SUDAN UNIVERSITY OF SCIENCE AND TECHNOLOGY

COLLEGE OF GRADUATE STUDIES

إخفاء متعدد الطبقات على بروتوكول TCP/IP

MULTI-LEVEL STEGANOGRAPHY OVER THE TCP/IP

A Thesis Submitted in Partial Fulfillment of the Requirements of Master Degree in Computer Science

BY:

MUTWKIL FAISAL SAYED

SUPERVISOR:

DR. TALAT WAHBI

September 2014

آيـــــــــــــه

قال تعالى:(ٱللَّهُ لَآ إِلَٰهَ إِلَّا هُوَ ٱلۡحَيُّ ٱلۡقَيُّومُۚ لَا تَأۡخُذُهُۥ سِنَةٞ وَلَا نَوۡمٞۚ لَّهُۥ مَا فِي ٱلسَّمَٰوَٰتِ وَمَا فِي ٱلۡأَرۡضِۗ مَن ذَا ٱلَّذِي يَشۡفَعُ عِندَهُۥٓ إِلَّا بِإِذۡنِهِۦۚ يَعۡلَمُ مَا بَيۡنَ أَيۡدِيهِمۡ وَمَا خَلۡفَهُمۡۖ وَلَا يُحِيطُونَ بِشَيۡءٖ مِّنۡ عِلۡمِهِۦٓ إِلَّا بِمَا شَآءَۚ وَسِعَ كُرۡسِيُّهُ ٱلسَّمَٰوَٰتِ وَٱلۡأَرۡضَۖ وَلَا يَـُٔودُهُۥ حِفۡظُهُمَاۚ وَهُوَ ٱلۡعَلِيُّ ٱلۡعَظِيمُ) البَقَرَةِ 255

الحـــــــــــــمد

الحمد لله نحمده ونستعينه ونستغفره ونتوب اليه ونعوذ بالله من شرور انفسنا وسيئات اعمالنا من يهد الله فلا مضل له ومن يضلل فلا هادي له واشهد ان لا إله إلا الله وحده لاشريك له واشهد ان محمدا عبده ورسوله(صلى الله عليه وسلم). نحمد الله تبارك وتعالى ان تفضل علينا بأن زودنا بأدوات العلم من السمع والبصر والفؤاد فعلمنا مالم نكن نعلم وزادنا من العلم بفضله. مما أعاننا على إخراج هذا البحث.

DEDICATION

To my dear father

To my dear beloved mother

To my dear fellow brothers and sisters,

To all my friends and all those who have conferred their favors upon me and paved my way to success, all words and expressions of gratitude and thankfulness will be a drop in your sincere wide… wide sea of help and support.

ABSTRACT

To perform hidden communication through the network, network protocols and/or relationships between them have been utilized as a carrier to transmit secret data. For each network steganography method there is always a trade-off necessary between maximizing steganographic bandwidth (how much data we are able to send using this particular method) and still remaining undetected.

In this work a new steganographic method is developed that aims to achieve undetectability and relatively increase steganographic bandwidth. This method depends completely on concept called Multi Level steganography (MLS).

In MLS, at least two steganographic methods are utilized simultaneously in such a way that one method's (the upper-level) network traffic serves as a carrier for the second method (the lower-level).

Experimental results were obtained demonstrating that the average transmission time of network decreased by 14.8% due to using of MLS, and the time required to transfer steganogram file of size equal to 50 bytes through the system is 166.43 seconds, about (2 minutes and 46 seconds).

المستخـــــــــلص

لإجراء إتصالات مخفية عبر الشبكة، يتم إستخدام بروتوكولات الشبكة او العلاقات بينها كوسيط لإخفاء البيانات السرية. لكل طريقة إخفاء في الشبكة هناك دائما مفاضلة بين زيادة حجم البيانات المراد إخفاءها وإبقاء طريقة الإخفاء غير مكتشفة.

في هذا العمل تم تطوير إسلوب جديد لإخفاء البيانات في الشبكة يهدف إلى زيادة نسبة حجم البيانات المراد إخفائها وفي نفس الوقت زيادة صعوبة الإكتشاف. هذا الاسلوب يعتمد كليا على مفهوم يسمى الإخفاء متعدد المستوى (MLS). الإخفاء متعدد المستوى يستخدم على الأقل اثنين من اساليب الإخفاء المعروفة في الشبكة في آن واحد بحيث يمثل الاسلوب الاول(المستوى العلوي) وسيط او ناقل للأسلوب الثاني(المستوى الأدنى).

تم تطبيق النظام بإستخدام لغة C، ومن ثم تم الحصول على النتائج التجريبية التي تدل على ان متوسط معدل ارسال الشبكة إنخفض بنسبة 14.8 % وذلك نتيجةً لإستخدام الإخفاء متعدد المستوى، كما اوضحت النتائج ان الزمن اللازم لنقل ملف سرى حجمه 50 بايت عبر النظام المقترح يلزم 166.43 ثانية، اى مايعادل دقيقتان وست واربعون ثانية تقريبا.

TABLES OF CONTENTS

LIST OF TERMS

LSB	least significant bit
DHT	Deep Hiding Techniques
MLS	Multi-Level Steganography
VOIP	voice over IP
RTP	Real-Time Transport protocol
SGS	Steganogram Scattering
SGH	Steganogram Hopping
IPS	Inter-Protocol Steganography
CMC	Carrier modifications camouflage
MM	Multi Media
RGB	Red Green Blue
LACK	Lost Audio Packets Steganography
STEGCRYP	Steganography and Cryptography
MD5	Message digest 5
SSCE	Secret steganography code for embedding
SS	Steganogram sender
SR	Steganogram receiver
RSA	Rivest, Shamir Adleman
TCP	Transmission control protocol
UDP	User datagram protocol
SIP	Session initiation protocol
RTCP	Real-Time Control Protocol
SDP	Session Description Protocol
HICCUPS	Hidden Communication System for Corrupted Networks

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Overview

Oftentimes throughout history encrypted messages have been intercepted but have not been decoded. While this protects the information hidden in the cipher, the interception of the message can be just as damaging because it tells an opponent or enemy that someone is communicating with someone else, an alternative technique that make the existence of secret message unknown is called Steganography.

Steganography is a type of hidden communication that literally means “covered writing” or “hidden in plain sight” the message is out in the open, often for all to see, but goes undetected because the very existence of the message is secret. [1]

In contrast to cryptography where the message is scrambled unreadable and the existence of a message is often known, Steganography takes the opposite approach and attempts to hide all evidence that communication is taking place.

Steganography aims to hide secret data (steganograms) in innocent-looking carriers (cover). The more commonly a carrier is used, the less likely people are to find the existence of the carrier itself an anomaly.

1.2 Introduction

In modern digital steganography, secret data is inserted into redundant (provided but often unneeded) data, e.g. least significant bit (LSB) in graphic image and audio file.

Another kind of steganography methods called “Network Steganography” encompasses information-hiding techniques that can be used to exchange secret data in telecommunication networks.

Network Steganography is currently seen as a rising threat to network security. Contrary to typical steganographic methods which utilize digital media (pictures, audio and video files) as a (cover) for hidden data (steganogram), Network Steganography utilizes network protocols, their basic intrinsic functionality and/or relationships between them as steganogram carrier.

Network Steganography achieves security through obscurity; as long as the steganographic procedure remains unknown to third parties, it can be freely used to exchange hidden data. [2]

1.3 Problem statement

Network steganography often depends on a single steganographic method to hide data, as long as the steganographic method remains unknown to third parties, it can be freely used to exchange hidden data.

The problem arises when the functioning of the steganographic method is no longer secret. In such cases, anyone who is able to capture traffic may extract and read the hidden information.

Moreover almost all known network steganographic method achieves little bandwidth (which describes how much secret data we are able to send using a particular method per time unit) to still remaining undetected.

So the problem here is how to build a good and practical network steganographic method that perform undetectability, relatively increase steganographic bandwidth and make steganogram extraction harder to perform.

1.4 Research scope

This Research aims to develop a new network steganographic method from scratch within TCP/IP network (IPV4 only) according to Multi-Level Steganography (MLS) _that is not widely used in network steganography.

Then the method will be applied using suitable hidden communication scenario. Later any suitable network application is used as an innocent (cover) carrier for our method.

Finally Experimental results that demonstrate the effectiveness of proposed method in term of performance will be included. Also time elapsed to transfer steganogram file of different sizes will be calculated.

1.5 Research methodology and tools

C programming language, sniffing, injection and raw socket technologies are used to build two routers that forwards packets being exchanged between two communicating network applications located in two clients connected through routers. Then regarding to MLS our own steganographic method is added to those routers in order to exchange steganogram file between them using applications mentioned above as a carrier.

Later one of the available network speed testing tools is used to obtain the results.

1.6 Objectives

- Increase the total steganographic bandwidth achieved for user data compared with a single network steganography method.
- Increase Undetectability, because MLS uses two levels (An upper-level and lower-level method) or more to hide steganogram.
- Make steganogram extraction and analyses harder to perform.

1.7 Research questions

- Which part of the packet is suitable for steganographic purpose? The packet header or the data section?
- Which field of packet header is suitable and which of them perform high bandwidth and high rate of undetectability?
- How many levels of MLS are suitable for our proposed system?
- How receiver can distinguish between ordinary packet and those contain secret data?
- What is the affection of the proposed steganographic method on network performance?

1.8 Thesis layout

The rest of the research has been organized as follows: Chapter 2 gives detailed description about steganography and MLS then discusses about some of the related works done based on MLS. Chapter 3 shows work environment then describes and analyses the proposed system. Chapter 4 contains the analysis and discussion of the results. The last chapter draws the conclusion, and then shows recommendations and future work.

CHAPTER 2

LITERATURE REVIEW AND RELATED WORK

2.1 Introduction

Steganography is of Greek origin and it means "Covered or hidden" (stegano) writing (graphy). [3]

In recent years, digitalization made digital media easily transmitted over the network, so messages can be transmitted secretly through the digital media using the steganography techniques. Although all digital file formats can be used for steganography, but the image and audio files are more suitable because of their high degree of redundancy.

