A VHF Based Low Cost Solution for Tsunami Early Warning System, Sri Lanka

A.M.U.G.J Poddalgoda[1], T.D.P.M De Silva[1], P.D.S.T Pitiyage[1], M. Kalyanapala[1] and N.Fernando[1]*
[1]*Sri Lanka Institute of Information Technology*
**Corresponding Author: nimalika.f@sliit.lk*

Abstract— Disaster Management Center, Sri Lanka (DMC-SL) currently operate a proprietary system to control and manage Tsunami early warning towers. The current system does not match the DMC-SL requirements and the cost to maintain. DMC-SL is requested to design a system based on VHF communication to operate remote warning stations in the costal belt of Sri Lanka. This paper focuses on the transmission of digital data over analog VHF radio link and data security over the transmission

***Keywords*—DTMF, Disaster Management Centre, Early Warning, Encryption, Radio Communication, VHF, Security**

I. INTRODUCTION

In 2004 tsunami which devastated the coastal areas of Sri Lanka put an unforgiving impact on countries economic and social structures. Unfortunately most of this terror could have being prevented and mitigate the damage if affected people were notified and emergency services dispatched in time. But at that time Sri Lanka lacked such mechanism. After the 2004 tsunami Sri Lankan government took immediate actions to establish organizational structures and technological structures to manage disaster situations.

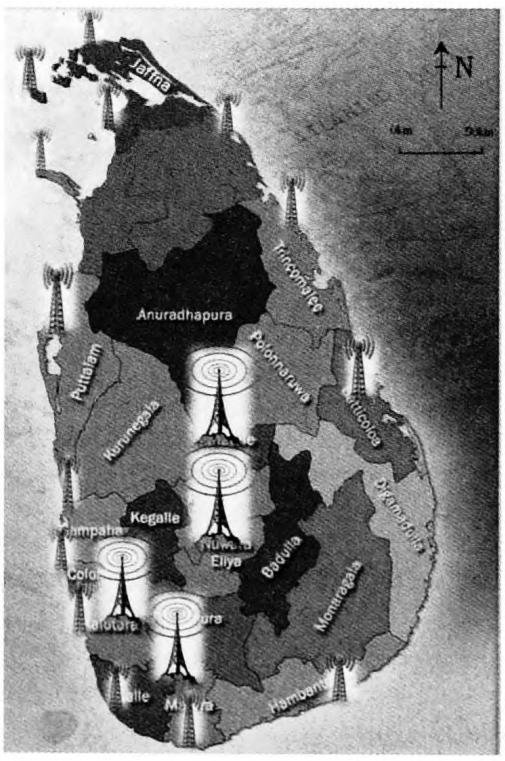

Figure 1. EW towers and repeater stations

As a result Disaster Management Centre (DMC) of Sri Lanka deployed Emergency Warning Towers over the coastal area of Sri Lanka as a method to inform people. There are seventy seven towers around the Sri Lankan coastal line. These towers equipped with array of powerful speakers and upon activation they can play a predefined message to the public.

The system needs to communicate using VHF radio links. All the towers are controlled by the central station at the DMC headquarters. Since the requirement was to use existing infrastructure the system has to use VHF radios to communicate between towers and command center. The research team has to focus on several areas in designing the system.

- Data Communication
- Security
- Network Topology

Data communication includes encoding and decoding of digital data into analog signal and vice versa. The structure of the messages and what are the necessary information they carry. Then how to secure the data using encryption mechanism to prevent from ears dropping. Network topology include how the communication network laid off and what are the design methods use to avoid some problems in radio communication.

The purpose of this paper is to discuss the solutions for above key areas and how to integrate them to create a complete system. Further it will discuss the system has a whole, including other parts to make it complete comprehensive system.

II. METHODOLOGY

After analysing the available equipment and environment, project group come up with plan to achieve the requirements of the DMC-SL. As shown in the figure 2 user can access the user interface as a web interface via the Ethernet port of the controller module. Another method is connect controller module to internal network and user will be able to access the controller interface through the network. The second option greatly increase the scalability and accessibility of the controlling software/interface. Controlling module in the Base-station side host lightweight web server and a database which provide the controller interface for the system as a web interface.

