Integrated C5ISR System for National Defense Force

Bahru Teshome Bekele

A Thesis Submitted to the Department of Electronics and Communication Engineering

School of Electrical Engineering and Computing

Presented in Partial Fulfillment of the Requirement for the Degree of Master's in Communication Engineering

Office of Graduate Studies

Adama Science and Technology University

Julay, 2023

Adama, Ethiopia

Integrated C5ISR System for National Defense Force

Bahru Teshome Bekele

Advisor Dr. Demissie Jobir

Co-Advisor Mr. Eshetu Tessema

A Thesis Submitted to the Department of Electronics and Communication Engineering

School of Electrical Engineering and Computing

Presented in Partial Fulfillment of the Requirement for the Degree of Master's in Communication Engineering

Office of Graduate Studies

Adama Science and Technology University

Julay, 2023

Adama, Ethiopia

APPROVAL PAGE OF M.Sc. THESIS

We, the advisors of the thesis entitled “Integrated C5ISR system for national defense force” and developed by Bahru Teshome Bekele; hereby certify that the recommendation and suggestions made by the board of examiners are appropriately incorporated into the final version of the thesis.

Major Advisor	Signature	Date
Co-advisor	Signature	Date

We, the undersigned, members of the Board of Examiners of the thesis by Bahru Teshome Bekele have read and evaluated the thesis entitled “Integrated C5ISR system for national defense force ” and examined the candidate during the open defense. This is, therefore, to certify that the thesis is accepted for partial fulfillment of the requirement of the degree of Master of Science in Communication Engineering.

Chairperson	Signature	Date
Internal Examiner	Signature	Date
External Examiner	Signature	Date

Finally, approval and acceptance of the thesis is contingent upon submission of its final copy to the Office of Postgraduate Studies (OPGS) through the Department Graduate Council (DGC) and School Graduate Committee (SGC).

Department Head	Signature	Date
School Dean	Signature	Date
Office of Postgraduate Studies Dean	Signature	Date.

DECLARATION

We hereby declare that this Master Thesis entitled “Integrated C5ISR System for National Defense Force ” is my original work. That is, it has not been submitted for the award of any academic degree, diploma, or certificate in any other university. All sources of materials that are used for this thesis have been duly acknowledged through citation.

Bahru Teshome Bekele

_____	_____	_____
Name of the Student	Signature	Date

RECOMMENDATION

We, the advisors of this thesis, hereby certify that I/we have read the revised version of the thesis entitled “Integrated C5ISR system for national defense force ” prepared under our guidance by Bahru Teshome Bekele submitted in partial fulfillment of the requirements for the degree of Mater’s of Science in Communication Engineering. Therefore, we recommend the submission of a revised version of the thesis to the department following the applicable procedures.

_____	_____	_____
Major Advisor	Signature	Date
_____	_____	_____
Co-advisor	Signature	Date

ACKNOWLEDGMENT

Firstly, I would like to thank you, my almighty God, Lord Jesus who helped me with the completion of this partial fulfillment of my MSc thesis. Next all, I would like to express my gratitude and appreciation to my Advisor Dr. Demissie Jobir Galmecha for his encouragement, guidance, engagement, constructive criticism, and useful suggestion that made this thesis a precious learning experience for me. This work would have never been possible without his vital support and valuable assistance. Next thanks to my co-advisor Mr. Eshetu Tessema.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS AND ABBREVIATIONS

AM	Amplitude Modulation
ARP	Antenna Radiation Period
C2	Command Control
C4IRSR	Command Control Communication Computer Intelligence Surveillance And Reconnaissance
C5 I SR	Command,Control,Communication,Computer,Cyber,Intelegence,Surveillance And Reconnaissance
CMP	Comprise Multiplexer
CP	Command Post
CRT	Cathode Rays Tube
CW	Continuous Wave
ECCM	Electronics Counter Counter Measure
ECCM	Electronics Counter Counter Measure
ECM	Electronics Counter Measure
ECM	Electronics Counter Measure
ESM	Electronics Support Measure
ESP	Electronics Support Measure
EW	Electronics Ware Fare
EW	Electronics Ware Fare
GFE	Government Furnished Equipment
GHQ	General Head Quarter
GIS	Geographic Information System
HF	High Frequency
HQ	Head Quarter
HW	Hard Ware
ILS	Integrated Logistic Support
IP	Internet Protocol
IRCS	Integrated Radio Communication System
IT	Information Technology
PRR	Pulse Repletion Rate

ROIP	Radio Over IP
RWR	Radar Waring Receiver
SATOM	Satellite Communication
SSB	Side Side Band
TCP	Transition Control Protocol
TMR	Tactical Multimedia Router
UHF	Ultra-High Frequency
VHF	Very High Frequency
VOIP	Voice Over IP
VTY	Virtual Telnet

ABSTRACT

The integrated of command control communication computer cyber intelligence surveillance reconnaissance (C5ISR) system for national defense arm is aimed to provide a variety of operational objectives and benefits in all battlefield dimensions, strategic, operational and tactical, as future growth. It assures full connectivity across various operational theaters and provides the command operation centers and combat forces with interoperability along the chain of command and across all operational disciplines. The C5ISR System improves battlefield situation understanding significantly, establish common situation awareness among all elements, and enhance collaborative planning, mission management, intelligence, border-guard, air-defense and maritime surveillance capabilities. The C5ISR system supports all combat conditions in which high-Intensity operations, low-intensity operations, raising forces mobility and maneuverability on continuous basis. The C5ISR System supports various conflict characteristics and provide seamless operations management according to battlefield conditions over the operational spectrum range. In fact, this includes joint operations, special operations, mounted and dismounted operations. The results from the theoretical analysis and simulation confirmed that the advanced hacking and electronic warfare technology, C5ISR system, deny all system from enemy attack by means of network access control, crypto encryption algorism and secure the radios message by means of direct spread spectrum techniques.

Keywords: *Access List Control, Electronics Warfare, Spread Spectrum ,Command control*

CHAPTER ONE

1. INTRODUCTION

1.1 Background of the Study

Over the world, many countries and its governments have an obligatory task to build a professional armed force to safeguard its people's human security and protect, sustain the national interests and sovereignty of the nation from various hostile actions or national security threats. In Ethiopia's case, the predominant thinking that guides the army-building process is to deter the war if the country may be forced to enter into the war. If this is so, the ultimate goal of the armed commander has to be to accomplish the given mission with minimum expenditure (material and logistic costs, Energy and time) and human life as much as possible to restore and keep peace and stability of the country. Moreover, create a conducive environment to realize fast and equitable economic growth and development, the establishment of good governance and democratization (December, 2022).

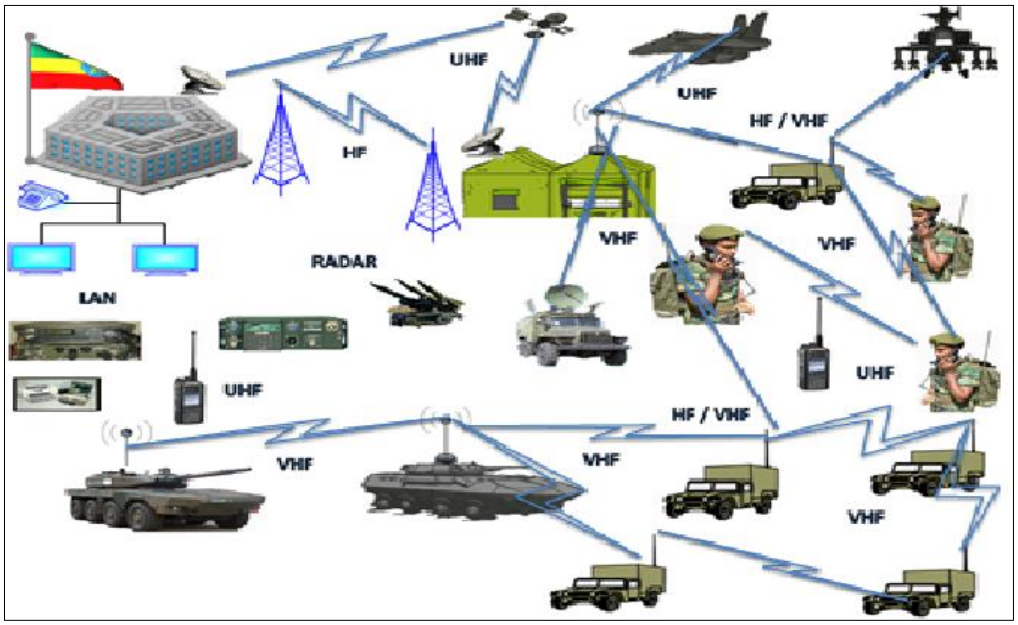


Fig 1.1 Integrated Communication Network

Therefore, to conclude the war in a manner that we need to accomplish our constitutional missions effectively, and achieve our goals and objectives of the war, our armed forces should make necessary comprehensive preparations during peacetime. Since the beginning of the war as a social phenomenon, the nature and conduct of the war have reached their peak point through conducting fast, fundamental, and dramatic developmental changes and advancements in military thought and the concept of war, technology, and social structure (Bommakanti & Observer Research Foundation, 2020).

Due to such advancements, the causes of war, the strategies, tactics, and techniques of war, information/intelligence sharing infrastructure and culture, the organizational structure of the army, and the command and control system of war have been constantly evolving from time to time (Metz, 1995).

On other hand, globalization has made our world to be connected as one village. This situation by itself creates lots of opportunities and challenges to the security and national interests of nations through creating positive and negative influences on diplomacy political, information, military, economy, Social and technological sectors. Some of the opportunities of globalization concerning army modernization are Market accessibility of advanced military technologies, ease to realize know-how and technology transfer, having fertile ground to create a global, continental and regional military alliance and strategic partnership, and availability of long-term loans with reasonable interest and financial support aid and so on (Mingqian & Shuai, 2020).

On other hand, globalization has created the following challenges: foreign forces' intervention on internal issues of undeveloped nations, challenges of technological advancements like social networks, computer crime and cyber-attacks, widespread thought of narrow nationalism, terrorism and extremism, colonization of culture, weaponization, illegal trade, army smuggling, human traffic, and unfair competition. So, our army modernization and reform program have to be implemented in a way that ensures building capabilities to utilize those opportunities effectively and efficiently and avoid and/or minimize the negative impacts of globalization (Thomas, 2014).

To tackle national security challenges that emanate from actual and anticipated adversaries and realize our military concept of operations which are clearly defined in our military doctrine, military science, and art effectively and efficiently, it is important to identify and characterize our national security threats and clearly understand our military concept of operations (Barzelay & Campbell, 2003). Based on our brief assessment, our national security challenges includes conventional warfare, narrow nationalism, terrorism and extremism, cyber-attack and computer crime, psychological warfare, insurgents and ant-peace organizations, transnational organized crimes, water politics, illegal trades, and so on. On other hand, in our military doctrine, military science, and art, clearly defined the concept of operation as follows:

Create information superiority by ensuring a fast, reliable, and secured information/intelligence sharing system, protect our valuable information and information

infrastructure from adversary's hostile course of actions, intercept and manipulate enemy information transmission and deny, disrupt and destroy enemy sensor networks and information infrastructures by using soft and hard kill advanced military firing weapons, EW and Cyber warfare systems (Thiele, 2013).

The following figure shows land forces over network and radio architecture.

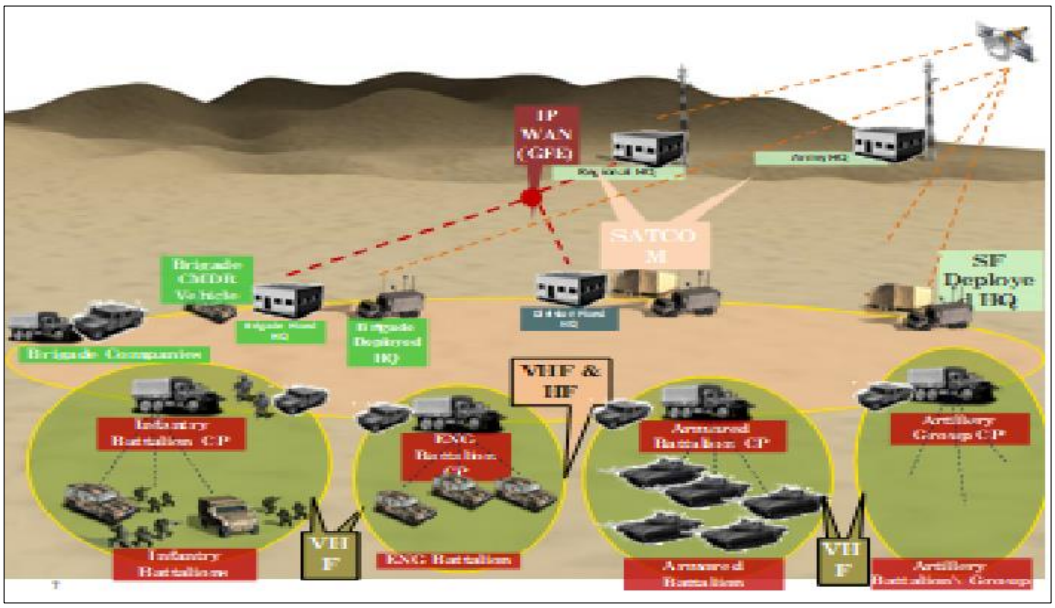


Fig 1.2 Ground Force Overall Network And Radio Architecture

To build long-standing and sustainable strategic capabilities to realize our concept of operation, accomplish our constitutional missions effectively and efficiently and confront all national security challenges on all war fronts, it is important and mandatory to design, implement and continuously improve the comprehensive C4ISR system and Cyber warfare (Billo & Chang, 2004). In modern contexts, cyber warfare capabilities have become the weapons for military forces to attack very important and valuable military and civilian target on land, air, sea, and space.

Current military attack statistics show that worldwide cyber-attacks are happening almost on daily bases on military, high-tech, and financial institutions. As a result, countries have begun to make efforts to build cyber warfare capabilities in addition to the traditional military capabilities (Sarty & Palmer, 2006).

The focus of cyber warfare is on identifying, preventing, and protecting cyber-attacks on information and information infrastructure, gathering and analysis of cyber intelligence, and taking necessary counter-attack measures if it is needed. Similarly(Lilly et al., 2021), C4ISR has emerged as a strategic capability for modern military forces and civil

organizations to ensure a fast, reliable, and secured information intelligence sharing system, to build well designed and developed command and control system(Stein et al., 2000), to have well-developed intelligence and electronic warfare capabilities to defiance our information and information infrastructure from hostile actions of our adversaries, to collect, analyze and disseminate relevant, accurate and timely intelligence and take necessary counter-attack measures on information and information infrastructure of our adversaries if it is required (Demchak, 2011).

1.2 Statement of the Problem

The advanced of modern hacking and electronic warfare technology, become limited on availability of high frequency and very high frequency radio communication to challenge the institution's capacity and efficiency radio networks. Most of military radio communication systems are not have high capacity, high-speed communication system between sender and receiver. Specially Very high frequency range radio communication are naturally to established net between radios to radios by line of sight (LOS) , due to this reason the signal strength between each radios are become week because of natural and manmade factor on performance of radio net. I will propose to find a gap that mention in above state of problem in military communication radio. Currently, the world uses C4IRS in the military organization, but for the reason of advanced of hacking and electronic warfare, technology the C4IRS component is not sufficient in items of cyber and information security risk. Therefore to fill this gap and enhance C5IRS for more confidential, dynamic, and efficient communication in the nation arm forces. Therefore, this thesis work mainly focuses on cyber and electronic defence on the top of C4IRS.

1.3 Objectives of the Study

1.3.1 General Objective

The general objectives of this thesis is to implement confidential and reliable radio communication networking system in the national arm force by focusesing on cyber and electronic defence on the top of C4IRS.

1.3.2 Specific Objectives

The specific objectives of this thesis are as follows:

- Sustain the effectiveness and efficiency of the command and control system of national Armed Force.
- Build well-defined and developed relatively full spectrum EW (EPM, ECM, and ECCM) capabilities based on critical assessment of National security threat levels and technological trends.
- Establish secured and integrated communication infrastructure make sure fast, reliable, robust, and secured information from enemy cyber-attack.

1.4 Significance of the Study

The C5ISR (Command, Control, Computers, Communications, Intelligence, Surveillance and Reconnaissance) system is a distributed system, which includes sensor network, information network and combat network. It enables independent data transfer from a variety of sites over various communication media (broad and narrow band); where each site is able to operate autonomously under variable readiness conditions. The C5ISR System supports the following enhanced features:- Continuous Operation; the system operates continuously in routine, emergency and training programs.

Support of various Deployment Outlines – the system can be operated in various site deployment configurations, including: fixed command posts deployed command posts, mobile platforms and dismounted commander. Unified User Interface – the system provides a unified and simple user interface, which integrates high performances and user experience. The user interface will guide and focus the user on the operational processes, and will not constitute an operational burden. Interfaces – the system allows linkage of land agents to all branches and commands establishing multi-force arrays and using a wide variety of interfaces with various sensor and weapon systems operated in all battle space dimensions. It interfaces with external C5ISR systems and allows future growth of the system. Standards & Formats- the C5ISR System organizes entity data structure in accordance with NATO formats.

It controls entity data flow according to its scope and usage and exchange its messages, using common messaging protocols. Communication Media Support, the system data is disseminated over various communication media types, including: broad and narrow bands: fiber-optic (WAN), Microwave, HF, VHF, UHF and SATCOM.