Another information hiding techniques that may be used to exchange secret data (steganograms) in telecommunication networks are called network steganography.

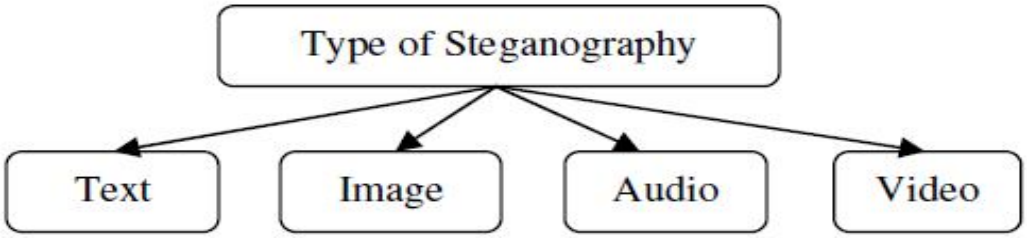

Figure 2.1: Types of Steganography

Regarding to steganography four objects have been defined:

- **Message objects (steganogram):** The secret message that we want to hide.
- **Cover (carrier or overt object):** The picture, sound, or movie, packet that will be used to carry the message.
- **Stego key:** The code that the person sending the secret message is going to use to embed the message into the cover object; the same stego-key will be used by the recipient to extract the secret message.
- **Stego object:** Is the combination of the cover object, the stego-key, and the secret message.

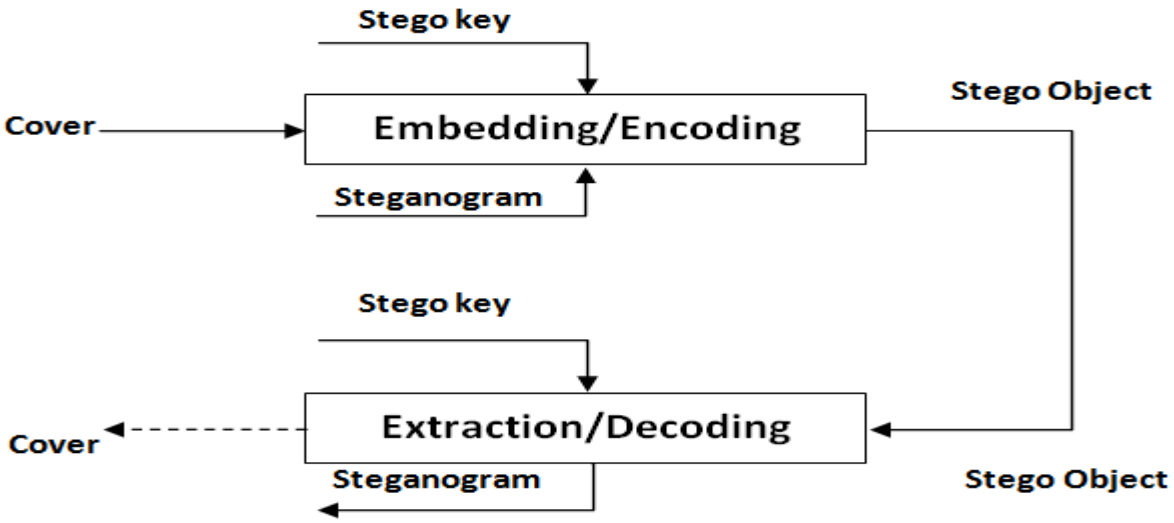

Figure 2.2: Generic steganographic system

2.2 Network steganography

The terms network steganography and covert channels are used interchangeably (and incorrectly), but historically they are sovereign of each other.

Network steganography utilizes as a carrier for steganograms a one or more network protocols simultaneously - relying on the modification of their intrinsic properties for the embedding of steganograms and/or relationships between them. [4]

Regarding to network steganography, steganographic methods may be classified into three groups as shown in Figure 2.3.

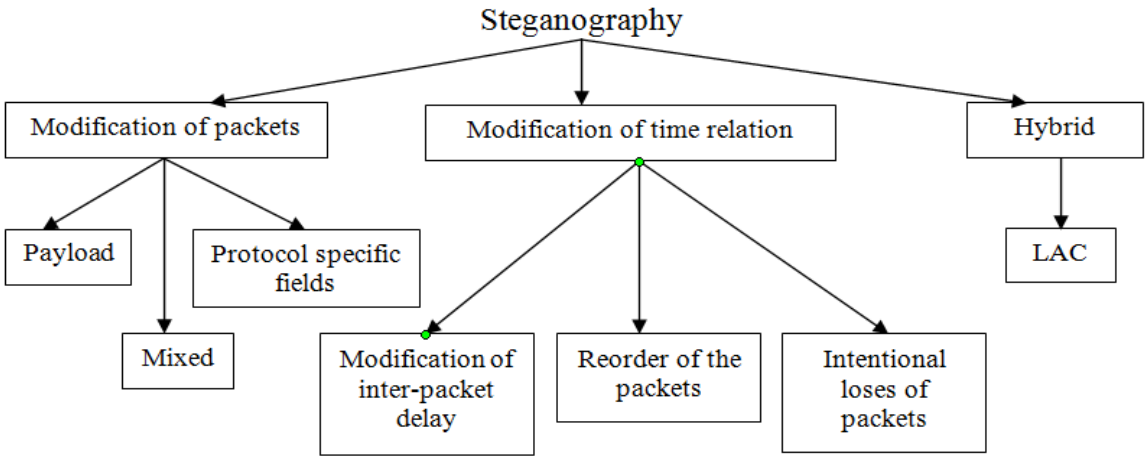

Figure 2.3: Steganography classification

Steganographic methods which modify packets modify the Network protocol headers or payload fields. Examples:

- Methods which modify protocols specific fields – SIP, SDP, RTP, RTCP (VoIP specific protocols) and additionally: IP, TCP, UDP (network specific protocols).
- Methods which modify packets' payload: audio watermarking algorithms, speech codec steganographic techniques (e.g. using SID frames or codec specific steganographic methods).
- Mixed techniques: HICCUPS (Hidden Communication System for Corrupted Networks).

Steganographi**c** methods which modify packets time relations affect the sequence order of RTP packets, modifying their inter-packet delay or by introducing intentional losses. Examples:

- Methods which affect sequence order of packets (in VoIP possible only for RTP).
- Methods which modify inter-packet delay (in VoIP possible for RTP and RTCP; for some protocols, e.g. SIP, not useful due to small number of messages).
- Methods which introduce intentional losses by skipping sequence numbers at the sender (for RTP and RTCP protocols).

Hybrid steganographic methods modify both the content of packets and their time relation. An example of such solution is the LACK (Lost Audio Packets Steganography) method which modifies both packets and their time dependencies.

Regarding to any network steganography method, Deep Hiding Techniques can be applied to it, to improve undetectability and make steganogram extraction harder to perform.

2.3 Deep Hiding Techniques (DHTs)

Based on what particular DHT affect – a steganogram or a carrier, five types of the Deep Hiding Techniques are defined. [5]

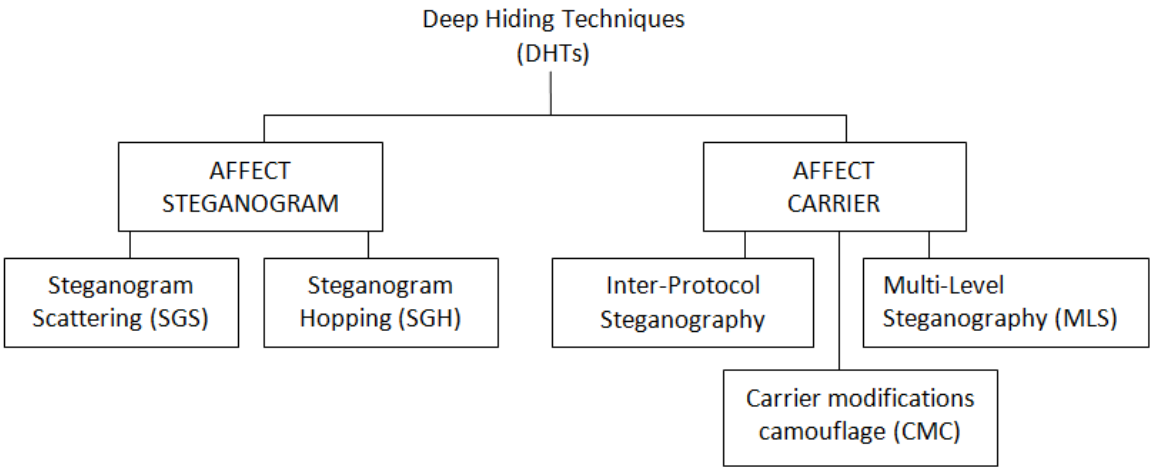

Figure 2.4: Deep Hiding Techniques classification

2.3.1 Steganogram Scattering (SGS)

The idea of Steganogram Scattering techniques is to split steganogram into pieces and send it as separate messages. Each part may be transmitted using different steganographic method.

2.3.2 Steganogram Hopping (SGH)

Steganogram Hopping techniques utilize periodical change of the steganographic method during single hidden connection. This causes the steganogram localization change thus making it harder to detect and extract. SGH techniques concept is similar to SGS. However, the main difference is that SGH utilizes single connection and single steganogram fragment transferring in a given moment of time, while SGS experiences no such constraints.

