International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-4 Issue-2, December 2014

Secure Data Communication using Protocol Steganography in IPv6

Sandip Bobade, Rajeshawari Goudar

Abstract- In secure data communication Network Security is important. Basically in cryptography Encryption is used for data security. Still attacker can attract towards encrypted data due to different form of data.so this limitation could overcome by using steganography. Steganography is the technique of information hiding. In steganography different carriers can be used for information hiding like image, audio, video, network protocols. Network steganography is a new approach for data hiding. In network steganography network layer protocol of TCP/IP suite are used for data hiding. In Network layer covert channels are used for data hiding. Covert channels violate security policies of the system. Covert channels are either used for steal the information or communicate secrete information overt a network. Covert channel in TCP, IPv4 are previously implemented and studied. IPv6 is a new generation protocol which slowly replaces IPv4 in future because IPv4 is rapidly running out. So there is need to examine security issues related IPv6 protocol. Covert channels are present in IPv6 protocol. 20 bit Flow label field of IPv6 protocol can be used as covert channel. RSA algorithm is used for data Encryption.Chaotic method used for data encoding. Secret data communication is possible in IPv6.

Index Terms--Covert channel, Steganography, TCP/IP ,Network Security, Chaos Theory.

I. INTRODUCTION

Protection of information that is sent over network can be done by using the principles of cryptography. It is considered that the use of encryption is enough for secure communication in network. However, it is possible for an attacker to find the existence of encrypted channel between two remote entities and decrypt the captured traffic. Steganography eliminates this problem by concealing the existence of the messages. Steganography is the ability and skill of writing hidden messages to a cover medium in such a way that no one, separately from the sender and planned receiver, suspects the existence of the message. Applications of steganography are dedicated to multimedia applications in which hidden data are distributed via files of sound, images and videos. According to [1],[2] steganography can be applied in digital watermarking for defending copyrights in a variety of digital audio, video and software entities. Hiding data at network level such as protocols is relatively new, but it becomes a very important issue for network security. All information hiding techniques that can be used to exchange secret data in computer networks can be divided under the General term of network steganography[3].

Manuscript published on 30 December 2014.
* Correspondence Author (s)
Sandip Bobade, MIT Academy of Engineering Alandi (D),Pune, India.
Rajeshawari Goudar, Savitribai Phule Pune University, India.

different to the typical steganographic methods which utilize digital media (images, audio and video files) as a carrier for data hiding, network steganography use communication protocols, control Fields and their basic predefined functionality. Typical network steganography methods or network based covert channels use certain properties of the communications medium in an unexpected or eccentric way in order to transmit secret information through the medium without drawing attention by anyone other than the entities operating the covert channel. Network Steganography is synonym to covert channels is divided into three broad categories as shown in Figure 1.

1. Methods modifying network packet's header or payload.
2. Methods modifying the structure of packet streams.
3. Hybrid Schemes.

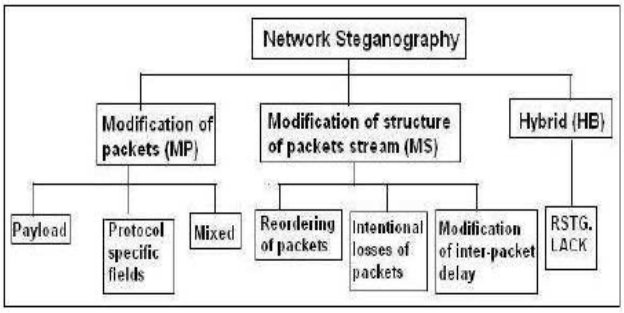

Figure 1.The classification of Network Steganography [6]

1. Methods modifying network packet's header or payload.- In this method the data hiding is carried out by modifying the protocol-specific fields. For example TCP, IP or UDP headers are modified to insert secret messages as discussed in literatures [1] and [4].All the steganographic techniques under this method have high steganographic capacity. Some of the application layer based steganographic techniques modify payloads of the packets. There is another method which involves hiding the data in both header and payload of the network packet as stated in [3] and HICCUPS [3](Hidden Communication System for Corrupted Networks). This method offers high steganographic capacity but the implementation is more difficult than any of the other methods. It needs reprogramming of Network Interface Cards. Drawbacks include increased frame error rate.

