SLACOZE : Secure LoRa Ad-hoc Communication network Over the deadZonE

2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT) | 979-8-3503-3509-5/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICCCNT56998.2023.10307672

***Abstract*— Wide Area Network (WAN) technologies, like cellular 4G and 5G, are well-known and enable data transmission over long distances. Cellular WAN consumes a lot of power, and it allows us to transmit large amounts of data at high speeds over long distances. High power usage is the cost of this trade-off. Because of that, it required a wireless network that uses very low power but covers a wider area than Wi-Fi. Solution for that is enter to the LoRa. Long-range is referred to as "LoRa". Semtech's LoRa technology is a pro-priority radio modulation that only addresses the physical layer of the stack. Low-power, long-distance transmission over the unlicensed ISM band is made possible by the Lora technology's usage of pro-priority Chirp Spread Spectrum modulation. The bit rate of LoRa transmissions is quite low. The speed is in the range of 10 kilobits per second. In this scenario, it maintains a secure communication with Low powering nodes in areas with no signal and to implement a system to recognize & notify the rest of the team, if they face to the abnormalities. Therefore, this whole system is a contribution of LoRa Key manager, Power control unit, Abnormalities tracking system & Location tracking system and the integration of several such devices creates a LoRa Ad-Hoc network. These kinds of projects are most important for teams who communicate inside a dead zone, like forest explorers, as well as for military terrain.**

Keywords*— *LoRa, RSSI, Abnormality Detection, Power, GPS.

I. INTRODUCTION

When a team is in a dead zone, which is a region where wireless communication is not possible because to radio interference or range limitations. Forests, deserts, marine missions, and war zones are just a few examples. At the moment if your network goes down to 'no network' on your mobile. They need a mechanism to detect the abnormalities, and it is crucial that they keep in touch with one another, though the secure mechanism. Therefore, it would be best if you used a device that works with low power consumption and is capable of long-range communication.

Normally, LoRa technology will enable low-power wide-area communication at a low bit rate. LoRa is capable of supporting a large number of sensor nodes and transmitting data over long distances. The range of a LoRa module is solely determined by environmental barriers. In a traditional operating mode with a remote control the range would be 1-2 km though integrating a LoRa module would increase range to close to 10 km. When compared to other technologies, battery consumption is quite low. However, when compared to Wi-Fi, Global System for Mobile Communications (GSM), and Bluetooth, data throughput is limited. Various studies and surveys show that LoRa technology practically meets certain real-time requirements. Many functions demonstrate LoRa's real-world implementation of environmental change monitoring.

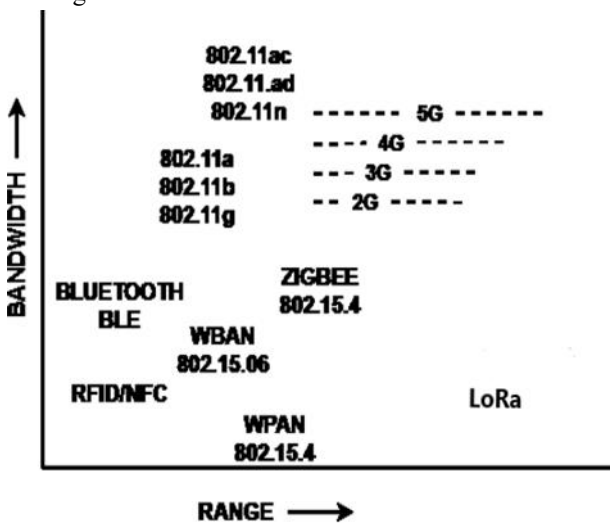


Fig. 1. *Comparison for different techniques between Range and Bandwidth*

In this case, LoRa communication would be used by the LoRa WAN protocol, and it is the only LoRa-based protocol accessible from end-users. The message is encoded by this LoRa WAN-capable node and sent to one or more gateways, which subsequently receive it and pass it on to the network server. The network server decodes the message that has been network-encoded and sends it on to the application server. The application-encoded message is then decoded, and the raw message is then made available via a web interface, a REST API, both, and other methods. [1]

In our research area, the system is proposed to develop a secure communication mechanism to transfer data among the team members within the dead zones. The four key components and its each main objectives that build up the proposed system are listed below.