2.3.3 Inter-Protocol Steganography (IPS)

It is defined as usage of the relationships between two or more different network protocols to enable secret communication. Protocols used by inter-protocol steganography can belong to the same layer of the e.g. TCP/IP stack or to different ones. In this approach utilization of more than one protocol to enable hidden communication provides greater undetectability thus limiting the chance of disclosure. That is why one may state that IPS hides better what has already been hidden.
The first example of the inter-protocol steganography was PadSteg (Padding Steganography). It benefits from utilizing relationships between Ethernet (IEEE 802.3), ARP, TCP and other protocols. [6]

2.3.4 Carrier modifications camouflage (CMC)

It aims to mask existence of the steganogram inside the carrier. This may be achieved using a wide spectrum of actions. Examples of the CMC techniques include:

- Intentional reduction of the steganographic bandwidth – steganogram is inserted into the carrier less frequently, thus less secret data is sent and a chance of detection is decreased. It is the simplest way of the steganogram insertion camouflage and can be utilized for every steganographic method.
- Utilization of the traffic characteristic features to camouflage hidden communication – for certain steganographic methods it is possible to utilize traffic features like anomalies, level of the network parameters like number of lost packets etc. or other events to mask steganographic exchange. For example, RSTEG (Retransmission Steganography) [7] enables hidden communication by not acknowledging a successfully received packet in order to intentionally invoke retransmission. The retransmitted packet carries a steganogram instead of user data in the payload field.

2.3.5 Multi-Level Steganography (MLS)

MLS is based on at least two steganographic methods. First, the upper-level method uses overt traffic as a secret data carrier. The second, the lower-level method, uses the way the upper-level method operates as a carrier. The indirect carriers for lower-level methods are still packets from overt communication, but the direct carrier is another (upper-level) method. Figure 2.5 left demonstrate MLS.

Creation of different-levels steganographic methods has two important features:

- The bandwidth of the lower level method is usually a fracture of bandwidth of the upper level method. It is similar to relationship of overt communication bandwidth and upper-level steganography bandwidth.
- The lower-level method entirely depends on upper-level one and adversary has to detect upper-level method before he/she starts to seek for lower-level one.

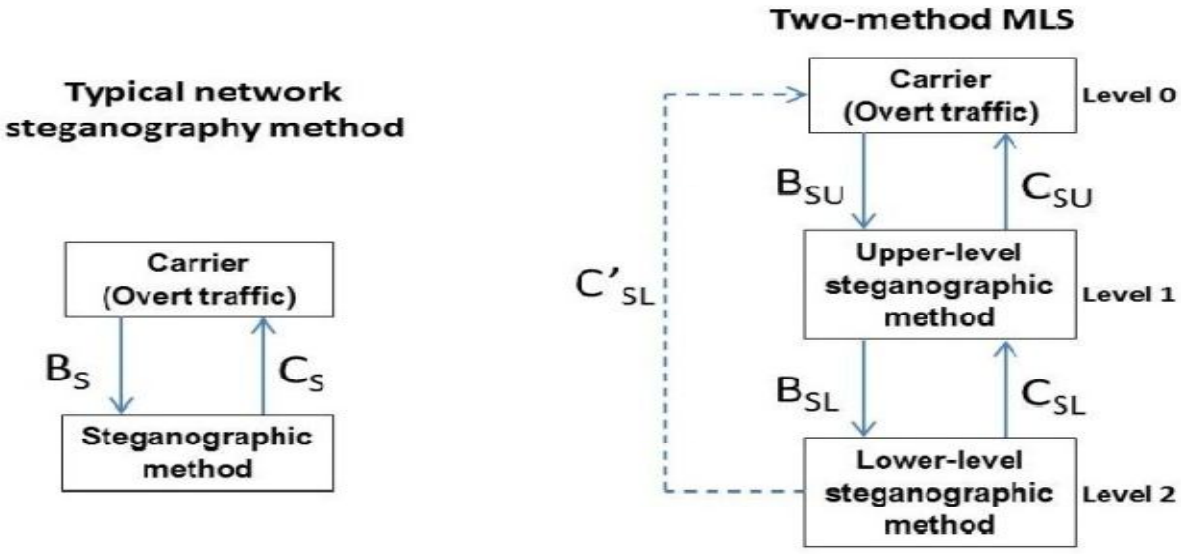

Figure 2.5: The typical network steganography method (left) and the two-method MLS (right) comparison

By modifying the carrier, a certain steganographic bandwidth (B_s), which is defined as the amount of the steganogram transmitted using a particular method in one second ([b/s]), is achieved. However, the utilization of B_s may result in a certain

steganographic cost (C_s) that expresses an impact (degradation) of a hidden data carrier due to steganographic procedure operations.

Based on where the steganogram is inserted; there are three possible cases:

- The steganogram is carried only by the upper-level method and the lower-level method utilized for special purposes. For example, it may carry a cryptographic key.
- The steganogram is carried only by the lower-level method and the upper-level steganogram can also be utilized to provide integrity or a cryptographic key.
- The steganogram is carried by both the upper- and lower-level methods.

2.4 Related works

In [8] Dr. AL-NAJJAR presented “The Decoy: Multi-Level Digital Multimedia Steganography Model”. This paper focuses on two folds: to develop an abstract multi-level model and to illustrate the model by hiding text represented using a black and white image into a gray decoy image and then into a color image in the RGB format.

Four objects are defined, the message-object (M), the intermediate-object (I), the cover-object (C), and the stego-object (S). The elements of M are given by the set {M}{AL-NAJJAR, 2008 #2} of size |M|, similarly, {I} of size |I| and so forth.

The message {M} is passed through the transformation T1 that can include many possibilities. It can be compression, private-key or public-key encryption, or a combination of techniques, as required by the particular application. The same can be said about the other transformations T2 and T3. Figure 2.6 demonstrate the proposed model.

Embedding and recovery is controlled by the embedding/recovery function pairs *f*/*g*. The embedding function from {M} to {I} (or {D}) and from {D} to {C} can be different, improving one or more of the three steganography attributes: Capacity, Robustness, and Transparency.

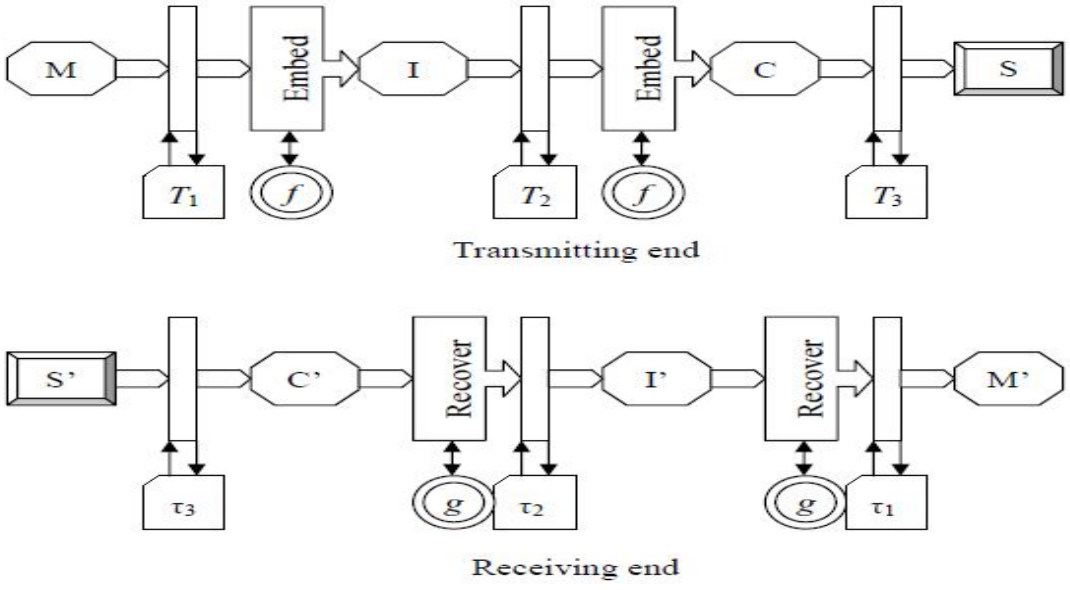

Figure 2.4: multi-level steganography model

In [2] Wojciech Frączek et al, presented “Multilevel Steganography: Improving Hidden Communication in Networks”. They extend and redefine the concept of MLS originally defined by Dr. AL-NAJJAR to work within network steganography. The focus of this paper is two folds: to present a detailed analysis of the potential MLS applications and to develop a proof-of-concept prototype implementation using two-method MLS for VoIP.

For MLS prototype development, two steganographic methods were used. As an upper-layer method, LACK was utilized. The idea of LACK is as follows. At the transmitter, some selected audio packets are intentionally delayed before transmitting. If the delay of such packets at the receiver is considered excessive, the packets are discarded by a receiver that is not aware of the steganographic procedure. The payload of the intentionally delayed packets is used to transmit secret information to receivers aware of the procedure.

The lower-level method is based on proper RTP sequence number matching. It modifies the choice of the RTP packet (its sequence number) used for LACK purposes depending on the steganogram bits to be sent. The functioning of the implemented prototype is as follow:

1. Following the LACK method, a RTP packet is selected for steganographic purposes
2. If the RTP sequence number is not suitable for the lower-level method, then one of the neighboring RTP packets is selected instead with a suitable sequence number.
3. Next, the chosen packet is delayed at the transmitter and then sent through the communication channel to the receiver, and the original payload is replaced with the steganogram.
4. At the receiver, the LACK packet was considered lost; thus, when it comes, it is not used for voice reconstruction. Instead, the payload of the RTP packet is extracted and treated as an upper-level steganogram, and based on this packet sequence number, a lower-level steganogram is also determined.

In [9] Neha Agrawal and Sourabh Singh Verma presented “STEGCRYP: A Multilevel Information Security Scheme”. They show that the Cryptography and Steganography techniques (STEGCRYP) can combined to enhance the security level of data communication over an unsafe distributed network.

Here images have been choose as cover object, because it contains a large amount of data whose modification doesn‘t effect it. Figure 2.6 below demonstrate the proposed method.