2. Methods modifying the structure of packet streams

Data Hiding can also be done through modifying the packet streams of the network as described in [5]. Some of the examples in this method are those which affect the sequence order of the packets [8], those that modify the inter packet delay [9] and those that introduce intentional losses by skipping sequence numbers [10] at the sender.

The main problem with these schemes includes synchronization between sender and receiver. Other drawback is that delays may affect transmission quality.

3. Hybrid Schemes

In hybrid scheme, the packet header and their time dependencies are modified. Lost Audio Packets Steganography[6,7] and Retransmission Steganography is one of the example which fall under this scheme. Compared to the other methods, this method has higher steganographic capacities. Another advantage of this method is that it is hard to detect.

2.1. COVERT CHANNEL

A covert channel is a medium in which information can pass, but this medium is not normally used for information exchange. Covert channels are first introduced by Lampson[11].covert channel is defined as any communication channel that can be exploited by a process to transfer information in a manner that violates the system's protection rule. In theory, almost any process or binary data can be a covert channel. Covert channels can be divided into two categories: storage covert channel and timing covert channel.

Storage Covert channel: In covert storage channel, the sender and receiver use a shared variable where one person will insert covert data inside it and other person will read covert data from it. In network environment, fields of header will acts as shared variables. One of the processes directly or indirectly writes to a particular storage location where as other process reads from that particular storage location. Several tools employ TCP, IP, ICMP, and HTTP protocols to establish storage covert channel. In these protocols unused fields are used to transmit the information because these fields generally go undetected by intrusion detection systems and firewalls.

Timing Covert Channels: In a timing channel, the receiver and sender agree a priory on a timing interval and the starting protocol. During each time interval the sender either transmits a single packet or maintains silence. The receiver monitors each interval to determine whether a packet was received. Note that the raw data that flows across the channel is binary but the actual interpretation of the binary stream is up to the communicating parties. Timing covert channel focuses on conveying the message through the arrival pattern of packets rather than the contents of message. Moreover, covert timing channel does not use packet header or payload to encode covert messages. Timing covert channel is divided into two channels: packet sorting channels and timing channels where information is conveyed by the arrival order of packets in packet sorting channel. On the other hand information by timing channel is conveyed by the presence or absence of packets in a specified time interval.

II. RELATED WORK

Network Protocol stack have various layers that contains various header fields for proper communication. These fields can be used as covert storage channels for covert communication. The OSI model is the standard network model against which nearly all current network models are compared. The OSI model includes TCP, IP and ICMP protocols which are implemented at different layers. Figure 2 shows Hierarchy of Network Steganography.