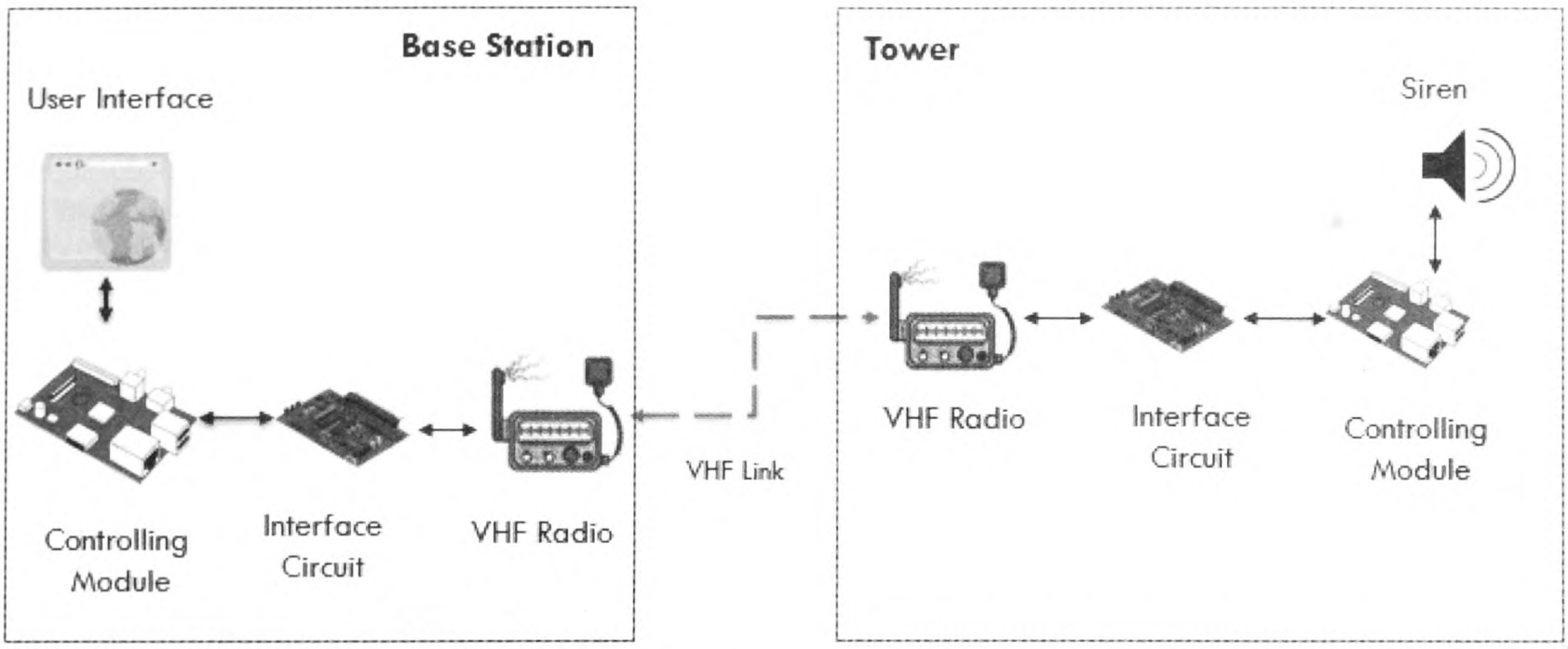

Figure 2. System Diagram

Controlling module is Linux based computing module of the system. Controlling module consist of processor, main memory and flash memory which hold the programme instructions. On Base Station Control module act as central hub for communication. Base Station take user commands through its user interface and then transmit them to the Tower sites. Tower side Controlling module listen to the Base Station command and perform accordingly. Communication methodology is further explained in the paper under Network Topology.

To control the VHF radio, radio being connected to an Interfacing Circuit which connects to the Controlling module at the other end. The Interface circuit works as a bridge between the VHF radio and the Controlling module. Interface circuit also work as encoder and decoder. Data converted to audio tone before send through the VHF link, then converted back to data at the other end.

A. Data Communication

To send digital data over a voice band, there are several methods in practice.