The system supports various operational disciplines in all battlefield dimensions, including: Strategic level conventional and unconventional or counter insurgency and counter-terrorism operations, border defense, airspace surveillance, early warning and maritime surveillance. Operational level:- ground situation picture management, operation management, target management, fire management and CSS management; and battle management capabilities:- Support tactical situation picture management, Mission planning and control, Navigation assistance, Combat resource management and Combat reports messaging. Fire assistance capabilities:- Support fire mission planning, Unit deployment and Survey meteorological data integration, fire control and fire resource management.

The C5ISR system provides a variety of services and tools which create a rich application framework, easing the development, customization and maintenance of oriented applications within the C5ISR framework, including: Data anagement services:- support generic management of entities and relationships, data replication, personalization of profiles, and messaging. User interface tools:- provides graphical, textual and statistical display tools; based on unique HMI infrastructure and standard symbols management and display. GIS, mapping & imagery services:- support map management and display capabilities, terrain analysis, 2nd and 3rd mapping, image processing, and various visualization tools. GIS support for the uploading and display of raster maps, vector maps and elevation maps.

All components of C5ISR system together or/and separately have predefined functions in conducting effective and efficient joint and unified mission planning and operations. For instance; command and control (C2) enables mission planning, create common operational picture (situational awareness) in all level of chain of command, leading and directing joint and unified operation using real time information and realize effective and efficient logistics management system. The Communication sub-system plays pivotal role in establishing integrated communication infrastructure and ensure fast, reliable and secured information sharing.

Functions of intelligence sub system are:- make decision making process fast, relevant and productive; support to formulate well designed and developed policies and strategies; help armed forces to conduct effective and efficient operations against National security threats and manmade and natural disasters; and identify emerging threats and build structured and organized knowledge concerning their intent, motive, plan and capabilities.

Similarly SR sub-system functions of C5ISR system is: trough providing precise and accurate location and tracking information create better operational picture/ common situational awareness, guide fire support systems, air defense weapons and EW counter measures, and prioritize threat level based on predefined set of criteria.

In general C5ISR System improves battlefield situation understanding significantly, establish common situation awareness among all elements, and enhance collaborative planning, mission management, intelligence, Border-Guard, Air- Defense and Maritime surveillance capabilities.

1.5 Expected Outcomes of the Study

Build well-designed and developed C5I2\SR platform and integrated communication infrastructure which are vital and backbone for effective and efficient realization of national Armed Force Modernization Program and accomplishment of constitutional missions,

- Establish a well-structured and organized Command and control system with a clear concept of operation and properly utilize it to build a digital battlefield infrastructure that enables national Armed Forces to achieve information superiority with the help of valid and useful real-time information.
- Develop well-trained Commanders and Professionals at each level of the command chain and subordinate units that have the required knowledge, skill, and attitude to accomplish their missions effectively and efficiently, and
- Gradually reduce foreign professional assistance and technology dependency through the well-designed and effective realization of the Transfer of Technology (TOT) Program.

1.6 Scope of the Study

- The significance of this study integrated components of Command, Control, Computers, Communications, Intelligence, information, Surveillance and Reconnaissance.
- The operating frequency range of very high frequency (VHF) radio communication is from 30MHZ -87.5 MHZ for tactical and operational unit.
- The operating frequency range of ultra-high frequency (UHF) radio communication is from 87.5 MHZ -512 MHZ for ground to sky communication.
- The operating frequency range of high frequency (HF) radio communication is from 1.5 MHZ - 29.5 MHZ for long distance communication

1.7 Limitation of the Study

This thesis is limited only to simulation based results. That means the performance of all detection techniques are evaluated based on simulation results only.

1.8 Organization of the Thesis

The thesis has been organized into four chapters.

Chapter 1 briefly discusses the background of the study. The problem statement, scope of the study, significance of the thesis and thesis objectives are laid out here with its limitation.
A Chapter 2 start by discussing a brief introduction about command, control, communications, computers, intelligence, surveillance, and reconnaissance this chapter covers a related work of thesis.
Chapter 3 presents the research method that has been used in the thesis and how to increasing the performance and the security issue in the C4ISR system interims of cyber security and enemy's electronics warfare attack. In addition, this chapter introduced materials that have been used for simulating the results.
Chapter 4 includes the results IP access control and anti-Jamming resist techniques. Lastly, the Conclusion and Recommendation of the thesis ware presented.

CHAPTER TWO

2. LITERATURE REVIEWS

2.1 Introduction

The integrated command, control, communication, computer, intelligence, surveillance, and reconnaissance (C4ISR) of for national defense arm system is a comprehensive to use the modern technology electronic warfare technology information and device under the guidance of modern combat theory, and is closely integrated with operational command unit during national mission accomplished. The man-machine standard system for the command of solders and operational weapons, which integrates command, control, communication, intelligence, reconnaissance, detection, continuous warning and comprehensive provides, is the infrastructure of military command automatic integration , and it is also the reality of the commander control the given mission .

The depth technical means of giving command and control with the growth military change and information flow technology, the traditional architecture and component-based pyramid command and control find system solutions can no longer meet the needs of joint operations, mainly for the following reasons. One of the clients is directly integrated to the server, and the server spent some resources to deal with the integrated with the user, which cannot get the specific -time requirements of the command and control system. On the other hand in this high level –low level command and control structure, if the line integrated to the high level server or the high level stops working for some reason, the whole system will be destroyed. Moreover, the distribution of user components is extremely tedious, the business logic of the command and control system is compiled in the client, resulting in abnormal bloated client; the other reason, the component-based solution is realized by distributing the related business components to different seats. The functions of the components get by the seats are relatively constant and missing. Lack of task-oriented flexibility, because pyramid command and control system cannot meet the needs of information (Mingqian & Shuai, 2020).

2.2 Related Works

The authors observed on China Naval modernization: implications for U.S. Navy capabilities-background and issues for congress China’s military modernization effort, including its naval modernization effort, is the top focus of U.S. defence planning and budgeting. China’s naval modernization effort has been underway for more than 25 years,

since the early to mid-1990s, and has transformed China's Navy into a much more modern and capable force. China's navy is a formidable military force within china's near seas region, and it is conducting a growing number of operations in the broader waters of the western pacific, the Indian Ocean and waters around Europe. China`s navy is, by far, the largest of any Country in East Asia, and sometime between 2015 and 2020 it surpassed the U.S. Navy in numbers of battle force ships (meaning the types of ships that count toward the quoted size of the U.S. Navy). DOD states that China's navy "is the largest navy in the World with a battle force of approximately 340 platforms, including major surface combatants, submarines, ocean-going amphibious ships, mine warfare ships, aircraft carriers, and fleet auxiliaries. this figure does not include approximately 85 patrol combatants and craft that carry anti-ship cruise missiles (ASCM). the overall battle force [of China's Navy] is expected to grow to 400 ships by 2025 and 440 ships by 2030."

the U.S. Navy, by comparison, included 294 battle force ships at the end of FY2021, and the navy's FY2023 budget submission projects that the navy will include 290 or 291 battle force ships by the end of FY2030. u.s. military officials and other observers are expressing concern or alarm regarding the pace of china's naval shipbuilding effort and resulting trend lines regarding the relative sizes and capabilities of China's navy and the U.S. navy. China's naval modernization effort encompasses a wide array of ship, aircraft, weapon and C4ISR (command and control, communications, computers, intelligence, surveillance, and reconnaissance) acquisition programs, as well as improvements in logistics, doctrine, personnel quality, education and training, and exercises. China's navy has currently has certain limitations and weaknesses, which it is working to overcome, china's military modernization effort, including its naval modernization.

Effort is assessed as being aimed at developing capabilities for, among other things, addressing the situation with Taiwan militarily, if need be; achieving a greater degree of control or domination over china's near-seas region, particularly the South China Sea; defending China's commercial sea lines of communication (slocs), particularly those linking china to the persian gulf; displacing U.S. influence in the Western Pacific; and asserting China's status as the leading regional power and a major world power. Observers believe China wants its navy to be capable of acting as part of an anti-access/area-denial (A2/AD) force a force that can deter U.S. intervention in a conflict in China's near-seas region over Taiwan or some other issue, or failing that, delay the arrival or reduce the effectiveness of intervening U.S. forces. The U.S. Navy has taken a number of actions to

counter China's naval modernization effort. Among other things, the U.S. Navy has shifted a greater percentage of its fleet to the Pacific; assigned its most-capable new ships and aircraft to the Pacific; maintained or increased general presence operations, training and developmental exercises, and engagement. All so cooperation with allied and other navies in the Indo-Pacific; increased the planned future size of the Navy; initiated, increased, or accelerated numerous programs for developing new military technologies and acquiring new ships, aircraft, unmanned vehicles, and weapons; developed new operational concepts for countering Chinese maritime A2/AD forces; and signalled that the Navy in coming years will shift to a more-distributed fleet architecture that will feature a substantially greater use of unmanned vehicles. The issue for Congress is whether to approve, reject, or modify the Biden Administration's proposed U.S. Navy plans, budgets, and programs for responding to China's naval modernization effort (O'Rourke, 2021).

Research on C4ISR Requirement Demonstrating Method Based on System Configuration. Requirement demonstrating is an important link of C4ISR construction. The paper design a requirement demonstrating architecture framework of C4ISR based on the research on DOD2.0. The paper describes how to design capability requirement view, information requirement view, services requirement view, systems requirement view, project requirement view. The standards requirement view emphatically. Project viewpoints have great significance in the field of C4ISR requirement demonstrating. Demonstration of needs is an important and hot issue in the research of information system construction. This article uses the thought of system structure and the DOD2.0 framework to conduct a systematic demand demonstration for the information system. The requirement demonstration method described in this paper clearly and completely expresses the capability requirements, information requirements, service requirements, system requirements, procurement requirements and technical standard requirements of information system through formatted graphics, tables and texts, and establishes a complete set of requirements demonstration specifications, providing reference for the capability formation, detailed design and system implementation of information system.

By adopting the method of architecture requirement demonstration, we can accurately demonstrate how the system functions support the needs such as conformation activities and how the system construction supports the formation of capabilities. Therefore, the design of system performance index has a quantitative basis, which provides reference for

the decision-making of user departments and leading organs, thus improving the top-level design level of the system and the success probability of development (Jinfeng et al., 2021).

According to survey on C4ISR system architecture technique with the rapid development of information technique. The warfare modes changes continuously, converting from “Platform Centric Warfare” to “Network Centric Warfare” gradually. C4ISR system becomes networking, service oriented and intelligent. C4ISR systems are required to possess higher capability of situation awareness and coordination decision-making due to the integrative joint operations. In this paper, C4ISR systems are studied comprehensively. The development and main technique of C4ISR are outlined, and the current research states of its architecture are reviewed in detail. Finally, the major problems confronting in the research are summarized. With the development of science and technology, the mode of modern warfare has changed from traditional mechanized warfare to information warfare and network warfare. This puts forward more requirements for C4ISR command and control system and the transmission of information. Sharing capability and cooperative combat capability have a great influence on the process and result of war. C4ISR architecture technology contains the key technologies of its whole life cycle.

This paper first introduces the concept, development and main technologies of C4ISR; secondly, summarizes the research status of C4ISR architecture technology in foreign countries, including C4ISR architecture framework, modelling method, design and development method, and Verification and evaluation methods; Finally, the paper analyses the main problems facing at present (Mingqian & Shuai, 2020). The researcher proposed Decision support and knowledge exploitation technologies for C4ISR. In military operations, commanders and decision-makers at all levels work in an information saturated environment. Turning pieces of information into situation awareness requires the expertise and experience of many. Two main aspects will impact on the next generation of C4ISR systems: advances in command and control (C2), and information technologies, in particular in situation analysis, knowledge exploitation technologies and decision support systems. In order to facilitate interoperability, growth and maintainability, C4ISR systems must be developed by adhering to a number of open standards. Information technologies will be used to develop net-centric enterprise services (NCES) in order to provide modularity, sharing of decision support tools and services, and interoperability of C4ISR systems. Knowledge exploitation technologies will provide new C4ISR systems with tools and processes to build actionable knowledge. Like situation awareness, knowledge

management is about getting the right information to the right people at the right place and time. Therefore, in the military context, any knowledge management model and any decision-making model, including people, processes and technologies, must contribute directly to the achievement of this goal. Future C4ISR systems will also require the development and application of new decision science principles adapted to new and evolving decision-making contexts.

They will need to incorporate both the decision science principles and new tools into a science-based decision support framework process leveraging information and knowledge exploitation technologies. This document presents a generic, high-level view of current research activities in each of the areas mentioned previously. The Revolution in Military Affairs (RMA) has moved to centre-stage the requirement for information dominance in the joint battle space. It is predicted that the greatest change in the conduct of future military operations will be the result of the application of information technology to military command and control. Commanders and decision-makers at all levels need enough information to make decisions but need to be supported by technology so that they are not overwhelmed with information. By leveraging advances in information technologies such as data and information fusion, knowledge management and exploitation, information visualization, human-computer interactions and decision support systems, future C4ISR systems will definitely allow the improvement of situation awareness and decision-making. Future C4ISR systems will need to incorporate both the decision science principles and new tools into a science-based decision support framework sustained by information and knowledge exploitation technologies. By exploiting open standards and net-centric enterprise services, these systems will also provide increased interoperability and support modular software development(Auger et al., 2006).

According to this paper the authors proposed understanding command and mission provide. Dr. Alberts is credited with significant contributions to our understanding of the Information Age and its implications for national security, military Command and Control, and organization. These include the tenets of Network Centric Warfare, the coevolution of mission capability packages, new approaches to Command and Control, evolutionary acquisition of Command and Control systems, the nature and conduct of Information Warfare, and most recently the “Power to the Edge” principles that currently guide efforts to 208 Understanding Command and Control provide the enabling “info structure” of DoD transformation, and efforts to better understand Edge organizations and the nature of

Command and Control in a networked environment. These works have developed a following that extends well beyond the DoD and the Defence Industry. His contributions to the conceptual foundations of Defence transformation are complemented by more than 25 years. The pragmatic experience developing and introducing leading edge technology into private and public sector organizations. This extensive applied experience is augmented by a distinguished academic career in Computer Science and Operations Research and by Government service in senior policy and management positions. As President and founder of Evidence Based Research, Inc.,Dr. Hayes specializes in multi-disciplinary analyses of Command and Control, intelligence, and national security issues; the identification of opportunities to improve support to decision makers in the defence and intelligence communities. The design and development of systems to provide that support; and the criticism, test, and evaluation of systems and procedures that provide such support. His areas of expertise include crisis management; political-military issues; research methods; experimental design; simulation and modelling; test and evaluation; military command, control, communication, and intelligence (C3I or NII); and decision-aiding systems. Since coming to Washington in 1974, Dr. Hayes has established himself as a leader in bringing the systematic use of evidence and the knowledge base of the social sciences into play in support of decision makers in the national security community, About the Authors 209 domestic agencies, and major corporations. He has initiated several programs of research and lines of business that achieved national attention and many others that directly influenced policy development in client organizations. Dr. Hayes has co-authored several other CCRP titles, including: Campaigns of Experimentation (2005), Power to the Edge (2003), The Code of Best Practice for Experimentation (2002), Understanding Information Age Warfare (2001), and Command Arrangements for Peace Operations (1995)(Alberts et al., 2010).

2.3 Summary of Literatures

I am reading literature papers to the study a command control communication and computers. In those papers, there were the information gap on security, in terms of cyber security and electronic warfare attack , which the enemies were easily attacked friendly communication infrastructure. Due this, I was proposed to fill this security gap in my paper.

CHAPTER THREE

3. METHODOLOGY AND SYSTEM MODEL

3.1 Overview

In this thesis, different related papers and articles were reviewed from various journals such as articles from reputable journal, and books that were related to command, control, communications, computers, cyber, intelligence, surveillance, and reconnaissance. Depending on the reviewed papers and having the statement of the problem in mind the methodology that are listed under section 3.1 are followed to design and simulate the proposed methodological techniques.

3.2 Materials

In this thesis, MATLAB/R2016a and eNSP software tools are used for all simulations. MATLAB and eNSP is a high performance language for technical computing. Also it is computing software that consists of technical boxes and Simulink. Using MATLAB we can develop algorithms, analyze data, and create models and applications.

3.3 Methodology

In order to meet the above mentioned objectives of the thesis the following formal methodologies are followed.

Literature Review: This thesis work is inextricably linked to previous research on the subject by experts or scholars. As a result, studying the works of these scholars and getting relevant and important knowledge on the subject is essential. It is reviewed from a variety of sources, including papers, books, journals, the internet, etc. Hence, the literature review consists of reading articles, conferences, papers, books, journals, and searching from various sources on the internet for relevant topics (i.e., command, control, communications, computers, intelligence, surveillance, and reconnaissance).

Problem Identification: based on the paper reviewed from different journals, articles and conferences the problem (research gaps) is identified for research study.

System Designing: after the identification of research gap the systems are designed for proposed work.

Simulation of designed System using MATLAB and eNSP: after modeling of the proposed system the simulation are done using MATLAB tools.

Result and Discussion: depending up on the results from simulation, discussions are performed on the results and performance evaluations are also done on proposed techniques.