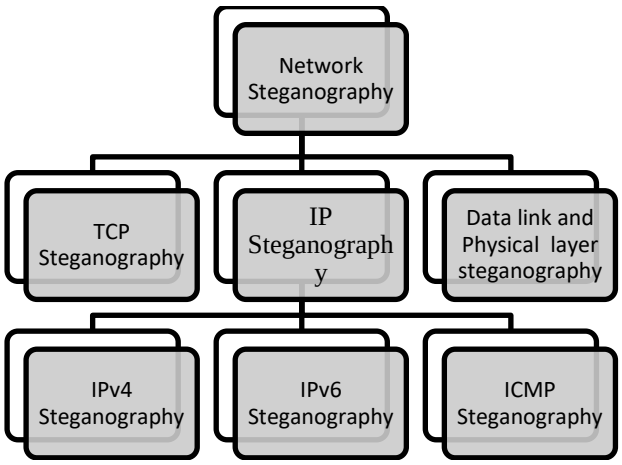

Figure 2. Hierarchy of Network Steganography

2.2 TCP Steganography

Transmission control protocol header contains different fields for communication. Each field has its individual properties and usage. Covert fields can be useful to hide information. These fields act as a carrier for steganography. The Initial sequence number (ISN), generated by OS, vary from OS to OS. Author of [12] explained how OPEN BSD and Linux 2 0 will generate ISN. For data hiding purpose ISN field serves as a perfect medium for transmitting over the internet because of its size and nature [13]. There are some fields in TCP/IP which are reserved for future use or unused such as 4-bit reserved field in TCP header, Padding and Options [17] fields in TCP/IP as shown in figure 3, and the unused bits of IP header's Type of Service (TOS) field, which can be used to encode secret data. There are also some unused combinations which make covert channels possible. In the TCP 8-bit flag field, ECE and CWR are newly added by RFC 3168 [22] for congestion control in ECN (Explicit Congestion Notification) enabled network, and the other six bits are used to interpret the other fields of a TCP header.

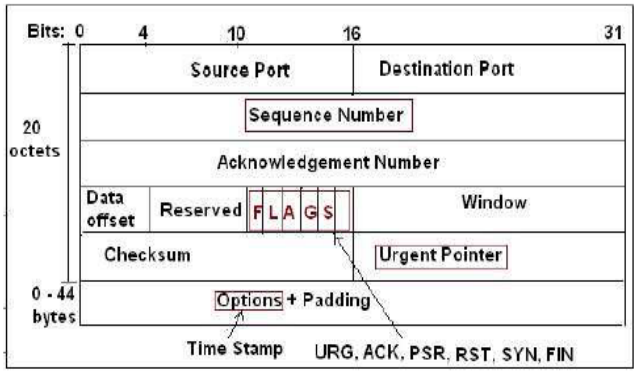

Figure 3. TCP Header

There are 64 possible combinations for the 6-bit flag field, out of that 29 are considered to be valid as per the rules set by the protocol. For example, Urgent Pointer field (16 bit) is significant only when URG is set. If URG is not set, then the Urgent Point field in TCP header becomes redundant, and therefore can be used for covert communication.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

2.3 IPv4 Steganography

Like TCP, IPv4 protocol also contains a number of fields in its header which helps in information hiding as shown in figure 4. IP Flags,IP identification field, IP Fragment offset, IP Options field and IP Type of service in the IPv4 header are used to hide secret information. several researchers came up with different kind of hiding techniques based on above covert channels. Ahsan, D.Kundur[14] mentioned four data scenarios based on IP identification and DF bit. In [14]the authors idea resides in the manipulation of the IP ID field. The packet Identification Field is assigned by the original sender. This number is random number generated while the packet was being constructed. When fragmentation occurs then Identification Field is used. Therefore assure that no fragmentation will occur because of the size of the packet; it is possible to hide data in this field without any consequence in the transmission. The advantage in this work is that it is used to send information from point to point, but the limitations are the quantity of information that you send. Furthermore if by any circumstances the datagram is fragmented, the receiver will observe noise in the transmission because it will receive the same information more than one time with every new fragment of the datagram. In [16] analyze possible covert channels in TCP/IP protocols and propose a new efficient scheme called Phase Reconstruction Method (PRM) to identify covert channels in TCP ISN and IP Identification fields. In [14] the work is focused in the manipulation of the Do Not Fragment Bit. There is possible to indicate if we do not want that our packet be fragment by the routers in the way. In consequence; again, this assures that our packet shall be not fragmented because of the size of it; we can hide information in the Do not fragment Bit at the flags field. A close study of [15] reveals that there exists redundancy in the Internet Protocol's fragmentation strategy. The Flags field contains fragmentation information. The first bit is reserved, the second is denoted DF (to represent Do not Fragment), and the third is denoted MF (to represent More Fragment). An un-fragmented datagram has all zero fragmentation information (i.e. MF = 0 and 13-bit Fragment Offset = 0) which gives rise to a redundancy condition, i.e. DF (Do not Fragment) can carry either "0" or "1" subject to the knowledge of the maximum size of the datagram. This aspect is exploited in Data Hiding Scenario. Some fields could be modified to encode secret information. TTL (Time to live) in IP header is a counter value that is decreased at each hop. When TTL reaches zero, the packet is discarded. This causes packets in routing loops to eventually be dropped. The current recommended default TTL value for the IPv4 (Internet Protocol Version 4) is 64 or 128 depending on different Operating Systems (OS). However, it can be changed. Sander [19] proposed to encode the covert information using two symbols: low-TTL signals a "0" whereas high-TTLsignals a "1".