1) LoRa Key Manager → To implement a secure method to communicate with LoRa nodes using a key management system.

2) Power Control Unit → To implement a nodes' State of Charge Voltage (%) dependent LoRa Message route control System.

3) Abnormalities Tracking System → To make a disaster tracking algorithm and automatically identifying a disaster in the middle of a journey.

4) Location Tracking System → To track the location using GPS Module and find the nearest node that is closest to the device that facing for an abnormality.

In an emergency case, the system detects abnormality and pass the live location details on time are incorporated as significant determinants in this entire system.

II. Literature Review

Several features of the LoRa technology and the LoRaWAN architecture, including coverage extension, scalability, and potential future use cases, have been examined in a number of research publications in recent years [2]. Eventually, this research paper discusses a number of studies that expand on the same concept and consider first-response after it occurs abnormalities, also that present findings have been used to support the proposed system idea.

When coordinating teams, communication networks are essential, and existing technologies are restricting the capabilities of teams like search and rescue teams and disaster response crews when general systems like cell-towers do not reach the target area. There are numerous new technologies that promise to address the restrictions of power and cost.

One of previous research paper [3] has proposed the system which is developed using Wi-Fi connection and LoRa to transceiver the text messages across a localized network. Furthermore, their GPS data is sent among the different clients to enable client mapping, which is shown in the mobile application. As well as, in that case they mainly used drone to maintain all the connections between each other ,because drones are able to get a better overview of a location due to its centralized and elevated positioning. Because of that, the system has proper data transmission, but high production cost.

The authors [4] presented a total measurement network system constructed by Local Sensing Node Network System (LSNNS), Host System (HS) and the communication method using “cloud” system to monitor landslide disasters. This "cloud" platform provides the convenience of accessibility from anywhere as well as the flexibility of data/information and command communication between HS and LSNNS. Also this system help us to find the one of mechanism for tracking the land side disasters. This gives test results only for the environmental disasters.

The research paper [5] has proposed most recent state-of-the-art mesh and multihop methods for LoRa and LoRaWAN. They discussed about the difficulties that multihop and mesh approaches still need to solve before IoT applications can benefit from the decentralized, autonomous, and infrastructure-free LoRa networks. In that paper, it compared three important situations with current state-of-the-art proposals and highlighted how they required various characteristics and capabilities beyond LoRaWAN's star of stars. Consequently, a number of issues still need to be resolved by researchers, developers, and vendors, including network scalability with hundreds or even thousands of nodes, maintaining network fragments and complex topologies, energy awareness, security and privacy concerns.

The authors present a brief explanation of how to implement a next-generation emergency communication system (ECS) that utilizes phone-based networks with no infrastructure and ensures long-range D2D communication. This system is able to capitalize on the widespread use of smartphones and the superior propagation properties of the LoRa technology to support data exchange even in extremely urgent situations. To achieve this, they proposed a novel mobile application that would enable users to broadcast emergency requests on the LoRA link with only the most crucial information, as well as a novel dissemination protocol that would enable multi-hop spreading of the emergency requests over phone networks with no infrastructure. Using comprehensive OMNeT ++ simulations and experimental observations, they have assessed the LOCATE system. However, our proposed system is creating as an implementation of separate LoRa devices without using mobile application. [6]

III. Methodology

After Proposed system is designed to forecast abnormality detections and passing the alert message through the LoRa in deserts, huge forest and hiking as soon as possible.