- DTMF (Dual Tone Multi Frequency)
- AFSK (Audio Frequency Shift Keying)
- Morse-code

DTMF which use combination of two sinusoidal tones to generate a unique signal [1]. DTMF can represent sixteen digits. AFSK transmit data by changing the frequency (pitch) of an audio tone. [2] By using Morse-code it also possible to send data by controlling signal duration. [3], [4]

After reviewing the requirements research group choose DTMF as the signalling method. DTMF is easy to encode and decode, can tolerate radio transmission impairments. System does not require entire ASCII character support and it also can tolerate delay. Because of these factors DTMF seems the better candidate.

1) *Message Structure:* To communicate between towers and command centre group defined a message structure. Message structure is simple compared to other networking message formats. That is due to the fact the radio signalling used and it need to be short and easy to process in low powered processors in the tower end.

*	<Sender ID>	<Receiver ID>	<Command>	#
Frame Start	3 Digits	3 Digits	2 Digits	Frame End

Figure 3. Message Structure

Message structure feature a start and end digit that indicate the start and end of a message. Asterisk sign (*) indicates the start of a message. When the controller receive an asterisk sign over the radio it will flush all the messaging registers and will ready to receive and store a new message. The hash (#) sign indicates end of a message. When the controller receive the hash sign it will start process the received message.

Table I Message Commands

Digit	Command
00	Requesting Response
01	ACK
02	NAC
03	Status Check Request
04	Status Okay
05	Status Not Okay
06	Deactivate Siren
07	Siren Activation - Cyclone Alert
08	Siren Activation - Cyclone No Threat
09	Siren Activation - Cyclone Evacuation
10	Siren Activation - Cyclone Withdrawal
11	Siren Activation - Tsunami Alert
12	Siren Activation - Tsunami No Threat
13	Siren Activation - Tsunami Evacuation
14	Siren Activation - Tsunami Withdrawal
15	Siren Test
16	<Not Assigned>

In between asterisk and hash contains the message data, first three digits indicate the senders ID, next three digits indicate the receivers ID and last two digits represent the command. Commands are predefined values each assign a specific task.

As shown in the table one last two digits are appointed for various tasks and these are in tower point of view.

B. Security

Since these messages send over air they are vulnerable to ears dropping and other sort of attacks. To secure the communication there are two methods that can follow

- Software base encryption
- Hardware based scrambling

Software based encryption based on high-level encryption using ciphering methods to scramble the data so no meaningful output will give when attacker intercept them. In hardware based scrambling the signals are altered in a way that only sender and receiver can reconstruct them into original form.

In this implementation we focus on software based encryption. The hardware based scrambling methods are proprietary and they are embedded into VHF radio. Using same radios with same scrambling modules hardware based scrambling can be implemented. But it out of the scope of this paper, so we focused on how to build software based encryption mechanism, which will not depend on underline hardware.

Software based encryption works in upper layers of the process. In today's communication world there are many encryption methods available, but almost all of them are not suitable for this scenario. Most of these encryption are based on full ASCII or Unicode characters and use fairly long keys for encryption and decryption. But this implementation is based on DTMF signalling which only support sixteen character digits plus the hardware doesn't have the computational power or other resources to compute complex algorithms.

The encryption algorithm proposed on this paper based on transposition cipher [5] and it is fairly simple algorithm based on symmetric key encryption [6]. When the message is constructed by the program it will be sent to encryption algorithm. The algorithm then take the original text and a key as inputs the produce encrypted output. The algorithm will randomly arrange the original text based on the key to create cipher text. Without knowing the key it's impossible to reconstruct the original text. The key is shared among tower nodes and controller node making it a symmetric key encryption.

As shown in the figure 4 the plain text message is send through encryption algorithm. The key is given as an input to the algorithm, it will output the encrypted message. Then the encrypted message will be modulated to series of DTMF signals and broadcast through the air. When another node receive the DTMF signals they will be decode back to digital text format. Then the text will send through decryption algorithm. The decryption algorithm also take the same key as an input and output the original message.

Even though intruder intercept the message and able to distinguish the DTMF signals. Then able to construct the message, the message is out of order and doesn't give any meaning. Without the key the intercepted message cannot be reconstructed.