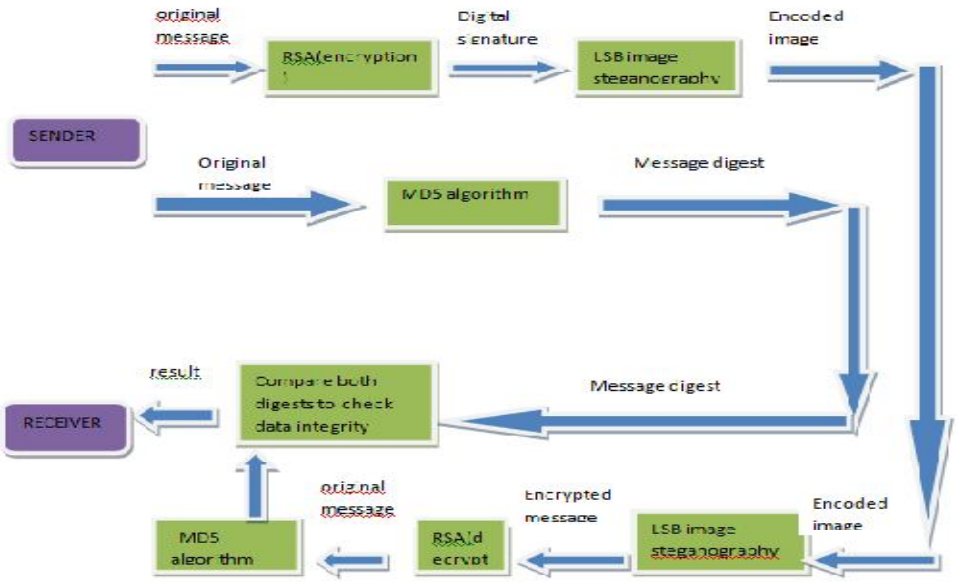

Figure 2.5: Block diagram of stegcryp

Also, they modified the classic LSB (Least Significant Bit) steganographic method by digitally signing a starting position of hided message in image.

As shown in Figure 2.6, any person (who wants to send a secret message to another person) first creates the digital signature of the secret message using RSA algorithm. Then he hides this encrypted message inside an image using improved LSB steganography technique. Then, Along with image he sends the digest of message (created using MD5) to receiver. When the message is received by the intended receiver, he extracts the message from image, then decrypts it and computes digest of received message. Then checks data integrity by comparing both computed and received digests.

In [10] Souvik Bhattacharyya et al presented “Data Hiding through Multi Level Steganography and SSCE”. They proposed that a steganographic model combining the features of both text and image based steganography technique for communicating information more securely between two locations. The authors incorporated the idea of secret key for authentication at both ends in order to achieve high level of security.

Figure 2.6 below show the block diagram of the proposed steganographic model. The input message is first encoded through SSCE (Secret steganography code for embedding) values and embedded into the cover text using the proposed text steganography method. This encrypted message generates the secret key. The encrypted message is then embedded in the cover text using the mapping technique method to form the stego text which in turn embedded in to the cover image through PMM (Pixel Mapping Method) to form the stego image and transmit to the receiver side.

At the receiver side, the stego image will be tested first for a specific feature. If that feature matches, the extraction process starts by extracting the stego text from the stego image. Next the stego text goes through the text extraction and decryption method and finally the receiver may be able to see the embedded message with the help of same secret key generated at the sender side. Figure 2.8 demonstrate the proposed model.

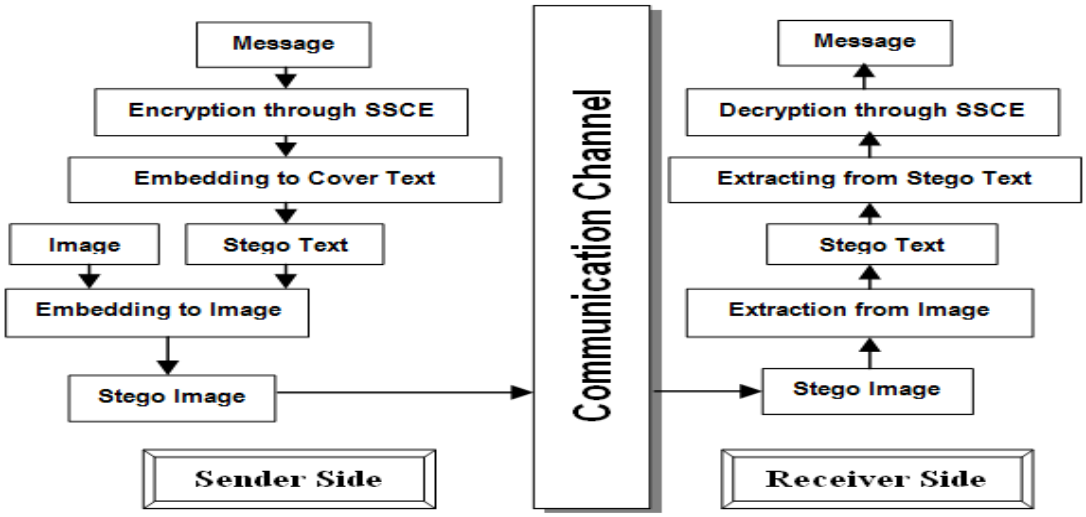

Figure 2.7: Proposed Steganography Model

In [11] Prof. Samir Kumar Bandyopadhyay and Barnali Gupta BanikIn have presented “Multi-Level Steganographic Algorithm for Audio Steganography using LSB Modification and Parity Encoding Technique”. They presented a two layered approach to hide information in digital audio.

At the first level, cover file (C) can be embedded with the first secret message S1. Assuming the stego file as C1 which is cover file for next level where secret message can be denoted as S2. Now the final stego file created as C12. So C12 holds both S1 and S2.

Two levels of steganography can be identified as layer 1 and layer 2. At layer 1 LSB modification technique and at layer 2 parity encoding technique has been used which intended to break a signal down into separate regions of samples and encodes each bit from the secret message in a sample region's parity bit. If the parity bit of a selected region does not match the secret bit to be encoded, the process flips the LSB of one of the samples in the region. Figure 2.8 below demonstrate the proposed MLS method.

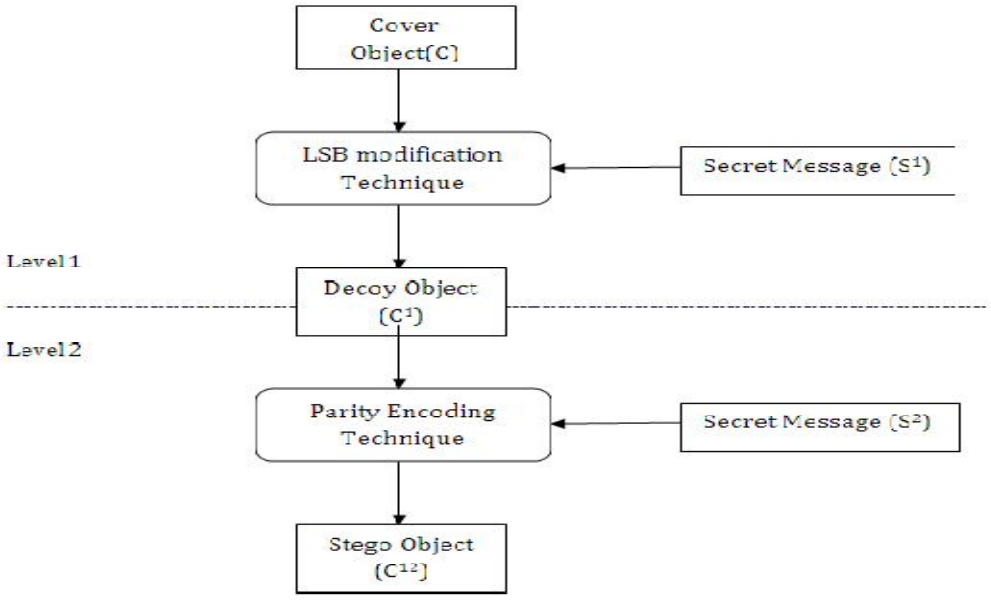

Figure 2.9: Proposed method for Multi level audio steganography

All related work mentioned above have been summarized in Table 2.1 below:

#	Paper name	Message object	Decoy/cover object	Level-1 method	Cover object	Level-2 method
1	The Decoy: Multi-Level Digital Multimedia Steganography Model	Text represented by black and white (B&W) image	A Gray scale image	LSB 2 bits steganography	RGB color image	LSB 3 bits of RGB Coloring scheme
2	Multilevel Steganography: Improving Hidden Communication in Networks	.wav audio file	RTP packet	LACK	RTP packet	Bits matching between steganogram and RPT sequence number
3	STEGCRYP: A Multilevel Information Security Scheme	Text message	Image	LSB	The same image	LSB
4	Hiding through Multi Level Steganography and SSCE	Text	Text object	Inserting indefinite articles ‘a’ or ‘an in conjunction with the non-specific or non-particular nouns in English	Image	PMM (Pixel Mapping Method)
5	Multi-Level Steganographic Algorithm for Audio Steganography using LSB Modification and Parity Encoding Technique	Two Secret messages S1and S2	Digital audio file	LSB	The same digital audio file	Parity encoding

Table 2.1: Summarization of related work

CHAPTER 3

WORK ENVIROMENT AND PROPOSED SYSTEM ANALYSIS

3.1 Introduction

This chapter describes specification of devices, operating system, programming language, protocol, and techniques used to build the system. Then explain how the system works. A general overview of the system environment and devices being used is shown in Figure 3.1 below:

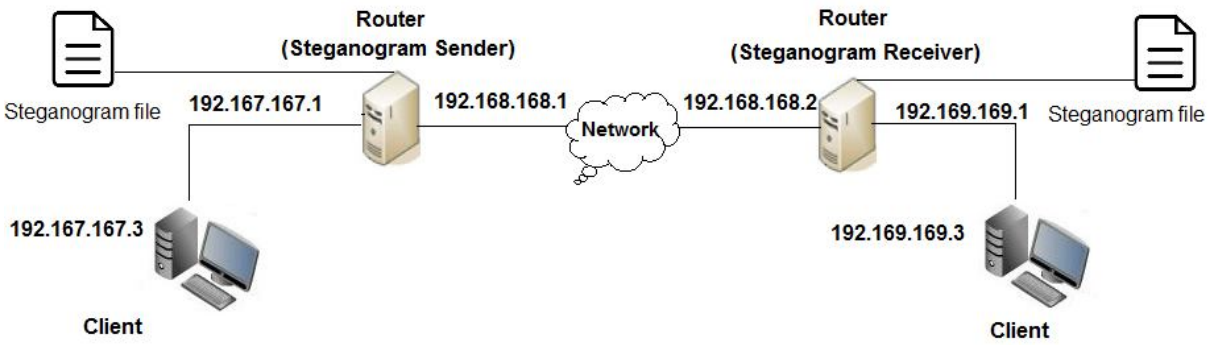

Figure 3.1: An overview of the system environment

3.2 Devices specification

Four devices have been used in this system as shown in Figure 3.2 above, two of which operate as clients and the other two are working as routers to connect clients to each other. Hardware and software specifications of these devices have been shown below.