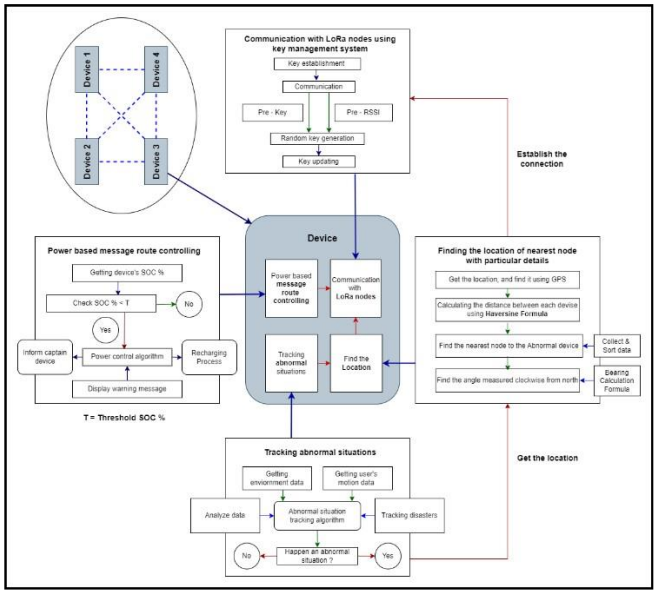


Fig. 2. *Overall System Diagram*

This diagram of the entire system provided a clearly described concept of the system, which is basically consist of following four components. In the OLDE display on each device shows processed data such as sensor data, nearest node, distance, bearing details and battery state of charge. Meanwhile, when the emergency incidence happens, it sent messages to the captain device and each device. And below

figure represents the “Schematic Diagram” of our system expect “Abnormality Tracking System”.

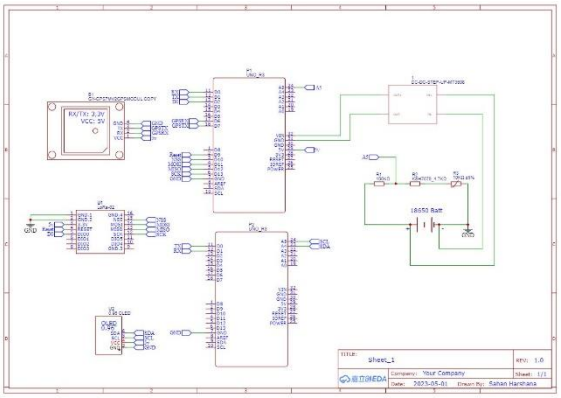


Fig. 3. Schematic Diagram

A. Implement a secure method to communicate with LoRa nodes using a key management system with the previous key and RSSI

In terms of cryptographic algorithms, LoRaWAN, the media access control (MAC) layer protocol for LoRa, supports the use of Advanced Encryption Standard (AES) for confidentiality and integrity protection. The AES algorithm is a symmetric key algorithm that uses the same key for both encryption and decryption. AES-128 is the most commonly used key length in LoRaWAN networks, but AES-192 and AES-256 are also supported.

Since we use the same key for encryption and decryption on both sides, we need a mechanism to manage the keys. Using LoRa with modern communication technologies is at risk of cyber-attacks. Our LoRa nodes are exposed to attackers because there is a large area. The GPS readings collected from nodes may face the threat of being sniffed, intercepted, or altered. If it happens like this it can be a major threat. In order to protect user privacy and the integrity of messages and GPS readings, it is of great importance to take security into consideration.

In this paper, our research aims to implement a key management system using the previous key and the RSSI value of the previous message. RSSI stands for Received Signal Strength Indicator and it is a measurement of the strength of the received signal in LoRa (Long Range) communication. The RSSI value in LoRa is a measure of the power level of the received signal, expressed in dBm (decibels relative to one milliwatt).

The security part of the complete communication between two nodes is divided into 3 main parts. They are key establishment, communication and key update. In the key establishment section, a previously generated secure key is exchanged by authenticating between the two nodes. In the communication part, the communication is done using the key that has been engaged. The sender encrypts the relevant message with the key and the receiver decrypts it. Then the receiver sends the RSSI value of the received message as an acknowledgment to the sender.