Documentation: After analyzing the results of the designed system, the whole work of the research study is concluded by suggesting an implied recommendation and further work to be done on the areas**.**

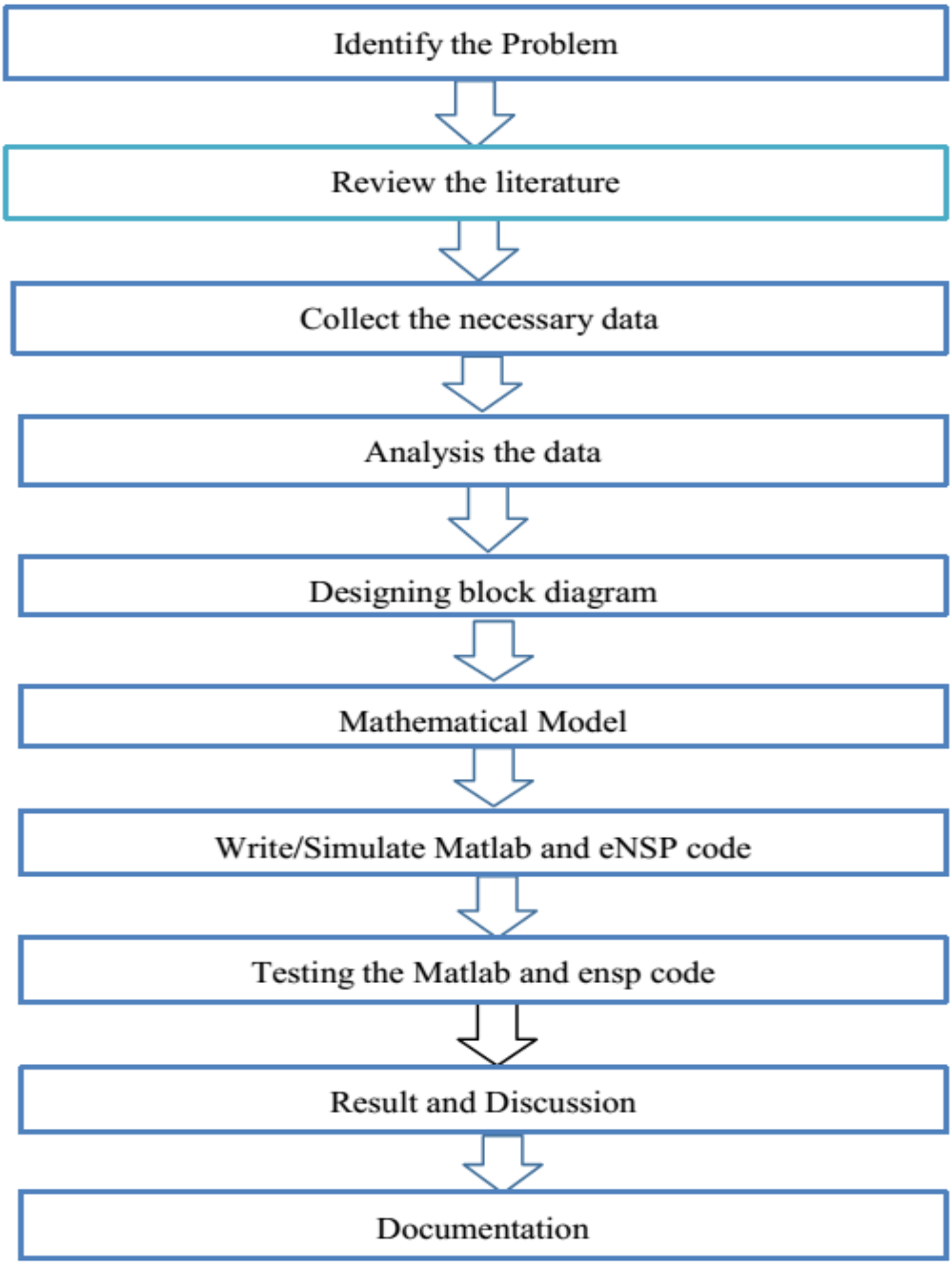


Fig 3.1 Methodology

3.4 Overviews of Cyber Security

When we say the concept cyberspace to describe systems and services integrated either directly to or indirectly to the information communication technology like telecommunications and computer topology network system. In the modern world culture depends upon the timely, adequate and security performance of cyberattack.

The cyber security system is necessary to all counties a reason that it endeavors to conform that cyber space continues to work when and as expected all in the security attack. We argue that cyber security is no longer a pure computer security issue. Instead, we see cyber security as a national policy matter because the illicit use of cyberspace could hamper capital influence , society health, safety and country security activities. Since governments mainly exist to maintain social order, protect the lives and property of their citizens and enable commerce, then national leaders are accountable for cyber security as it supports all the aforementioned services.

We recommend that head of country use all cyber security device of country power to minimize cyber risks appropriately. In specially, in country level all leaders have responsibility for instrument in cyber space security strategy and influenced local, state and global joint agreement. This thesis document is a state to model for state space security strategy elaboration. We discuss what next flows a state cyber space long plan ; the typical ends it seeks to accomplish and the context that influences its execution. The Guide also discusses how national and other relevant partners s such as private sector national space security can build ability to execute a space security plan and the capital required to pointed risks (Kang, 1997).

3.4.1 Cyber Security

From experience of being deny attack the criminal or unauthorized use of computer network system. Over the month to month or in annual range the term cyber space security attacked has been thrown specific to the location where it is all time applied with terms like computer security or data security. Its type of just saying all square is a rectangle, but not every rectangle is a square.

Cyber security divination: Every square is a rectangle because a square is a quadrilateral with all four angles being right angles. The same to that, cyber security is a part of the information communication technology security umbrella, along with its counterparts, physical security and information security (Blythe, 2014). But not every rectangle is a square, since the criteria to ability as a square means all body shade be the equal distance.

The idea is not all computer network securities determine qualify as cyber security, as cyberspace security has its own distinct assets to protect. organization TIA's main technology evangelist, different expert says it best when he defines Cyber Security as "Focusing on all protecting electronic emission assets including internet, wan and lan resources used to store and transmit that information." the enemy to these electronic emission assets are hackers who have malicious intent to destroy or take proprietary data and information via data network systems, this hall , it would seem the fully realized definition should include an evolving set of cyber security device designed to protect secured data from hacker body access, the do so, it's important to consider how society , processes and technology all doing balance important roles in our computer network security .

3.4.2 Necessary of Cyber Security

The basic important to living in a world where all instrument or tools is integrated is convenience. It's rapidly simply to conduct job, manage your social schedule, super market and make appointments from your modern laptop or tools. That's why it's become second nature to many of us. But, of course, the convenience of integrated data also means threats from wrest methods can do a lost of destroy . the space security initiatives are essential to deny our information and thus, our methods of life to world (Lehto, 2020).

Internes of distributed all of its necessary , an organization should increasing a balanced plan that includes not alone these four kinds of cyber security, but also the three parts that play active roles in a cyber-security program : end users system and growth of ICT(Kimani et al., 2019).

3.4.2.1. End User

Let's face it; no problem what precautions you put into different location , if end user don't respect the end user organizational policy all are still at risk. The saying "you're only as strong as your weakest link" comes to mind. In most cases, human error is just that – a mistake. Most end user aren't always by passing user policy – they either aren't trained to do so, or they aren't learn about the problem of their actions. Always cyber security risk training and enforcing the most basic cyber security organizational policy with workers s outside of the information communication technology sectors can make a big difference in your organizational security posture. Here are four ways the end user influenced can increase your cyber security problem.

3.4.2.2. Suspicious: URLs and Emails

Define to workers that if always plan to strange – it probably is! Motivation and awareness organizational employers to pay attention to URLS, remove emails that don't have holds or look like they are coming from a spoofed special address, and stress the necessary to of guarding individual information. As the information technology experts, it's your responsibility to raise awareness of ability to cyber security attack threats.

3.4.2.3. Password Idleness

We know that handle on to the same password for ages isn't a good idea. But, Bob in finance may not understand that. Educated workers about the necessary of always changing passwords and using complex character ,number ,symbols . We all carry a plethora of passwords and since it's a best practice not to duplicate your passwords, it's clear that some of us want to editing them down somewhere. Provide comment on where to store passwords.

3.4.2.4. End User Individual Information

Most workers should understand the need to keep individual browsing, like insurance and financial institution tasks, to their own tools . But all does a bit of browsing for job, right? Emphasize the necessary of keeping an eye on what websites may lead to others. And, all that addition to so internet media. Karen in customer service may not realize that sharing too much on Facebook, Twitter, Instagram, etc. (like personally identifiable information) is just single way hackers can collecting information.

3.4.2.5. Backups and Updates

It's fairly smiley for an always tech end users to go about their daily business without finical institution up their data day to days and updating their system's anti-virus. This is a work for the information communication technology division. The highest challenge here is getting work to understand when they need your support with these items.

3.4.2.6. Physical Security for Devices

Think about how many end user in your organization in each division according to their taxes leave their desk for meetings, collating and tea breaks. Are they locking their devices? Highlight the need to deny information each and all time a device is left unattended. You can use the bus station analogy. Bus station staff is always telling us to keep track of our bags and never leave them unattended.

Why? Well, because you just don't know who is walking by? Encourage worker to deny their devices with as much care as they protect their big bag (Al-Darwish & Choe, 2019).

3.4.2.7. Processes

If workers outside of the information communication technology division are trained, information communication technology pros can depend on process. The processes by which cyber security professionals go about protecting confidential data are multi-faceted. In short, these Information communication pros are tasked with detecting and identifying cyber security threats, protecting information and feedback to incidents as well as updating from them. Putting processes into place not only ensures each of these buckets are being always monitored, but if cyber security attacks overcome, referencing a good organized data process can save your organization time, wealth and the needs of your most valuable asset and capital your end users. The country ICT Standards and information communication under the America Commerce division have developed the Cyber security strategic structure for individual -sector companies to use as a lead in creating their own good experience .

3.4.2.8. Technology

Once you have structure and processes in location , it's time to think about the tools you have at your disposal to beginning to deployed . Technology has a dual meaning when it comes to your toolbox: The information communication technology you'll use to protect and combat cyber security attacks, like DNS identifying , malware protection, antivirus computer application , firewalls and email address security solutions. The technology your data lives on that needs your prevent at all , like computers, digital phones routers, computer networks and the cloud. Back in the day, cyber security initiatives depends on defensive mechanism inside the boundaries of traditional tech. But today, policies like Bring Your Own Device (BYOD) have blurred those lines and handed hackers a much broader realm to penetrate. Remembering cyber security basics like locking all of your doors, windows, elevators and skylights will keep you from joining the cyber-crime phenomena

3.4.3. Cyber Security Threats

To Staying ahead of cyber security threats isn't an simple work. There's a long list of threats that information communication technology pros pay attention to, but the problem is that the list keeps developing. know in the world cyber-attacks over come on the constant

period of time . While few attacks are small and simple contained, others rapidly spiral out of control and wreak havoc. Full cyber-attacks needs immediate attention and solution.

3.4.3.1 Security Attacks

There are four general categories of attack which are listed below.

Interruption. An asset of the system is destroyed or becomes unavailable or unusable. This is an attack onavailability e.g., destruction of piece of hardware, cutting of a communication line or disabling of file management system.

Interception

An unauthorized party gains access to an asset. This is an attack on confidentiality. Unauthorized party could be a person, a program or computer.

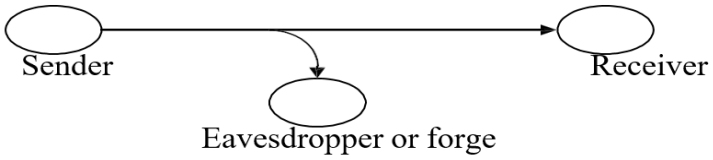


Fig 3.2 Security Interception

Modification

An unauthorized party not only gains access to but tampers with an asset. This is an attack onintegrity. e.g., changing values in data file, altering a program modifying the contents of Messages being transmitted in a network.

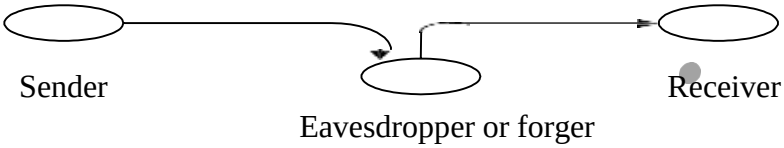


Fig 3.3 Security Modification

Fabrication

The person whose have permission to input or encoding data to counterfeit objects into the computers. This is an types of risk on authenticity.e.g., editing of spurious data in a computer or also of keep file to a file (Schultz et al., 2001).

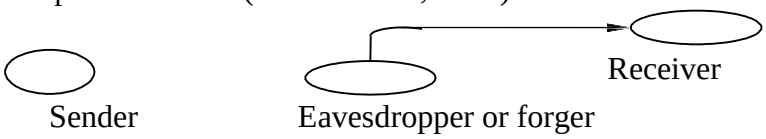


Fig 3.4 Security Fabrication

3.4.3.2. Cryptographic Attacks

3.4.3.2.1. Passive Attacks

Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. Passive attacks are of two types:

Release of message contents: A telephone conversation, an e-mail message and a transferred file may contain sensitive or confidential information. We would like to prevent the opponent from learning the contents of these transmissions.

Traffic analysis: If we had encryption protection in place, an opponent might still be able to observe the pattern of the message.

The opponent could determine the location and identity of communication hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of communication that was taking place. Passive attacks are very difficult to detect because they do not involve any alteration of data. However, it is feasible to prevent the success of these attacks (Pareek et al., 2017).

3.4.3.2.2 Active Attacks

These attacks involve some modification of the data stream or the creation of a false stream. Theseattacks can be classified in to four categories:

Masquerade – One entity pretends to be a different entity.

Replay: Involves passive capture of a data unit and its subsequent transmission to produce an unauthorized effect.

Modification of messages: Some portion of message is altered or the messages are delayed or recorded, to produce an unauthorized effect.

Denial of service: Prevents or inhibits the normal use or management of communication facilities. Another form of service denial is the disruption of an entire network, either by disabling the network or overloading it with messages so as to degrade performance.

It is quite difficult to prevent active attacks absolutely, because to do so would require physical protection of all communication facilities and paths at all times. Instead, the goal is to detect them and to recover from any disruption or delays caused by them. Symmetric and public key algorithms

- Encryption/Decryption methods fall into two categories.
- Symmetric keyPublic key

In symmetric key algorithms, the encryption and decryption keys are known both to sender and receiver. The encryption key is shared and the decryption key is easily calculated from it.In many cases, the encryption and decryption keys are the same. In public key cryptography, encryption key is made public, but it is computationally infeasible to find the decryption key without the information known to the receiver.

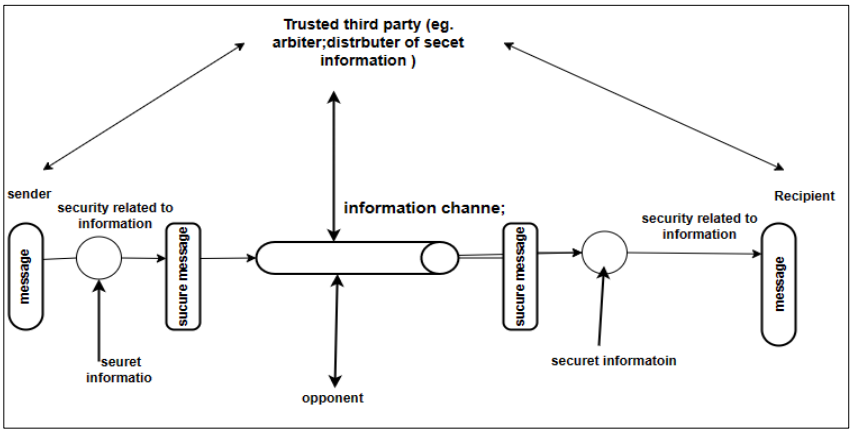


Fig 3.5 Model of Network Security

A message is to be transferred from one party to another across some sort of internet. The two parties, who are the principals in this transaction, must cooperate for the exchange to take place. A logical information channel is established by defining a route through the internet from source to destination and by the cooperative use of communication protocols (e.g., TCP/IP) by the two principals.

Using this model requires us to:

- design a suitable algorithm for the security transformation
- generate the secret information (keys) used by the algorithm
- develop methods to distribute and share the secret information
- specify a protocol enabling the principals to use the transformation and secure.