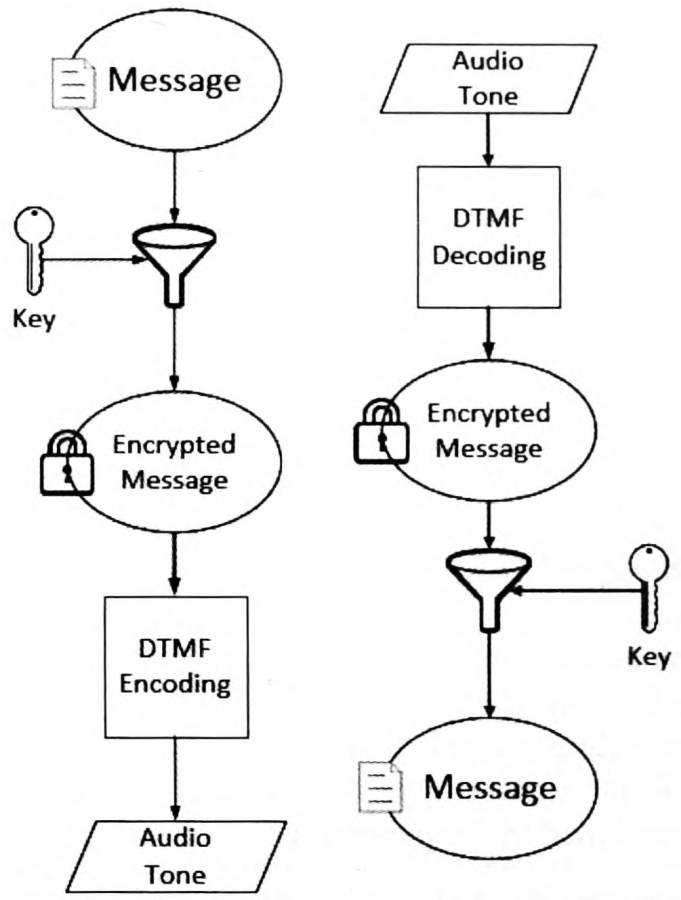

Figure 4. Encryption & Decryption Block Diagram

C. Network Topology

The towers and the control centre act as multiple node network and it necessary to create communication rules to ensure collision free communication. The topology of the system is common to hub and spoke topology of a LAN network. [7]

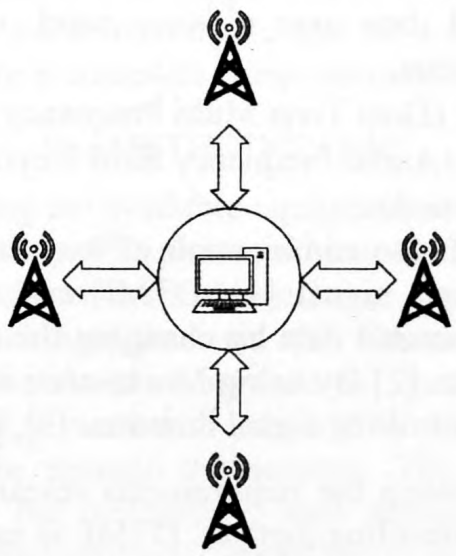

Figure 5. Hub & Spoke Topology

The command centre work as the hub of the topology and all the towers act as spokes. Command centre is the centre of the communication all the messages go through the command centre.

2) *Master Slave Relationship:* The command centre and Towers are in master slave relationship. The command center always initiate the communication and by default the towers are in listening state. Towers will only transmit if the command center explicitly request to transmit.

This will ensure the air space will be always be clear and command center has the authority to control the use of it. So there will be no unpredictable collisions occur during the communication.

