Development and Implementation of Marine Efficient Cryptographic OTH Communication Setup

Submitted by:

CDR NADEEM AIJAZ PN

Supervised by:

CDR DR SYED SAJJAD HAIDER ZAIDI PN

THESIS

Submitted to:

Department of Electronics and Power Engineering,

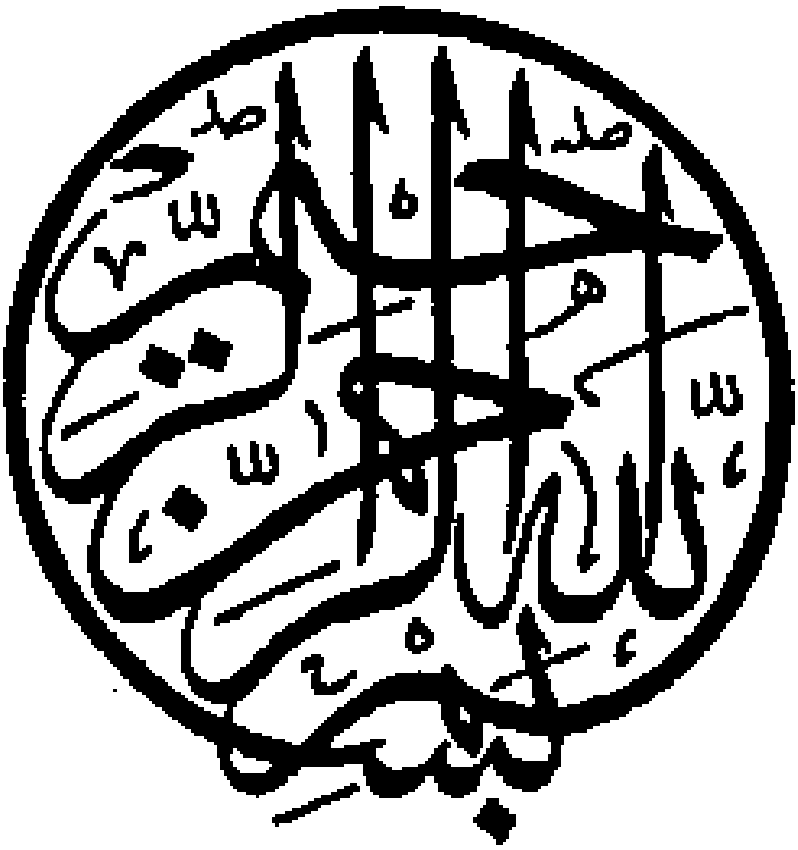
Pakistan Navy Engineering College Karachi,

National University of Sciences and Technology, Islamabad

In fulfillment of requirements for the award of the degree of

MSEE (Communications)

February 2013



ACKNOWLEDGMENT

1. I am grateful to almighty ALLAH (ever Merciful and Beneficent) for his blessings and giving me wisdom, knowledge and understanding without which I would not have been able to successfully complete this thesis work. I would like to express my sincere gratitude and acknowledge the guidance of all those who were helpful to me in the course of this thesis. My special thanks to Mr Nabeeg Mukhtar for giving me appropriate software assistance during my thesis work and Cdr Dr Syed Sajjad Haider Zaidi PN at PN Engineering College, my thesis supervisor, whose able guidance and support in every step of the research played a vital role in accomplishment of thesis work.

2. Moreover, I would like to thank the guidance committee comprising of following faculty members who professionally led me to achieve my target:

- Associate Professor Dr Ather Mehboob
- Cdr Dr Muhammad Farhan PN
- Assistant Professor Dr Khawaja Bilal

3. In the end, I would like to pay sincere gratitude to my family whose support made me achieve my post graduate degree successfully and played a great role in my success by sacrificing the valuable time throughout the research phase.

ABSTRACT

1. This research is aimed at developing and implementing cryptographic codes for Over-The-Horizon communication at sea. This will allow secure and efficient High Frequency communication between Pakistan Maritime Security ships over a very long range. The sea units will also be able to maintain safe communication with the base stations at coasts. The main components of the system are PC based software, a Personal Computer/Laptop, hardware interface between communication equipment and the HF transceivers on both the ends. The software has been developed for extracting audio coded noise which transmits via the HF link. It is primarily designed for keyboard to keyboard conversation modes on high frequency bands. The output of the computer gives input to the HF transceiver through a hardware interface which transmits to the other end.

2. In order to secure the message sent, this thesis presents a secure electronic link which will ensure message confidentiality, integrity, authenticity and non-repudiation. Moreover, public key infrastructure is configured with the open source tools and secure extension is implemented. This work will help to utilize the signal transfer in a secure and reliable mode for military usage. When the sender will transmits on this secure system, the information contained will be encrypted and will only be received by the intended recipient. This thesis uses the open source software and modules for message safety from malicious security incidents and ensure reliable/secure mode for efficient and fast transfer of messages coping up with the requirements of a military setup.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.1 GENERAL

Communication has always been vitally important in human race. Initially, it was achieved by voice but with the passage of time and access to humans to the remote places, various devices were introduced. This ultimately led to the inventions of optical and radio communication devices. Thus, leading to commercial radios and software defined radios for domestic and amateur use. The progress in the technology of communication has opened era of new equipment with accelerated data rate and added features for military as well as commercial applications. Navy, being the one arm of military setup, requires high efficiency and appropriate security measures for communication links. The linking of communication between fleet at sea and shore needs strong communication link for data as well as for voice. In order to achieve this, application of HF communication is made throughout the world which is also called Over The Horizon (OTH) communication. The HF frequency band covers the range between 3-30 MHz and is also called decameter band. As the radio waves reflects back to earth's ionosphere in the atmosphere, frequencies can be utilized for distant communication and continental distances. Therefore, HF is also known as sky- wave. This chapter as a whole will discuss the communication in general and HF communication specifically and its applications along with its security aspects.

1.2 **MORDERN USAGE OF RADIOs** Modern use of radios is discussed as following:

1.2.1 Joint Tactical Radio System It was United States military program to acquire radios providing communications which is flexible. The radios were vehicular,

handy, dismounted radios and airborne for sea as well as base stations. Open software communications architecture was achieved by application of SDR systems.

1.2.2 Amateur Radio An amateur radio software utilizes direct conversion receiver. Unlike previous era direct conversion receivers, the technology of mixers are based on sampling exciter and quadrature sampling detector. Dynamic range of the AD converters Radio is related to receiver performance of SDRs. It is sampled by high audio frequency ADC and frequency is converted to audio band. The first generation of SDRs uses sound card in order to achieve ADC functionality.

1.3 **UTILIZATION OF HF COMMUNICATION** Coming to the utilization of RF as general and HF specifically, The main users of the high frequency spectrum are:

a. Military and governmental communication systems
b. Aviation air-to-ground communications
c. Amateur radio
d. Shortwave international and regional broadcasting
e. Maritime sea-to-shore services
f. Over the horizon radar systems

1.4 **SECURE COMMUNICATION** In secure communication setup, many of the people are unaware that when transmitted messages goes on a media, it does not just go to the recipient but it mounts on the intended frequency from system to another system until it arrives at its required destination. If someone wants to intercept or alter the message then the information can be intercepted and manipulated effortlessly. This scenario led to secure communication parameters in general and in particular for military use in order to avoid any unintended intelligence. To cater for the same,

message integrity, confidentiality, message non repudiation and authentication are the properties required for maintain secure communication in a media.

1.5 **APPLICATION OF SECURE OTH COMMUNICATION** Application of secure OTH communication are in many fields. Some of them are described below:

1.5.1 Military Usage Due to revival in HF technology for connectivity and frequency selection, automatic link technology was developed in networks used by governments. High speed modems were utilized which conformed to the military standards (MIL-STD-188-110C) which supported 120 kilobit/s of data rates which has subsequently increased the application of high frequency transmission of video and data as well.

1.5.2 Radios These operate in the upper band i.e on 27 MHz. Continuous wave morse code transmissions and SSB voice transmissions are examples in the HF range than on other frequencies.

1.5.3 Aviation distress usage For transoceanic flights, HF communication systems are compulsory. These have frequencies down to 2 MHz to include “Compulsory Channel Watch” a 2182 kHz station. Some of the identification tags of radio frequency require high frequency called High Frequency Identification.

CHAPTER 2

THESIS THEME

The ensuing paragraphs will give details of the thesis theme covering the problem statement, detailed scope of the research work and methodology adopted till completion of the research work.

2.1 PROBLEM STATEMENT

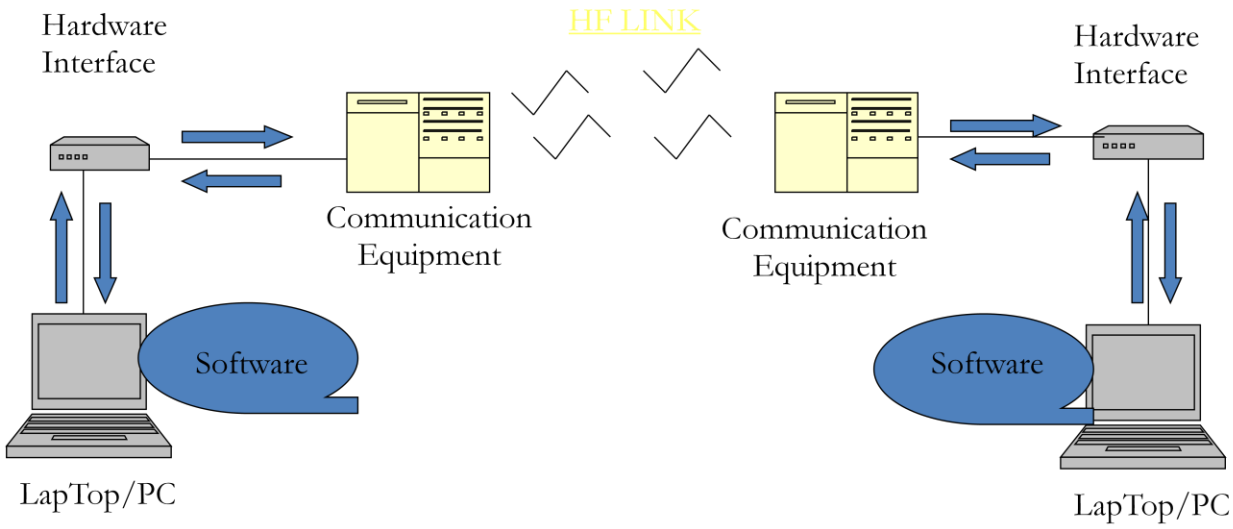
Pakistan Navy/Pakistan Maritime Security Agency has been facing problems in establishing reliable communication over long ranges specially voice/text messages requiring military use for secure and reliable means of communication. The organizations have been investing lot of foreign exchange for secure and reliable service at sea through OEMs abroad.

2.2 SCOPE OF THE RESEARCH WORK

To implement a secure/reliable military communication setup by developing indigenous software for data transmission through High Frequency link onboard ships at sea and base stations. The communication setup has been implemented specifically onboard Pakistan Maritime Security Agency corvettes at sea to establish communication with base station at shore. Upon successful trials and necessary modifications (if required) the same could be installed on Pakistan Navy ships and shore stations as well. This research work has provided a high performance and reliable communication setup at sea as well as at shore in order to maintain efficient encrypted transmission/reception of messages over a long range. Present economic conditions of country demand indigenous and cost effective solutions for technical problems faced by defence forces in particular and other departments in general. This project is will be a step towards

indigenization of secure communication technology for PMSA specifically and PN generally. The block apprehension of the thesis is given in the block diagram below:

BLOCK APPRECIATION



2.3 PROPOSED METHODOLOGY

The execution of the thesis has been proposed in two phase which are delineated below:

2.3.1 Phase I In Phase I, following two activities were planned basically involving the information gathering and feasibility of appropriate communication equipment and selection of open software tools:

a. Feasibility of HF communication equipment For the feasibility of appropriate high frequency communication device, three already acquired communication equipment by Pakistan Maritime Security Agency were studied in detail along with hardware configuration. Amongst the three, one equipment SGC-2000 was chosen for utilization in the thesis project.

b. Development of software using open source software tools For the development of PC based software, help of open source softwares were explored for formulation of modules of transmission/reception, encryption and compression of data.

2.3.2 Phase II In Phase II, The development of hardware was carried out along with simulated setup tests resulting in the practical implementation onboard ship. Same is delineated below:

a. Development of hardware interface A hardware module was developed for interface between the PC/Laptop and the HF communication equipment so that encrypted signal can be transmitted and received on HF link.

b. Implementation for simulated setup For the results of the developed software and hardware, the setup was tested in the lab and appropriate changes were carried out in the software for better results.

c. Practical implementation of the setup onboard ship upon successful lab test results, the same setup was carried out onboard corvette/ship and the shore station for practical implementation. After many communication trials, successful results were achieved.

CHAPTER 3

THEORETICAL BACKGROUND

This chapter will describe the theoretical background of the thesis work covering the Radio frequency spectrum specifically covering the high frequency domain. The software defined radios and software will also be discussed. Moreover, communication security aspects and basics of cryptography are illustrated in ensuing paragraphs.

3.1 **Radio frequency (RF)** RF is the oscillation rate which has range of 3 KHz to 300 GHz corresponding to radio waves frequencies. Radio Frequency refers to electrical oscillations, however, mechanical RF systems does occur. Radio frequency is actually the rate of oscillation, therefore, RF is used for radio to describe wireless communication. The radio frequency spectrum is attached as Appendix I.

3.2 **High frequency (HF)** High frequency is one of the parts of the radio frequency spectrum lying between 3 and 30 MHz. Below HF are medium frequencies and above are known as VHF very high frequency .The band is used by international shortwave broadcasting stations (2.310 - 25.820 MHz), communication, government time stations, aviation, weather stations, citizens band services and amateur radio, among other uses. The frequencies at which communication is possible are specified by lowest usable high frequency, maximum usable frequency and frequency of optimum transmission. After evenings and in winters, maximum usable frequency drops down below 10 MHz while it can easily crosses 30 MHz in the summer during daytime. It is dependent on angle of incidence and is higher with acute angles and is lowest when the waves are upwards. Worldwide communication is possible on High frequency upon

all optimum factors. Military communications normally uses high and low ends of bands of high frequency.