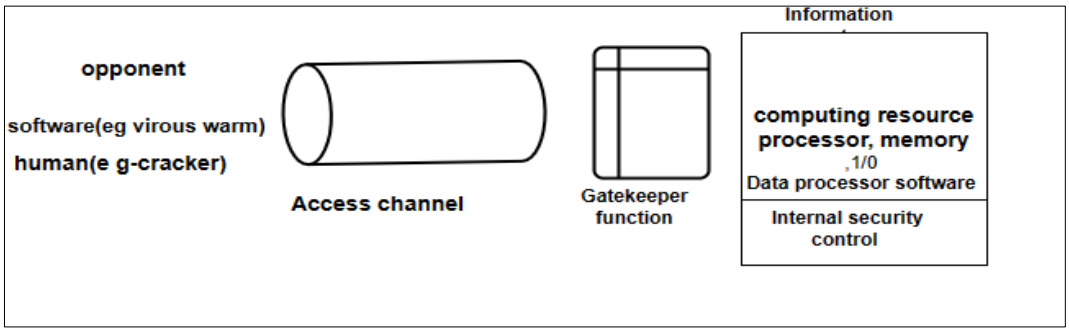


Fig 3.6 Model For Network Access Security Information ForA Security Service

Using this model requires us to:

- select appropriate gatekeeper functions to identify users
- implement security controls to ensure only authorized users access designated information or resources

Trusted computer systems can be used to implement this model conventional encryption

- Referred conventional / private-key / single-key
- Sender and recipient share a common key

All classical encryption algorithms are private-key was only type prior to invention of public-key in 1970"plaintext - the original message

Some basic terminologies used:

cipher text - the coded message

Cipher - algorithm for transforming plaintext to cipher text

Key - info used in cipher known only to sender/receiver

encipher (encrypt) - converting plaintext to cipher text

decipher (decrypt) - recovering cipher text from plaintext

Cryptography - study of encryption principles/methods

Cryptanalysis (code breaking) - the study of principles/ methods of deciphering cipher text without knowing key

Cryptology - the field of both cryptography and cryptanalysis

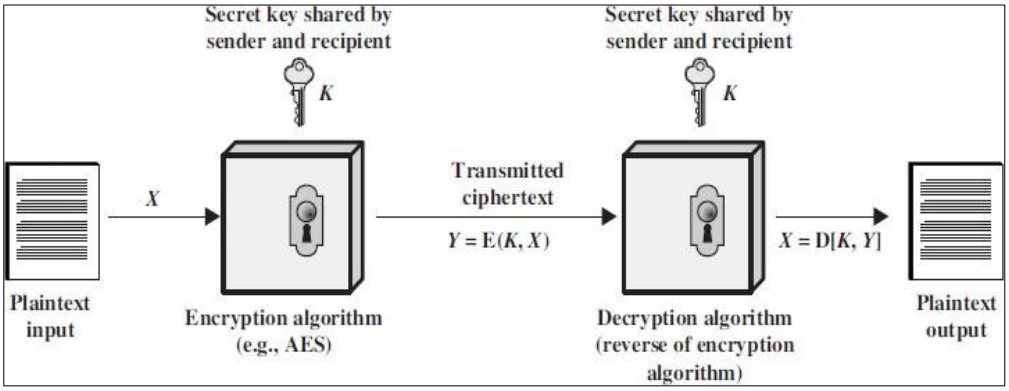


Fig 3.7 Encryption and Decryption System

Here the original message, referred to as plaintext, is converted into apparently random nonsense, referred to as cipher text. The encryption process consists of an algorithm and a key. The key is a value independent of the plaintext. Changing the key changes the output of the algorithm. Once the cipher text is produced, it may be transmitted. Upon

reception, the cipher text can be transformed back to the original plaintext by using a decryption algorithm and the same key that was used for encryption. The security depends on several factors. First, the encryption algorithm must be powerful enough that it is impractical to decrypt a message on the basis of cipher text alone. Beyond that, the security depends on the secrecy of the key,not the secrecy of the algorithm. Two requirements for secure use of symmetric encryption:

A strong encryption algorithm

A secret key known only to sender/ receiver

$Y = E_K(X)$

$X = D_K(Y)$

assume encryption algorithm is known

implies a secure channel to distribute key

A source produces a message in plaintext, X = [X1, X2… XM] where M are the number of letters in the message. A key of the form K = [K1, K2… KJ] is generated. If the key is generated at the source, then it must be provided to the destination by means of some secure channel. The message X and the encryption key K as input, the encryption algorithm forms the cipher text Y = [Y1, Y2, YN]. This can be expressed as

$Y = E_K(X)$

The intended receiver, in possession of the key, is able to invert the transformation:

$X = D_K(Y)$

An opponent, observing Y but not having access to K or X, may attempt to recover X or K or both. It is assumed that the opponent knows the encryption and decryption algorithms. If the opponent is interested in only this particular message, then the focus of effort is to recover X by generating a plaintext estimate.

Often if the opponent is interested in being able to read future messages as well, in which case an attempt is made to recover K by generating an estimate.

3.4.3.3 Access List Control

Access control lists (ACLs) perform packet filtering to control the movement of packets through a network.Packet filtering provides security by limiting the access of traffic into a network, restricting user and device access to a network, and preventing traffic from leaving a network. IP access lists reduce the chance of spoofing and denial-of-service attacks, and allow dynamic, temporary user-access through a firewall. IP access lists can also be used for purposes other than security, such as to control band width, restrict the content of routing

updates, redistribute routes, trigger dial-on-demand (DDR) calls, limit debug output, and identify or classify traffic for quality of service (QoS) features. An access list is a sequential list that consists of at least one permit statement and possibly one or more denystatements. In the case of IP access lists, these statements can apply to IP addresses, upper-layer IP protocols,or other fields in IP packets. Access lists are identified and referenced by a name or a number.

Access lists act as packet filters, filteringpackets based on the criteria defined in each access list. N After you configure an access list, for the access list to take effect, you must either apply the access list to aninterface (by using the ip access-group command), a vty (by using the access-class command), or referencethe access list by any command that accepts an access list. Multiple commands can reference the same access list. In the following configuration, an IP access list named branch offices is configured on Fast Ethernet interface 0/1/0 and applied to incoming packets. Networks other than the ones specified by the source address and mask pair cannot access Fast Ethernet interface 0/1/0. The destinations for packets coming from sources on network172.16.7.0 are unrestricted. The destination for packets coming from sources on network 172.16.2.0 must be 172.31.5.4.ip access-list extended branch offices10 permit 172.16.7.0 0.0.0.3 and 20 permit 172.16.2.0 0.0.0.255 host 172.31.5.4 interface fast Ethernet 0/1/0 .ip access-group branch offices in. .

3.4.3.4 Creating IP Access Lists

The following tips will help you avoid unintended consequences and help you create more efficient, usefulaccess lists.

- Create the access list before applying it to an interface (or elsewhere), because if you apply a nonexistentaccess list to an interface and then proceed to configure the access list, the first statement is put into effect, and the implicit **deny** statement that follows could cause you immediate access problems.
- Another reason to configure an access list before applying it is because an interface with an empty accesslist applied to it permits all traffic.
- All access lists need at least one **permit** statement; otherwise, all packets are denied and no traffic passes.
- Use the statement **permits any any** if you want to allow all other packets not already denied. Using thestatement **permit any any** in effect avoids denying all other packets with the implicit deny statement atthe end of an access list. Do not make your first access list entry **permit any any** because all traffic willget through; no packets will

reach the subsequent testing. In fact, once you specify **permit any any**, alltraffic not already denied will get through.

- Although all access lists end with an implicit **deny** statement, we recommend use of an explicit **deny**statement (for example, **deny ip any any**). On most platforms, you can display the count of packets denied by issuing the **show access-list** command, thus finding out more information about who your access list is disallowing. Only packets denied by explicit **deny** statements are counted, which is why the explicit **deny** statement will yield more complete data for you. While you are creating an access list or after it is created, you might want to delete an entry.
- You cannot delete an entry from a numbered access list; trying to do so will delete the entire accesslist. If you need to delete an entry, you need to delete the entire access list and start over.You can delete an entry from a named access list. Use the **no permit** or **no deny** command todelete the appropriate entry.
- In order to make the purpose of individual statements more scan able and easily understood at a glance,you can write a helpful remark before or after any statement by using the **remark** command.If you want to deny access to a particular host or network and find out if someone from that network orhost is attempting to gain access, include the **log** keyword with the corresponding **deny** statement so that the packets denied from that source are logged for you.

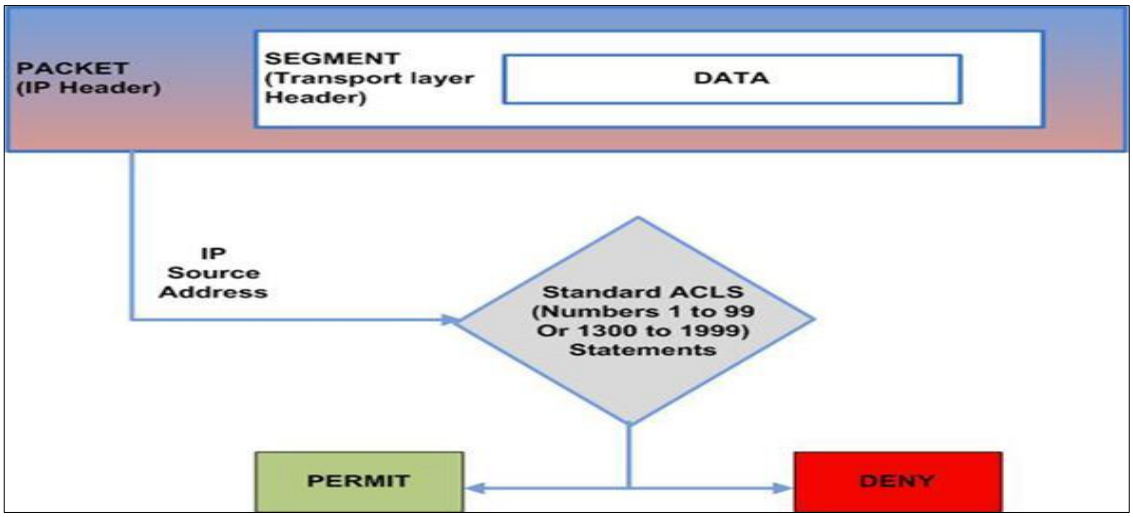


Fig 3.8 Standard Access Control List

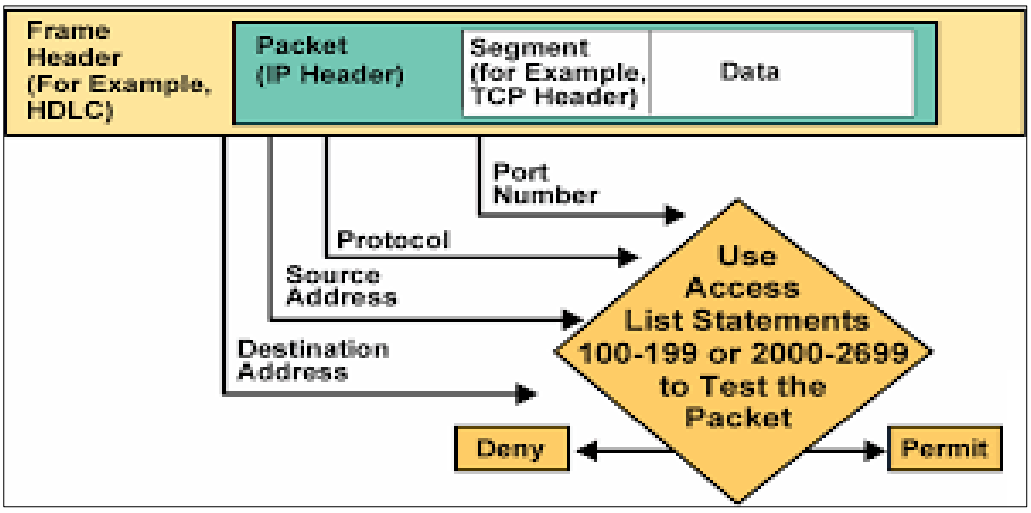


Fig 3.9 Extended Access List

This hint applies to the placement of your access list. When trying to save resources, remember that aninbound access list applies the filter conditions before the routing table lookup. An outbound access listapplies the filter conditions after the routing table lookup (Eronen & Zitting, 2001).

Table 3.1 Classification of IP Addresses

Address	Wildcard Mask	Match Results
0.0.0.0	255.255.255.255	All addresses will match the accesslist conditions.
172.18.0.0/16	0.0.255.255	Network 172.18.0.0
172.18.5.2/16	0.0.0.0	Only host 172.18.5.2 matches
172.18.8.0	0.0.0.7	Only subnet 172.18.8.0/29 matches
172.18.8.8	0.0.0.7	Only subnet 172.18.8.8/29 matches
172.18.8.15	0.0.0.3	Only subnet 172.18.8.15/30matches
10.1.2.0	0.0.252.255 (noncontiguous bits inmask)	Matches any even-numbered network in the range of 10.1.2.0 to10.1.254.0

3.5 Spread-Spectrum Technique

As the name ‘spread-spectrum’ suggests, this technique involves spreading the bandwidth to transmit data with more security. Spread spectrum technique was initially developed for military applications to avoid jamming and interception because a signal spread over a wider bandwidth make jamming more difficult. Bandwidth expansion is achieved by modulating again the modulated signal with a spreading code. This code is generated by a pseudo noise or pseudorandom number generator. A number of modulated signals (representing a number of users) could be carried over the same bandwidth by using a different code for each user. The first type of spread spectrum that was developed was

known as frequency hopping. A new type of spread spectrum is direct sequence(Moser & Gross, 1982)

3.5.1 Classification of Spread Spectrum Systems

Spread spectrum systems have been classified by their architecture and modulation concepts into the following categories as shown in Fig 3.9

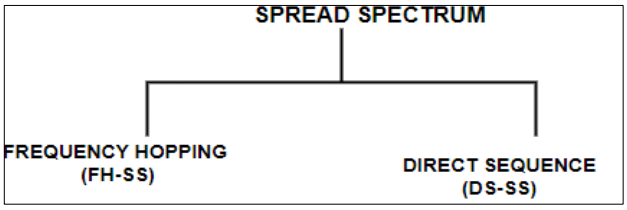


Fig 3.10 Classification of Spread Spectrum

The most frequently used spread spectrum techniques, DS and FH requires PN sequences for spreading, synchronization and dispreading. The PN sequences are described in next section.

3.5.2 Pseudo Noise Sequence

Pseudo noise sequence can simply be defined as a series of bits (1's and 0's) that seems to be random but repeat itself after *n* numbers (or bits) where *n* is the length of a Pseudo noise sequence (or PN code).The major work of pseudo noise sequence in wireless communication is:

- Spread the bandwidth of the user signal.
- Distinguish between different user signals sharing the same bandwidth by changing the PN sequence.

A random series of binary ones and zeros representing a PN sequence can be produced by PN generator. This PN sequence eventually repeats but appears to be random. PN sequence generated by an algorithm using some initial value called the 'Seed'. If the algorithm is good, the resulting sequences will pass many reasonable tests of randomness. At the receiver side, unless you know the algorithm and the seed. It is impractical to predict the sequence. Hence only a receiver that shares this information with a transmitter will be able to decode the signal successfully.

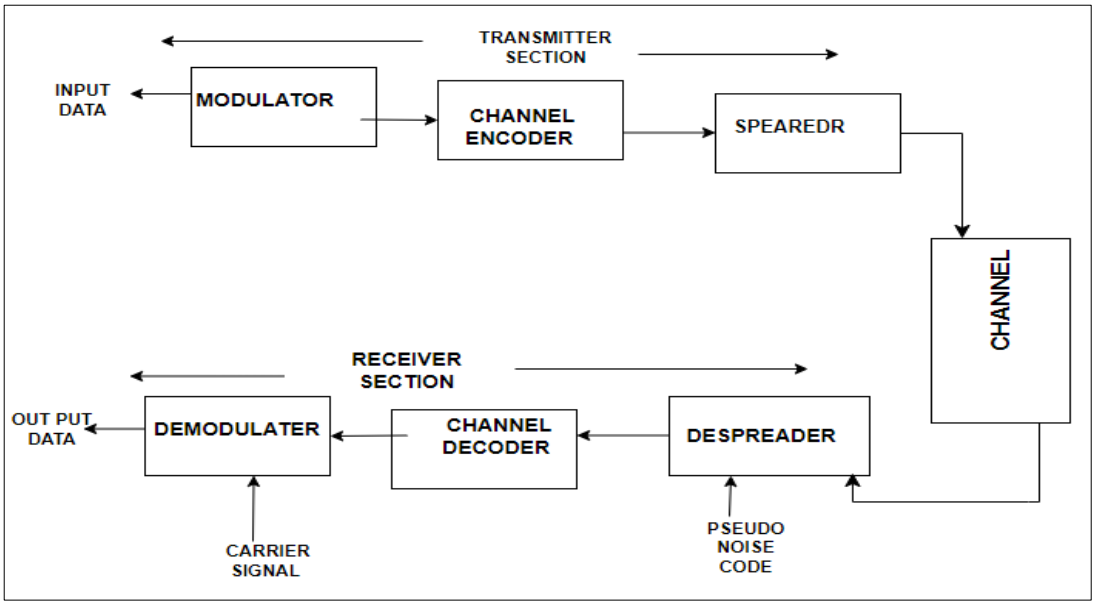


Fig 3.11 Block Diagram of Spread Spectrum Digital Communication System

The application of PN sequence in transmitter and receiver side is given as follows:

- **At transmitter side**: The correlator yields an encrypted digital representation of the original signal using PN sequence (chipping sequence). This encrypted signal is then spread over a very wide frequency spectrum.
- **At receiving side**: The signal is demodulated back to a narrow bandwidth and then fed to a ‘ decor relator’. This decor relator uses its unique PN code (chipping code) to extract only the information intended for it. A signal correlated with a given chipping sequence and decor related with the same chipping sequence returns the original signal. Decorrelation the signal with the wrong PN sequence would result in pure noise (Mutagi, 1996).