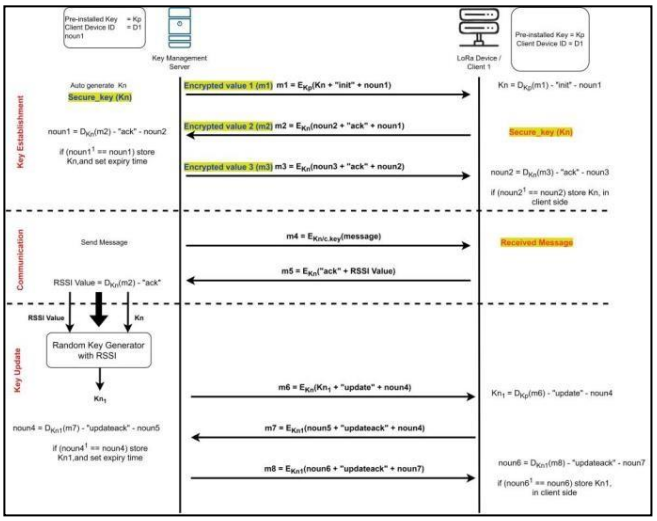


Fig. 4. *Key Management System*

After that, the mechanism of generating a new key starts using the received RSSI value and the previously used key. The process that takes place there is to regenerate the bits using the RSSI value and the previous key bitwise. Then the two separate bitstreams are converted into 2 new bit streams through a de-skewing method. The new key is generated by adding the XOR function to those 2 bit streams. Thus, the key updating part is completed successfully and the new key is exchanged between the two and the task is completed. Following Fig. 4. shows this method clearly.

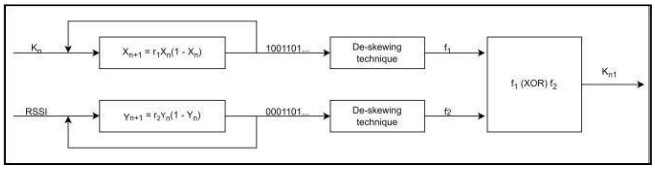


Fig. 5. *Key Generating Method*

In key establishment part sender and receiver need to initialize the initial key. Firstly, sender sends a packet with initial key, “init” flag value and first random noun. Let's we call it as M1. After receiving the M1 receiver decrypt the message and extracted the initial key. Then receive a sends a packet with acknowledgement flag, previously received noun and new random noun. Let me call it as M2.

After receiving this receiver extracted the noun 1. Then second receive a check similarity of previously send noun1 won and received noun 1. If these two values are equal first send establish the initial key as first initialized key. Then it sends the packet with acknowledge flag and noun2 and noun 3. After receiving this packet receiver extracted the noun 2 by suggested key. If previous noun same ad received noun, receiver side establish the initial key as previously received initial key.

Then both devices done the communication using established initial key. If one side sends a message receiver received the message with the RSSI value. Using the previous key and the previous messages RSSI value, key update part will happen. After creating the new key, need to establish that new key in both sides. Then the next message passing happened by the new updating key.

B. Power based LoRa Message route controlling

Always the shortest routes do not provide the better transmission performance between the node-to node communication. Sometimes it makes end-to-end delivery delays and reduce the average throughput of the network. And each node has specific size, power, and battery life. Maintaining a battery power of nodes' is really challenging in MANET. Therefore, Power control Algorithms are an essential requirement for mobile devices that use in dead zones. This sub system is described below; physical layer transmission power related Message Controlling Algorithm is the method that can used to improve the low – power communication networks' energy savings. It extends network longevity, by either:

- Enhance each device's lifetime
- Using node cooperation

It built a mechanism for proper interconnection between the nodes in LoRa network. As well as maintaining a continuous packet routing between the neighbors are important for this kind of dead zone based tracking systems. This Fig. 5. shows the main functions of a node (Active, Wait and Recharge) which are related of this algorithm.