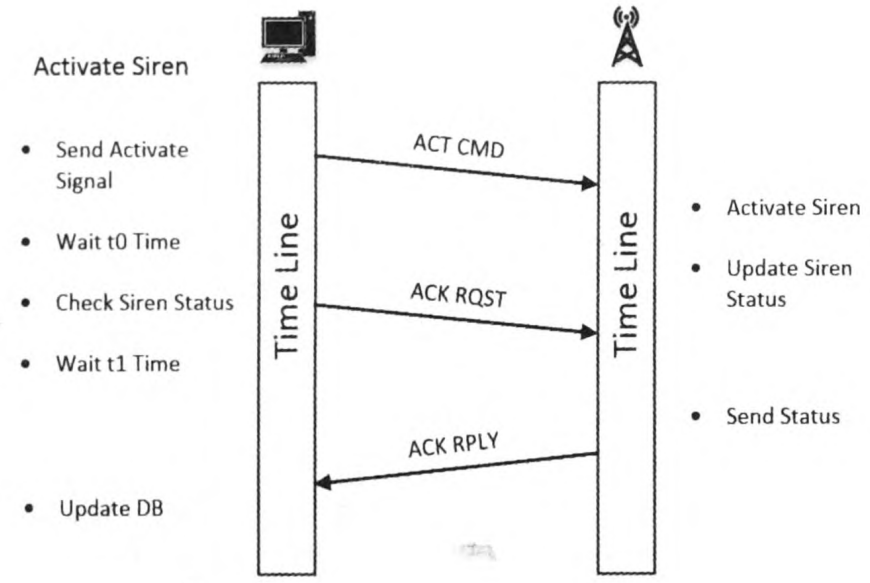

Figure 6. Siren Activation

Figure 6 illustrate an example of sending a siren activation command to a tower. The controlling center will initiate the communication by sending an activation command then wait t_0 predefined time. Then send another message to check the status of the siren. Mean time tower will activate the siren and update about its status. Until the tower receive a request for status acknowledgement it won't reply back to the command center. Only when command center request an acknowledgement it will send a reply hence maintaining the master salve relationship.

D. Transmitting & Receiving Data

Transmission and receiving is performed in the Controlling module. Figure 7 represent the flow of transmission of a message. First the program check for channel availability, if channel is free it will acquire PTT (Push To-Talk) which will indicate channel is busy to other sites and start sending the message. After transmitting the message program will release the PTT. If channel is busy program will wait until it become idle again.

Figure 8 represent the receiving of a message. In receiving the message received as digit at a time, and when a digit has been received and decoded it will trigger an interrupt [8]. When interrupt occurred controlling module will read the data from the DTMF decoder module in interface circuit and map it into corresponding digit. If the digit is an asterisk (*) it represent the start of a new message. Process will clear message variable and wait for new message. If the digit is hash (#) it indicate the end of a message. Sub process will be stated and message will be passed to the sub process for message processing. If digit is neither of asterisk nor hash, digit will be append to the message variable.