Working Detail:

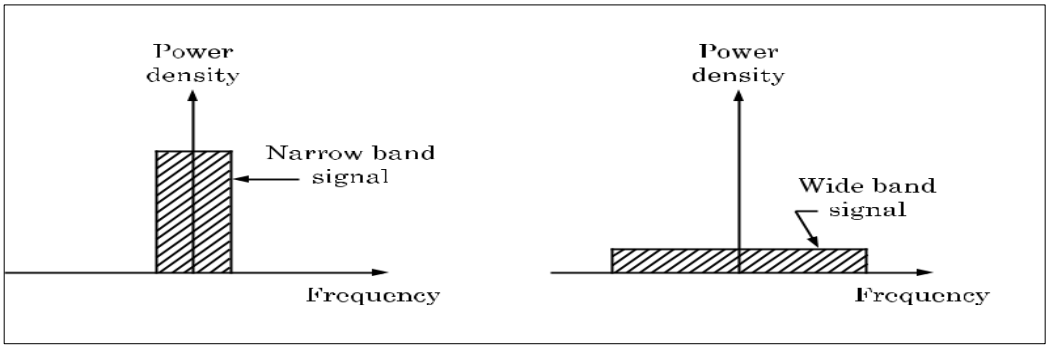
Following steps will clear the working of this system:

- Input data along with carrier signal is fed to the modulator.
- This modulated signal is then fed to a channel encoder that produces an analog signal with a relatively narrow bandwidth around some central frequency.
- After encoding, the signal is further modulated to spread the bandwidth using pseudo noise code i.e. a bandwidth spreading code.
- This spread spectrum signal is then transmitted over the channel.

- At the receiver side, the same pseudo noise spreading code is used to demodulate the spread spectrum signal.
- After demodulation, the spread spectrum signal is converted into narrow band. This signal is fed to channel decoder to recover the narrow band modulated signal.
- This decoded signal then finally pass again to demodulator where this signal is demodulated using carrier signal to recover the data bit.

3.5.3 Concept of Spreading and Dispreading

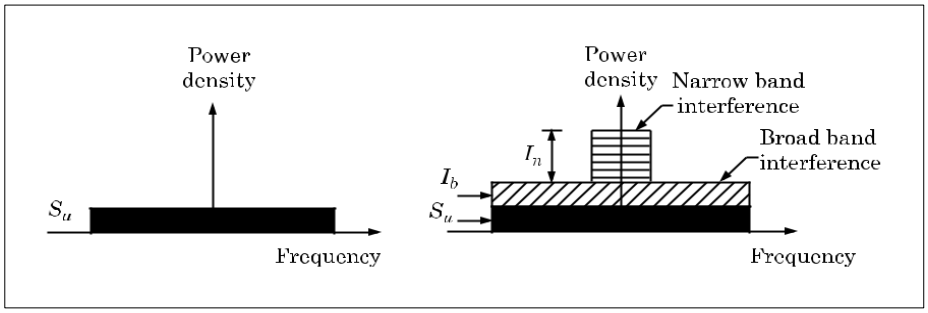
Conversion of a narrowband signal into a wide band spreaded signal has a lot of advantages as discussed in section. The main advantage is the reduction in narrowband interference. The signal is spreaded from the sender side (transmitter side) and it is desprreaded at the receiver side. Fig. 3.12 shows how a narrowband signal is converted into a wideband sign.



(*a*) Before Spreading (b) After Spreading

Fig 3.12 Spreading of a Narrowband Signal

Figure 3.13 (*a*) and (*b*) show that the energy needed to transmit the signal is the same in both cases (the shaded area shown in fig.) but the signal is now spread over a wider frequency range. The power level of the spread signal can be much lowers that of the original narrowband signal without losing any data.



(*a*) Signal at Transmitter side (*b*) Signal at receiver side

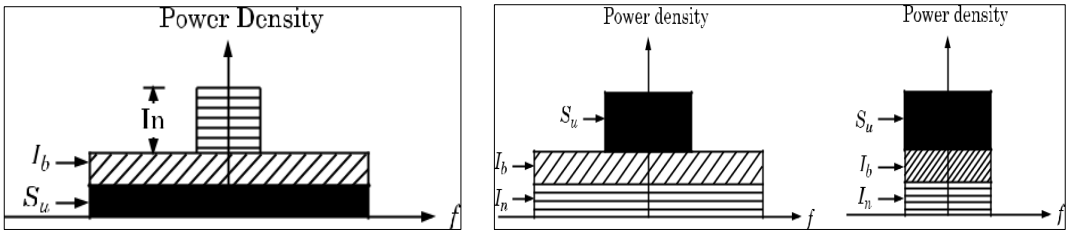
Fig 3.13 Interference Added During Transmission

When this narrowband signal is transmitted over a channel then some interference (narrowband and wideband) gets added in this signal i.e. received with the narrow-band signal at receiver side, as shown in Fig. 3.13.

Here $I_n \rightarrow$ Narrowband interference, $I_b \rightarrow$ Broadband interference and $S_u \rightarrow$ User Signal

At receiver side, a special process is done to remove the interference and recover the original signal. In the dispreading steps, the receiver performs the following operators. After these steps, received input [Fig. 3.14 (*a*)] changed into its replica [Fig. 3.14 (*b*)]

- Convert the spread user signal into a narrow band signal again.
- Spread the narrow band interference.
- Remain band interference as it is.
- After the conversion of broadband signal into narrowband signal, it is passed to bandpass filter to cut the left and right portion except narrow band signal shown in [Fig. 3.14 (*c*)]. By this way the original signal gets recovered because the original signal is much stronger than the remaining interference.



(a) Signal at Receiver in pass filter. (b) Replica of received Sign (c)Signal after passing through band

Fig 3.14 Dispreading of a wideband Signal

3.5.4 Direct Sequence Spread Spectrum (DS-SS)

So far we have discussed about spread spectrum now we will understand how spread spectrum is achieved using direct sequence. Direct sequence is a combination of bits (1*s* and 0*s*) that is used to code the user data. In DS-SS, user bit stream (user data) is exclusive-OR (XOR) with a random number (chipping sequence).

Chipping sequence is a set of smaller pulses which repeat with each user bit.EX-OR function is performed here due to the reason that EX-OR gives an output high at unequal input bits (0 and 1 & 1 and makes its output low at equal bits (00 and 11). Fig. 3.3 shows the truth table and symbol of EX-OR gate N.

Table 3.2 Truth Table

I/P–1	I/P–2	Output
0	1	1
1	0	1
1	1	0

The working can be explained by the follows

- When first input is zero, the output follows the second input.
- When first input is one, the output is replica of second input.

Now we can assume user bits as first input and chipping sequence as second input. It means that it user bit is '0' then the result is same as chipping sequence, and if user bit is '1' then the result is complement (or reverse) or chipping sequence.

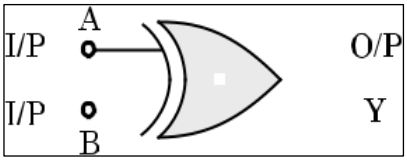


Fig 3.15 Truth Table and EX -OR Gate Symbole

This operation can be easily understood by the following example:

- User bits (I/p-1) = 0 1 1 0
- Chipping sequence (I/p-2) = 1010

Then the result is either the sequence 1010 (if user bit equals 0) or its complement (if user bit equals 1), as shown in Fig below.

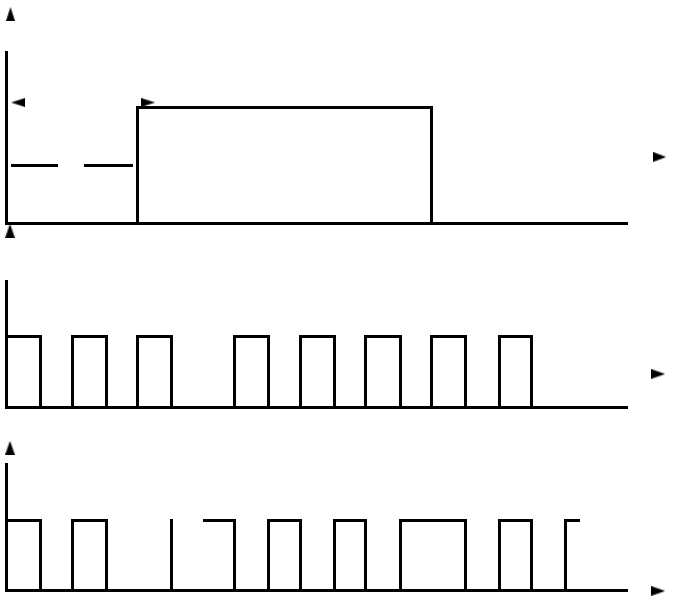


Fig 3.16 Spreading The Signal With DS-SS

Here in Fig 3.14, t_b represents each user bit duration and t_c represents chipping bit duration. Sometimes the chipping sequence is also known as Pseudo-noise sequence. From the above example (as shown in Fig 3.17) we may conclude that a 4 bit chipping sequence (spreading code) spreads each user bit 4 times greater than 1 bit spreading code.

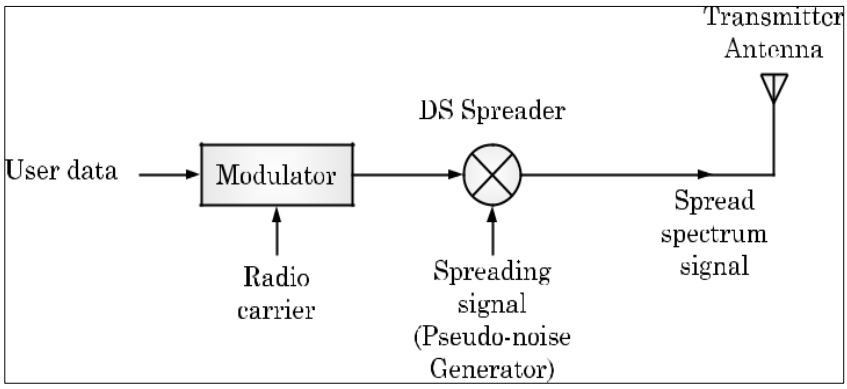


Fig 3.17 DS-SS Transmitter

The first step that is performed in the transmitter section is modulation of the user data with carrier signal. The modulated signal is then speeded with the chipping sequence (or spreading signal or pseudo noise signal) that is generated by pseudo noise generator. This signal is then transmitted using transmitting antenna.

3.5.5 DS-SS Receiver

DS-SS Receiver performs just the inverse function of the transmitter. The reconstruction process of the original data in the receiving path is more complex than that in transmitting path due to addition of the noises and multipath propagation. The very first step in the detection is that the receiver has to know the original chipping sequence that was used in transmitter to spread the signal. Sequences at the transmitter and receiver have to be precisely synchronized. This chipping sequence is then finally produced with the incoming signal received from antenna and given to integrator section that add all these products. This process is also known as correlation and the device performing this function is 'correlator'. Then the desprreaded signal is given to demodulator where the radio carrier is detected and original data (that was sent during transmission) is received demodulator where the radio carrier is detected and original data (that was sent during transmission) is received(Kohno et al., 1995).

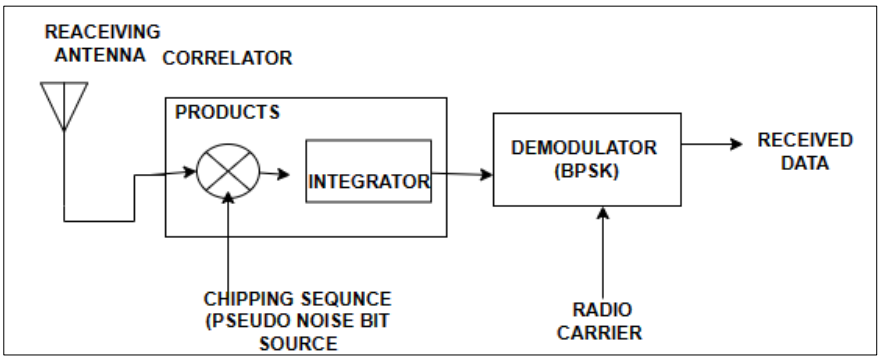


Fig 3.18 DS-SS Receiver

3.5.6 Frequency Hopping Spread Spectrum (FH-SS)

In the previous type of spread spectrum hopping technique (i.e. DS-SS), we have studied that the user data is speeded in bandwidth with the chipping sequence via digital modulation. The FH-SS scheme as an implementation concept similar to DH-SS system. In FH-SS, the signal is broadcasted over a random series of radio frequencies, hopping from one frequency to other fixed intervals. At receiver side, the message is reconstructed by hopping between same frequencies in synchronization with the transmitter. The total available bandwidth of the system is divided into many smaller bandwidths plus guard spaces between each bandwidth. Transmitter and receiver stay on one of these channels at one time and then hop on to another channel. According to hopping sequence, the FH-SS system is divided into two parts. Namely, slow frequency hopping (SFH) and fast frequency hopping (FFH).

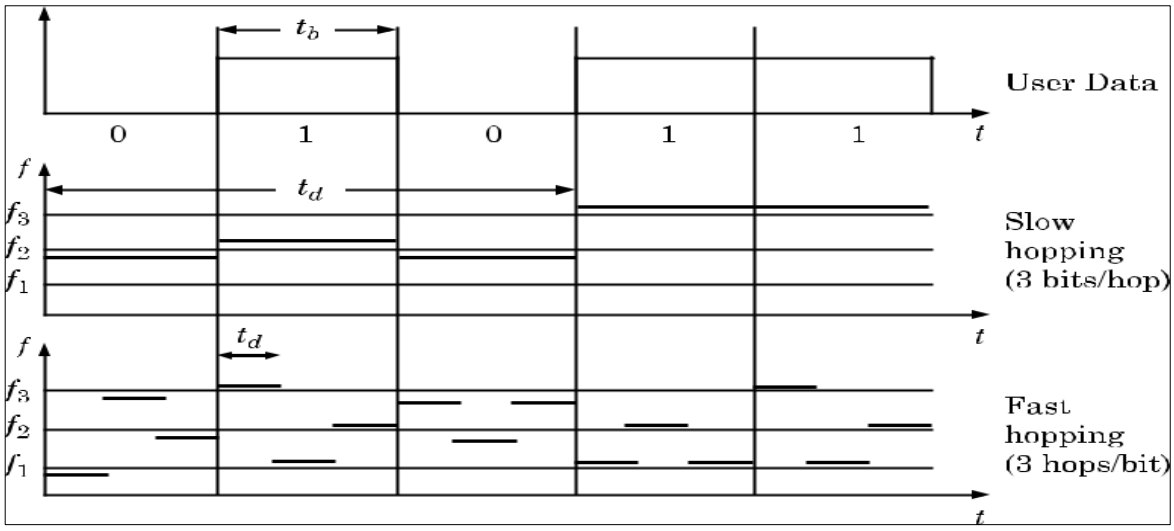


Fig 3.19 Slow and Fast Frequency Hopping

In Fig. 3.19, let hopping rate is denoted by t_h and data rate is denoted by t_d then in SFH → $t_h < t_{d\ and}$ in FFH → $t_h > t(i)$.

Slow Frequency Hopping: In slow frequency hopping system, the hopping rate (switching from frequency to frequency) is slower than the user data rate. It means that there are several or many bits per frequency hop. Fig. 4.11 shows that the transmitter uses frequency f_2 for transmitting the first three bits. After transmitting these three bits, the transmitter hops to the next frequency f_z.

(*ii*) Fast Frequency Hopping: In FFH system, the hopping rate is higher than user data rate. Therefore there are many hops per frequency bit. In the example of Fig. 3.22 the transmitter hops three times during a bit period. At the transmission of next bit, transmitter again hops three times (frequency changes three times.

3.5.7 FH-SS Transmitter

The first step in FH-SS transmitter is the modulation of user data (binary data) using some digital to analog encoding scheme, such as FSK or BPSK. For example, the modulating scheme uses FSK that generate:

1. f_0 frequency for binary 0, and 2. f_1 frequency for binary 1.

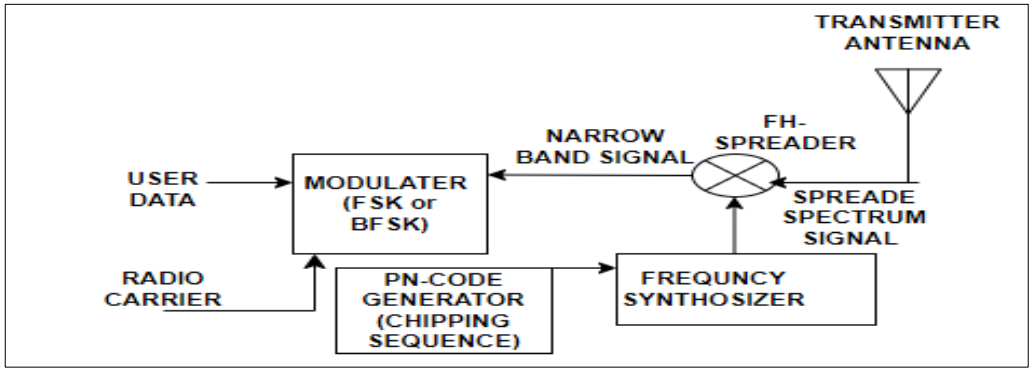


Fig 3.20 FH-SS Transmitter

This modulated signal is then fed to FH-SS spreader for spreading of modulated signal. In FH-spreader section, the chipping/ hopping sequence (i.e. generated by PN code generator) is fed into a frequency synthesizer. Here, each bits of the PN code generator specifies one of the 2^n carrier frequencies. At next n^k bit sequence, a new carrier frequency is generated. Let, the frequency synthesizer generate the carrier frequency f_C. Now, in FH-spreader, a second modulation takes place that spreads the signal with the frequency,

1. $f_c + f_0$ for binary 0, and 2. .$f_c + f_1$ for binary 1 respectively.

This spreaded signal over frequency f_c is transmitted through transmitting antenna.