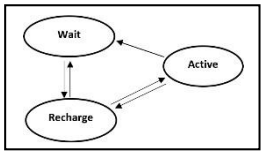


Fig. 6. *State transition diagram*

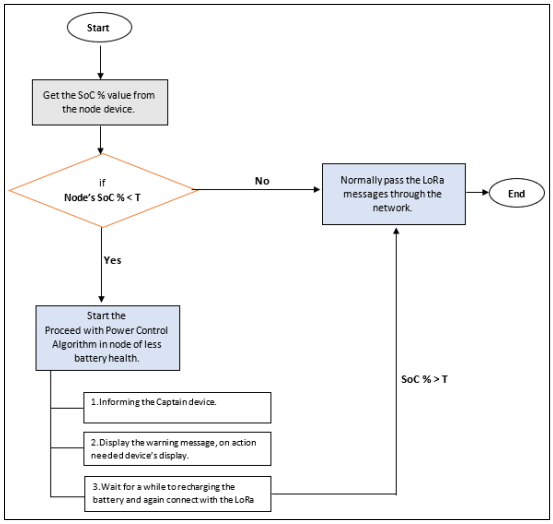


Fig. 7. *Flow diagram of Battery SoC % based message passing algorithm*

This message route control algorithm is a program that design to calculate SoC% of each device and get suitable actions through the packet flow. It is coded using Arduino IDE and after that the program is implemented on Arduino. Fig. 6. describes flow diagram of that controlling method.

Calculation of the State of Charge (SoC) %

To Convert Analog input to Digital value

- Voltage = reading * (5.0 / 1023.0)

To get State of charge Voltage of battery

- Vout = Vin (R2 / (R1 + R2))

About the Threshold Value Selection:

Here we assume minimum acceptable voltage level is 5V, if it goes down beyond that voltage level device's some operations becomes unreachable and also after few seconds devices getting down from the network. It is big issue for this type of network and the person carried that device. Therefore, avoiding those matters, for this power unit condition settings, we selected this V% as the threshold value for battery measurements.

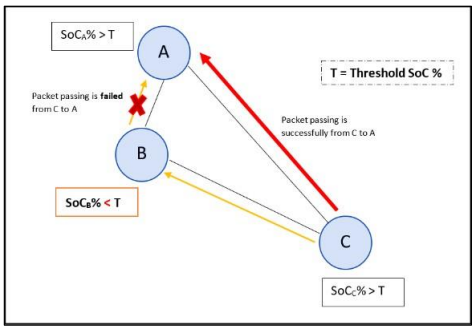


Fig. 8. *Packet routing according to SoC %*

Assuming this figure, it shows network topology that connect with three nodes. There are A, B, and C. As the SoC % here mention each of the node's battery percentage values separately. T indicate the Threshold Voltage SoC % value. It is a static value which is set according to the total voltage gain of one lora node.

According to that mechanism, to enhance the network lifetime and quality of the service, it blocks the Lora message routing paths, if any node's having less battery percentage value than the T. Also, all the messages' deliveries are stopping through this path, and that node drop from the network for a while.

In this figure 8, if we think C need to pass the message to A. In normal mesh routing it is having two routes (From C → A and C → B → A). But depend on this power algorithm, here choose the C → A path is suitable for message passing.

However, in our case, this type of blocking nodes can gain the link failures. Therefore, here we also added node's battery recharging process. It only works if any node having

less battery charge percentage than threshold value. That condition helps the protect device battery's health. Although, we use mini-solar power system to recharge this devices. Additionally, using DC power can recharge this device and using this device can charge other devices also. In that time those nodes inform about that issue to the captain node and wait for the LoRa network on going processes. After that completing the suitable charging level, automatically that nodes connect with normal LoRa network.

C. *An abnormalities tracking algorithm and automatically identifying an abnormality*

Mainly by identifying the movement characteristics of the person using the device and the external environment, this data is used to check if there is an abnormal situation. Here we have to add some kind of sensors to our device. Among them, a pressure sensor and a temperature sensor are used to obtain data from the external environment, a speedometer is used to detect the movement patterns of the user, and a pyzio sensor used to measure the heart rate. Data is always obtained from these devices and processed. The most important part of our device is the disaster tracking algorithm.