3.2.1 Router:

Processor	:	Pentium 4.
RAM	:	512 MB.
Hard Disk	:	60 GB.
NIC	:	Two NIC D-Links.
Mother board	:	INTEL.
Operating system	:	Linux (centos 5).

3.2.2 Client:

Processor	:	Pentium 4.
RAM	:	512 MB.
Hard Disk	:	60 GB.
NIC	:	Single NIC D-Links.
Mother board	:	INTEL.
Operating system	:	Any operating system running TCP/IP can be used.

3.3 Linux operating system

Linux is the fastest-growing server-side and networking operating system today. Unlike proprietary operating systems, Linux can be installed and upgraded for free. This makes it extremely attractive to those businesses that don't have a high budget but still want an excellent operating system. But cost is not the main factor. Many companies, large and small, prefer Linux simply because of its reliability: Linux can run for months, even years, without having to be rebooted. And because the source code is open, bugs can be fixed quickly and easily without having to wait for proprietary vendors to issue fixes on a schedule that suits them more than their customers.

3.4 C- Programming language

C is a powerful, flexible language that provides fast program execution and imposes few constraints on the programmer. It allows low level access to information and commands while still retaining the portability and syntax of a high level language. These qualities make it a useful language for both systems programming and general purpose programs specially network programming.

C is used for many different types of software, but it is particularly popular for system software, such as operating systems, device drivers and telecommunications applications. C is widely used because it runs very fast. It can also access a computer system's low level functions; this means it is closer to the hardware than some other

programming languages. C has become an official standard of the American National Standards Institute, or ANSI. Many other programming languages borrow syntax from C.

3.5 TCP/IP Protocol

To describe the way the system works, it is important to know about initial TCP/IP stack, which consists of five layers:

Physical Layer

Correspond to basic network hardware just as layer 1 in the ISO 7-layer reference model.

Network Interface

Specify how to organize data into frames and how a computer transmits frames over a network, similar to layer2 protocols in the ISO reference model.

Internet layer

Specify the format of packets sent across an internet as well as mechanisms used to forward packets from one or more routers to final destination.

Transport layer

Specify how to ensure reliable transfer.

Application layer

Layer 5 corresponds to layer 6 and 7 in the ISO model; each layer 5 protocol specifies how one application uses an internet.

Figure 3.2 below illustrates how these layers work with each other to provide communication services between two devices using TCP protocol.

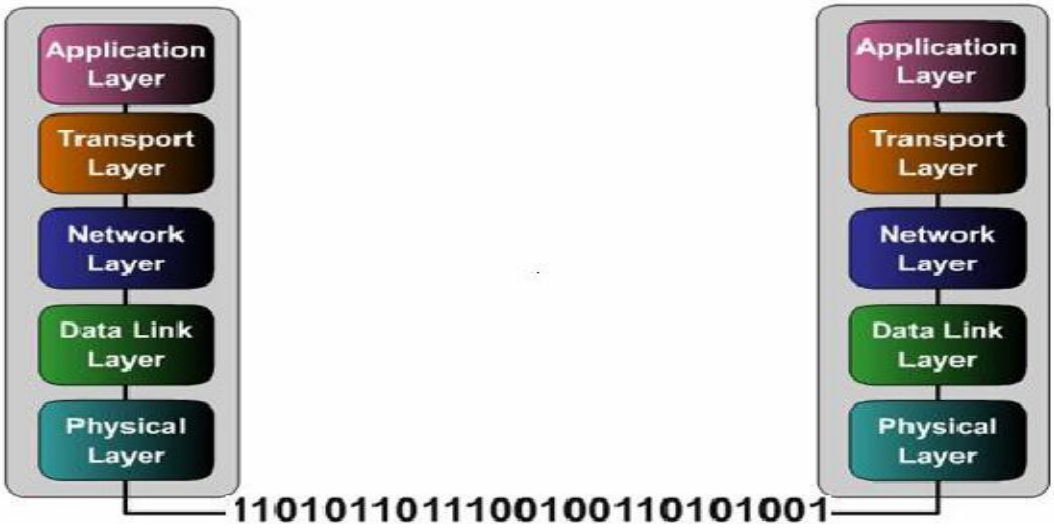

Figure 3.2: TCP/IP stack

3.6 Sniffing Technology

Sniffing is simple process in which the network interface card is used to receive and monitor data that is not intended only for that machine. The device or software that does sniffing is known as sniffer or more simply a network analyzer such as TCP Dump and Wire shark.

Every NIC (Network Interface card) have a unique MAC (Media Access Control) address. In general the NIC responds to those packets only contain its MAC address or broadcast address in the frames destination field.

Network Interface cards supports a mode known as promiscuous mode, in which it can receive all data packets and traffic travels across the network. In promiscuous mode, NIC generates a hardware interrupt to the CPU every packet's frame they encounter (instead of the only the frames having the MAC address or broadcast address).

So the sniffers puts the NIC in to the promiscuous mode in order to capture/monitor all packets traveling around the network, and then passing it to the operating system's TCP/IP stack.

3.7 Raw Socket

A raw socket is a socket that allows direct sending and receiving of network packets by applications, bypassing all encapsulation in the networking software of the operating system.

Usually raw sockets receive packets inclusive of the header, as opposed to standard sockets which receive just the packet payload without headers.

3.8 Packet Injection

It's a very important technique used in security research, it is about how to construct a full packet in memory and inject it into the network using raw sockets.

3.9 System analysis

This section describes how the system work and explain stages of packet traveling from the sender through the router (steganogram sender) which considered the core of this system that contains all required operations to hide steganogram inside the packet using MLS before sending it to the other router (steganogram receiver) where the opposite process is done to extract the data before sending packet again to its original destination**.**

3.9.1 Sender and receiver

Sender and receiver can be any computers running any operating system that has TCP/IP stack and communicating with each other's using any network application.

3.9.2 Steganogram sender (SS)

It's a computer running Linux operating system and has 2 NIC one of them connected to the sender's network and the other to the Steganogram receiver's network where the original receiver exists.

It contains two sniffers written in C language, each of them connected to different NIC using raw socket. The first one capture packets coming from the sender and then change its Destination MAC address field located in Ethernet header to the MAC of the Steganogram receiver as shown in Figure 3.3 , later it inject the modified packet in the other NIC. The second program does the opposite process, this make the computer work just like a router.

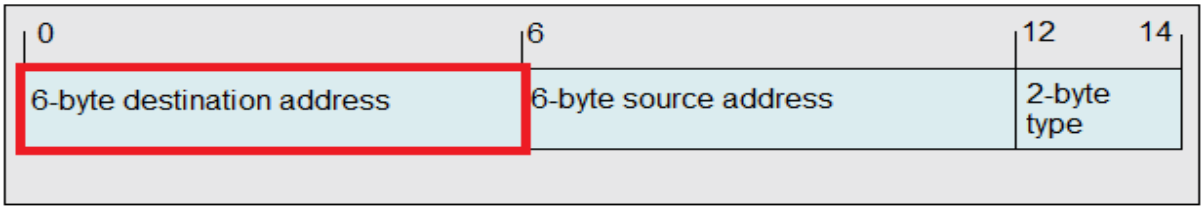

Figure 3.3: Ethernet Header Format

3.9.3 Steganogram receiver (SR)

It's a router with the same specifications and programs mentioned in SS. The first program capture packets coming from the SS and then change its Destination MAC address to the MAC of the original receiver, later it inject the modified packet in the other NIC. The second one does the opposite process.

Next the two routers were used to hide and extract steganogram respectively. All possible hidden communication scenarios are presented in Figure 3.4 below, in Scenarios (a) and (b) some intermediate network node is a steganogram sender and steganogram receiver is also intermediate network node. In scenarios (c) and (d) it is assumed that sender takes part in steganographic communication as a steganogram sender.