3.3 **SOFTWARE DEFINED RADIO (SDR)** A software radio system can be defined as a communication system which has elements that can be implemented by software on an embedded system or a computer instead of hardwares like amplifiers, mixers, filters, detectors, modulators/demodulators. Main SDR system consists of a computer with sound card or ADC preceded by some form of RF device. Signal processing is done by a processor than by a special-purpose device. This produces a radio which can transmit and receive different radio protocols based on the software.

3.4 **SDR SOFTWARE** Digital signal processing operations can be performed by a personal computer using software specific radio device. Majority radio softwares use open source SDR libraries. All demodulation, radio and audio frequencies modulations and signal enhancement are done by SDR software. Morse code, AM, FM, single sideband modulation and a many of digital modes like packet radio, slow scan television and radio teletype are the applications of SDR software.

3.5 **PROPERTIES FOR SECURE COMMUNICATON** Properties to maintain a secure and safe communication in a media is delineated below:

3.5.1 Message Integrity Upon achievement of authentication by the sender and a recipient and if it is desired that the contents of their communication are not changed during the transmission process. This can be achieved by calculating the Hash value of contents. Message integrity and authentication and is used side by side as message integrity is of no use if the sender is not authenticated or vice versa.

3.5.2 Confidentiality The sender and the intended recipient only should be able to understand the contents of the transmitted messages. The message is to be encrypted, either by symmetric or asymmetric algorithms, so that the intercepted message cannot be decrypted by any intruder or interceptor.

3.5.3 Message Non-repudiation The message transmitted could not be denied by the sender. Therefore, whenever a message is sent, the recipient can prove the sender. Certificates and digital signatures provide the non-repudiation because they authenticate the sender.

3.5.4 End-point Authentication The sender and the recipient must be able to confirm the identity of each other. Visual authentication of two sides is quite simple as compared to the communication entities exchange messages over the media. Sender authentication is provided by use of digital signatures. Digital Signature and Encryption can be used in three ways:

a. First encrypt the document and then sign it.

b. First sign the document then encrypt the document content only leaving the signature in clear.

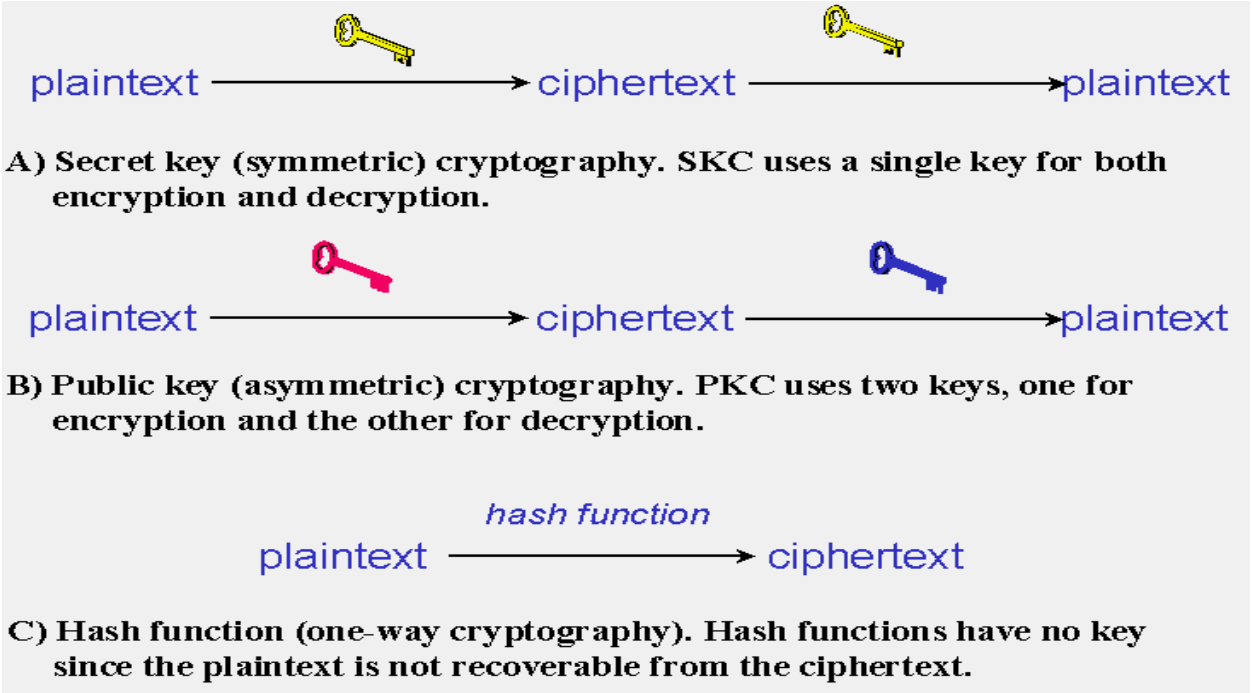
c. First sign the document then encrypt both the document contents and its signature.

3.6 **CRYPTOGRAPHY**

The term “Cryptography” can be defined as the art of writing in secret code. First documented application of cryptography was done by an Egyptian scribe used non-standard hieroglyphs in 1900BC. Experts say that cryptography seems unexpectedly when writing was invented. The development of computers resulted with the new forms of cryptography. In telecommunications and data links, cryptography is mandatory when communicating over any unreliable media.

3.7 TYPES OF CRYPTOGRAPHIC ALGORITHMS

There are many ways to classify cryptographic algorithms. The main three types of algorithms are :



3.7.1 Secret Key Cryptography Single key for encryption and decryption is used in SKC. A single key is utilized for encryption and decryption. The transmitter uses a key to encrypt the plaintext and sends the ciphertext to other end. The receiver applies same key to decrypt the message and recover the content. As single key is used for both functions, therefore, SKC is also known as symmetric encryption. These are generally categorized as being stream ciphers or block ciphers.

3.7.1.1 Stream ciphers This operates on single bit at a time and implement feedback mechanism in order to constantly change its keys. In a block cipher, same plaintext block will always encrypt to the same

ciphertext when utilizing the same key whereas in a stream cipher, same plaintext will encrypt to different ciphertext.

3.7.1.2 Block ciphers This can operate in one of several modes amongst which four as delineated below are important:

a. EC - Electronic Codebook

b. Output Feedback

c. Cipher Feedback

d. Cipher Block Chaining

3.7.3 SECRET KEY CRYPTOGRAPHY ALGORITHMS Most common SKC being used today are:

a. Data Encryption Standard (DES) It is a common SKC scheme which is being used. Designed by IBM in the 1970s and adopted by NIST in 1977 for commercial government and unclassified applications. It is a block-cipher utilizing 56 bit key in 64 bit blocks. It has a difficult set of rules that were designed to have fast hardware and slow software implementations.

b. Advanced Encryption Standard (AES) In 1997, a new cryptosystem was developed for U.S. government applications started by NIST. In Dec 2001, it became official successor to DES. SKC scheme known as Rijndael is utilized by AES which is a block cipher developed by Belgian cryptographers. Block lengths and variable key length are used by this algorithm. The latest length of key combination of 256, 192 and 128 bits and blocks of length 256, 192 or 128 bits are utilized in AES.

c. CAST-128/256 It is a permutation crypto algorithm similar to DES with a 128 bit key on a 64 bit block. In AES process, ‘CAST-256’ is one of round 1 algorithms.

d. International Data Encryption Algorithm (IDEA) It was developed by Xuejia Lai and James Massey in 1992 and then patented by ASCOM. It is basically a 64bit Secret Key Cryptoghraphy block cipher on a 128bit key.

e. Blowfish This was invented by Bruce Schneier. Symmetric. It is basically a 64-bit block cipher optimized for huge data caches which is more faster than DES. Key lengths vary in length from 32 to 448 bits.

f. Twofish It is developed by Bruce Schneier and his team. In the AES process, it is Round 2 algorithm. It is 128bit block cipher on 256, 192 and 128 bit keys. It is designed for more flexible and secure communication requirements. It is compatible for large microprocessors, dedicated hardware and 8-bit smart card microprocessors.

g. Camellia In 2000, it was developed by Nippon Telegraph and Mitsubishi Electric Corporation. It is basically a secret-key, block-cipher and has some features of with AES. It is compatible for software as well as implementations on 8 and 32 bit processors.

h. MISTY1 It a block cipher designed at Mitsubishi Electric Corporation. It uses 128 bit key on 64 bit blocks. It is used for software and hardware and is challenging to linear and differential cryptanalysis.

i. Secure and Fast Encryption Routine (SAFER) It is used for software implementation. Same has been given in versions for 128, 64 and 40 bit keys.

j. KASUMI It was designed by Universal Mobile Telecommunications System. Basically a block cipher with 128bit key. It is

utilized for integrity and confidentiality algorithm for signaling data and message content for cellular communications systems.

k. SEED It is a standard encryption algorithm in South Korea which was developed by the KISA. It is a cipher 128bit blocks on 128 bit keys.

l. ARIA A South Korean algorithm utilizing 128bit block cipher on 256, 192 and 128 bit keys.

m. CLEFIA The CLEFIA algorithm published in 2007 by Sony Corp. It utilizes 128bit block cipher with 128, 192, and 256 bits of key lengths. It has high performance in light weight hardware and softwares.

n. SMS4 It is wireless LAN authentication and Privacy Infrastructure used in Chinese National Standard. It is basically a 128bit block cipher on 128-bit keys.

o. Skipjack SKC scheme was proposed for Capstone. Skipjack is a block cipher on 80bit key.

3.7.2 PKC (Public Key Cryptography) This utilizes one key for encryption and another for decryption. It is a momentous development in the field of cryptography in last 400 years. Modern PKC was developed by Professor Martin Hellman of Stanford University and a graduate student Whitfield Diffie in 1976. The paper explained the crypto system engaging in a safe communication over unreliable communications medium without sharing secret key. Generic PKC employs two keys that are mathematically related in which knowledge of one key does not allow to determine the other key. One key is used to encrypt the plaintext and the other key is used to decrypt the ciphertext. This approach is known as asymmetric cryptography as pair of keys is required. In PKC, one is the public key and other is the private key which is not revealed to each other. PKC being used today includes:

a. RSA It is the first common PKC known by three Ronald Rivest, Adi Shamir and Leonard Adleman. It utilizes many applications for digital signatures, key exchange or encryption of small data blocks and software products.

b. Diffie-Hellman Diffie and Hellman made another algorithm. DH is not used for igital signatures/authentications but for only secret key exchange.

c. Digital Signature Algorithm It is specified by NIST's Digital Signature Standard is used for authentication of digital signature.

d. ElGamal It was made by Taher Elgamal. It is same as Diffie-Hellman used for key exchange.

e. Elliptic Curve Cryptography It is dependent on elliptic curves. ECC can give levels of security with small keys in comparison with RSA and other PKC methods. It was developed for hardware with less memory or computer power like PDAs and smartcards.

3.7.3 Hash Functions This function utilizes mathematical transformation to irreversibly encrypt message. It is also known as one-way encryption or message digests. In this fixed length hash value is calculated on plaintext and no key is used. It makes it very difficult contents or length of the plaintext for recovery. This algorithm gives a fingerprint digitally of a file's contents to ensure non alteration by intruder or viruses. These are used to encrypt passwords and provide integrity. Common Hash algorithms includes:

a. Message Digest (MD) algorithms It is a series of algorithms that gives 128 bit hash value.

b. Secure Hash Algorithm (SHA) Algorithm for NIST's Secure Hash Standard. SHA gives 160bit hash value and details five algorithms in the SHS.

c. RIPEMD It was developed by Hans Dobbertin, Bart Preneel and Antoon Bosselaers. It is used for 32 bit functions. It also includes RIPEMD128, 256 and 320.

d. HAVAL (Hash of Variable Length) It was developed by Zheng, J&J Seberry and Pieprzyk. It has many security levels. It can produces hash values of 256, 224, 192, 160 and 128 bits length.

e. Whirlpool It was developed by P.S.L.M. Barreto and V. Rijmen. It is a new function which acts on messages which are less than 256 bits length and gives 512 bits of message digest. It is different than SHA-1 and MD5, thus, preventing attacks as on hashes.

f. Tiger Developed by Eli Biham and Ross Anderson. It is made to run efficiently on 64-bit processors, secure and replaces SHA and SHA-1, MD4 and MD5 in other applications. Tiger/192 gives 192bit output and is attuned with 64bit architectures. Tiger/128 and Tiger/160 gives a hash of 128 and 160 bits lengths and is compatibility with other hash functions.

3.8 **TRUSTED MODELS**

Trust is required for secure use of cryptography. No system can be workable without trust although SKC ensures message confidentiality and hash codes ensure integrity. There are many trusted models by many cryptographic schemes. Following are the main trusted models:

a. Pretty Good Privacy (PGP) has own set of trusted public keys.

b. Kerberos is distribution of secret key utilizing trusted third party.

c. Certificates allow set of trusted parties for authentication.

3.9 **SECURITY TOOLS**

Tools used to obtain security are delineated below:

3.9.1 Encryption When data is difficult to apprehend and can be trivially achieved by authorized user, it is called encryption. Encryption is more difficult and many communication tools are used to weaker the encryption or to try backdoors for rapid decryption. Many governments allow backdoors for security purpose. Encryption would be secure If sufficiently powerful, correctly programmed and keys are not intercepted.

3.9.2 Steganography Stegnography is the hidden writing where data can not be seen amongst other harmless data. A watermark provides embedded information in picture data in such a way that it is not easy to search it unless known.

3.9.3 Identity based networks The possibility of malicious data on the internet is a danger to the own system as it is inherently unknown. Therefore, known identity based network replaces the unknown node. It is trustworthy as identity of senders as well as recipient is known.