The disaster tracking algorithm is a program that can determine whether or not an abnormal situation occurs by analyzing the received data. It is coded using C++ and then the program is implemented in the Arduino board. Here, the measure 'Force' is mainly used as a measure of data analysis. We use the user's instantaneous 'acceleration' to measure the nature of the force. We use Newton's second law to determine whether a motion is changing or not. It clearly shows that an external unbalanced force acting on an object can change its motion. In addition, to further increase the accuracy of the data obtained from the data analysis, the data of external environment pressure, temperature, and user's heart rate are used as additional parameters.

Here we examine the abnormal situations that may occur in several environmental factors. Environmental conditions with a normal pressure level, environmental conditions with high pressure, environmental conditions with high temperature, and environmental conditions with low temperature are the main ones. For example, things like whether the user is on land or in water can be identified by the above data. Before using this device, it is given as inputs the mass of the user and the average pressure of the environment he is currently in. As the device always receives the set of data related to the pressure of the environment when it is working, the person checking it can calculate the current pressure of the environment and the deviation from the normal pressure of the environment. This algorithm gives a prediction about the current environment of the user. Similar prediction techniques are used for the rest of the data.

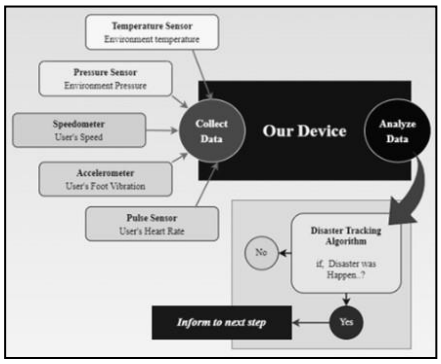


Fig. 9. *Abnormality Tracking System*

All these events work continuously in a loop and the data given by the device is processed by the algorithm. There are several steps in which the algorithm works and the data is analyzed repeatedly in each step. Finally, if the analyzed data matches with an abnormal situation, an output will be returned saying that such a situation has occurred.

D. *Finding the nearest node and its' location with angle measured clockwise from north*

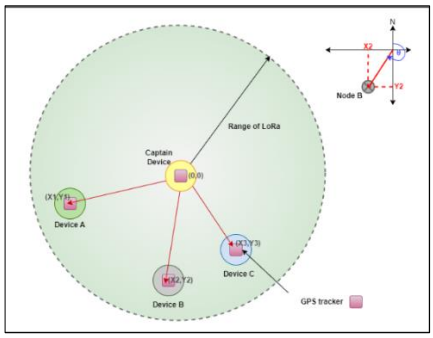
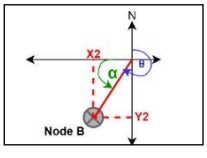


Fig. 10. *Interconnection of the system to entire project*

According to the above figures, it basically shows how this "Location tracking using GPS and find the nearest node that is closest node where the abnormality occurred" do. To explain this process, assume that Device B has been occurs an abnormal, that person needs the help from their team.

After GPS has found the location according to its latitude and longitude of each device from the captain device, it can find the live location of that point and can calculates the direction for it. In this case, it calculates the direction from the North side at every time, because it may be easy to other device holders to find the location. The basic calculation of it is shown as below.



$\tan \alpha = Y2 / X2$

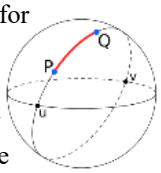
$\alpha = \tan^{-1} (Y2 / X2)$

$\theta = 270o - \alpha$

$\theta = 270o - \tan^{-1} (Y2 / X2)$

Fig. 11. *Basic Direction Calculation*

So, in here after track the location then it needs to find the nearest location to above location for help that person. To do that, from the receiving location details form other devices, we can find the nearest location by using "Haversine Formula". It can compare distances between Captain Device and Device A with Device B (abnormal device). Then it needs to sort these distances tofind the shortest distance.