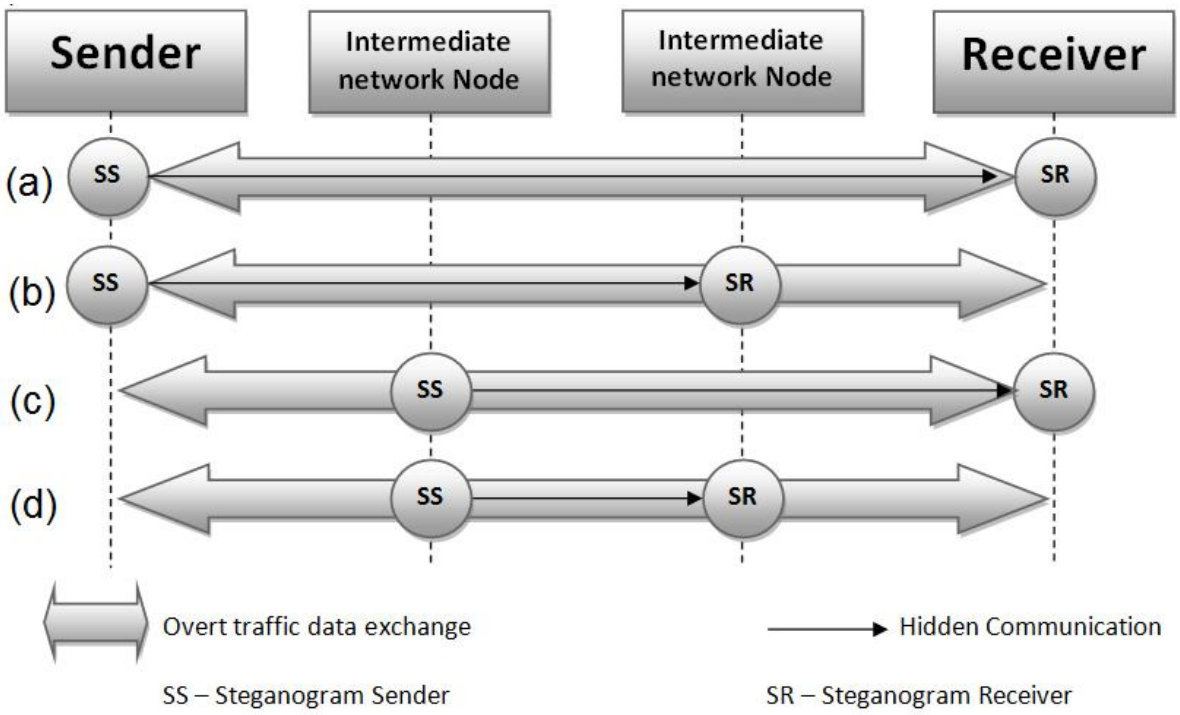

Figure 3.4: Possible hidden communication scenarios between two nodes in a network

From these four scenarios only (a) will be used. It is worth noting that in scenario (a) both sides of overt communication are not aware of hidden communication. Moreover, in this scenario it is possible that steganograms sender (SS) and steganogram receiver (SR) can utilize the whole overt traffic coming from particular LAN for steganographic purposes and thus achieve higher steganographic bandwidth.

3.9.4 Steganographic method for steganogram sender(SS)

The steganogram sender has a text file containing steganogram to be sent, when the program start it read the whole file data in array of characters, then for each incoming packet the following process is done:

- Check that the incoming packet is a TCP packet and contain data.
- Read one character from steganogram file located in steganogram sender, and then convert it to binary array (8 bits).
- Then Check that the two most significant bits of the binary array matches the two least significant bits of the IP identification field located in IP header(As an

- Upper-layer method) as shown in Figure 3.5.
- If so, the remaining 6 bits will be added to the data section of the packet (As an
- Lower-layer method) as shown in Figure 3.6, otherwise packet will be sent the steganogram receiver without modification and another captured packet is checked.
- A flag is added to help steganogram receiver determine whether the packets contain steganogram or not.
- The total length field located in IP header will be incremented by 2 byte (Steganogram + flag) if steganogram is added or by 1(1 byte of flag) byte if is not added, then header check sum recomputed again.
- Modified packet will be injected into NIC and sent to the steganogram receiver.
- Get the next character to be send.

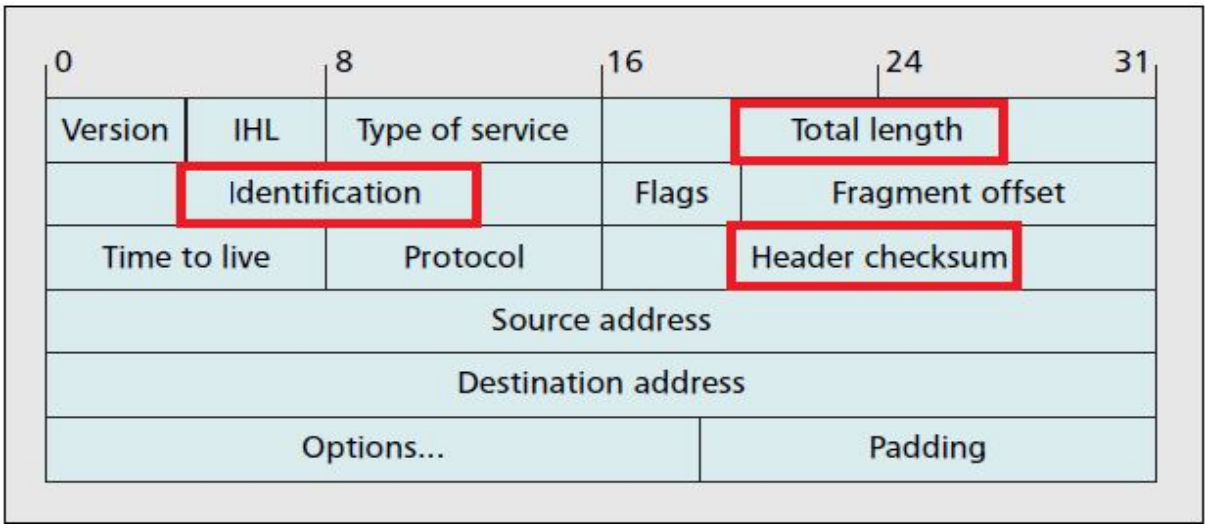

Figure 3.5: IP Header Format

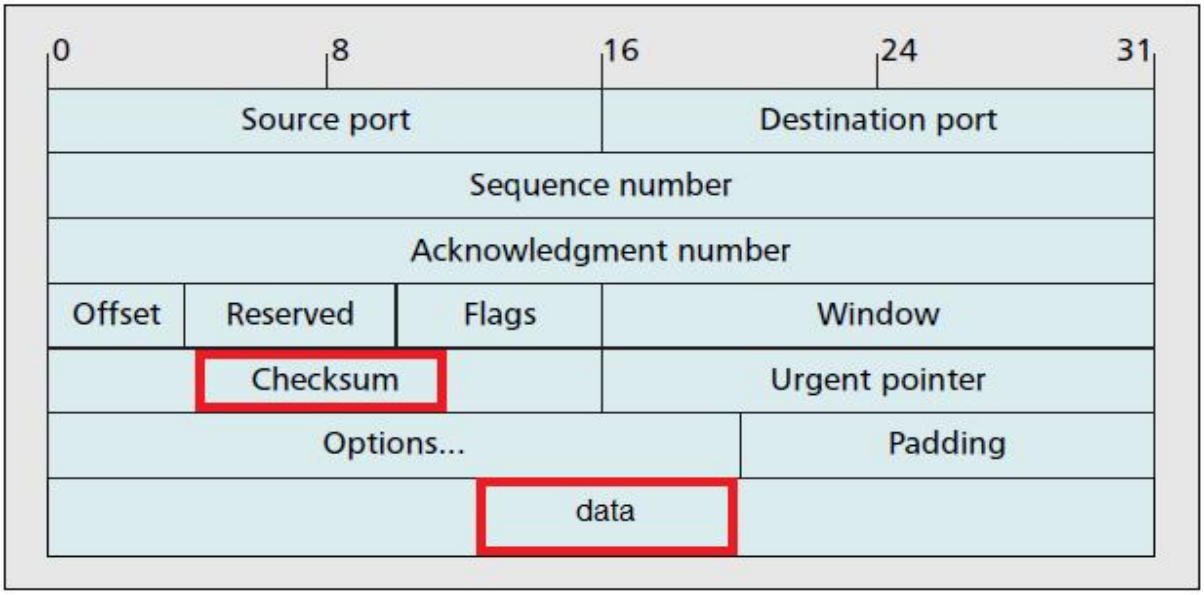

Figure 3.6: TCP Header

Figure 3.4 shows the DFD of the proposed method for SS.