CHAPTER 4

LITERATURE REVIEW

In this chapter, history including the past and the present scenario has been discussed in relation to the thesis work. Lot of papers has been written on the communication security related to different media. However, the specific and few known papers have been tried to be included in the forthcoming paragraphs. With the advancement of the work the research on the topic has expanded resulting in new inventions and modifications for the customized applications. Naval forces started utilizing high frequency for radio communications in World War I when few newly developed communications systems were in use. The high frequency band is shared by many foreign as well as domestic users. The sections scattered throughout the band are allotted for the military purpose. Naval requirements have also grown with passage of time like any other agency. Capacity of Navy's assigned band of HF spectrum has become strictly taxed. Therefore flourishing in field of this long range communication is in demand and requires enhancement with the development pace.

4.1 History

4.1.1 Green Hornet During World War II, Winston Churchill used famous system of secure communication called Green Hornet. In that he used to discuss prime matters with Franklin D. Roosevelt. Any eavesdropping in between would give distorted noise but the conversation was good at both ends. As confidentiality was vital, the location of the Green Hornet was known by Winston Churchill and its inventors. Same was kept in closet 'Broom Cupboard.' The working principle of Green Hornet was on one-time pad which is unbeatable even today.

4.1.2 Link 11 In 1980s, NATO, a new tactical message standard was provided on the improvement of Link 11. It produced a mission which specified a layered communication architecture and enhance data exchange.

4.1.3 Link 22 This provides beyond Line of sight communication. It connects air, surface, ground and subsurface based tactical data systems. It is used for the tactical data communication within the military units of the nations taking part in the exercise. It was to be utilized for war support and peacetime crises of allied warfare tasking and NATO. It has a mature communications security system developed by the addition of an encryption/decryption equipment in the system. Security of the transmission security was done by the use of frequency hopping radios.

4.2 **PAST**

4.2.1 DEVELOPMENT OF SPEECH ENCIPHERMENT This survey was carried out by N R F MacKinnon in 1980 which explains past and present principles of speech coding. The advent of digital logic systems and integrated circuit components is seen as a major turning point in the implementation of effective coding principles that could not previously be used satisfactorily. The problems of key generator integrity, synchronization, received voice quality and recognizability, channel bandwidth restrictions and the security offered by different systems are considered. The author concludes that in the immediate future high security speech encipherment systems will be of the digital output crypto-vocoder type, with audio bandwidth analogue output coders offering an increasingly secure alternative for the majority of applications. Digital output coders will continue to be used effectively in those applications where the communication equipment and transmission path have the necessary characteristics to carry low error rate digital signals. Advances in analogue to digital speech conversion providing acceptable quality at bit rates below 9.6 k bit/s should eventually enable a simple digital output coder to be as effective as a cryptovocoder for audio band high security applications.

4.2.2 AN ALTERNATIVE APPROACH FOR IMPLEMENTING A MULTIBAND VHF/UHF HANDLED RADIO WITH NARROWBAND SECURE VOICE The author of the paper were Grusell, Neuburger, Penny, Sullivan. The authors, in 1989, outlined a concept utilizing 2.4-kb/s LPC-10 linear predictive error correction coding and decoding , voice encoding, hybrid radio-frequency and digital modulation techniques in radio. It was achieved by a handheld radio which could operate in 12.5-kHz channels over the High and low VHF and UHF bands. This would achieve better communications results with more reliability at lower cost by use of a digital signal processor and microprocessor by an RF design. Continuously variable slope, encryption devices, delta modulation and Frequency modulation is used to implement secure voice digitally. Multiband operation is can be found by the use of interchangeable RF modules.

4.3 **PRESENT**

4.3.1 SPECTRALLY EFFICIENT FREQUENCY HOPPING SYSTEM DESIGN FOR WIRELESS NETWORKS This paper, in 2007, was written by Tongtong Li of Michigan State University which explains frequency hopping systems. The transmitter hops in pseudorandomally within available frequencies according to a algorithm and the receiver operates in synchronization with the transmitter's hopping pattern. A collision happens when more than one users transmit in same frequency band simultaneously in a multiple access systems. Two major limitations with conventional frequency hopping are strict requirement on frequency acquisition/synchronization and very low spectral efficiency due to inefficient utilization of the available bandwidth. In this paper, a new concept of collision free frequency hopping is given. Based on the OFDM framework and the secure subcarrier assignment algorithm, the proposed CFFH system can achieve high information capacity through collision free multiple access and can successfully resolve the strict synchronization limitation. At the same time, as each user still transmits through a pseudorandom frequency hopping scheme, CFFH can maintain the inherent anti jamming/interception security features of the conventional FH system.

The proposed CFFH scheme can be used for both civilian and military applications where secure high speed information transmission is needed.

4.3.2 HIGH ASSURANCE MULTIPLEXER TECHNIQUES FOR USE WITH SECURE DIGITAL COMMUNICATIONS Harris D., in Nov 2008, presented a survey which entails new tactical communications systems are often required to be able to support independent operations on several channels simultaneously where each channel may be operating at a different level of security classification. Maintaining the separation of these channels from a security integrity perspective is possible using a MSLS approach. By using this, communication paths are confined to single set of connected resources.

4.3.3 A SECURE RFID AUTHENTICATION PROTOCOL WITH LOW COMMUNICATION COST Gene Tsudik, in 2009, proposed an easy RFID authentication protocol (YA-TRAP) in which valid tag becomes incapacitated after exceeding the pre stored threshold value and is vulnerable to DOS attack. The scheme provides solution by allowing a tag to refresh its pre-stored threshold value and it forwards secure and provides resistance against replay, timing and tracking attacks. The reader uses authentication to keep the rogue tags out of the aggregate function.

4.3.4 HYBRID DS/FFH SPREAD-SPECTRUM It is the secure and robust transmission technique for communication in harsh environments. This paper was presented by Olama M.M, in 2011. Spread-spectrum modulation techniques have been adopted for many military communication systems for high data rates with link integrity even in the presence of interfering signals and multipath effects. A synergistic combination is a direct sequence spread spectrum signaling with the use of coordinated frequency hopping and time hopping modulation. It is generically dubbed hybrid spread-spectrum (HSS). A highly useful form of this transmission scheme for many types of command, sensing applications and control is the specific code related combination of standard DSSS modulation with "fast" frequency hopping, wherein multiple frequency hops occur within a single data-bit time. In this paper, detailed error-probability analyses are performed for a hybrid DS/FFH system over standard Gaussian and fading-type channels, progressively including the effects from wideband, partial band multi-user

interference, follow-on jamming and varying degrees of Rayleigh and Rician fading. Moreover, a simulation based study of the DS/FFH performance is performed and compared to several forms of existing standard DSSS and FHSS wireless networks. The parameter space of HSS is also explored to further demonstrate the adaptability of the waveform for varied harsh RF signal environments.

CHAPTER 5

SELECTION OF OPEN SOURCE SOFTWARES

For development of indigenous software for establishing Over The Horizon communication setup, open source softwares/specs and add-ons were utilized for specific module development. Same are explained in ensuing paragraphs.

5.1 SOFTWARE ENCRYPTION

For the development of software for encryption for use in radio link, the lead was taken from an open source software MT-63 which is a software used for extracting output from audio coded noise. The software PMSA LINK II has been developed for keyboard to keyboard modes while distributing the encoding of characters over several tones and long time period. It utilizes FEC error correction processes then ARQ. It is used for modulating and demodulating the noise signal received and transmitted via communication media. The software sends 64 tones in the 1 KHz bandwidth. These tones are bipolar phase shift keyed differentially at 10 baud. As the forward error correction code is 64 bit, therefore, throughput with FEC is about 100 WPM which is ten 7 bit ASCII characters/sec. The symbol rate is same as the symbol rate. There are three bandwidths which can be used i.e. 500, 1000 and 2 KHz. Baud rate and tone spacing can be halved or doubled. 1 KHz long interleave version is normally used for data sharing. The interleave doubling period improves the burst noise. Variable speeds are achieved through scaling although the lowest carrier frequency keeps constant at 500 Hz. This software spreads in the frequency domain (spectrally) and time domain (temporally). Encoded character is expanded on 32 sequential symbols to ensure time domain interferences and noise bursts. The character is also expanded spectrally by using tones across the transmission width. The disadvantage of this software is its heavy processing of data and utilization of more memory space in the computer. Moreover it transmits fewer characters in a less time frame.

5.2 USE OF ONE TIME PAD

One Time Pad is proven encryption, and if used correctly, then it is impossible to crack. The "pad" part of the name was referred with respect to the early implementations as a pad of paper which could be torn off and destroyed after utilization. The pad was contracted to a small size that a magnifier is required to view it. Therefore, this is best cryptosystem with theoretically perfect secrecy. In this, modular addition is done on each bit of plaintext with a character from a pad of secret random key of the same length as the plaintext and same results in cipher text. If the key is truly random and kept secret and it can not be used again then cipher text will be impossible to break or decrypt.

a. One Time Pad is a handy method of encryption which does not require assistance of a computer, both parties can do all work by hand. This was, therefore, important in the era before computer eras. However, same is considered useful in situations when no computer is held or no trustworthy system is available.

b. One-time pads keeps perfect secrecy within the environment and the parties must be able to depart from one another.

c. The one-time-pad can also be used for super encryption.

d. Quantum key distribution is mostly associated with the algorithm in OTP.

e. The OTP is normally taken by the stream ciphers.

5.3 USE OF DEFLATE

It is the combination of Huffman coding and LZ algorithm. It is used by deflat for a lossless data compression algorithm. It was designed by P Katz for second version of PKZIP archiving tool then onwards specified in RFC 1951. The original algorithm was patented and assigned to PKWARE. Deflate is implementable in a manner which was not covered by patents. This led to extensive application for compressing files, ZIP file

format and PNG image files. The stream consists of block series and every block is preceded by a 3 bit header which is delineated below:

a. “1 bit: Last-block in stream marker

b. 1: is the last block in stream

c. 0: there are more blocks to process after this one

d. 2 bits: Encoding method used for this block type

e. 00: a stored/raw/literal section between 0 and 65, 535 bytes in length.

f. 01: a static Huffman compressed block utilizing Huffman tree.

g. 10: a compressed block complete with the Huffman table supplied.

h. 11: reserved”

The compression is achieved by two steps:

a. Replacement and matching of duplicate strings with pointers.

b. Replacing of symbols with weighted, new symbols based on frequency.

5.3.1 Encoder/compressor During compression, the encoder chooses the time spent looking for matching strings. The gzip/zlib reference allows user to select from a sliding scale of speed of encoding versus compression level. Options range from 0 to 9 representing the capability of the reference implementation. Other deflate encoders produce a compatible bit stream capable of being decompressed by deflate decoder. Variations will be produced by differing implementations on final encoded bit stream. The focus with non zlib versions of an encoder is to produce an efficient compressed and reduced encoded stream.

5.3.2 Decoder/decompressor The decoding process which takes a deflate bit stream for decompression and produces original file or data is called inflating. Inflate implementation is optimized by predictable RAM usage for microcontroller embedded systems and decoding speed.

5.4 UTILIZATION OF ASCII CODES

For the transmission of raw data where data not in the encrypted form, ASCII keys are used. It is a character encoding scheme based on the English alphabets. These represent text in computers, communication equipment and devices using text. It includes definitions for 128 characters in which 95 are printable characters including the space and 33 are non-printing control characters and. Table of ASCII codes are given in Appendix II.

5.5 CODING

The code 'Walsh–Hadamard ' was known by an american and a french mathematician Joseph Leonard Walsh and Jacques Hadamard. This is applied in linear code over binary alphabet which maps length of messages to coded words. This means that it can transmit additional bit of information on a codeword but with complex construction.

5.6 DOT NET FRAMEWORK 4

The DotNet Framework is software designed by Microsoft that works on Microsoft Windows. The software gives language interoperability across several programming languages and has a large library. Common Language Runtime (CLR) is the program for DotNet Framework to function on a software environment. This software is an function of virtual machine providing services like management of memory, exception handling and memory. Dot Net framework is constituted by class library and the CLR. This software is used by own source codes and other libraries. Visual Studio developed by Microsoft is an integrated development environment especially for Dot Net

framework. The .NET Framework is a technology that supports utilization and processing the next generation of XML Web services and applications. It consists of the common language runtime and the framework class library. The common language runtime i.e. as memory management, remoting and thread management is the base of the .NET Framework. It enforces code accuracy promoting robustness and security. Concept of code management is a basic principle of runtime. The .NET Framework is developed to fulfill the under mentioned objectives to give code execution environment for :

a. Minimizing versioning conflicts and software deployment.

b. Safely execute codes which include code developed by an unfamiliar third party.

c. Elimination of the problems of performance related to script or interpreted environment.

d. To experience the developer for varying and dependable uses like window and web based applications.

e. Develop communication so that code of DotNet framework can be compatible/integrate with any other code of commercial standards.

5.7 **VISUAL STUDIO 2012**

Microsoft Visual Studio is IDE i.e, Integrated Development Environment used to develop interface applications of graphics and console in addition to web sites, web applications, windows application forms and web services in codes for all platforms supported by Microsoft. Visual Studio has feature of a code editor which supports IntelliSense as well as code refactoring. The integrated debugger functions as a machine level as well as source level debugger. Visual Studio supports numerous languages by means of language services allowing debugger/code editor to support any programming

language, so that language related services exist. The built in languages features has C/C++, C# , F# and VB.NET.

5.8 C-SHARP PROGRAMMING LANGUAGE

C-sharp is the first component oriented language in C/C++ family. It is next generation robust and durable software. It uses integrated document using XML and enables one stop programming. Same can be embedded in web pages. This software can integrated with Java setup and has no memory leak. The implementation is compatible with XML, SOAP, Net languages and DLL. C# has been planned to be modern, simple, object oriented and general purpose programming language.

CHAPTER 6

TECHNICAL DESCRIPTION OF SOFTWARE

The technical description of the developed software PMSA Link II along with its parameters have been discussed in this chapter. The application of the open source software and setting of operational parameters, codes and protocols have also been in cooperated in the delineated paragraphs.