• Converts degrees to radians	(lat) * (π / 180.0)
• Difference between two latitude values in radians	(lat2 - lat1) * (π / 180.0)
• Difference between two longitudes values in radians	(lon2 - lon1) * (π / 180.0)
• Use Haversine Formula to find the distance	➢ a = sin2(dLat / 2) + sin2 (dLon / 2) * cos(converted_lat1) * cos(converted_lat2) ➢ c = 2 * a sin (√a) ➢ d = rad * c ➔ average radius of the Earth is 6371km

Table. 1."*Haversine Formula" Calculation*

When it found the distances, it finds the bearing, that is an angle measured clockwise from north by using "Bearing Calculation Formula".

• Calculates the latitude value in radians	φ_1 = (lat A) * (π / 180.0) φ_2 = (lat B) * (π / 180.0)
• Difference between the longitudes of points A and B in radians	λ_2 = (lonB – lonA) * (π / 180.0)
• y-coordinate of a point in a two-dimensional coordinate system that represents a sphere	sin(λ_2) * cos(φ_2);
• x-coordinate of a point in a two-dimensional coordinate system that represents a sphere	cos(φ_1)*sin(φ_2) - sin(φ_1)*cos(φ_2)*cos(λ_2)
• Angle in degrees between the positive x-axis and the point (x, y)	➢ $\tan^{-1}$ (y / x) ➢ [$\tan^{-1}$ (y / x)][180.0 / π] + 360 ← Convert into degrees and ensure that the result is in the range [0, 360)

Table. 2. Bearing Calculation Formula

After finding those elements, these nearest nodes, distance, and the bearing details are taken by the captain device, and itwill share this nearest node to abnormal device through the secure LoRa communication.

IV. Results and Discussion

This research primarily focuses on the secure LoRa communication between travelling or exploration team on landslip. Standard range of LoRa communication distance is around 10-15km, but in Asian countries it has less limited radio frequency range. Because of that, in Sri Lanka we had chance to implement our project only for approximately 5km coverage area.

From the abnormality tracking algorithm in our device can automatically detects some kind of abnormality like as falling, animal pursuits and collision damages that can happen to member of that team. After that, it tracks the live location using GPS Module and find the nearest node with the angle measured clockwise from North that is closest to the device that facing for an abnormality. Furthermore, intruders should not be integrated with our network because system has periodically key updating mechanism using one of LoRa's parameter. These LoRa nodes are connected without any gateway, but with an encryption. Although here each devices having their own State of Charge (SoC)% measuring system and it check those values are above or below the threshold value. And the system includes important alert passing process. This can helps avoid the link failures due to the low battery power.

Finally, we can use calculations, mechanisms and algorithms that we used in here to other appropriate applications. These considerations could be a basic beginning point for more in-depth investigation, even though they may be oversimplified given our minimal experience with these kinds of data.

Below figure shows the comparison table of LoRa signal passing with Distance between two devices, that we created.

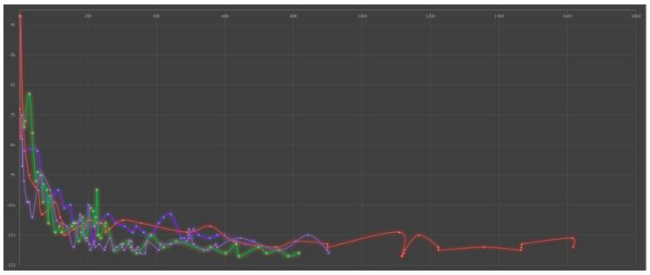


Fig 12: *Comparison table of LoRa signal passing with Distance*

V. Conclusion and Future Work

In this paper we have presented LoRa based communication network to support to any land side area, which does not have proper signal coverage. This system is built on the LoRa radio technology and the LoRaWAN architecture. In order to determine strength and speed of the signal. Also, one device contributed by four units that combined with each other, which is easy to carry while team-mates travelling and doing explorations etc. As well as it is important to communicate long-range, that allow users to be spread further apart and still maintain a reliable connection.