3.5.8 FH-SS Receiver

The receiver section of FH-SS system should work in synchronization with the transmitter section. A simplified block diagram of FH-SS receiver is shown in Fig. 3.21. Receiver section performs just the inverse function of transmitter to reconstruct the user data. Several fitters are also required for this operation (not shown in Fig. 3.20). On reception, the spread spectrum signal is demodulated using the same PN code (chipping sequence), that is why the receiver and transmitter should always work in synchronization. After passing through FH-despreader the spreaded signal is converted into narrow-band signal. Here, it is again demodulated to reproduce the original user data (Liu, 2011).

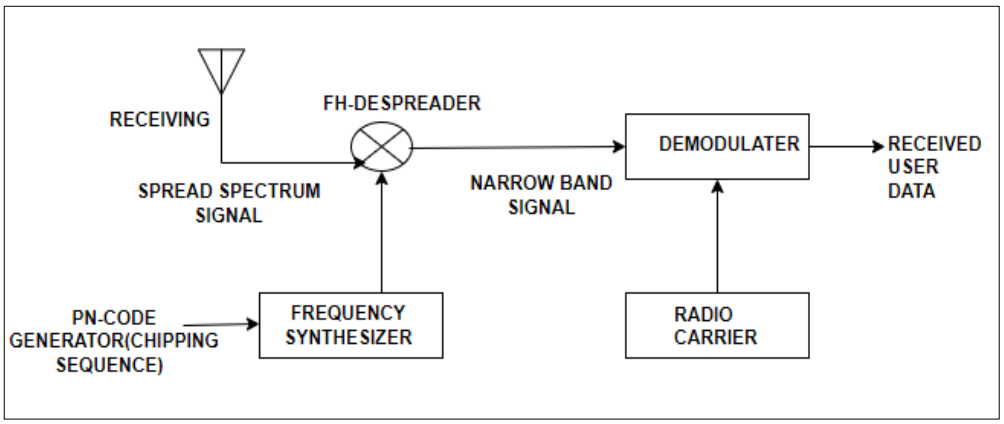


Fig 3.21 FH-SS Receiver

CHAPTER FOUR

4. RESULT AND DISCUSSION

4.1 RESULTS

This chapter presents both results and discusions based on simulation results and theoretical analysis. It ephesasis on C5IRS system on the top of C4IRS system which is the future target in moderen military organization. The result is depending on cyber and electronocs warfare defence.

4.1.1 Cyber,Information and Computer Security

An access list control mechanism is one the two defense cyber security, information security and computer security defense in c4isr it is a sequential list that consists of at least one permit statement and possibly one or more deny statements. In the case of IP access lists; these statements can apply to IP addresses, upper-layer IP protocols, or other fields in IP packets. Access lists are identified and referenced by a name or a number.

Access lists act as packet filters, filtering packets based on the criteria defined in each access list. After you configure an access list, for the access list to take effect, you must either apply the access list to an interface (by using the ip access-group command), a vty (by using the access-class command), or reference the access list by any command that accepts an access list. Multiple commands can reference the same access list Firewalls provide the ability to control access to the protected network. The network could be effectively sealed off from unwanted access or allow limited access to mail servers or information servers. Firewalls also provide access control from the protected network to the Internet.

From figure 4.1 the topology is shown as 4 user Ip address of 178.165.80.1, 178.165.80.2, 178.165.80.3 and 178.165.80.4 are get the internet access from ISP Ip address of 1.1.6.7, but the user shown on network topology IP address 192.168.100.1, 192.168.100..2 and 192.168.100.3 are outside of our network topology, and also maybe those thee user are a hacker due this we use access list control deny the flow of traffic of those users. The due to result of these phenomena the hacker cannot access our server

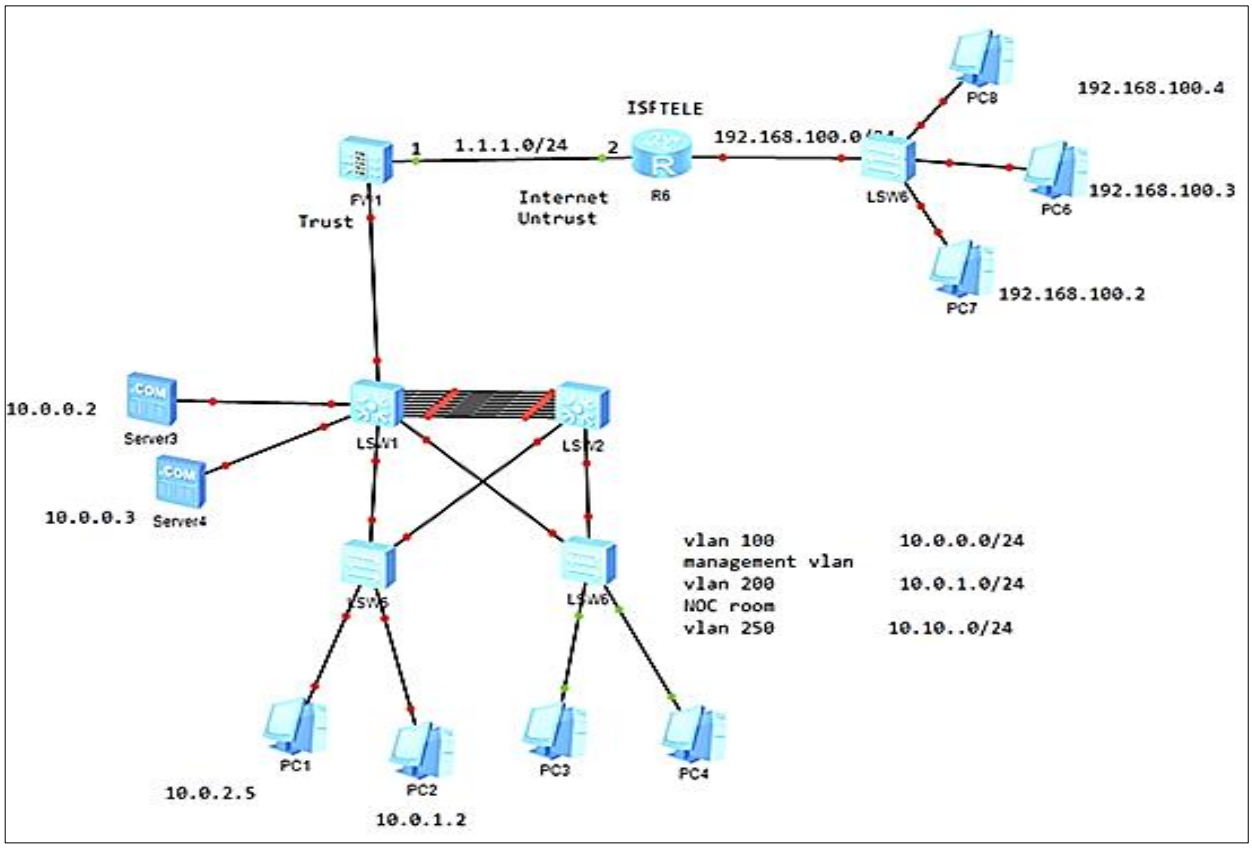


Fig 4.1 Organizational Network Topology

From figure 4.2 showun below is to permit tfrom intrnal organization network tafi flow for any user between from out side IP address to 172.168.100.2 tthe internal network IP address 178.165.80.1 ,that means from any internal netwok we can acess any out side net work by acess list control of permit techenic.the meaning that we are acess from any intrnal network to out side net work.

```
Welcome to use PC Simulator!

PC>ping 192.168.100.2

Ping 192.168.100.2: 32 data bytes, Press Ctrl_C to break
Request timeout!
From 192.168.100.2: bytes=32 seq=2 ttl=126 time=235 ms
From 192.168.100.2: bytes=32 seq=3 ttl=126 time=203 ms
From 192.168.100.2: bytes=32 seq=4 ttl=126 time=172 ms
From 192.168.100.2: bytes=32 seq=5 ttl=126 time=172 ms

--- 192.168.100.2 ping statistics ---
  5 packet(s) transmitted
  4 packet(s) received
  20.00% packet loss
  round-trip min/avg/max = 0/195/235 ms

PC>
```

Fig 4.2 Ping From 192.168.100.2 to 10.20.2.5

From figure 4.3 shown below is to permit from internal organization network tafi flow for any user between from outside IP address to 172.168.100.1 the internal network IP address

178.165.80.1, that means from any internal network we can access any outside network by access list control of permit techenic, the meaning that we are access from any internal network to outside network.

```
PC>ping 192.168.100.1

Ping 192.168.100.1: 32 data bytes, Press Ctrl_C to break
From 192.168.100.1: bytes=32 seq=1 ttl=254 time=109 ms
From 192.168.100.1: bytes=32 seq=2 ttl=254 time=140 ms
From 192.168.100.1: bytes=32 seq=3 ttl=254 time=125 ms
From 192.168.100.1: bytes=32 seq=4 ttl=254 time=78 ms
From 192.168.100.1: bytes=32 seq=5 ttl=254 time=94 ms

--- 192.168.100.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 78/109/140 ms
```

Fig 4.3 Ping From 192.168.100.1 to 10.0.1.5

The figure 4.4 shown below is to permit from internal organization network tafi flow for any user between from outside IP address to 172.168.100.3 the internal network IP address 178.165.80.1 ,that means from any internal network we can access any outside network by access list control of permit techenic, the meaning that we are access from any internal network to outside network.

```
PC>ping 192.168.100.3

Ping 192.168.100.3: 32 data bytes, Press Ctrl_C to break
From 192.168.100.3: bytes=32 seq=1 ttl=126 time=203 ms
From 192.168.100.3: bytes=32 seq=2 ttl=126 time=187 ms
From 192.168.100.3: bytes=32 seq=3 ttl=126 time=141 ms
From 192.168.100.3: bytes=32 seq=4 ttl=126 time=141 ms
From 192.168.100.3: bytes=32 seq=5 ttl=126 time=187 ms

--- 192.168.100.3 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 141/171/203 ms
```

Fig 4.4 Ping From 192.168.100.3 to 10.0.1.6

The figure 4.5. shown below is the network traffic outside our net should be deny the access list control because my be this traffic attack our all network infrastructure and hack our server .due this any the outside of IP address 172.168.100.3 cannot access friendly network

infrastructure the IP address of 10.0.0.2, that means from any outside traffic the farewell, should be block this IP.

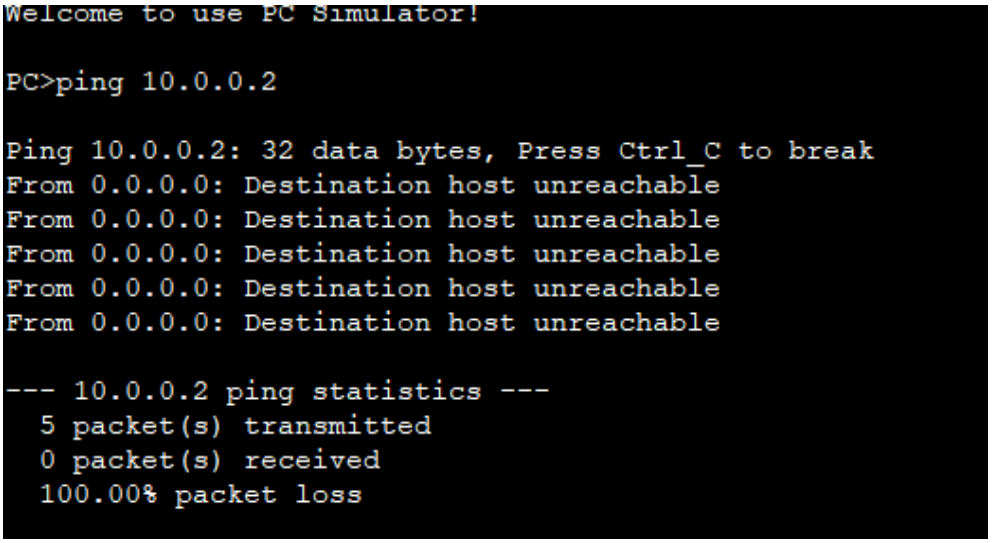


Fig 4.5 Ping From 10.0.0.2 to 192.168.100.1

The figure 4.6 shown is the network traffic outside our net should be deny the access list control because my be this traffic attack our all network infrastructure and hack our server .due this any the outside of IP address 172.168.100.2 cant not access friendly network infrastructure the IP address of 10.0.0.3, that means from any outside traffic the farewell, should be block this IP.

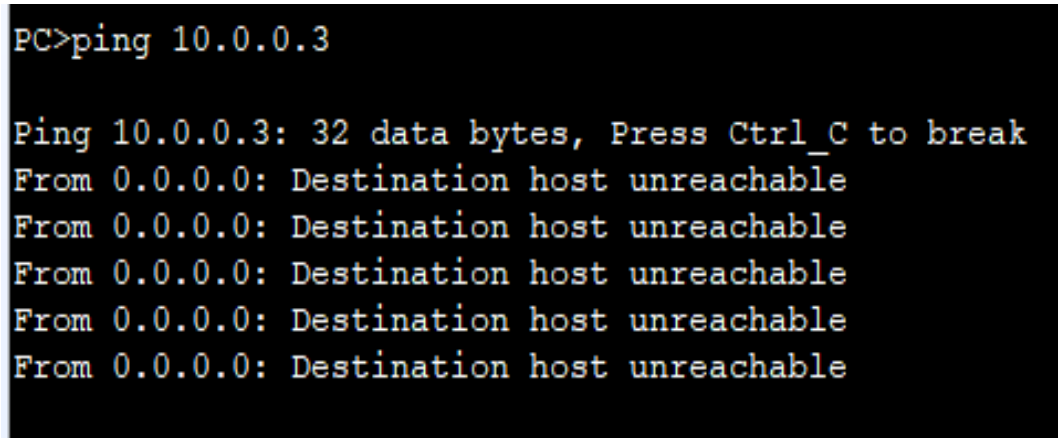


Fig 4.6 Ping From 10.0.0.2 to 192.168.100.2

The figure 4.7 shown below is the network traffic outside our net should be deny the access list control because my be this traffic attack our all network infrastructure and hack our server .due this any the out outside of IP address 172.168.100.1 cannot access friendly network infrastructure the IP address of 10.0.2.3, that means from any outside traffic the farewell, should be block this IP.

Fig 4.7 Ping From 10.0.0.2 to 192.168.100.1

4.1.2 Spread Spectrum

Spread Spectrum refers to a system originally developed for military applications, to provide secure communications by spreading the signal over a large frequency band. The increasing demand for wireless communications has problems due to limited spectrum efficiency and multipath propagation. The use of spread spectrum communication has simplified these problems. In the spread spectrum, signals from different sources are combined to fit into larger bandwidth.

Most stations use air as the medium for communication, stations must be able to share the medium without an interception and without being subject to jamming from a malicious intruder. To achieve this, spread-spectrum techniques add redundancy means it uses extended bandwidth to accommodate signals in a protective envelope so that more secure transmission is possible. The spread code is a series of numbers that looks random but are actually a pattern. The original bandwidth of the signal gets enlarged (spread) through the spread code show as figure 4.7

On figure 4.8 Pseudo Random Number Generator (PRNG) refers to an algorithm that uses mathematical formulas to produce sequences of random numbers. PRNGs generate a sequence of numbers approximating the properties of random numbers. A PRNG starts from an arbitrary starting state using a seed state. Many numbers are generated in a short time and can also be reproduced later, if the starting point in the sequence is known. Hence, the numbers are deterministic and efficient**.**

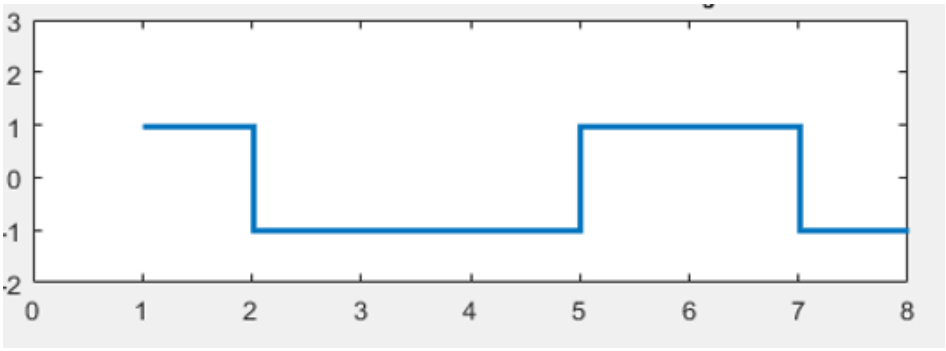


Fig 4.8 Pseudo Random Bit Sequence

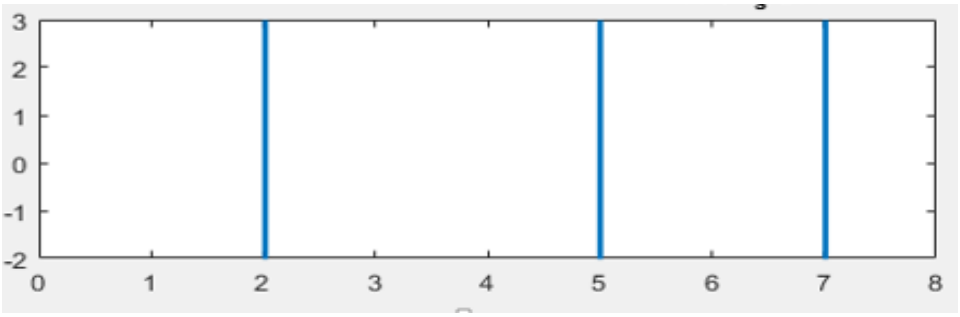


Fig 4.9 Multiplier Out Put Sequence Bit

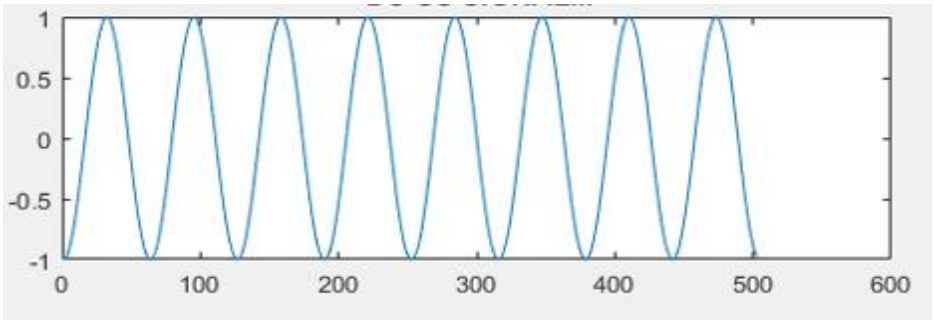


Fig 4.10 Spread Spectrum Signal

Figure 4.11 and figure 4.12 shows as Rayleigh fading is a statistical model for the effect of a propagation environment on a radio signal, such as that used by wireless devices. Rayleigh fading models assume that the magnitude of a signal that has passed through such a transmission medium (also called a communication channel) will vary randomly, or fade, according to a Rayleigh distribution, the radial component of the sum of two uncorrelated Gaussian random variables.