6.1 SOFTWARE FEATURES

Link PMSA sounds like a roaring noise it transmits noise on HF media. Same was tested for marine environment which has harsh conditions as compared to ground though even. The input from keyboard is then encoded in 64 bits. It is worth mentioning that as the signal logic is able to lock within ±50 Hz frequency error therefore no tuning technique is done. The confidence on FEC is degraded upon mistuning. FFT techniques known as 'buckets' is used by the decoder and tracking logic tracks for frequency and timing frequency error. Differential carrier phase detection is used by the software to track phase changes due to ionosphere variations. The main features of this software are delineated below:

a. Although it is developed for Windows OS, however, can be scaled to any OS/device with minor adjustments to the codes.

b. It is low on hardware requirements

c. It is hardware friendly and uses 5Mb memory usage.

d. Allows message analysis (give reports about message length, estimated transmission time, sending time, receiving time, memory usage)

e. Full duplex radio

f. Easy to use visual user interface

g. Allows to send messages by different techniques

h. Allows encrypted messages, compressed messages, raw messages and emergency alert messages.

i. New encoding schemes can be easily by doing few additions to code so as to update this radio functionality.

j. Works on frequencies 500Hz, 1000Hz and 2000Hz.

k. Can perform both in-memory processing and file based processing for the transmitted signal.

6.2 **PROTOCOL**

The protocols are manually controlled and unconnected asynchronous symbols with Forward Error Correction. The 64 PSK tones having spaces of 1/64th of bandwidth.

6.3 **CODING AND CHARACTER SET**

The ASCII-128 user interface is related with 64 tones through a Walsh-Hadamard function and utilizes an interleave to expand each character in 64 symbols. Character mapping is done by interleave and coding function. The ASCII characters which can be transmitted through PMSA LINK II are appended at Appendix III. Three modes are scaled in all dimensions includes baud rate, typing speed, spacing and two interleaver

options. One deficiency of the mode is toughness that is compromised with the short interleaver and delay between overs is long with the long interleavers.

6.4 **DATA TRANSMISSION SPEED**

PMSA LINK has three transmission speeds based on the band width used:

a. At 500 Hz, default message takes 25.4 seconds to transmit

b. At 1000 Hz, default message takes 12.706 seconds to transmit

c. At 2000 Hz, default message takes 6.359 seconds to transmit

The transmission statistics are attached as Appendix IV. In addition to the bandwidth, there are two choices for the Interleave used in the Walsh Forward Error Correction scheme integral :

a. Long interleave

b. Short interleave

The following table combines the options above and shows how long it takes for the interleaving to complete sending one character. Each character is sent on each of the tones (0 to 63) and spaced in time, This scheme allows for 16 of the 64 copies of each of the characters to be received incorrectly but still have the actual character come through without error.

BANDWIDTH	INTERLEAVE	CHARACTER RATE	TIME FOR 1 CHARACTER
500Hz	Long	5 char/sec	12.8m/sec
500Hz	Short	5 char/sec	6.4m/sec

1000Hz	Long	10 char/sec	6.4m/sec
1000Hz	Short	10 char/sec	3.2m/sec
2000Hz	Long	20 char/sec	3.2m/sec
2000Hz	Short	20 char/sec	1.6m/sec

Table: Character Rate w.r.t Bandwidth

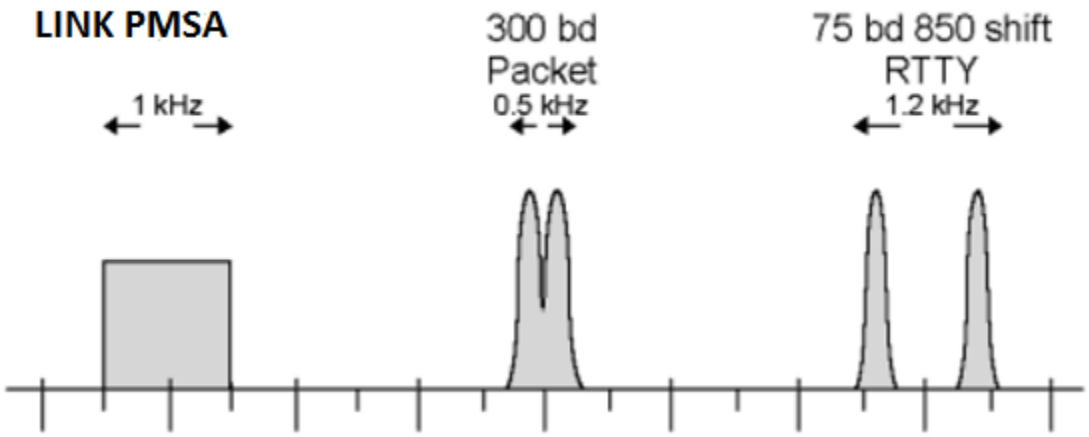
Decoding of 64 signals BPSK is like decoding PMSA LINK II. The problems were faced in determination of the following:

a. The offset frequency on transmission.

b. Frequency differences of sound cards.

6.5 **BANDWIDTH**

LINK PMSA II has 64 tones and its transmission is 1 KHz. It has sharp edges as it can accommodate two transmissions in width of SSB transmission. The bandwidth below half the of a SSB transmission.



6.6 RECOMMENDED FREQUENCIES

Frequencies mentioned below are considered for optimum operations with software

LINK PMSA:

1822, 1838, 3580, 3590, 3635, 7035, 7037, 10140, 10145, 14106, 14109, 14114, 18100, 18105, 21130, 24925, 28130 KHz

Successful Trials on 1000 KHz upto 180NM have been achieved.

6.7 TECHNIQUE USED

The cryptographic technique used in the software is Secret Key Cryptography (SKC) in which a single key is used for both encryption and decryption. The software is based on the scheme called Rijndael. The algorithm can use a variable block length and key length; the latest specification allowed any combination of keys lengths of 128, 192, or 256 bits and blocks of length 128, 192, or 256 bits. The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the plaintext into the ciphertext. The number of cycles of repetition are as follows:

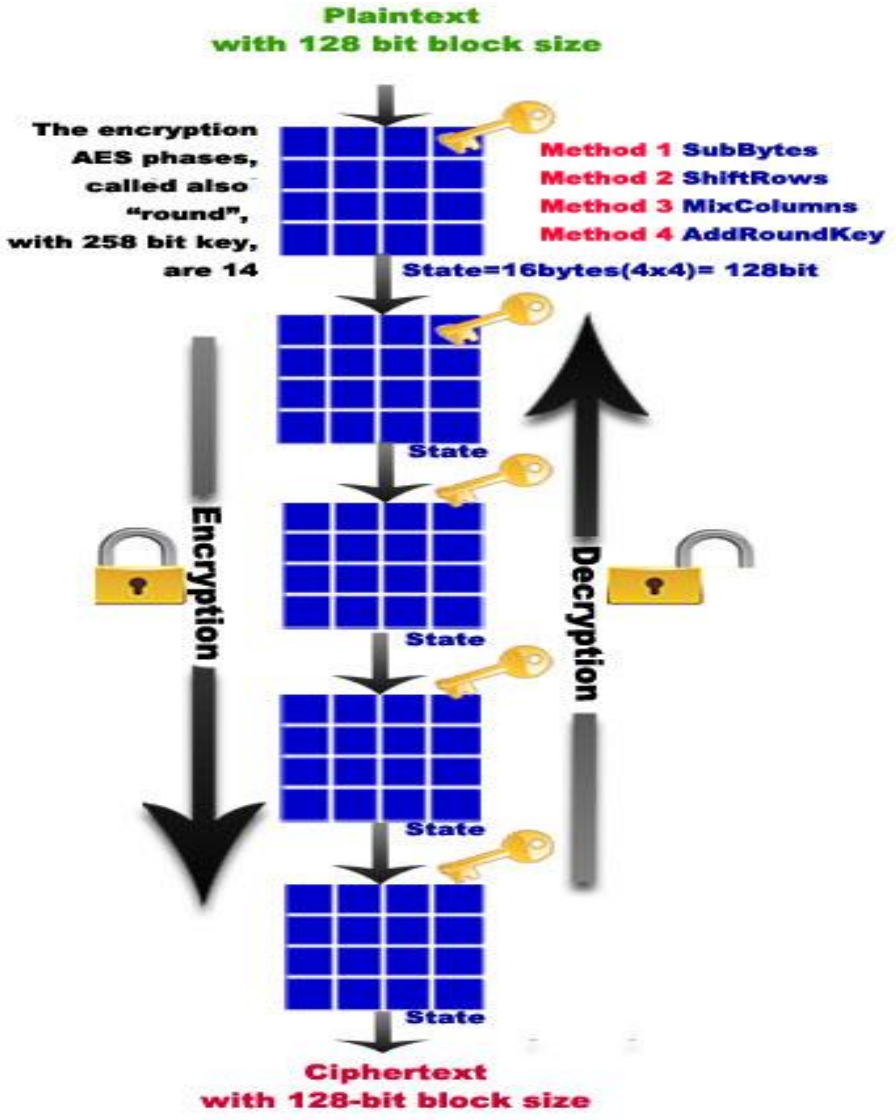
- 10 cycles of repetition for 128-bit keys.
- 12 cycles of repetition for 192-bit keys.
- 14 cycles of repetition for 256-bit keys.

Initial Round

  - AddRoundKey—each byte of the state is combined with the round key using bitwise xor.
- Rounds
  - SubBytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.

- ShiftRows—a transposition step where each row of the state is shifted cyclically a certain number of steps.
- MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
- AddRoundKey

- Final Round (no MixColumns)
  - SubBytes
  - ShiftRows
  - AddRoundKey



Moreover, One Time Pad was been used in other mode. In this, modular addition is done on each bit of plaintext with a character from a pad of secret random key of the same length as the plaintext and same results in cipher text. If the key is truly random and kept secret and it can not be used again then cipher text will be impossible to break or decrypt.

6.7.1 **AES Pseudocode**

```
Cipher (byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])
begin
byte state[4,Nb]
state = in
AddRoundKey(state, w)
    for round = 1 step 1 to Nr-1
    SubBytes(state)
    ShiftRows(state)
MixColumns(state)
    AddRoundKey(state, w+round*Nb)
  end for
   SubBytes(state)
ShiftRows(state)
  AddRoundKey(state, w+Nr*Nb)
```

```
  out = state
end
```

6.7.2 OTP Pseudocode

Encryption

```
begin
 variable ciphertext
   for round = plaintext begin to plaintext end
ciphertext += (plaintext + key) MOD  alphabet length
  end for
  return ciphertext
end
```

Decryption

```
begin
 variable plaintext
   for round = ciphertext begin to ciphertext end
    plaintext += (ciphertext - key + alphabet length) MOD alphabet length
  end for
  return plaintext
end
```

CHAPTER 7

HARDWARE SETUP REQUIREMENTS

The hardware requirements for the conduct of thesis have been explained in detail for application of developed software. Effective data transmission in both directions i.e. transmission and reception through PMSA Link II software for digital data transmission mode requires following:

a. HF Communication Equipment

b. Computer

c. PMSA LINK II Software

d. Hardware Interface

7.1 HF COMMUNICTION EQUIPMENT

The HF equipment to be linked with LINK PMSA II software had following options for interfacing with the computer:

a. Audio Input

b. Audio Output

c. Push To Talk circuit

Following three types of HF sets were made available and which could be linked via interface cable for data transmission:

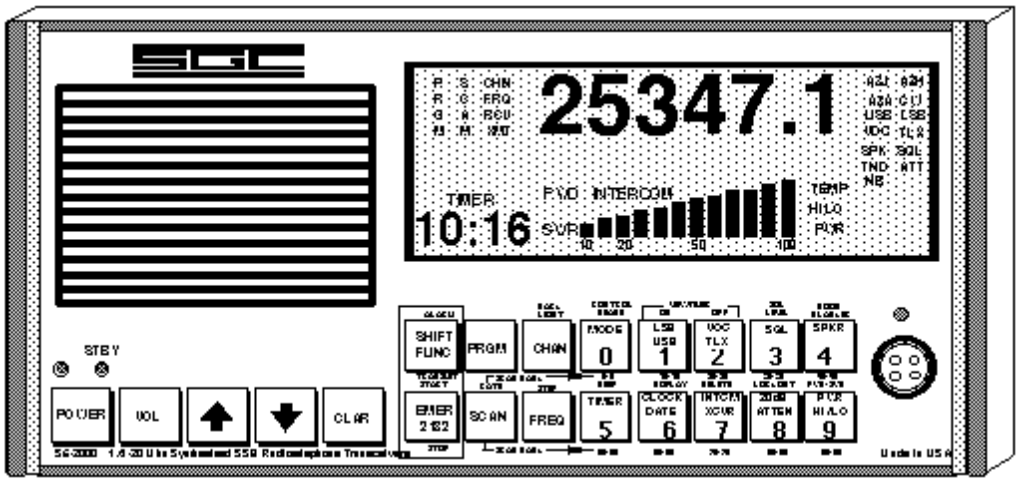
a. HF TX/RX SGC-2000

b. HF TX/RX MICOM 2E

c. HF TX/RX CODAN NGT

7.1.1 HF TX/RX SGC-2000

Amongst the three sets, HF TX/RX SGC-2000 was successfully interfaced with software with the computer. SG-2000 is a high performance, microprocessor controlled multi mission HF SSB radio designed to meet the needs of marine, commercial, paramilitary, and amateur radio users. It was conceived by SGC President Pierre Goral and the SGC Engineering Staff. It covers a frequency range of 1.6-30 MHz with a power output of 150 Watt. The SG-2000 also benefits from SGC's expertise in microprocessor design, developed as the company evolved its line of fully automatic antenna couplers. The front panel of the equipment is shown below:



The connector J301 at the back of the set provides the above mentioned connection option as shown in Figure.