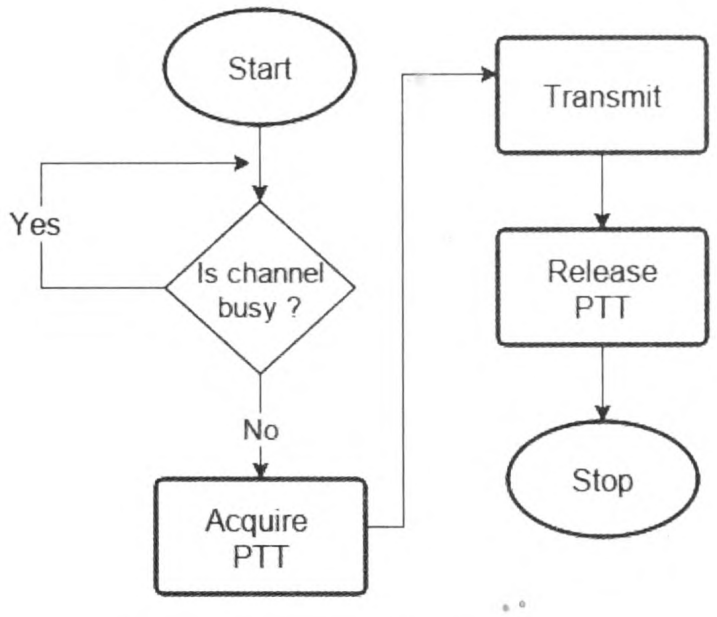

Figure 7.Transmission Flow Diagram

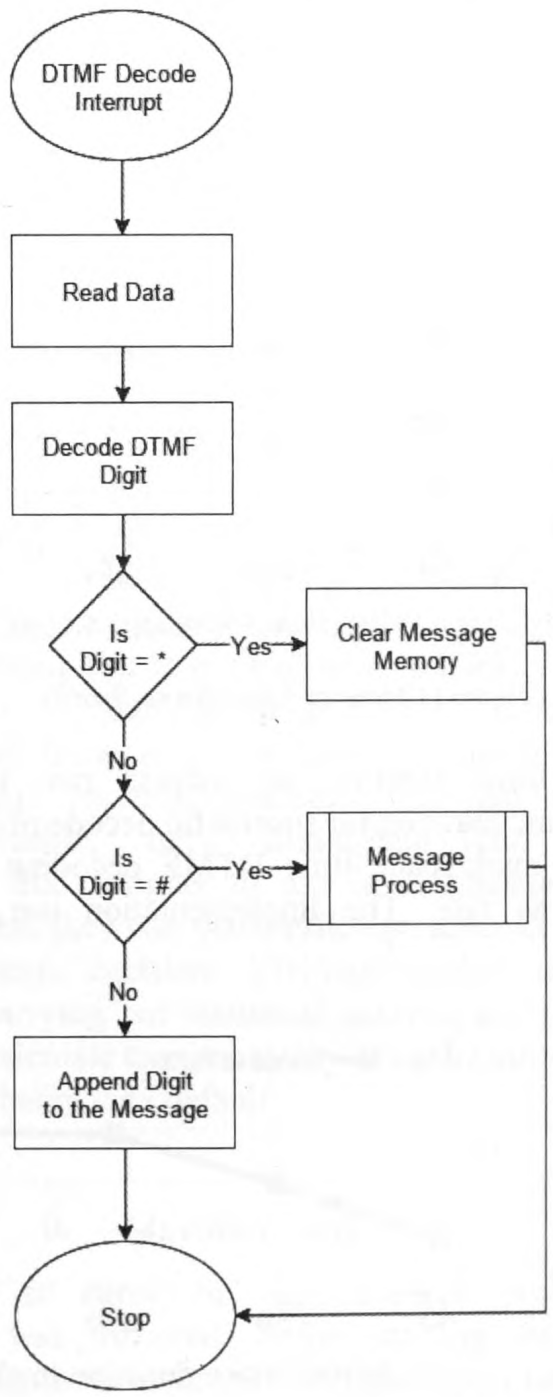

Figure 8. Receiving Flow Diagram

III. RESULT

The proposed system was successfully tested with the above implementations and successfully transmit and receive messages over VHF radio link.

Test were conducted in two scenarios, in first scenario as shown in the figure 9 radio in direct communication using same frequency for Rx & Tx approximately in 1km distance. In second scenario radio link goes through a repeater station before reaching its destination. This test simulate long distant communication. Test were conducted on 10km radius.