Rayleigh fading is viewed as a reasonable model for tropospheric and ionospheric signal propagation as well as the effect of heavily built-up urban environments on radio signals. Rayleigh fading is most applicable when there is no dominant propagation along a line of sight between the transmitter and receiver. If there is a dominant line of sight, Rici an fading may be more applicable. Rayleigh fading is a special case of two-wave with diffuse power (TWDP) fading ayleigh fading is a statistical model for the effect of a propagation environment on a radio signal, such as that used by wireless devices. Rayleigh fading models assume that the magnitude of a signal that has passed through such a transmission medium will vary randomly, or fade, according to a Rayleigh distribution, the radial component of the sum of two uncorrelated Gaussian random variables. Rayleigh fading is viewed as a reasonable model for tropospheric and ionospheric signal propagation as well as the effect of heavily built-up urban environments on radio signals. Rayleigh fading is most applicable when there is no dominant propagation along a line of sight between the transmitter and receiver. If there is a dominant line of sight, Rician fading may be more applicable.

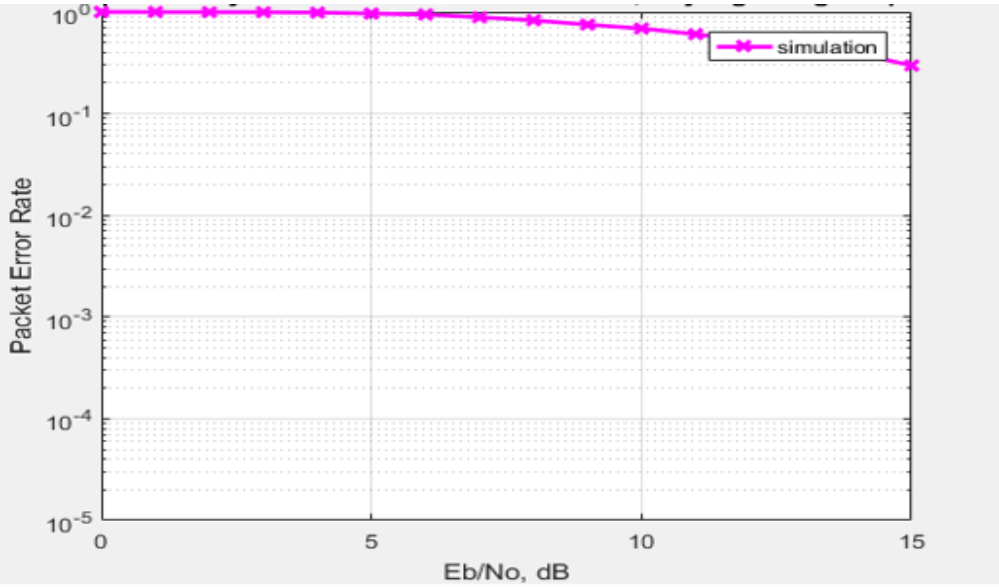


Fig 4.11 Rayleigh Curve For 16-QAM With DSSS Rayleigh Signal Top And Rank

From fig-4.13 and fig-4.14 to show that improve the signal detection performance of binary-sequence frequency hopping communication when the complementary channel is jammed, a binary-sequence frequency hopping communication system based on pseudo-random liner frequency modulation (LFM) is proposed.

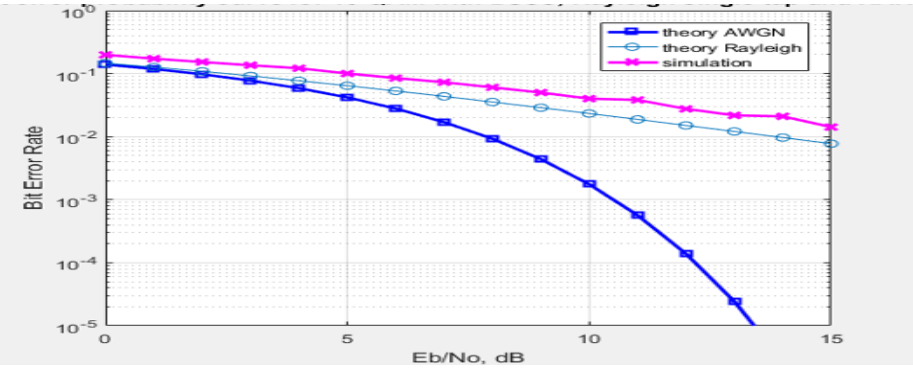


Fig 4.12 Packet Error Probability Curve For 16-QAM With DSSS Rayleigh Top Rank

The transmitting end uses the chirp signal to carry out the in-band spread spectrum of the binary-sequence frequency hopping signal, and then sends it out through the radio frequency front end. At the receiving end, the received signal is dehopped and processed by fractional Fourier transform. The source information is obtained by sampling decision. Firstly, a binary-sequence frequency hopping system model based on pseudo-random LFM is constructed. Secondly, the bit error rate expression of anti-partial band jamming and follower jamming under the Rice channel is derived.

The results show that this method has at least 5 dB performance gains than binary sequence frequency hopping for different parameter settings under partial band jamming and follower jamming, and the anti-jamming performance is significantly better than the conventional frequency hopping communication.

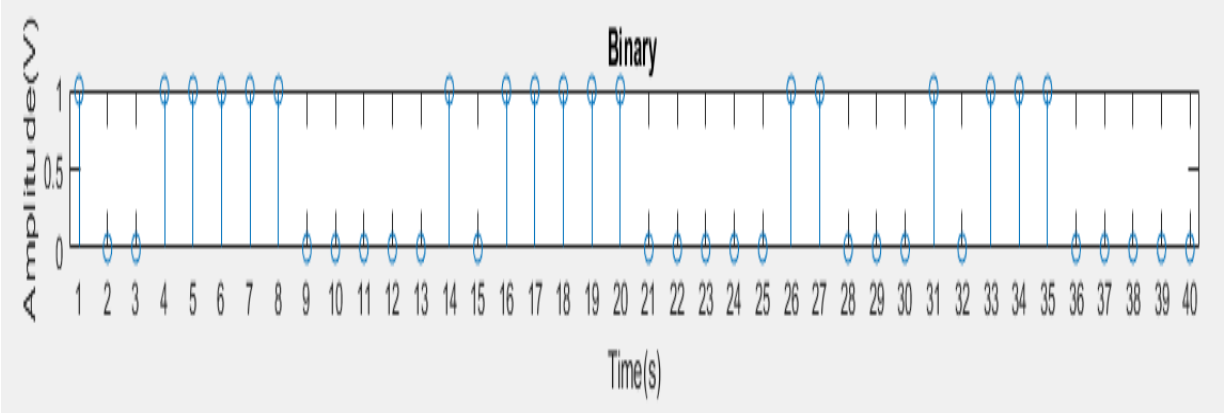


Fig 4.13 Binary Information

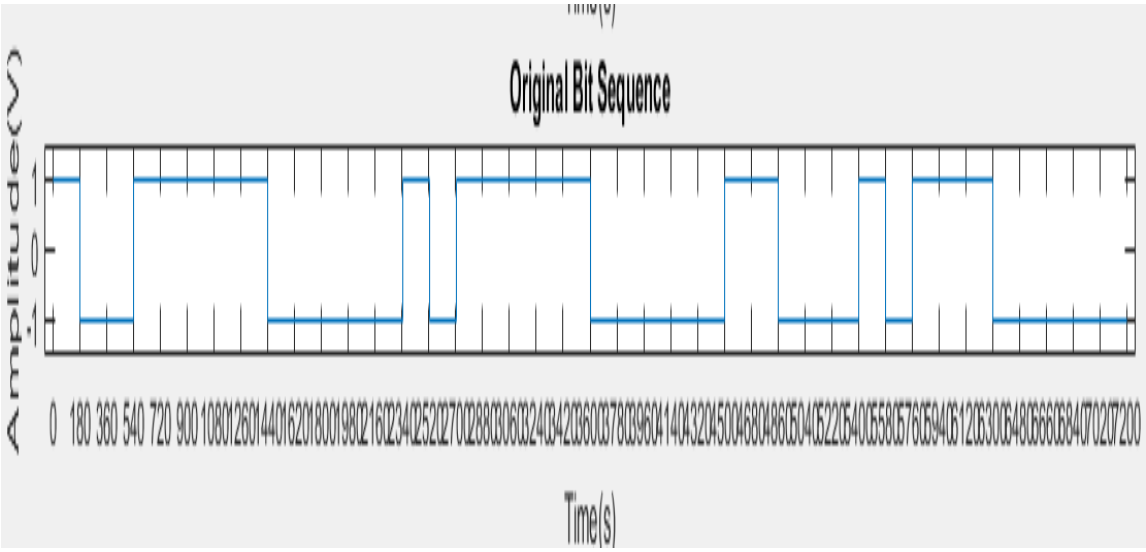


Fig 4. 14 Original Bit Sequence

From figure 4.15 and figure 4.16 the first modulation considered is binary phase shift keying. In this scheme during every bit duration, denoted by T, one of two phases of the carrier is transmitted. These two phases are 180 degrees apart. This makes these two waveforms antipodal.

Any binary modulation where the two signals are antipodal gives the minimum error probability (for fixed energy) over any other set of binary signals. The error probability can only be made smaller (for fixed energy per bit) by allowing more than two waveforms for transmitting information

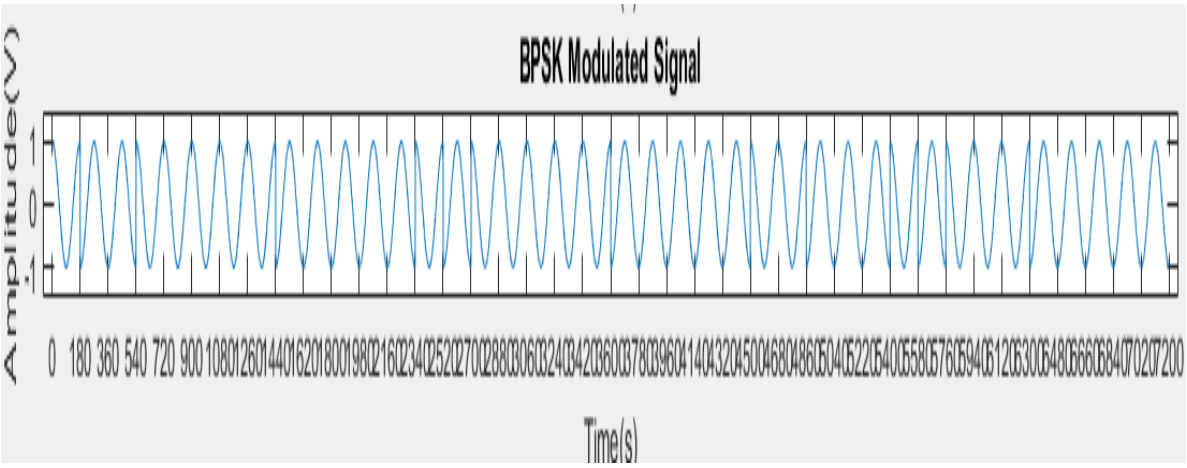


Fig 4.15 BPSK Modulated Signal

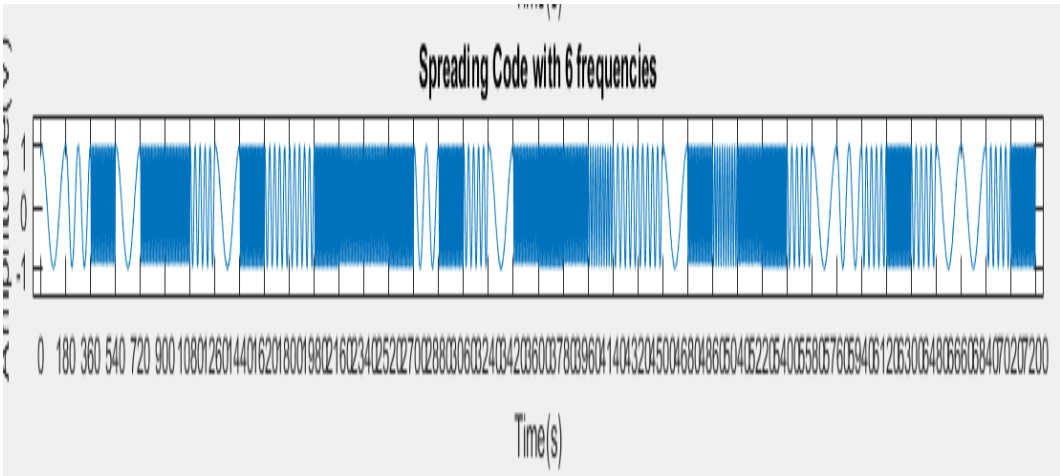


Fig 4.16 Spreading Code With 6 Frequencies

From figure 4.17 and fig-14.18 will be discussed that during DSSS signal, the PN sequence spreads the spectrum of the signal by the chipping rate, resulting in the instantaneous widening of the spectrum. On the other hand, in FHSS, the PN sequence is used to drive the synthesizer and pseudo-randomly hop the signal bandwidth across a much wider band. In this case, the synthesizer is being sequentially programmed with different frequencies by the PN sequence to modulate the desired signal over a much wider frequency band.

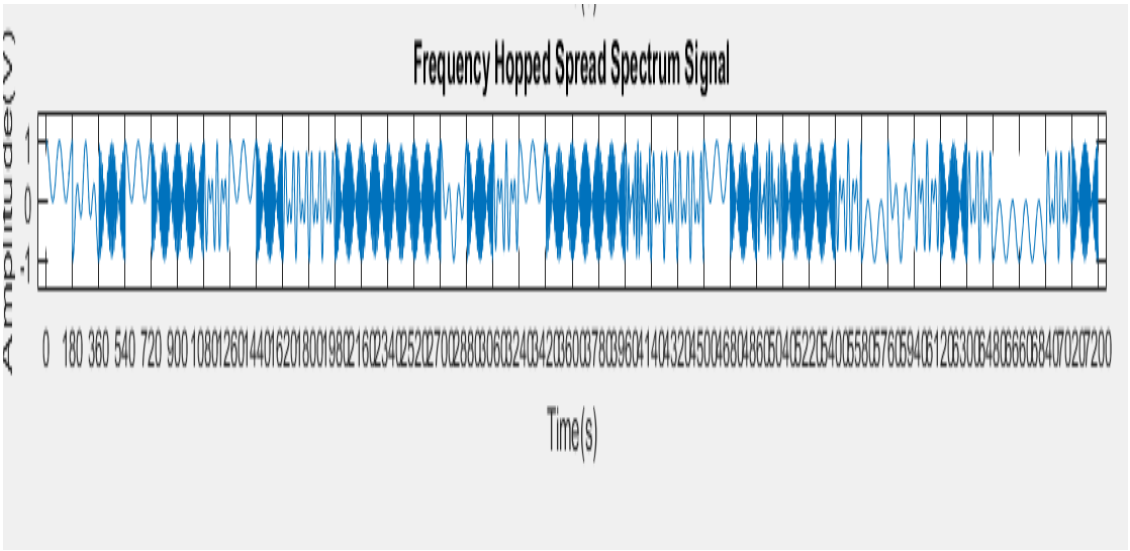


Fig 4.17 Frequency Hopping Spread Spectrum Signal

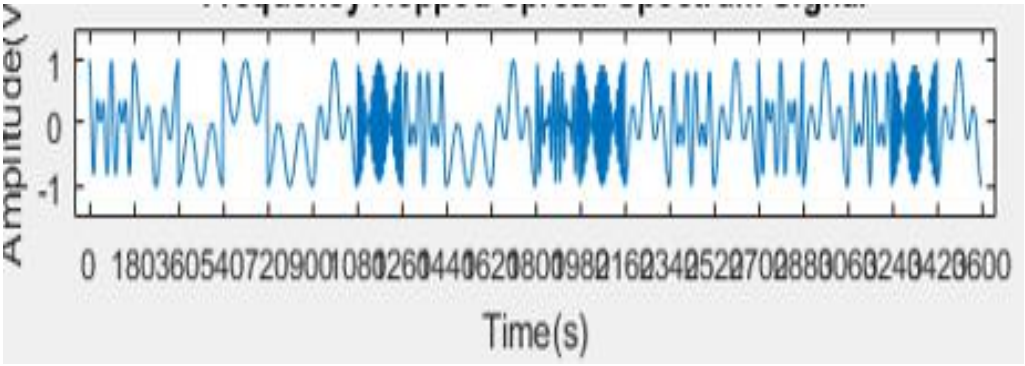


Fig 4.18 FH Spread Spectrum Signal

In the Figure 14.19 in the coherent receiver, the received signal is multiplied by Demodulation is the process of restoring the data bits back from a digitally modulated signal In BPSK, we take a stream of bits and map these bits to a stream of symbols with value -1 or +1. Next, each symbol is expanded into a pulse shape. The pulse shape is chosen such that the bandwidth required to transmit the symbol sequence is minimal, and that the symbols do not affect each other in a continuous-time symbol stream. The minimal bandwidth for a continuous-time symbol means one symbol per second per Hz of bandwidth. Next the smooth symbol stream is multiplied by a carrier.