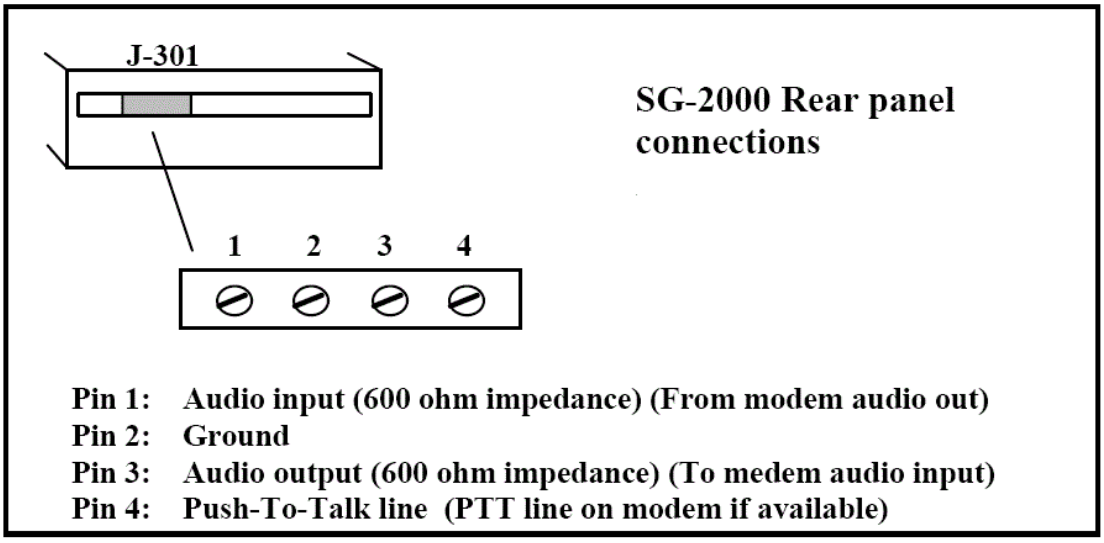


Figure : SGC 2000 Connections

7.2 **COMPUTER**

Computer Core 2 Duo with minimum 512MB RAM and Windows Vista or higher is considered suitable for good operation. In addition, the computer should have sound card with driver properly installed on the computer. PMSA Link II software uses speaker jack connection and microphone jack connection on the CPU for connection of input/output audio to the computer and serial port for the connection of DB-9 connector for Push to talk.

a. A computer with Windows Vista or higher.

b. A reasonably fast processor at least 500 MHz Pentium or above.

c. 32 bit sound card that works with Windows i.e drivers properly installed.

7.3 **HARDWARE INTERFERENCE**

Interface interface in a special case has been fabricated to link HF set with computer for data transmission and reception. Hardware interface consists of following three main connections:

a. Microphone jack, for connection of radio set audio output to the computer microphone port for receiving encoded audio signal.

b. Speaker jack, for connection of radio set input to the computer speaker port for transmitting audio signal.

c. DB-9 connector for connection of radio set PTT to the computer serial port for switching it between transmission and reception.

d. A small circuit to control PTT of the radio set with the computer serial port output from DB-9 RTS.

An interface circuit is developed to link HF transceiver with the computer. Transmitter is controlled by a signal from DTR pin 4, serial port and COM1 to COM4. The circuit which is used for PTT is a 10k base series resistor with an NPN open collector transistor. It has a shunt diode. Parts of interface are delineated below:

a. Audio input line for Reception

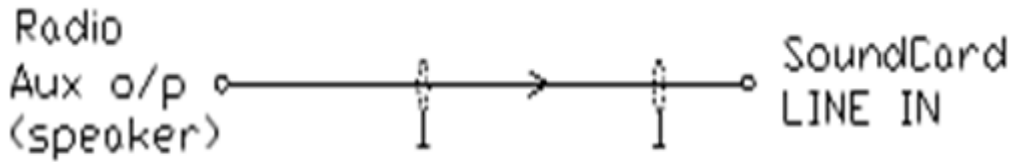
b. Audio output line for Transmission

c. PTT circuit

d. Serial Port connector (DB - 9)

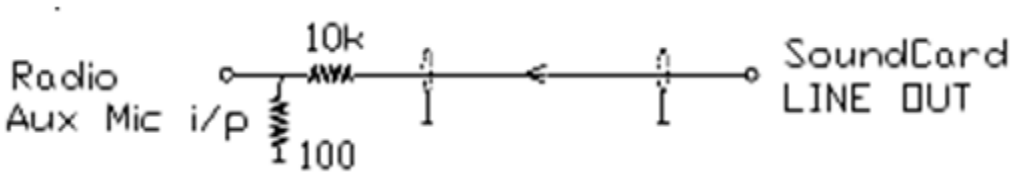
7.4 **AUDIO INPUT LINE**

A simple single pair copper cable is used for audio line input from HF set. Picture shown below shows the construction of the audio input cable.



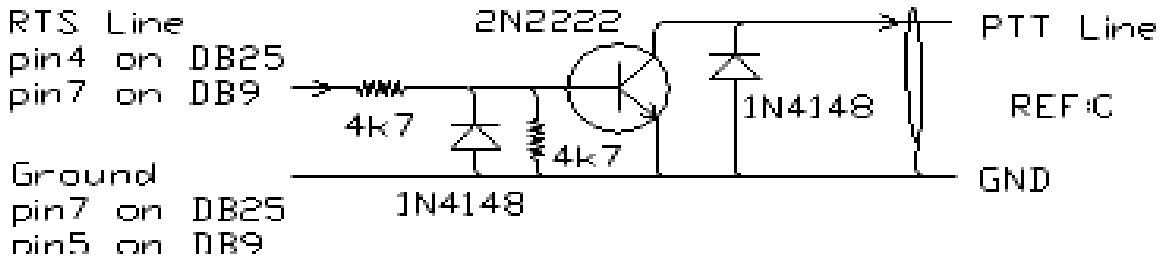
7.5 **AUDIO OUTPUT LINE**

A simple single pair copper cable is used for audio line output to the HF set. Picture shown below shows the construction of the audio input cable.



7.6 **PTT CIRCUIT**

A small circuit is designed for switching of HF Set between Transmission and Reception. Transistor 2N2222 NPN transistor has been used for switching Push to talk PTT from RTS signal from Pin No 4 of serial port through DB-9 female adapter. Detail circuit diagram of fabricated PTT circuit is shown below.



CHAPTER 8

TRANSMISSION AND RECEPTION MODULES

This chapter explains the features of the transmission and reception modules of the developed PMSA LINK II software.

8.1 TRANSMISSION MODULE

For transmission, the PC Sound card speaker or line output is connected with auxiliary audio input to the transceiver via interface module. The PC sound card is configured for proper output of the signal. Thus, it transmits noise to the transreciever which subsequently rides on HF waves at sea for reception onboard. The text written can be seen on the transmitter module of the software giving time of transmission as well. Upon successful transmission of the message, time of message transmitted along with confirmation of the sent message is seen on the screen. In addition to plain or raw text, for AES, 128, 192 and 256 bits options can be used and same parameters are to be configured on reception side. Moreover, for One Time Pad option can also be exercised. The transmitter module consists of main received text box, configuration, send, analyze and type of encryption buttons. The main text box transmits all the text transmitted by the sender. The send button is used for transmission of the message from the sender side. The configuration button gives the parameters on which the messages are transmitted. The messages can be removed from the screen through “clear text” or “flush” options. The “configuration” button is very important for the software as it contains all the parameters within. The analysis button gives the report of original message length, message verification, estimated transmission time and estimated memory usage.

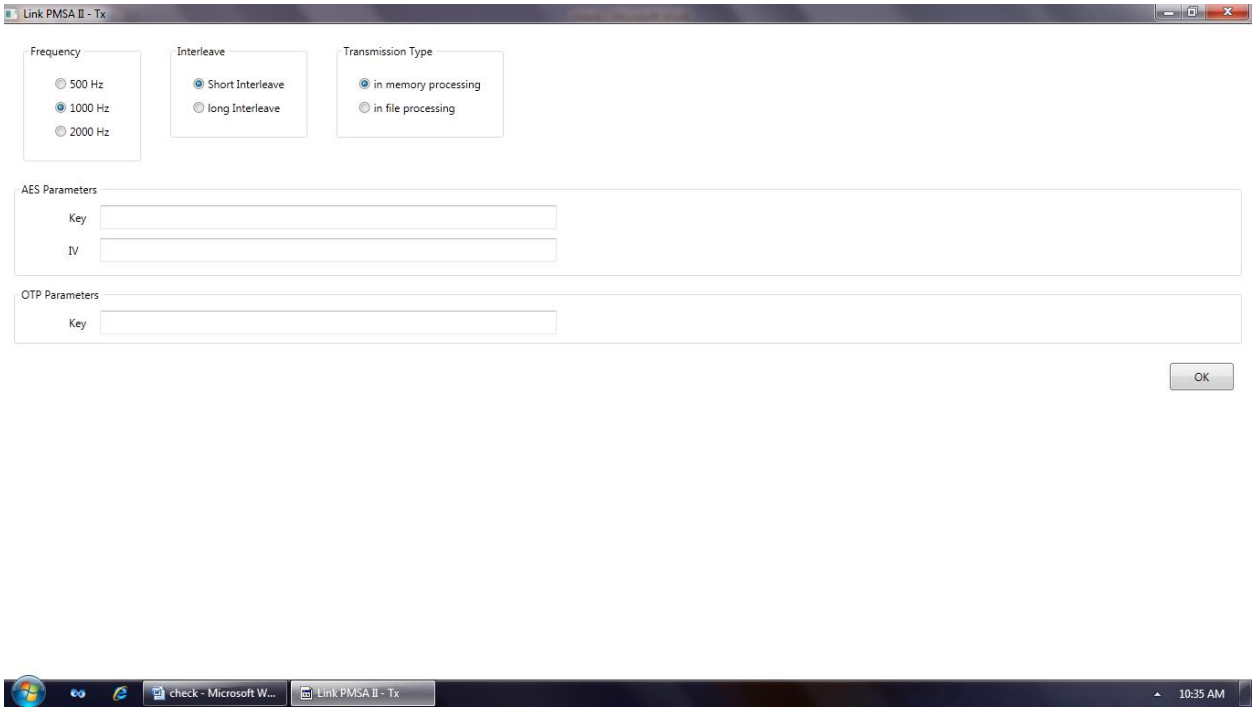
The software basically transmits the messages in 3 modes. These are delineated below:

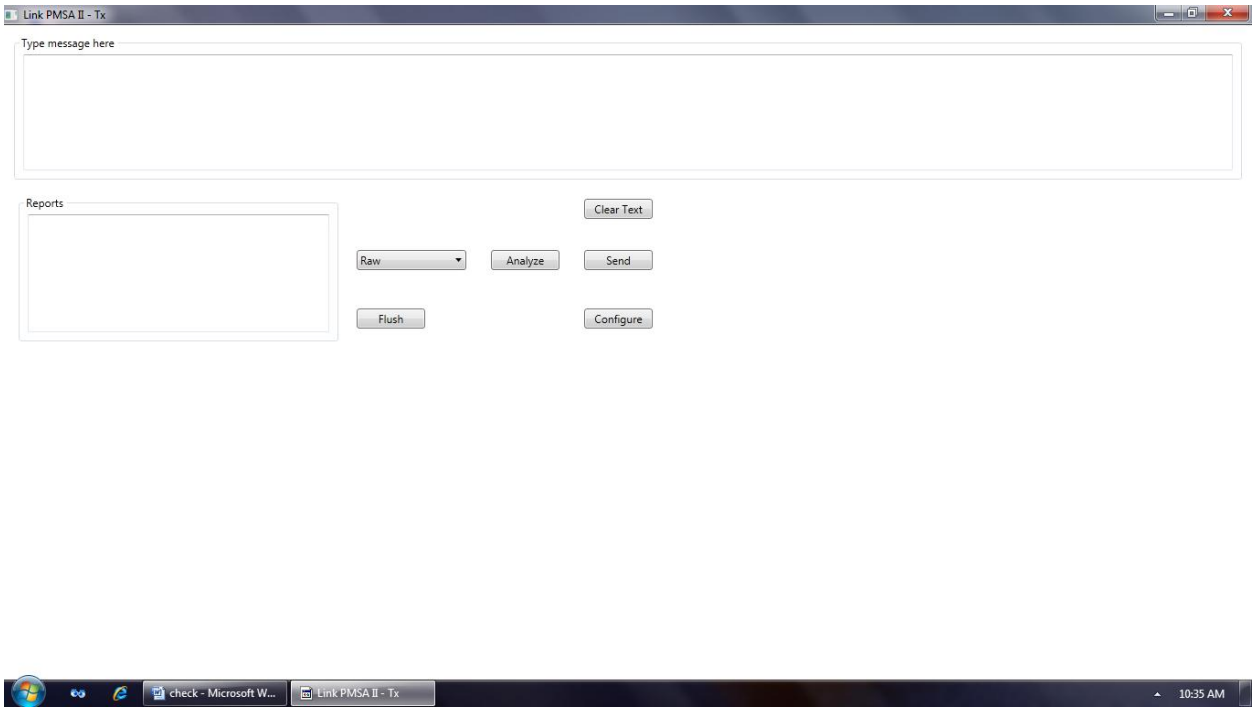
Mode 1 -------- Plain Text

Mode 2 -------- AES Cypher

Mode 3 --------- OTP

The messages can, therefore, be received using three of the modes mentioned above. However, the frequency, integration and interleave parameters can be altered for reception. The pictures of the same are delineated below:





8.1.1 **PSEUDO CODE FOR TRANSMITTER**

The pseudo code for the transmission module is delineated below:

begin

Initialize

Run tx configuration

Tx

Transmit (message, encoding, tx configuration)

[

Tx -> Transmit

- Set audio rate
- Initialize (message)