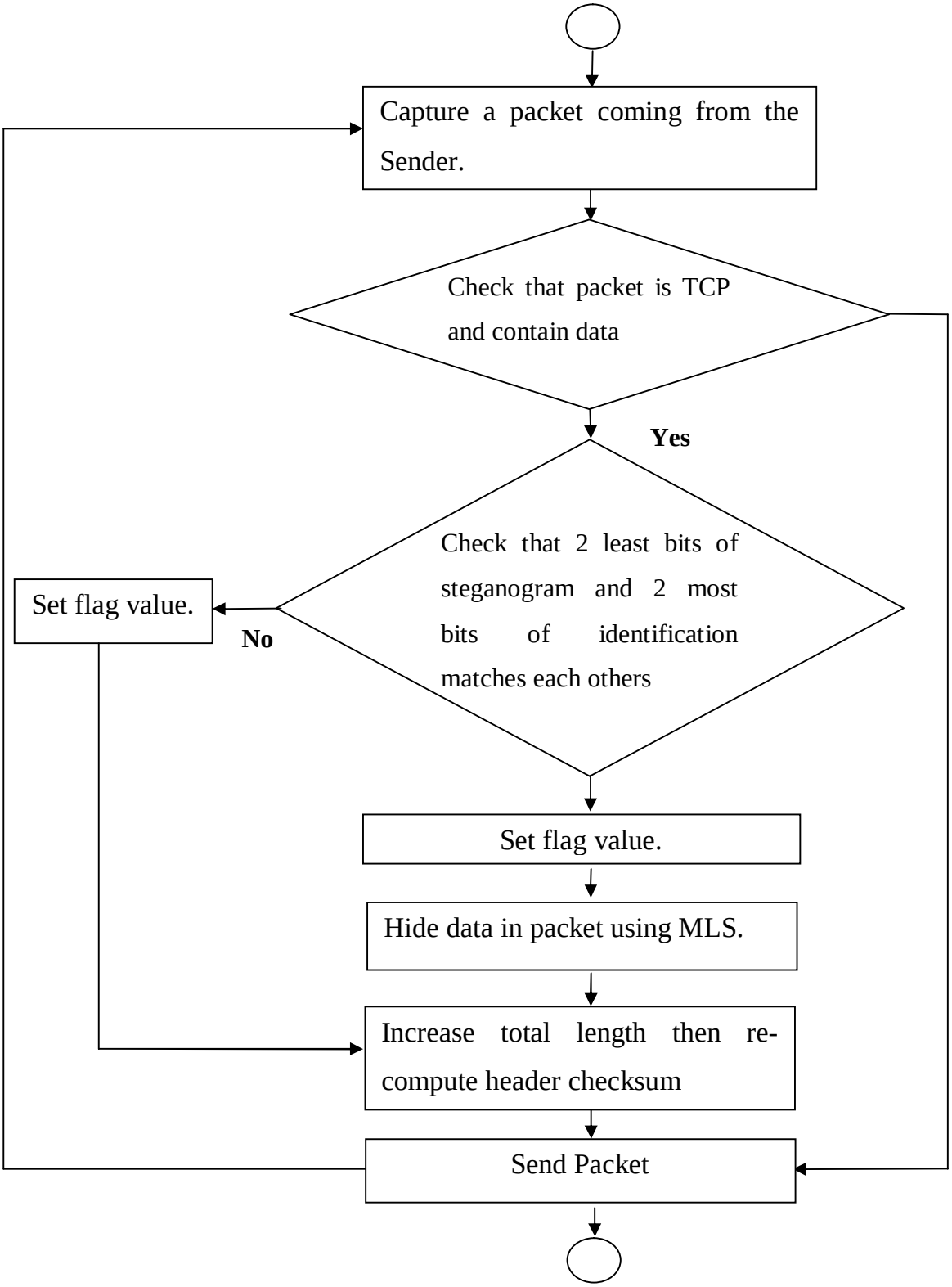

Figure 3.7: Proposed steganographic method for Steganogram sender

3.9.5 Steganographic method for Steganogram receiver(SR)

For each incoming packet from SS the following process is done:

- Check that the incoming packet is a TCP packet and contain data.
- Check that the flag is set on the packet.
- If so, the 2 least significant bits of the IP identification field and the 6 least significant bits of the packet data section are concatenated respectively to form 1 byte of steganogram, otherwise packet will be sent to the receiver without modification and another captured packet is checked.
- Write the steganogram to the steganogram file located in steganogram receiver.
- The total length field located in IP header will be decremented by one and header check sum recomputed again.
- Modified packet will be injected into NIC and sent to the original receiver.

Figure 3.5 shows the DFD of the proposed method for SR.

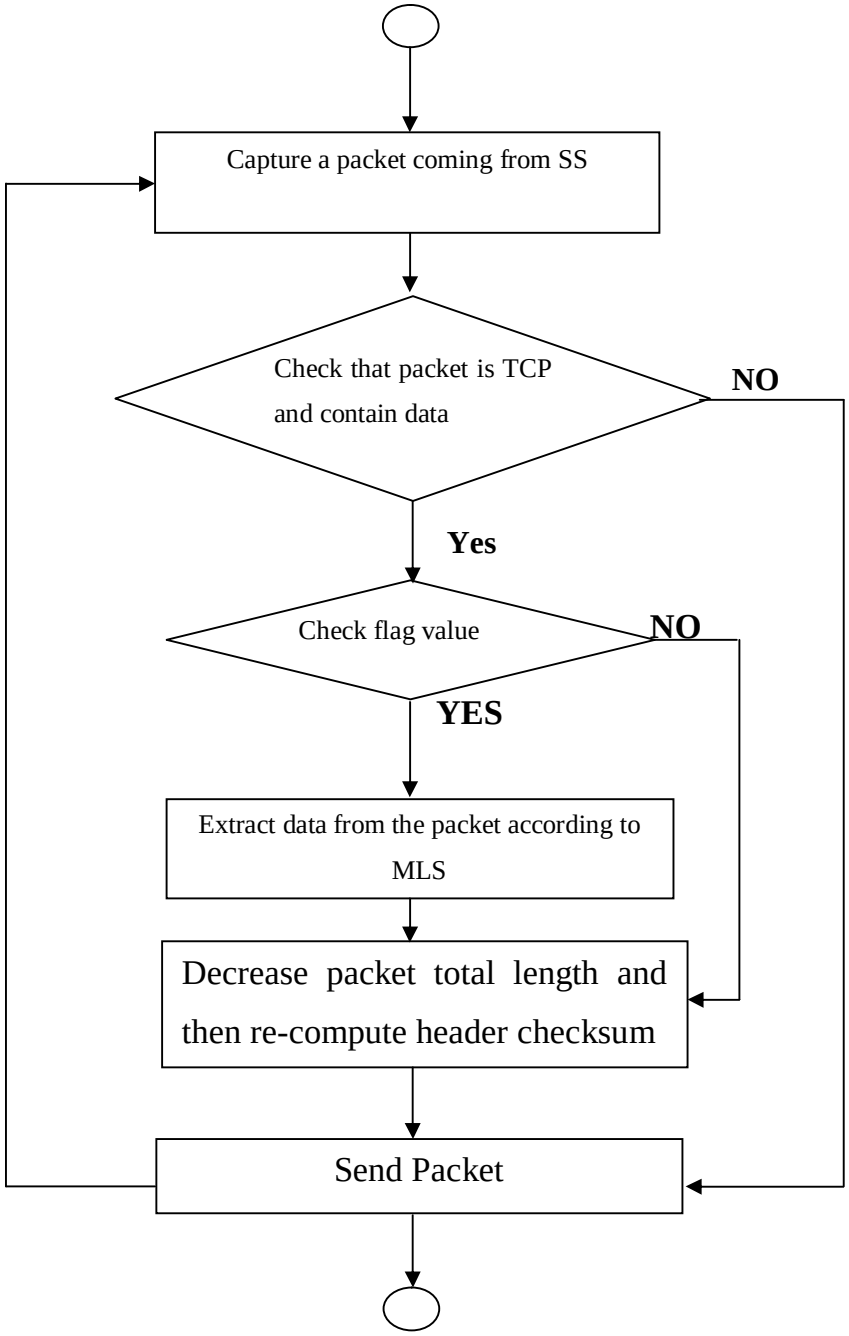

Figure 3.8: Proposed steganographic method for Steganogram receiver

3.9.6 Flag value

For each TCP packet matched steganographic requirement, a flag is added to the TCP data section to help SR differentiate between ordinary packet and those contain steganogram.

The Flag is one byte filled with random number between 0 and 255. If the 2 most significant bits of steganogram and 2 least bits of IP identification match each others, a random number between 0 and 127 is used; otherwise the number is between 128 and 255.

Figure 3.6 shows the DFD of the proposed method for flag value.

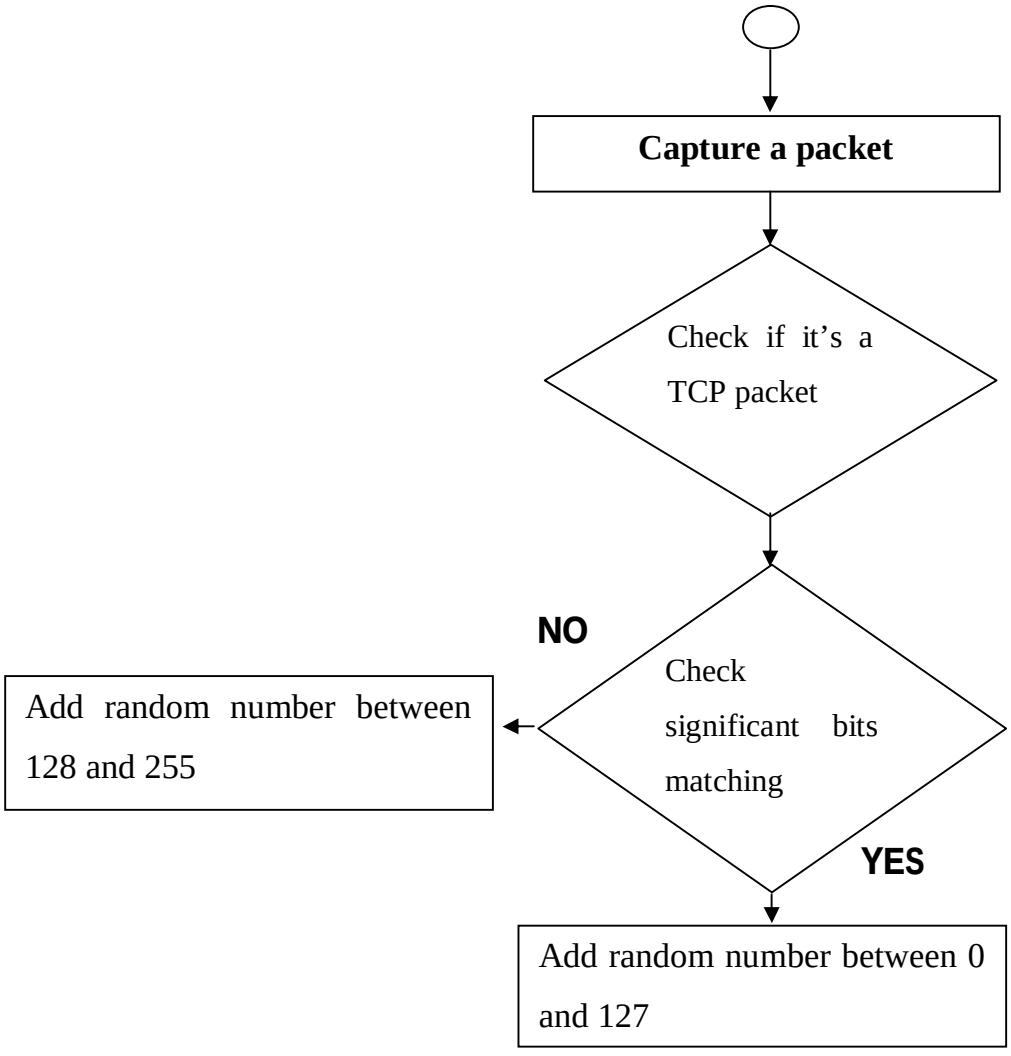

Figure 3.9: Proposed method for flag value

CHAPTER 4

RESULTS AND DISCUSSION

4.1 Results

The environment for the experiment was a LAN network, so no packets were lost or excessively delayed except intentionally, which permitted us to evaluate the sole impact of MLS on network transmission speed, without any interferences.