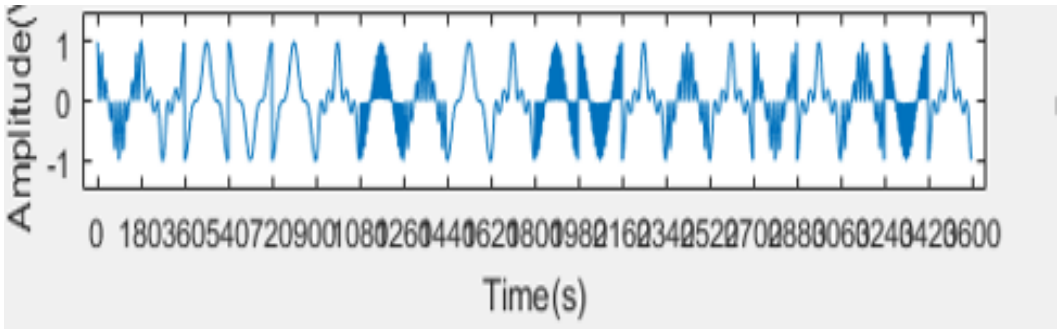


Fig 4.19 Demodulated BPSK Signal

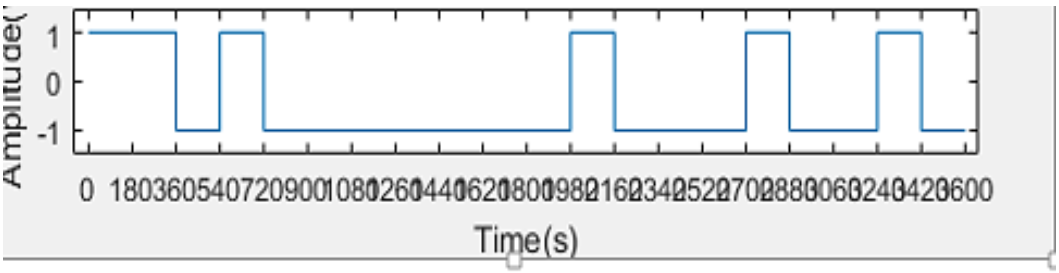


Fig 4.20 Demodulated Binary Signal

From figure 4.21 shown as a chirp is a signal in which the frequency increases (up-chirp) or decreases (down-chirp) with time. In some sources, the term chirp is used interchangeably with sweep signal. It is commonly applied to sonar, radar,

and laser systems, and to other applications, such as in spread-spectrum communications (see chirp spread spectrum). This signal type is biologically inspired and occurs as a phenomenon due to dispersion (a non-linear dependence between frequency and the propagation speed of the wave components). It is usually compensated for by using a matched filter, which can be part of the propagation channel. Depending on the specific performance measure, however, there are better techniques both for radar and communication. Since it was used in radar and space, it has been adopted also for communication standards. For automotive radar applications, it is usually called linear frequency modulated waveform (LFMW).

In spread-spectrum usage, surface acoustic wave (SAW) devices are often used to generate and demodulate the chirped signals. In optics, ultrashort laser pulses also exhibit chirp, which, in optical transmission systems, interacts with the dispersion properties of the materials, increasing or decreasing total pulse dispersion as the signal propagates. The name is a reference to the chirping sound made by birds; see bird vocalization.

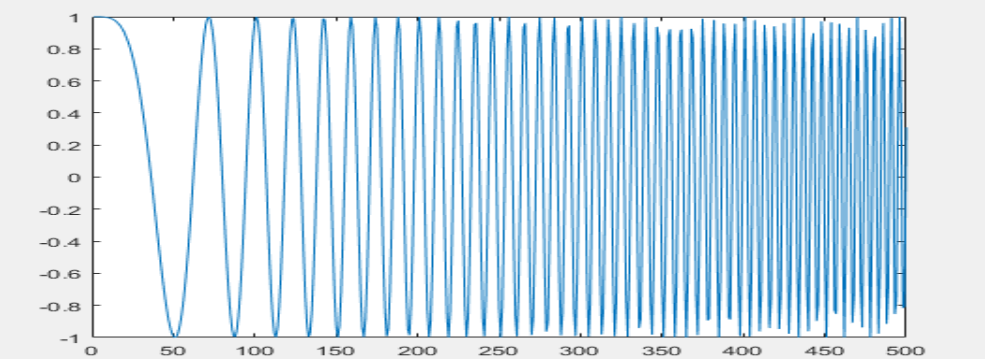


Fig 4.21 Direct Spread Spectrum FH Chirp Signal

In fact, to make our work very clear, the difference between the C4ISR and C5ISR presented as a comparative analysis as it can be shown in the following Table 4.1.

Table 4.1 The Main Difference Between The C4ISR And C5ISR

Functions	C4ISR	C5ISR
Command	• The authority to direct, coordinate, and control forces.	• It requires the coordination of government agencies, military forces, and private sector companies.
Control	• The process of directing and organizing forces to achieve desired outcome.	• Protect military forces from cyber-attacks. It provides the tools and capabilities to identify and mitigate cyber threats, as well as to recover from cyber-attacks.
Communications	• The means of exchanging information between different elements of a force.	• It allows military forces to gather and process information from a variety of sources, including sensors, satellites, and human intelligence.
Computers:	• The systems used to process and store information.	• It requires the integration of a wide range of technologies, including sensors, communications systems, computers, and software.
Intelligence	• The collection, analysis, and interpretation of information about an adversary or potential adversary.	• It allows military forces to gather and process information from a variety of sources, including sensors, satellites, and human intelligence.
Surveillance	• The systematic observation of an area or person in order to gather information.	• It provides the tools and capabilities to identify and mitigate cyber threats, as well as to recover from cyber-attacks.
Reconnaissance	• The collection of information about an area or person by direct observation or through the use of sensors.	• Complex and constantly evolving system. It requires the integration of a wide range of technologies, including sensors, communications systems, computers, and software.
Vulnerability	• As military forces become increasingly reliant on information systems and networks, they are also becoming more vulnerable to cyber attacks.	• A more comprehensive framework than C4ISR that includes the necessary elements to protect military forces from cyber-attacks and other threats.

5. CONCLUSION AND RECOMMENDATIONS

5.1 Conclusion

Communication is the one of the basic important for command and control for accomplished a mission. C5ISR which is the basic enabler of NCW for national arm force to increasing the mobility of forces in terms of accomplished the mission. like Optical fiber provides high capacity connectivity in (Tbps) but has lesser technology for remote deployment and also Satellite is the best suited to provide into probability, mobility and combat ability for remote and mobile setups due to easy deployment however it has limited bandwidth capacity and greater propagation delay. The SATCOM is a basic requirements for C5ISR. In deploying mobile tactical forces, also In providing ideal continuity for operational services.

The secure and reliable ICT infrastructure one of interface as an open system architecture approach allows easy interconnectivity and interoperability to connect all C5ISR nodes.

5.2 Recommendations

- In this thesis, the performance of C5ISR system security spectrum is evaluated under simulation result only using the MATLAB and eNSP software tool. In the future, the experimental result of C4ISR system security technique should be done using the software define radio and commuter network security .such as all wireless military radio communication like HF,VHF,UHF frequency range.
- In this thesis, we were assumed that the transmitted signal from those frequency range as a BPSK signal as well as chirp signal due to anti -enemy electronics ware fare resist.. In the future, the proposed techniques should be evaluated by considering different types of wireless radio signals such as QPSK, M-ary and TDMA signal.
- Another on the hand interims of defends cyber-attack from C4ISR infrastructure possibility for future research is to adapt the proposed access list control scheme to analyze enemy network attack.
- In order to provide talented and qualified C5ISR and cyber manpower for military organization there should be clear human resource development policy, strategy sand roadmap.
- Considering the sources of manpower, the eligible workforce should be secured at the very beginning from military college, from military academies and civilian cyber security dedicated personnel.
- We have to think in advance the realization of the project might force us to some extent

to reshuffle of organizational structure and to mobilize our skilled human power.

- The needed E-Map with best quality and all level of details/scales, Imagery and other GIS modules should be necessary identify location
- Special Operation Forces for special mission should be equipped with new and advanced communication systems appropriate for their special mission.

REFERENCES

Al-Darwish, A. I., & Choe, P. (2019). A framework of information security integrated with human factors. *HCI for Cybersecurity, Privacy and Trust: First International Conference, HCI-CPT 2019, Held as Part of the 21st HCI International Conference, HCII 2019, Orlando, FL, USA, July 26–31, 2019, Proceedings 21*, 217–229.

Alberts, D. S., & Hayes, R. E. (2003). *Power to the edge: Command... control... in the information age*. Office of the Assistant Secretary of Defense Washington DC Command and ….

Alberts, D. S., Huber, R. K., & Moffat, J. (2010). *NATO NEC C2 maturity model*. OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE WASHINGTON DC COMMAND AND ….

Auger, A., Gouin, D., & Roy, J. (2006). Decision support and knowledge exploitation technologies for C4ISR. *Available: http:/pubs. drdc. gc. ca/PDFS/unc52*, 525876.

Barzelay, M., & Campbell, C. (2003). *Preparing for the future: Strategic planning in the US Air Force*. Brookings Institution Press.

Billo, C., & Chang, W. (2004). Cyber warfare. *An Analysis of the means and motivations of selected nation states. Dartmouth, ISTS*.

Bittencourt, R. P. (1976). *Electronic warfare technology*. https://apps.dtic.mil/sti/citations/ADA028210%0Ahttps://apps.dtic.mil/sti/pdfs/ADA028210.pdf

Bommakanti, K., & Observer Research Foundation. (2020). *Strengthening the C4ISR capabilities of India's armed forces : the role of small satellites* (Number June).

Boyd, J. A., Harris, D. B., King, D. D., & Welch Jr, H. W. (1978). Electronic countermeasures. *Electronic Countermeasures*.

December, U. (2022). *China Naval Modernization : Implications for U . S . Navy Capabilities — Background and Issues for Congress*.

Demchak, C. C. (2011). *Wars of disruption and resilience: cybered conflict, power, and national security*. University of Georgia Press.

Eronen, P., & Zitting, J. (2001). An expert system for analyzing firewall rules. *Proceedings of the 6th Nordic Workshop on Secure IT Systems (NordSec 2001), 11*, 100–107.

Güvenlik Kavramı", U. İ. (2008). *the Importance of Electronic Warfare Systems in the Security*

of the Future and Turkey ' SElectronic Warfare Systems. *5*, 24.

Heikell, J. E. (2005). Electronic warfare self -protection of battlefield helicopters: A holistic view. In *ProQuest Dissertations and Theses*. http://ezproxy.rice.edu/login?url=https://search.proquest.com/docview/305359591?accountid=7064%0Ahttp://sfxhosted.exlibrisgroup.com/rice?url_ver=Z39.88-2004&rft_val_fmt=info:ofi/fmt:kev:mtx:dissertation&genre=dissertations+%26+theses&sid=ProQ:ProQuest+Dis

Jinfeng, L., Bingcheng, S., & Zheng, D. (2021). Research on C4ISR Requirement Demonstrating Method Based on System Configuration. *IOP Conference Series: Earth and Environmental Science*, *1802*(4). https://doi.org/10.1088/1742-6596/1802/4/042084

Kang, J. (1997). Information privacy in cyberspace transactions. *Stan. L. Rev.*, *50*, 1193.

Karppinen, K. (2005). *Security Measurement based on Attack Trees in a Mobile Ad Hoc Network Environment: Master's thesis*. VTT Technical Research Centre of Finland.

Khawaja, A. (2015). *Cryptography and Network Security Assessment of QPR Software's QPR Suite 2015.1*.

Kimani, K., Oduol, V., & Langat, K. (2019). Cyber security challenges for IoT-based smart grid networks. *International journal of critical infrastructure protection*, *25*, 36–49.

Kohno, R., Meidan, R., & Milstein, L. B. (1995). Spread Spectrum Access Methods for Wireless Communications. *IEEE Communications Magazine*, *33*(1), 58–67. https://doi.org/10.1109/35.339882

Kuppuswamy, P., & Al-Khalidi, S. Q. Y. (2014). Hybrid encryption/decryption technique using new public key and symmetric key algorithm. *International Journal of Information and Computer Security*, *6*(4), 372–382.

Lehto, M. (2020). Cyber security in aviation, maritime and automotive. *Computation and Big Data for Transport: Digital Innovations in Surface and Air Transport Systems*, 19–32.

Levis, A. H., & Wagenhals, L. W. (2000). C4ISR architectures: I. Developing a process for C4ISR architecture design. *Systems engineering*, *3*(4), 225–247.

Lilly, B., Moore, A. S., Hodson, Q. E., & Weishoff, D. (2021). *RAND's Scalable Warning and Resilience Model (SWARM): Enhancing Defenders' Predictive Power in Cyberspace*. RAND Corp.

Liu, Y. (2011). Frequency hopping spread spectrum: An effective way to improve wireless

communication performance. *Advanced Trends in Wireless Communications*, 187.

Lu, J. (2019). *Design Technology of Synthetic Aperture Radar*. John Wiley & Sons.

Metz, S. (1995). *Strategy and the revolution in military affairs: from theory to policy*. Diane Publishing.

Mingqian, W., & Shuai, C. (2020). Global Journal of Engineering and Technology Advances. *Global Journal of Engineering and Technology Advances*, *2*(03), 54–66.

Moser, R. J., & Gross, G. J. (1982). Spread Spectrum Techniques. *Microwave journal*, *25*(10), 89–92. https://doi.org/10.1016/b978-0-7506-1729-1.50038-x

Mutagi, R. N. (1996). Pseudo noise sequences for engineers. *Electronics & communication engineering journal*, *8*(2), 79–87.

NAWCWP. (2013). *Electronic Warfare and Radar Systems Engineering Handbook 2013*. *April*, 455.

Nellis, A. (2000). *Electronic Warfare Fundamentals*. *November*, 351.

Norris, W. J. (1975). Electronic Warfare. *RUSI Journal*, *120*(4), 54–58. https://doi.org/10.1080/03071847509421216

O'Rourke, R. (2021). Renewed great power competition: Implications for defense — Issues for Congress. *Congressional Research Service*, 1–53.

Pareek, S., Gautam, A., & Dey, R. (2017). Different type network security threats and solutions, a review. *PASJ International Journal of Computer Science (IIJCS)*, *5*(4).

Promoteur, A. (2022). *Study and Design of UAS Jamming Systems Author : Reading committee : Master ' s thesis carried out to obtain the degree of Master of Science in Electrical Engineering by Heuchamps Alexandre . Academic year 2021-2022* .

Pywell, M. (2013). *Development and management of high-fidelity test technology for comprehensive performance evaluation of electronic warfare systems in multi-threat environments.* *1*(September). http://clok.uclan.ac.uk/9299/%0Ahttp://clok.uclan.ac.uk/9299/60/19Sep19 Final MPywell PhD Thesis - Volume 1.pdf

Sarty, R., & Palmer, M. A. (2006). Command at Sea: Naval Command and Control since the Sixteenth Century. In *International Journal* (Vol 61, Number 3). https://doi.org/10.2307/40204202

Schultz, E. E., Proctor, R. W., Lien, M.-C., & Salvendy, G. (2001). Usability and security an

appraisal of usability issues in information security methods. *Computers & Security*, *20*(7), 620–634.

Stein, F., Garska, J., & McIndoo, P. L. (2000). Network-centric warfare: Impact on army operations. In *IEEE/AFCEA - EUROCOMM 2000: Information Systems for Enhanced Public Safety and Security*. https://doi.org/10.1109/EURCOM.2000.874819

Stresser, M. (2009). *Novel Techniques for Thwarting Communication Jamming in Wireless Networks*. *18772*.

Sturza, M. a. (n.d.). *Spread Spectrum Techniques and Technology*.

Suman, S., & Agrawal, E. A. (2016). IP traffic management with access control list using cisco packet tracer. *Int. J. Sci. Eng. Technol. Res*, *5*(5), 2278–7798.

Thiele, R. D. (2013). *Building C4ISR Capabilities in and for the Gulf*.

Thomas, T. (2014). Russia's information warfare strategy: Can the nation cope in future conflicts? *The Journal of Slavic Military Studies*, *27*(1), 101–130.

Tomar, K., & Tyagi, S. S. (2014). Enhancing Network Security and Performance Using Optimized ACLs. *International Journal in Foundations of Computer Science & Technology (IJFCST)*, *4*(6), 25–35.