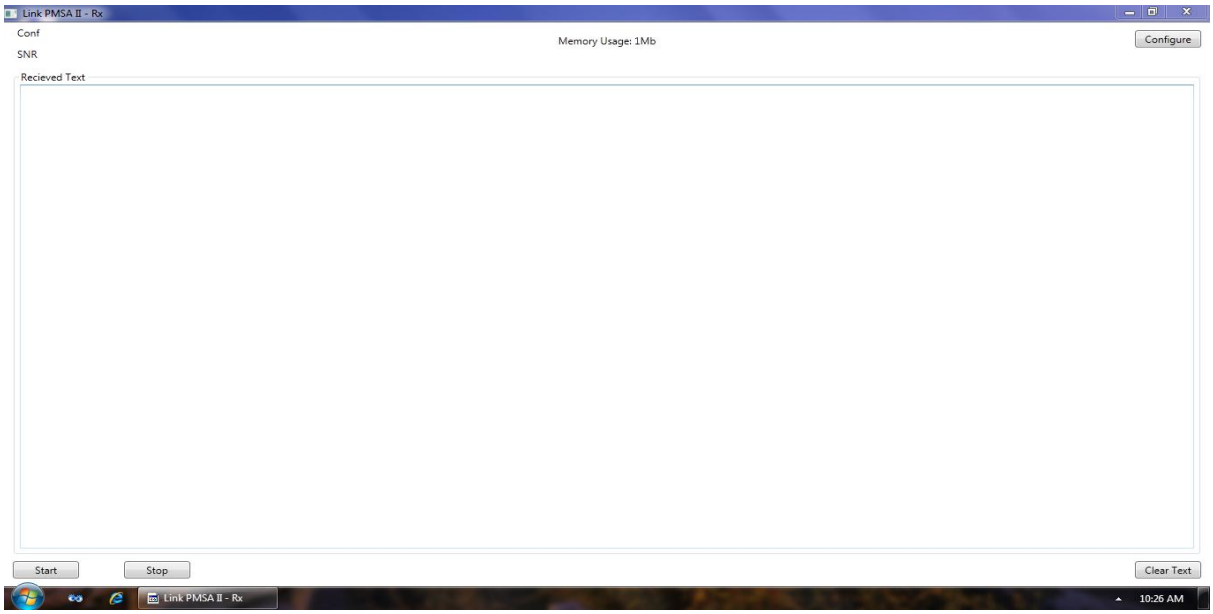
- Sendmessage (encoding)
- Flush memory

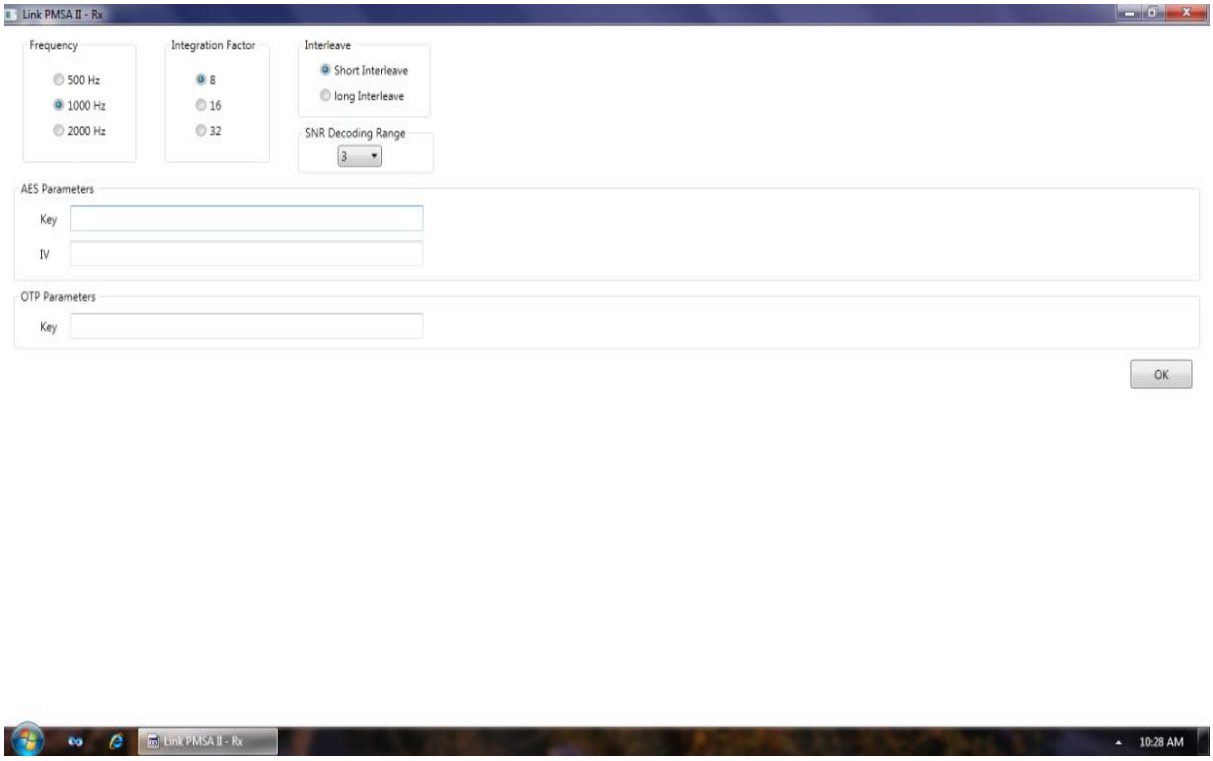
]

end

8.2 **RECEPTION MODULE**

An audio source of HF set is required to bond audio received into the computer sound card line input or microphone. Upon wiring of audio output from the receiver to the PC sound card input through the interface module, a noise scrolling will be heard from the PC through PMSA LINK II software screen. Text message will be seen on the receiver module of the software. The reception module consists of main received text box, sound to noise ratio, confidence, start/stop buttons and configuration buttons. The main text box receives all the text transmitted by the sender. The start/stop button is make the reliever ready for the initialization and reception of messages. The configuration button gives the parameters on which the messages is transmitted and subsequently received. The memory utilized in the process is also displayed. The messages can be removed from the screen through “clear text” option. The “configuration” button is very important for the software as it contains all the parameters within. The software basically receives the messages in 3 modes. The messages can, therefore, be received using three of the modes mentioned above. However, the frequency, integration and interleave parameters can be altered for reception. The pictures of the same are delineated below:


Link PMSA II - Rx
Conf
SNR
Memory Usage: 1Mb
Configure
Recieved Text
Start
Stop
Clear Text
Link PMSA II - Rx
10:26 AM


Link PMSA II - Rx
Frequency
500 Hz
1000 Hz
2000 Hz
Integration Factor
8
16
32
Interleave
Short Interleave
long Interleave
SNR Decoding Range
3
AES Parameters
Key
IV
OTP Parameters
Key
OK
Link PMSA II - Rx
10:28 AM

8.2.1 **PSEUDOCODE FOR RECIEVER**

The pseudo code of receiver is delineated below:

begin

Initialize

- Run rx configuration
- Rx
  - Receive (noise)
  - Return message

[

rx -> Receive

- Calibrate audio rate
- Initialize (noise)
- getmessage (decoding)
- Flush memory

]

end

CHAPTER 9

IMPLEMENTATION

9.1 IMPLEMENTATION MODEL OF PROPOSAL

This chapter covers the tests and trials conducted first in the laboratory and then onboard ship for practical implementation of the thesis at Pakistan Security Agency premises. Whole of setup of software and hardware was tested and all loopholes were cleared stepwise. Same are delineated in the ensuing paragraphs.

9.2 SIMULATED RESULTS

After development of the PC based software by taking help from open source softwares/modules, interface for HF communication equipment and PC based software was setup in the laboratory. The software was tested for all three modes i.e for Plain text, AES and OTP. Moreover, different parameters of interleave, frequency and transmission types was adapted. All the hiccups were cleared stepwise as and when the hardware and software problems of settings and developing were faced. Overrall the results went successful. One of the results of the simulated transmission and reception is attached as Appendix V.

9.3 ONBOARD RESULTS

After successful trials in the laboratory, the setup was tested onboard the ship i.e Corvette PMSS VEHDAT and the Headquarters Pakistan Maritime Security in harbour on 10 Jan 13 at shore as well on 21 Jan13 at sea. Secure communication upto 180NM

was tested successfully in all three modes with different parameters. The results of the same are attached as Appendix VI.

9.4 **STATISTICS**

The statics of the tests carried out onboard ship are delineated below:

a. A total of 50 messages were transmitted through the developed software during implementation phase at different occasions from sea as well as shore in which the garble in 3 of the messages was observed. Therefore, almost 5% probability of error was observed.

b. Cyphered text is almost twice in the size as of the plain text.

c. The transmission is time is reduced with the increase of frequency within the band.

CHAPTER 10

CONCLUSION, FUTURE WORK AND RECOMMENDATIONS

10.1 **CONCLUSION** This thesis work has provided high performance and reliable communication setup at sea as well as at shore in order to maintain efficient encrypted transmission/reception of messages over a long range. The thesis presents a secure electronic link which has ensured message confidentiality, integrity, authenticity and non-repudiation. Moreover, public key infrastructure is configured with the open source tools and secure extension is implemented. This indigenous effort will help to utilize the signal transfer in a secure and reliable mode for military purpose. Present economic conditions of country demand indigenous and cost effective solutions for technical problems faced by defence forces in particular and other departments in general. . This thesis will meet an emerging need in HF communications for a relatively low cost, highly reliable yet flexible communications platform which would be suited to multiple control-point operations. It will be a step towards indigenization of secure communication technology for Pakistan Maritime Security Agency.

10.2 FUTURE WORK AND RECOMMENDATIONS

The future work and recommendations of subject OTH setup are delineated below:

a. This setup with other same or other communication equipment can be installed onboard Pakistan Navy ships as well and related fields.

b. The software can be optimized for more speed, crypto protocols, transfer of other file types and mediums.

c. Same setup can be used with compact devices like cell phones enabling it through java script especially on android phones for amateur/emergency use.

REFERENCES

1. Paul Harden (2005). "Solar Activity & HF Propagation". QRP Amateur Radio Club International. Retrieved 2009-02-22.

2. Radio-frequency identification ISO/IEC 14443-2 Radio frequency power and signal interface

3. ISO/IEC 14443-2:2001 Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 2: Radio frequency power and signal interface". Iso.org. 2010-08-19. Retrieved 2011-11-08.

4. Jeffrey S. Beasley; Gary M. Miller (2008). Modern Electronic Communication (9th ed.). pp. 4–5. ISBN 978-0132251136

5. "Amateur Radio Emergency Communication". American Radio Relay League, Inc.. 2008. Retrieved 2009-02-22.

6. D. P. Agrawal and Q-A. Zeng, Introduction to Wireless and Mobile Systems (2nd Edition, published by Thomson, April 2005) ISBN 978-0-534-49303-5

7. J.K. and K. Ross, Computer Networking (2nd Ed, Addison Wesley, 2003) ISBN 978-0-321-17644-8

8. Software Defined Radio: Architectures, Systems and Functions (Markus Dillinger, Kambiz Madani, Nancy Alonistioti) Page xxxiii (Wiley & Sons, 2003, ISBN 0-470-85164-3)

9. Gregory Staple and Kevin Werbach. "The End of Spectrum Scarcity". IEEE Spectrum. March 2004.

10. Aaron Swartz. "Open Spectrum: A Global Pervasive Network"

11. P. Johnson, "New Research Lab Leads to Unique Radio Receiver," E-Systems Team, May 1985, Vol. 5, No. 4, pp 6-7

12. P. Hoeher and H. Lang, "Coded-8PSK modem for fixed and mobile satellite services based on DSP," in Proc. First Int. Workshop on Digital Signal Processing Techniques Applied to Space Communications, ESA/ ESTEC, Noordwijk, Netherlands, Nov. 1988; ESA WPP-006, Jan. 1990, pp. 117-123.

13. Mitola III, J. (1992), Software radios-survey, critical evaluation and future directions, pp. 13/15 to 13/23, doi:10.1109/NTC.1992.267870, ISBN 0-7803-0554-X

14. First International Workshop on Software Radio, Greece 1998

15. RJ Lackey and DW Upmal, "Speakeasy: The Military Software Radio", IEEE Communications Magazine, May 1995.

16. Youngblood, Gerald (July/Aug. 2002), "A Software Defined Radio for the Masses, Part 1", QEX (American Radio Relay League): 1–9

17. Youngblood, Gerald (Sept/Oct 2002), "A Software Defined Radio for the Masses, Part 2", QEX (American Radio Relay League): 10–18

18. Youngblood, Gerald (Nov./Dec. 2002), "A Software Defined Radio for the Masses, Part 3", QEX (American Radio Relay League): 1–10

19. Youngblood, Gerald (Mar/Apr 2003), "A Software Defined Radio for the Masses, Part 4", QEX (American Radio Relay League): 20–31

20. Radio and Electronic Engineer, Volume 50, issue4, April 1980, p. 147 – 155

21. Gary C. Kessler 17 July 2012

22. Bellare, Mihir; Rogaway, Phillip (21 September 2005) Introduction to Modern Cryptography. p. 10.

23. AJ Menezes, PC van Oorschot, and SA Vanstone, Handbook of Applied Cryptography ISBN 0-8493-8523-7.

24. Introduction to Cryptography 89-656,Yehuda Lindell1,October 19, 2006

25. Military Communications Conference, 1988. MILCOM 88, Conference record. 21st Century Military Communications - What's Possible? 1988 IEEE

26. Wireless Algorithms, Systems and Applications, 2007. WASA 2007.

27. Military Communications Conference, 2008. MILCOM 2008. IEEE

28. Complex, Intelligent and Software Intensive Systems, 2009. CISIS '09

29. Military Communications Conference, 2011 - MILCOM 2011

30. Shannon, Claude (1949). "Communication Theory of Secrecy Systems". Bell System Technical Journal 28 (4): 656–715.

31. Miller, Frank (1882). Telegraphic code to insure privacy and secrecy in the transmission of telegrams. C.M. Cornwell.

32. David, Salomon (2007). Data Compression: The Complete Reference (4 ed) Springer. p. 241. ISBN 978-1-84628-602-5.

33. DEFLATE Compressed Data Format Specification version 1.3. IETF. May 1996. p. 1. sec. Abstract. RFC 1951. Retrieved 11 November, 2012.

34. ASCIIbetical definition. PC Magazine. Accessed 2008-04-14.

35. Audio pronunciation for ASCII. Merriam Webster. Accessed 2008-04-14.

36. Arora, Sanjeev; Barak, Boaz (2009), Computational Complexity: A Modern Approach, Cambridge, ISBN 978-0-521-42426-4, Zbl 1193.68112.

37. "Releasing the Source Code for the NET Framework". Archived from the original on 07 September 2010. Retrieved 15 September 2010.

38. "Description of Visual Studio 2010 Service Pack 1". Microsoft. Retrieved 2011-03-25.