Performance test 7.0 was used to obtain average transmission for the system in 30 seconds duration by sending packets with fixed block size equal to 1500 bytes for all the following three conditions:

- Both SS and SR are configured to work as routers using default Linux IP forwarding configuration existing in the kernel without using of steganography.
- Linux IP forwarding is disabled then sniffers programs are installed in both SS and SR to make them working as routers without using of steganography.
- Linux IP forwarding is disabled then sniffers programs are installed in both SS and SR to make them working as routers besides using of MLS.

For each condition, experiment was done 5 times and results were obtained in the Table 4.1below:

Technique	**Network Average transmission (Mbps)**					**Average (Mbps)**
	1	**2**	**3**	**4**	**5**	
Linux IP forwarding	68.43	69.49	69.64	68.11	69.25	68.984
Sniffers without steganography	68.14	68.72	68.39	69.42	68.34	68.602
Sniffers using steganography	63.08	60.52	62.91	45.44	60.5	58.49

Table 4.1: System's average transmission

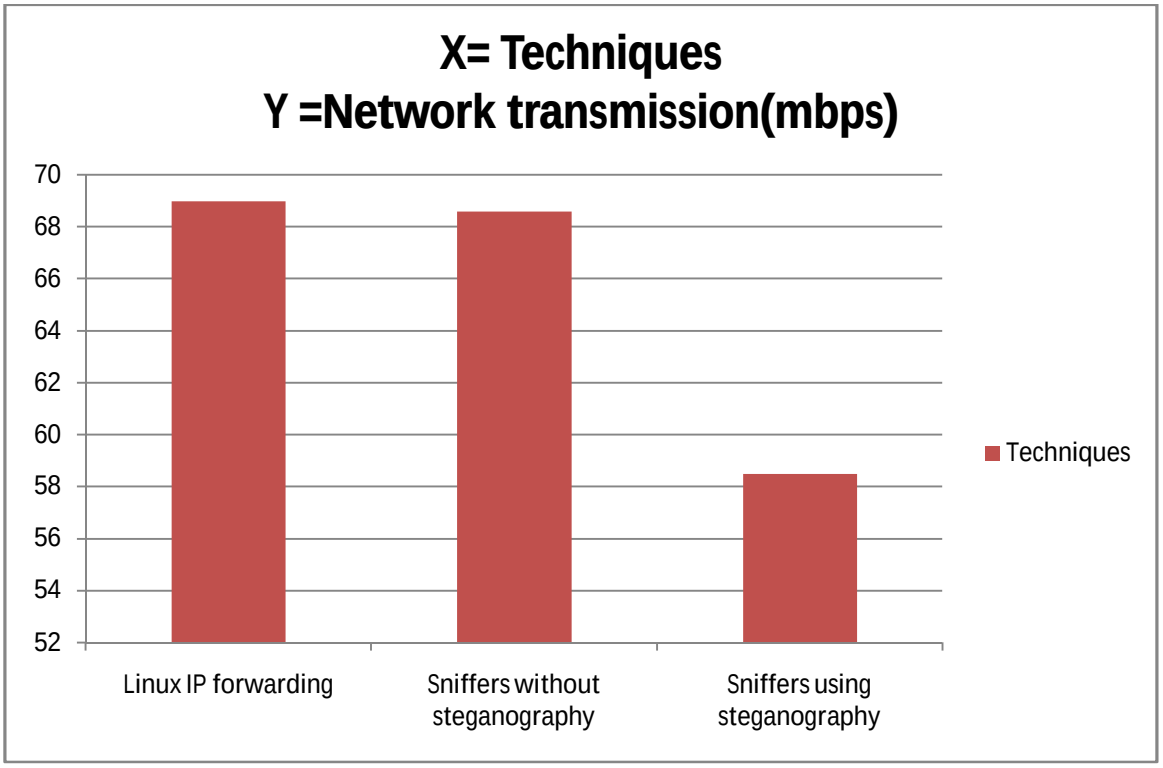

Figure 4.1: System's average transmission

Table 4.2 below illustrates time required by the system to transfer a complete steganogram file from steganogram sender to steganogram receiver. Files of different size have been and experiment was repeated 5 times for each file size, then the average is calculated.

File Size (Byte)	Time required to receive steganogram file (Second)					Average (Second)
	1	2	3	4	5	
10	27.02	27.98	28.03	27.98	28.00	27.80
20	64.04	67.01	63.03	63.03	65.01	64.42
30	99.97	100.00	99.02	102.02	99.97	100.20
40	130.00	132.04	130.07	132.08	131.99	131.24
50	168.01	165.05	166.06	168.03	165.01	166.43

Table 4.2: Time required for SR to receive steganogram file

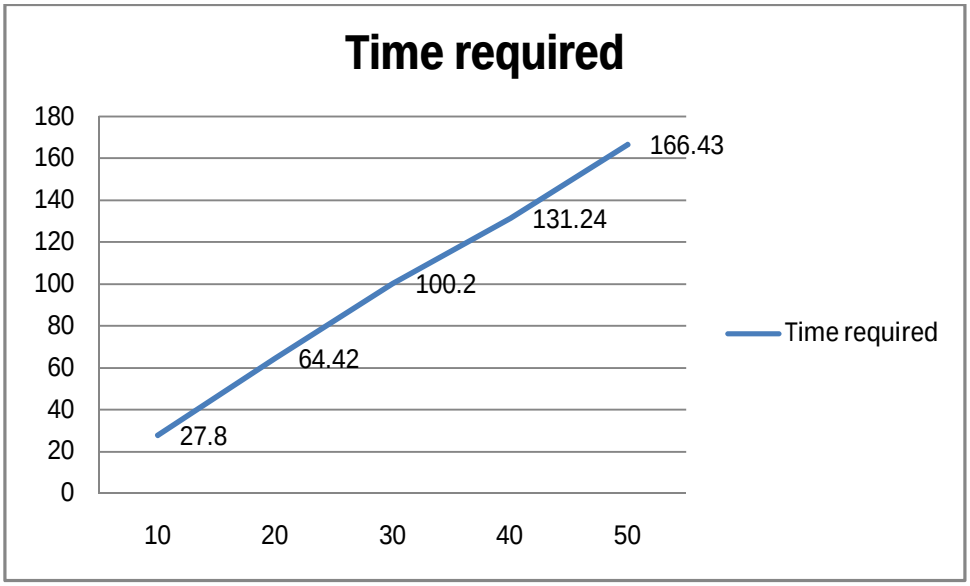

Figure 4.2 Average time required to transfer steganogram file from SS to SR

It is clear from Figure 4.2 above that our program written in C language to simulate the router has a performance ratio (68.602 mbps) close to original Linux (68.984 mbps) configured router, but this ratio (58.49 mbps) is decreased by 14.8% when MLS is add to our program.

The greater the size of the file a more time is required to move it through the system as shown in Figure 4.2 Since the file size of 10 byte require 27.80 sec where file size of 50 byte require 166.43 sec.

CHAPTER 5

RECOMMENDATIONS AND FUTURE WORK

5.1 Conclusion

A two-method MLS prototype was developed using C language to work within IP network by using identification field in IP header to carry 2 bits of steganogram(as an upper-level method) and TCP data section to carry the remain 6 bits(as a lower-level method).

Experimental results were obtained demonstrating that the average transmission time of network decreased from by 14.8% due to using of MLS, and the time required to transfer steganogram file of size equal to 50 bytes through the system is 166.43 seconds, about (2 minutes and 46 seconds).

5.2 Recommendations

- Upper-level method can be used to carry a cryptographic key that deciphers the steganogram carried by the lower-level method**.**
- Steganographic bandwidth can be increased by adding steganogram with size equal to (MTU – original packet length) for each packet.

5.3 Future work

- System can be extended to involve all protocols not only TCP packet that contain data.
- System can be extended to hide all other data types like images, audio, video not only text data.

REFERENCES

[1] G. Kipper, *INVESTIGATOR'S GUIDE TO STEGANOGRAPHY*, p.^pp. 221, 2003.

[2] W. M. Wojciech Frączek, Krzysztof Szczypiorski, "Multilevel Steganography: Improving Hidden Communication in Networks," *Journal of Universal Computer Science*, vol. 18, 2012.

[3] M. H. Rajyaguru, "CRYSTOGRAPHY-Combination of Cryptography and Steganography With Rapidly Changing Keys," *International Journal of Emerging Technology and Advanced Engineering*, vol. 2, 2012.

[4] W. M. a. K. S. Elżbieta Zielińska, "Development Trends in Steganography," Warsaw University of Technology, Institute of Telecommunications, p. 13.

[5] W. M. Wojciech Frączek, Krzysztof Szczypiorski, "How Hidden Can Be Even More Hidden?," W. M. a. K. S. Wojciech Frączek, ed.

[6] W. M. a. K. S. Bartosz Jankowski "PadSteg: introducing inter-protocol steganography," *Telecommun Syst*, 2013.

[7] M. S. Wojciech Mazurczyk, Krzysztof Szczypiorski, "Hiding Information in Retransmissions."

[8] D. A. J. AL-NAJJAR, "The Decoy: Multi-Level Digital Multimedia Steganography Model," pp. 6, 2008.

[9] S. S. V. Neha Agrawal, "STEGCRYP: A Multilevel Information Security Shceme," *International Journal of Emerging Technology and Advanced Engineering*, vol. 3, 2013.

[10] I. B. a. G. S. Souvik Bhattacharyya, "Data Hiding Through Multi Level Steganography and SSCE," *Journal of Global Research in Computer Science*, vol. 2, 2011.

[11] P. S. K. B. a. B. G. Banik, "Multi-Level Steganographic Algorithm for Audio Steganography using LSB Modification and Parity Encoding Technique," *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, vol. 1, 2012.