7.2 Impact of Bandwidth

Our results indicate a trend of decreasing performance as bandwidth is increased. This is consistent with expectations, as higher bandwidth leads to quicker message transmission, and therefore more significant signal attenuation, which can increase the susceptibility of packets to interference [1]. This trend is reflected in figures 3 and 2, which demonstrate an increased packet corruption rate (PCR) and decreased packet delivery rate (PDR), respectively, as bandwidth rises.

As anticipated, the time for packet transmission also reduces as bandwidth is increased, as shown in figure 5. This is caused by a decreased transmission time per byte in LoRa [2].

7.2.1 Anomaly in Packet Delivery Rate. Our findings for bandwidth also present an anomaly: a significant drop in PDR to 50% when the bandwidth is reduced to 50 KHz for the 'Inside' node setup. This was unexpected. Looking at our logs reveals a peculiar pattern: at a bandwidth of 50 KHz, nodes 2 and 3 consistently receive only every second message. We hypothesize that in this case, the time taken to receive and re-broadcast messages exceeded the one-second gap between the source node transmitting each message. This is reinforced as the transmit times shown in figure 5 reach their highest value at a bandwidth of 50 KHz. Therefore, this is not indicative of a decrease in link quality, but rather is an important illustration of potential issues that the network could experience when packets are transmitted too quickly.

7.3 Impact of Spreading Factor

The modifications made to the spreading factor appeared to have a smaller influence on the packet delivery rate (PDR) than the other tested LoRa parameters. Nevertheless, as the spreading factor increased, we recorded a rise in PDR and a decline in packet corruption rate (PCR), as shown in figures 2 and 3. These results align with the expected rise in signal-to-noise ratio with increasing spreading factor [2].

A significant increase in packet transmission time was also observed as the spreading factor was increased, as seen in figure 5. This shows a similar effect on the transmit times as decreasing bandwidth. We believe that this is the cause of the similar halving of PDR when the spreading factor reaches a value of 10, as was also observed for a bandwidth of 50 KHz. As explained for the 50 KHz bandwidth test, we believe that this halving is not due to a degradation in link quality, but rather due to packets being transmitted faster than they could be read and re-broadcast.

Intriguingly, a divergence in packet transmission times between the 'Inside' and 'Outside' node setups was observed at higher spreading factors, as seen in figure 5. It is unclear why the node setup would affect the source node's packet transmission, and this discrepancy invites further investigation to find its cause.

7.4 Impact of Building Interference

Our results for the 'Inside' and 'Outside' node setups demonstrate the significant influence that building interference has on LoRa packet transmission on the UWA campus. The packet delivery rate (PDR) was often lower for the 'Inside' node setup than the 'Outside' setup, as seen in figure 2. Although, we did observe that increases in the transmit power improved the PDR across both the 'Inside' and 'Outside' node setups, illustrating its potential to combat building interference.

Investigation into the effects of bandwidth and spreading factor also revealed more nuanced results. Lower bandwidths and higher spreading factors were associated with a higher PDR for the 'Inside' node setup than the 'Outside' setup. This result suggests that reducing bandwidth or increasing the spreading factor could both act as viable tactics for circumventing building interference.

Importantly, our results also emphasised the value of efficient routing protocols in addressing building interference, as node 2 was still able to receive re-broadcast packets from node 3 when it was not receiving packets directly from the source node. This finding demonstrates the value of routing and suggests that more advanced routing protocols could augment the resilience of the network even further in more complex setups.

8 RECOMMENDATIONS

Our analysis underscores the importance of LoRa parameter selection for deploying a robust messaging network on the UWA campus. Increased transmit power emerged as a prominent factor that substantially improved the PDR, without extending the transmission time. As such, we strongly advocate for a high level of transmit power. Notably, we did not observe significant diminishing returns with increased transmit power. This provides evidence that increasing transmit power is an efficient method for improving PDR. We believe that the increases to transmit power would also be more efficient for power consumption than alternatives such as packet re-transmissions.

Bandwidth was observed to significantly impact the PDR, particularly in the presence of building interference. Similarly, increasing the spreading factor also demonstrated improvements in PDR in the presence of building interference. However, these adjustments to both bandwidth and spreading factor lengthened the packet transmission time. While acceptable when message frequency is low, these increased transmission times could slow network routing as each node would require more time to forward each message. Moreover, increased transmission time necessitates additional power consumption, potentially reducing the lifespan of the battery-operated devices. In light of these considerations, we recommend adopting moderate bandwidth and spreading factor values. We believe that this approach could improve network resilience against building interference while maintaining lower transmission times.

The recommended LoRa parameters, distilled from our analysis, are outlined in table 4. These parameters provide a balance between packet delivery rate, transmission time, and power consumption, which are all necessary factors in creating a reliable and resilient emergency messaging network.