39. *C# Language Specification* (4th ed.). Ecma International. June 2006. Retrieved January 26, 2012.

40. SG-2000 Manual©1995, SGC, Inc.

APPENDIX I

RADIO FREQUENCY SPECTRUM

The radio frequency spectrum is delineated below:

"Frequency	Wavelength	Abbreviation
3 – 30 Hz	10^4 – 10^5 km	ELF
30 – 300 Hz	10^3 – 10^4 km	SLF
300 – 3000 Hz	100 – 10^3 km	ULF
3 – 30 kHz	10 – 100 km	VLF
30 – 300 kHz	1 – 10 km	LF
300 kHz – 3 MHz	100 m – 1 km	MF
3 – 30 MHz	10 – 100 m	HF
30 – 300 MHz	1 – 10 m	VHF

300 MHz – 3 GHz	10 cm – 1 m	UHF
3 – 30 GHz	1 – 10 cm	SHF
30 – 300 GHz	1 mm – 1 cm	EHF
300 GHz - 3000 GHz	0.1 mm - 1 mm	THF”

APPENDIX II

ASCII CODES

ASCII codes are shown below:

"Binary	Oct	Dec	Hex	Abbreviation	Name
000 0000	000	0	00	NUL	Null character
000 0001	001	1	01	SOH	Start of Header
000 0010	002	2	02	STX	Start of Text
000 0011	003	3	03	ETX	End of Text
000 0100	004	4	04	EOT	End of Transmission
000 0101	005	5	05	ENQ	Enquiry
000 0110	006	6	06	ACK	Acknowledgment
000 0111	007	7	07	BEL	Bell
000 1000	010	8	08	BS	Backspace

000 1001	011	9	09	HT	Horizontal Tab
000 1010	012	10	0A	LF	Line feed
000 1011	013	11	0B	VT	Vertical Tab
000 1100	014	12	0C	FF	Form feed
000 1101	015	13	0D	CR	Carriage return
000 1110	016	14	0E	SO	Shift Out
000 1111	017	15	0F	SI	Shift In
001 0000	020	16	10	DLE	Data Link Escape
001 0001	021	17	11	DC1	Device Control 1 (oft. XON)
001 0010	022	18	12	DC2	Device Control 2
001 0011	023	19	13	DC3	Device Control 3 (oft. XOFF)
001 0100	024	20	14	DC4	Device Control 4

001 0101	025	21	15	NAK	Negative Acknowledgement
001 0110	026	22	16	SYN	Synchronous idle
001 0111	027	23	17	ETB	End of Transmission Block
001 1000	030	24	18	CAN	Cancel
001 1001	031	25	19	EM	End of Medium
001 1010	032	26	1A	SUB	Substitute
001 1011	033	27	1B	ESC	Escape
001 1100	034	28	1C	FS	File Separator
001 1101	035	29	1D	GS	Group Separator
001 1110	036	30	1E	RS	Record Separator
001 1111	037	31	1F	US	Unit Separator
111 1111	177	127	7F	DEL	Delete”

APPENDIX III

ASCII 128 USER INTERFACE

The ASCII-128 user interfaced via Walsh-Hadamard function is given below:

ASCII Non Printing Control Characters

“0.	NUL	Null	8.	BS	backspace	16.	DLE	data link escape	24.	CAN	Cancel
1.	SOH	start of heading	9.	HT	horizontal tabulation	17.	DC1	device control 1	25.	EM	end of medium
2.	STX	Start of text	10.	LF	line feed	18.	DC2	device control 2	26.	SUB	Substitute
3.	ETX	end of text	11.	VT	vertical tabulation	19.	DC3	device control 3	27.	ESC	Escape
4.	EOT	end of transmission	12.	FF	form feed	20.	DC4	device control 4	28.	FS	file separator
5.	ENQ	enquiry	13.	CR	carriage return	21.	NAK	negative acknowledge	29.	GS	group separator
6.	ACK	acknowledge	14.	SO	shift out	22.	SYN	synchronous idle	30.	RS	record separator
7.	BEL	Bell	15.	SI	shift in	23.	ETB	end of transmission block	31.	US	unit separator
									127.	DEL	Delete

ASCII Printable Characters

32.		48.	0	64.	@	80.	P	96.	`	112.	P
33.	!	49.	1	65.	A	81.	Q	97.	A	113.	Q
34.	"	50.	2	66.	B	82.	R	98.	B	114.	R
35.	#	51.	3	67.	C	83.	S	99.	C	115.	S
36.	$	52.	4	68.	D	84.	T	100.	D	116.	T
37.	%	53.	5	69.	E	85.	U	101.	E	117.	U
38.	&	54.	6	70.	F	86.	V	102.	F	118.	V
39.	'	55.	7	71.	G	87.	W	103.	G	119.	W
40.	(	56.	8	72.	H	88.	X	104.	H	120.	X
41.	)	57.	9	73.	I	89.	Y	105.	I	121.	Y
42.	*	58.	:	74.	J	90.	Z	106.	J	122.	Z
43.	+	59.	;	75.	K	91.	[	107.	K	123.	{
44.	,	60.	<	76.	L	92.	\	108.	L	124.	|
45.	-	61.	=	77.	M	93.	]	109.	M	125.	}
46.	.	62.	>	78.	N	94.	^	110.	N	126.	~
47.	/	63.	?	79.	O	95.	_	111.	O	127.	“

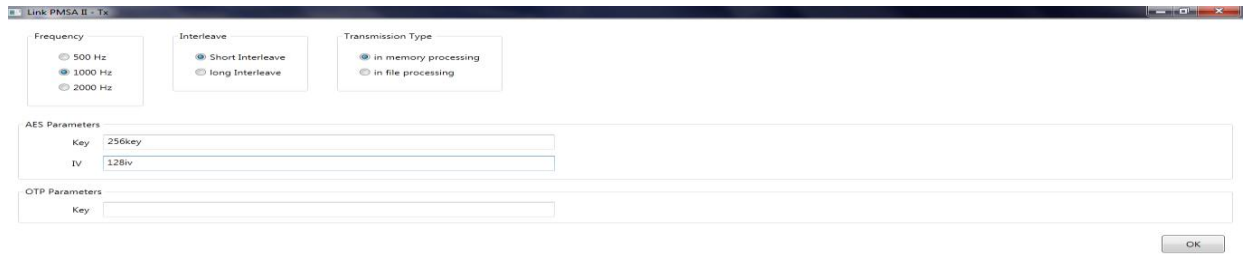
APPENDIX IV

	A	B	C	D
1	**frequency**	**500Hz**	**1000Hz**	**2000Hz**
2	**message length = 0**	25.4 sec	12.706 sec	6.359 sec
3	**message length = 1**	25.6 sec	12.806 sec	6.409 sec
4	**message length = 2**	25.8 sec	12.906 sec	6.459 sec
5	**message length = 10**	27.4 sec	13.706 sec	6.859 sec
6				
7	**Conclusions**	default message takes 25.4 seconds to transmit.	default message takes 12.706 seconds to transmit.	default message takes 6.359 seconds t transmit.
8		each new char/symbol adds a time of 0.2 seconds to the default time.	each new char/symbol adds a time of 0.1 seconds to the default time.	each new char/symbol adds a time of 0.05 seconds to the default time.
9	**Note:** encoded message may have twice the length of the original message so calculate properly or reference the software.			
10	**Note:** this is the estimated time without considering delays caused by software, hardware or transciever malfunctioning.			

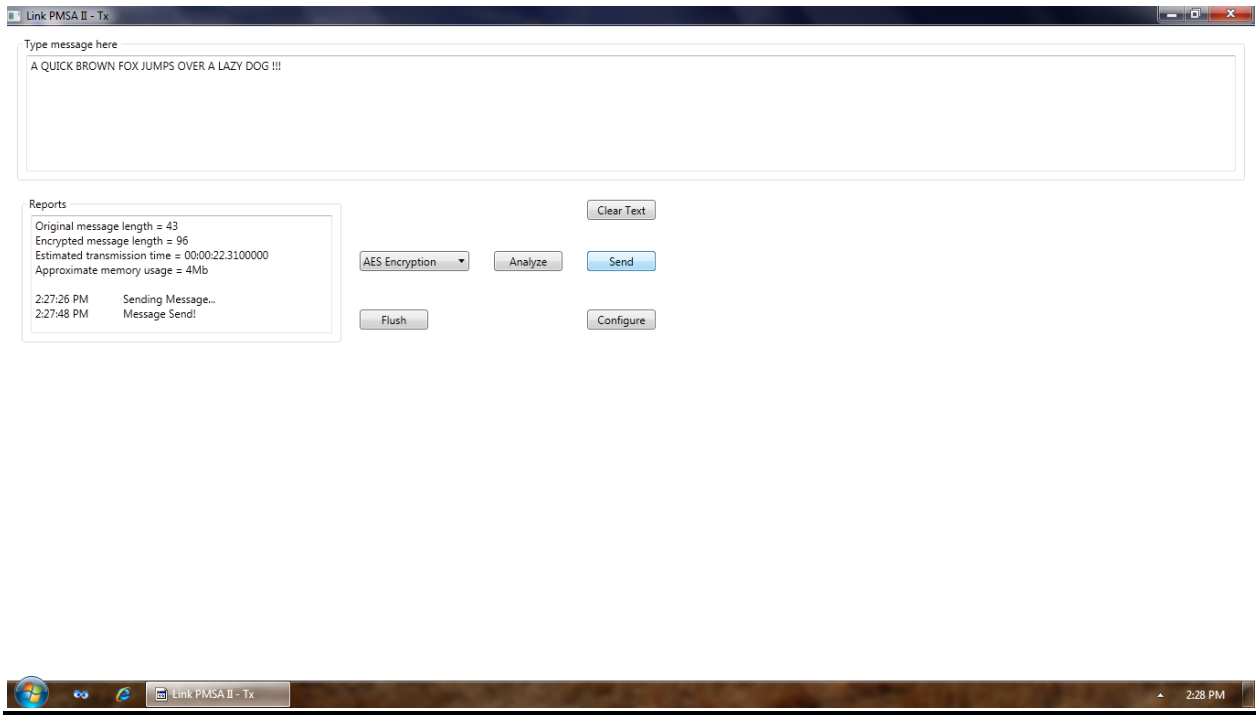
APPENDIX V

LAB TEST RESULTS OF TRANSMISSIONS AND RECEPTIONS

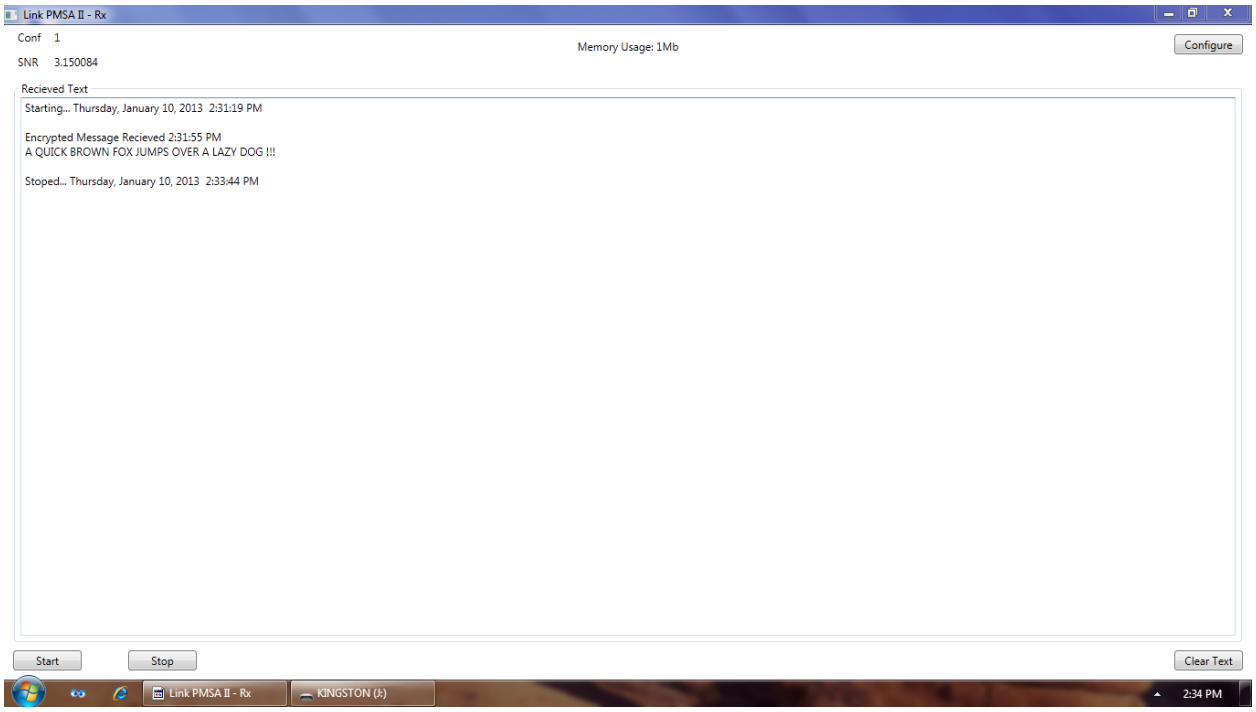
PARAMETERS FOR TRANSMISSION AND RECEPTION