Figure 9 Direct Connection

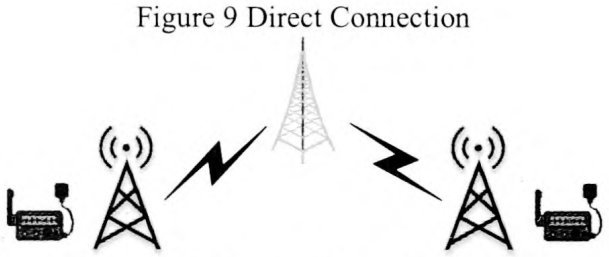

Figure 10 Through Repeater Station

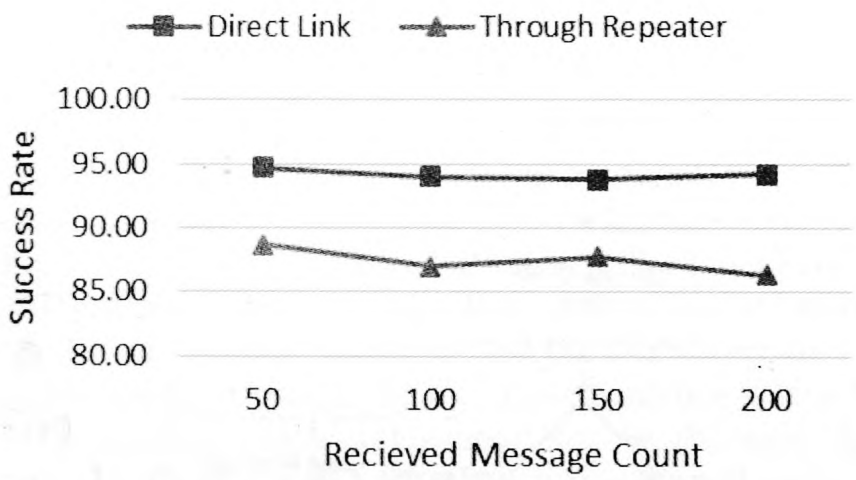

Figure 11 Message Transmission Results

Mark/Space time duration vs success rate indicate the appropriate time duration for successful decode of DTMF tone. With 100ms mark/space time DTMF decoding rate shows perfect success rate. The implementation use the 100ms duration.

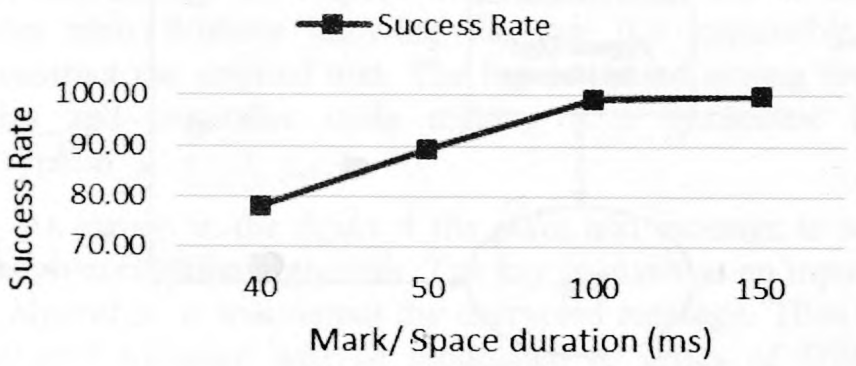

Figure 12 Mark/Space Time Results

IV. CONCLUSION & FUTURE WORK

The main objective of this paper was to introduce VHF communication protocol to establish communication of early warning towers. This paper identify the problems faced in developing the system requested by DMC and how to overcome them. The protocol is design to this system specifically but it can be easily adopted to other telemetry systems which use similar radio signaling to communicate.

As future work the encryption algorithm can be further developed to more advance encryption mechanism. To make the algorithm more robust the secret key can be randomly generated using a common denominator.

ACKNOWLEDGMENT

Research group would like to express our sincere gratitude to Dr.Malitha Wijesundara and Mr.Jayantha Amararachchi for their guidance and encouragement which they gave us during planning and implementing our solution on the research. Also would like express our warm thanks to Mr. Thusitha Waidyarathna and Lt.Col. W.S.N.Perera for their support and guidance at Disaster Management Center - Sri Lanka.

REFERENCES

[1] The MathWorks, Inc., "Dual-Tone Multi-Frequency (DTMF) Signal Detection," The MathWorks, Inc., 2004. [Online]. Available:http://in.mathworks.com/products/demos/signaltlbx/dtmf/dtmfdemo.html. [Accessed 5 March 2015].

[2] B. Watson, "FSK: Signals and Demodulation," WJ Communications, Inc., 2001.

[3] J. Bray, in *Innovation and the Communications Revolution*, London,, The Institution of Engineering and Technology, 2002, pp. 36-40.

[4] International Telecommunication Union (ITU), "International Morse code," ITU, Geneva, 2009.

[5] D. Kahn, The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet, Scribner, 1996.

[6] H. K. Hans Delfs, Introduction to Cryptography: Principles and Applications, Springer, 2007, pp. 11-13.

[7] T. Lammle, CompTIA Network+ Study Guide, Sybex, 2012.

[8] MT8870D/MT8870D-1 ISO2-CMOS Integrated DTMF Receiver, 1st ed. Mitel Networks Corporation, 2006, pp. 13-21.