Transmit Power	Bandwidth	Spreading Factor	Coding Rate	Frequency
16	100 KHz	9	5	915 MHz

Table 4. The recommended set of LoRa parameters for use in an emergency messaging network on the UWA campus.

9 LIMITATIONS

Whilst we endeavoured to test with realistic settings, there were some variables that would differ for a real implementation of the proposed emergency messaging network:

- We only used 3 TTGO boards for testing, which is less than would be used in a real deployment.
- Whilst we chose an area that we believe was indicative of the larger UWA campus, we did only test in one area of the UWA campus, and only under two node setups.

- Our experiments did not cover every possible combination of LoRa parameters, and therefore it is possible that more optimal LoRa parameters could be found.
- The nodes were kept in the same location during testing of each node setup, and were not mobile. Therefore, our results are not representative of moving nodes.
- We were not able to measure the actual power usage of the nodes. Therefore, all inferences we made about the lifetime of the network used assumptions about the effect that each LoRa parameter has on power consumption.

10 SECURITY

Despite security and privacy implications of the proposed system being beyond this study's scope, their potential impact on the network merits consideration. Given the system would only be used in emergency situations, the amount of time during which the system may be exploited is limited, which could diminish potential motivation of bad actors to exploit the network. However, this doesn't negate the existence of possible vulnerabilities.

The system's design, rooted in an ad-hoc network that disseminates messages over a shared channel, could be prone to Denial of Service attacks. Opportunistic actors might exploit this open structure, launching flooding or jamming attacks to disrupt node communication. Further, malicious nodes could be introduced into the network, which could allow unauthorised packet sniffing, and could allow the transmission of forged packets. These potential security breaches underline the importance of integrating robust safeguards into the system, despite its infrequent usage.

11 CONCLUSION

This feasibility study extensively explored the practicality of utilizing LoRa technology, in conjunction with a flooding protocol, to establish a resilient emergency communication network on the University of Western Australia (UWA) campus. Our experimental study highlighted the critical role of LoRa parameter selection in fostering reliable, power-efficient, and effective communication in the face of potential challenges on the UWA campus such as building interference.

Increased transmit power emerged as an efficient strategy for enhancing the Packet Delivery Rate (PDR) without extending transmission time, while moderate adjustments to bandwidth and spreading factor significantly improved network resilience against building interference. Additionally, our findings underscored the importance of strategic routing protocols in circumventing building interference and boosting the resilience of the network.

However, it must be noted that all parameter modifications inevitably involve trade-offs, particularly concerning transmission time and power consumption. Hence, our recommendations lean towards striking a balance that optimizes performance while minimizing resource consumption, which we believe is crucial for maintaining the longevity of battery-operated devices.

While our research focused on the UWA campus, the insights gleaned may have broader implications. They may inform the design of similar communication systems in comparable environments, such as sensor networks on other university campuses.

In conclusion, the adoption of LoRa technology for emergency communication represents a promising strategy to supplement traditional systems, ensuring consistent communication during critical moments. But further investigations would be beneficial, exploring advanced routing protocols, conducting long-term performance assessments, and investigating the effects of node density and placement on network performance. The intersection of technology and emergency response communication, as demonstrated in this study, is a fertile area of research with the potential to make significant impacts on safety and disaster management.

The source code of this project is available on GitHub at https://github.com/Sothatsit/CITS4419-EmergencyNetwork.

REFERENCES

[1] Ari Asp, Yaroslav Sydorov, Mikko Valkama, and Jarno Niemelä. 2012. Radio signal propagation and attenuation measurements for modern residential buildings. In *2012 IEEE Globecom Workshops*. 580–584. https://doi.org/10.1109/GLOCOMW.2012.6477638

[2] Martin Bor, John Vidler, and Utz Roedig. 2016. LoRa for the Internet of Things. *EWSN* (02 2016), 361–366.

[3] Kimmo Laakso and Jari Palomäki. 2013. The importance of a common understanding in emergency management. *Technological Forecasting and Social Change* 80, 9 (2013), 1703–1713. https://doi.org/10.1016/j.techfore.2012.12.012 Planning and Foresight Methodologies in Emergency Preparedness and Management.

[4] Sandeep Mistry. 2023. Arduino LoRa. https://github.com/sandeepmistry/arduino-LoRa.

[5] James P.G. Sterbenz, David Hutchison, Egemen K. Çetinkaya, Abdul Jabbar, Justin P. Rohrer, Marcus Schöller, and Paul Smith. 2010. Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. *Computer Networks* 54, 8 (2010), 1245–1265. https://doi.org/10.1016/j.comnet.2010.03.005 Resilient and Survivable networks.