TEST MESSAGE TRANSMISSION



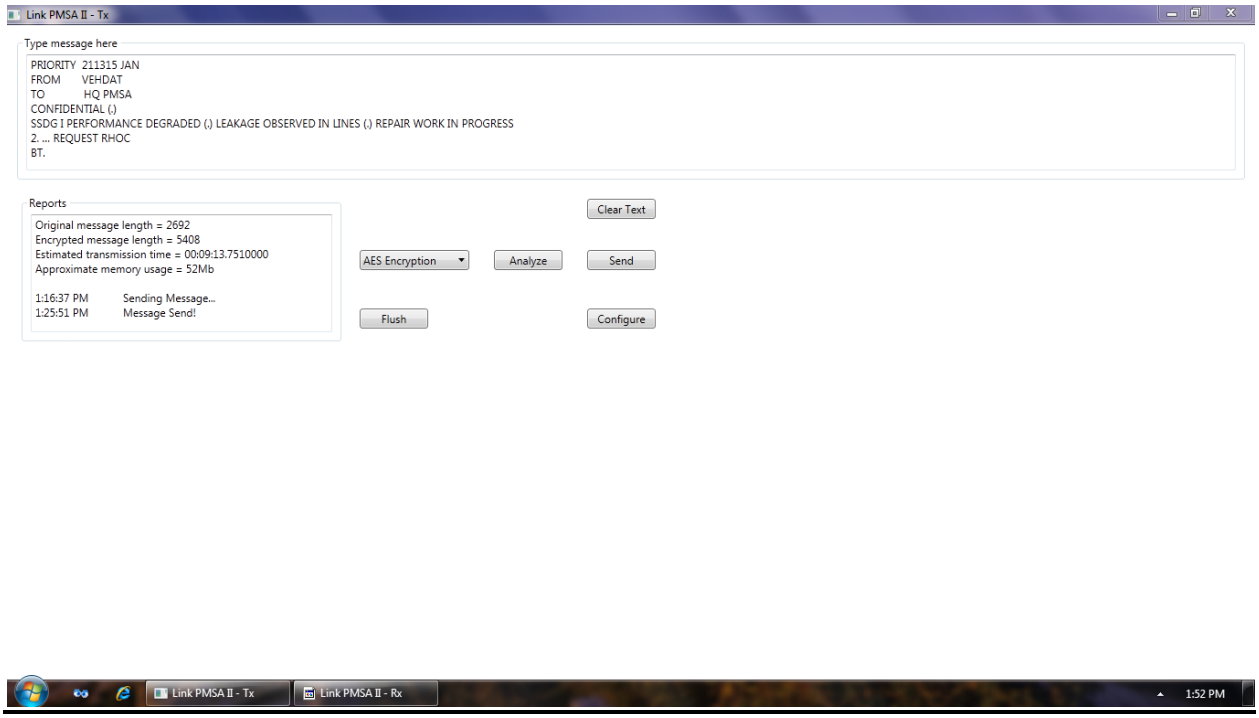
TEST MESSAGE RECEPTION



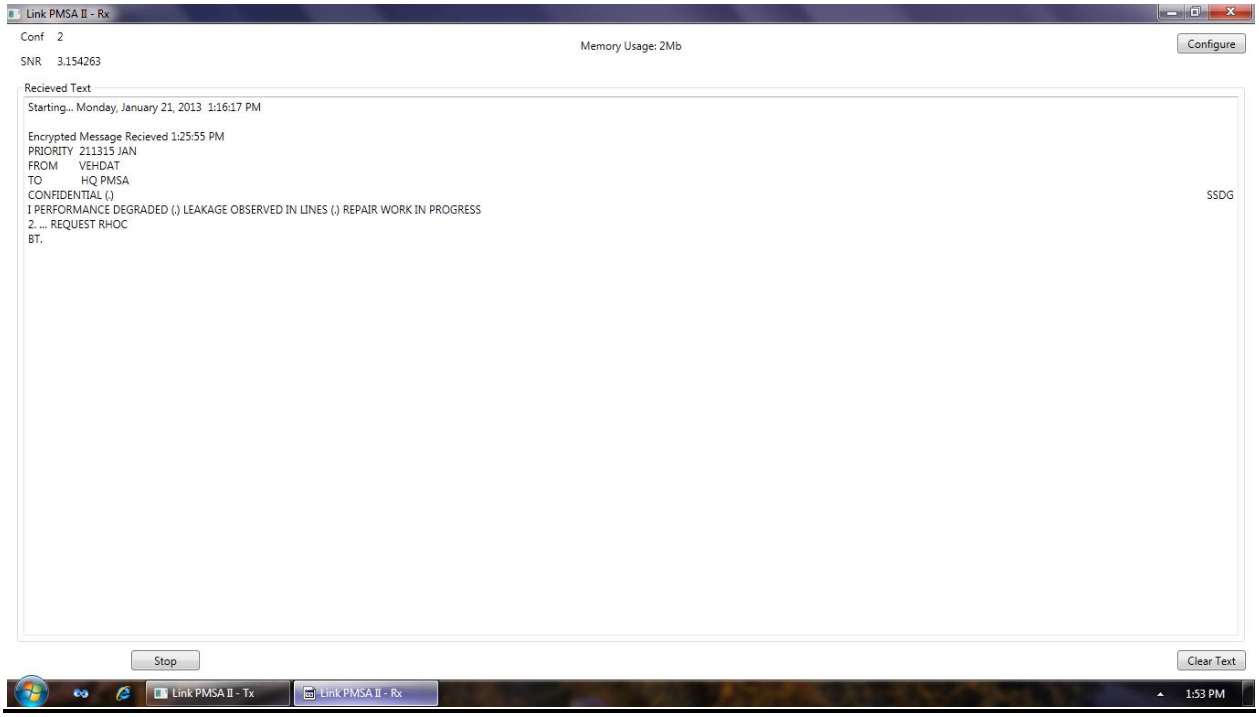
APPENDIX VI

ONBOARD TEST RESULTS OF TRANSMISSION AND RECEPTION

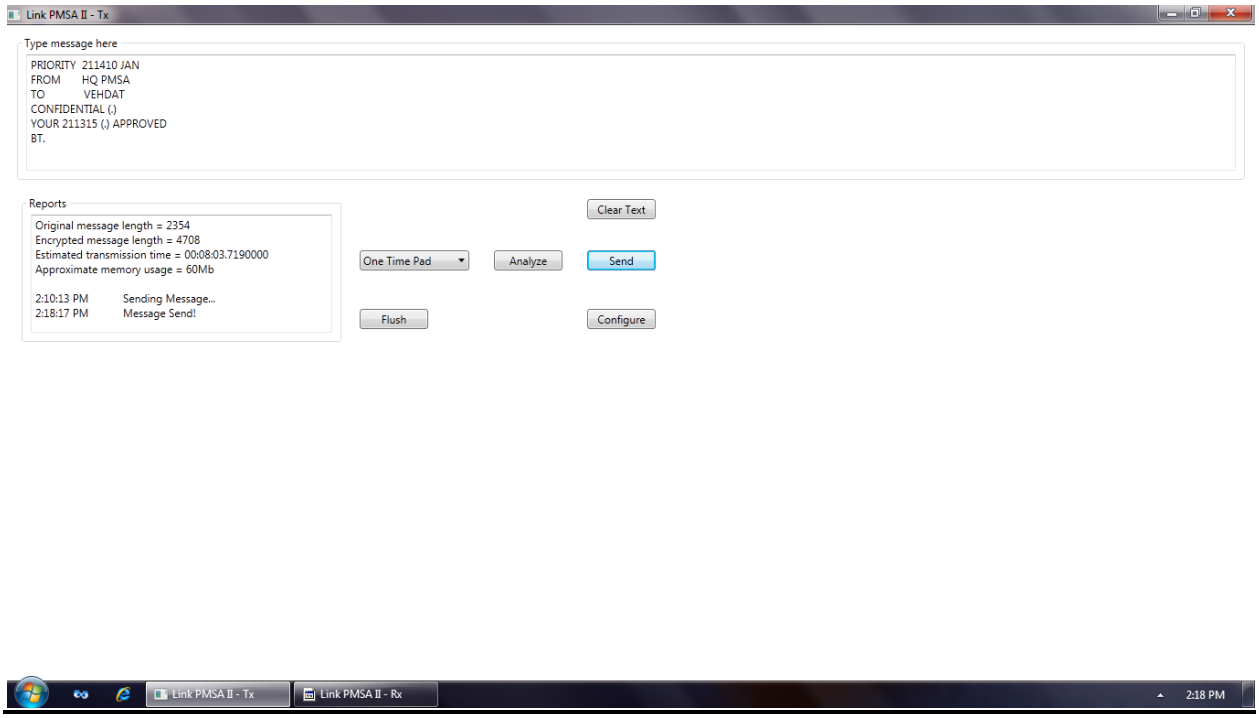
MESSAGE TRANSMISSION FROM SHIP AT SEA ON AES MODE



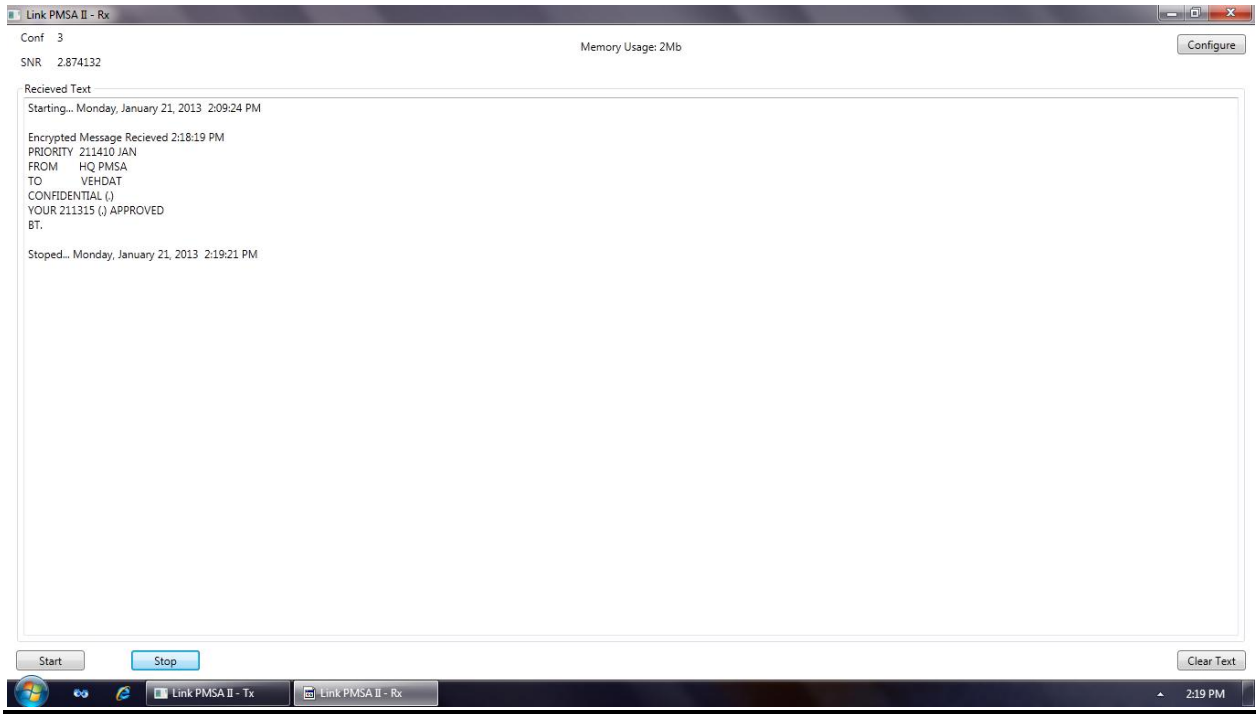
MESSAGE RECEPTION AT SHORE



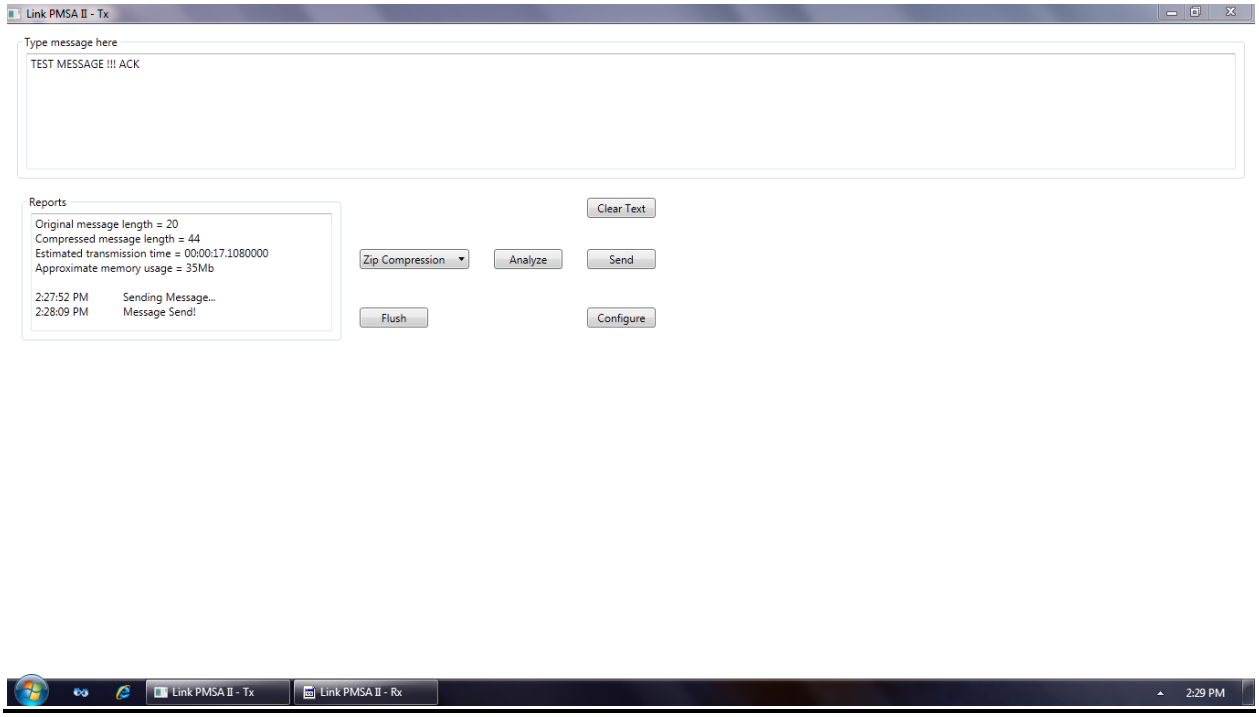
MESSAGE TRANSMISSION FROM SHORE ON OTP MODE



MESSAGE RECEPTION ONBOARD AT SEA



MESSAGE TRANSMISSION ONBOARD AT SEA ON ZIP COMPRESSION MODE



MESSAGE RECEPTION AT SHORE