As a begging of our project, we used different kind of simulation platforms to test and simulate each four components. By considering above test results, we thought that it has possible probability to complete our project by using hardware components. So, finally as a result we implemented our system through the real devices without any problem. The system will be constructed using a range of the best technologies currently possible with a ultimately focus on data security to avoid signal interferences of devices between one team and another unknown exploration team. In addition to certain other highly technologies, which are highly developed, we use encrypted key management mechanism, which is one of most recent and extremely secure method.

In future, this research project can be modified by increasing proposed devices count, because at this moment we planned to provide this network that including only few devices to the society. By adding more devices to the system, it can be helps to expand the coverage area of communication and it can be decreased the drawbacks of D2D message passing. As well as it may use to different kind of suitable applications.

REFERENCES

[1] Giovanni Santini, “Integration and evaluation of LoRa sensors in GreenIoT”, Department of Information Technology, Uppsala University, June 2019.

[2] Haxhibeqiri, J.; De Poorter, E.; Moerman, I.; Hoebeke, J. “A Survey of LoRaWAN for IoT”: From Technology to Application. Sensors 2018, 18, 3995. doi:10.3390/s18113995

[3] Cameron Anderson, Jon Evans, Alex Krebs, and Connor Patten, "Skynet: A Localized Mesh Communication Network", 2020.

[4] S.Takayama, J.Akiyama, T. Fujiki, N.A.B.Mokhtar, "Wireless Sensing Node Network Management for Monitoring Landslide Disaster", Journal ofPhysics:ConferenceSeries 459 (2013).

[5] Roger Pueyo Centelles , Felix Freitag , Roc Meseguer , and Leandro Navarro, "Beyond the Star of Stars: An Introduction to Multihop and Mesh for LoRa and LoRaWAN", IEEE Pervasive Computing, April-June 2021.

[6] Sciullo, L.; Fossemo, F.; Trotta, A.; Di Felice, M. “LOCATE: A LoRa-based mObile emergenCy mAnagement sysTEm”. In Proceedings of the 2018 IEEE Global Communications Conference (GLOBECOM), Abu Dhabi,UAE, 9–13 December 2018.

[7] J. P. Shanmuga Sundaram, W. Du, and Z. Zhao, “A Survey on LoRa Networking: Research Problems, Current Solutions, and Open Issues,” IEEE Commun. Surv. Tutorials, vol. 22, no. 1, pp. 371–388, 2020, doi: 10.1109/COMST.2019.2949598.

[8] Emil, Örtlund,Malin, Larsson, “Man Overboard detecting systems based on wireless technology”, Gothenburg, Sweden 2018.

[9] Y. Lu, Y. Liu, C. Hu, J. Xu, Z. Wang, and S. Chen, “LoRa- based communication technology for overhead line internet of things,” 2019 4th Int. Conf. Intell. 2019, pp. 471–474, 2019.

[10] Usha, M.S.;Ravishankar, K.C.Implementation of trust-based novel approach for security enhancements in MANETs. SN Comput. Sci. 2021.

[11] Roger Pueyo Centelles , Felix Freitag, Roc Meseguer, Leandro Navarro, Sergio F. Ochoa and Rodrigo M. Santos, A LoRa- Based Communication System for Coordinated Response in an Earthquake Aftermath, Published: 21 November 2019.

[12] W. Xu, S. Jha, and W. Hu, “LoRa-Key: Secure Key Generation System for LoRa-Based Network,” IEEE Internet of Things Journal, vol. 6, no. 4, pp. 6404–6416, Aug. 2019.

[13] M.Gughan raja, B.John Samuel, Dr.N.Kirubanandasarathy, "Disaster alert notification and rescue management through Smart phones using GPS", June 2015.

[14] K. Mikhaylov, . J. Petaejaejaervi, and T. Haenninen, “Analysis of capacity and scalability of the lora low power wide area network technology,”; 22th European Wireless, Conference,IEEE May 2016.