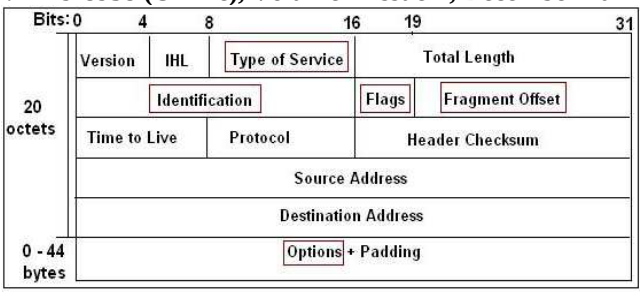

Figure 4. IPv4 Header

2.4 IPv6 Steganography

In IPv6 protocol number of covert channels are present which can be used as covert channel for concealing of data [21].

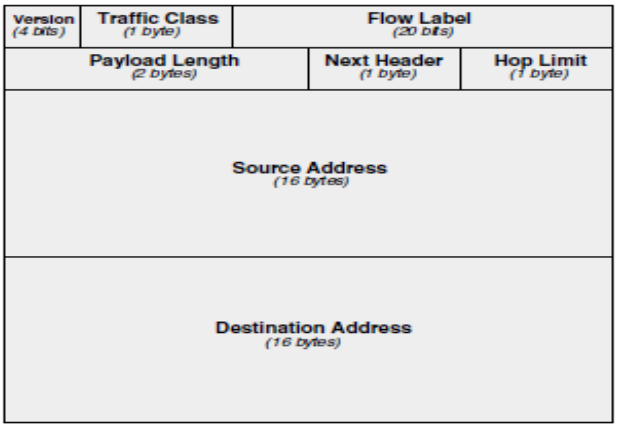

Figure 5. IPv6 Header

False value can set in a Traffic class field and the bandwidth of this channel varies up to 8 bits per packet. Flow label 20 bit field can use for covert data in IPv6 header as shown in figure 5. Value of payload length can increase append extra data at the end of the packet. The bandwidth of this channel varies depending on the size of the original packet. Source address field can also be used to send 16 bytes of covert data [21].Long MAC encoding technique applied on Source address field of IPv6.because of source address change in every packet. it is a IP spoofing. attacker can easily identify spoofed source address.

2.5 Chaos Theory

Chaos, in the mathematical logic, is stochastic ("random") behavior in a deterministic ("non-random") system. Chaotic systems have three key properties: they are **bounded** they are **non-repeating** they are **sensitive to initial conditions.** Our encoding system is based on using chaotic sequence. Chaotic sequence has the following characteristics.

(1) A chaotic map can output fixed sequence with a random input. The generation of chaotic sequence can be controlled by user, that is, we can have a fixed length sequence.

(2) Given a chaotic map and an input, the chaotic sequence can be calculated. But given an output sequence, it cannot find the equivalent input. The chaotic sequence is pseudorandom, so it is impossible that two data in a certain length is same.There are three main chaotic maps, logistic chaotic map, the improved logistic chaotic map and Chebyshev chaotic map.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Table 1. Different chaotic map[23]

Chaotic maps	expressions
Logistic chaotic map	$x_{n+1} = \lambda \cdot x_n(1-x_n),\ x_n \in (0,1)$
Improved logistic chaotic map	$x_{n+1} = 1-2\cdot x_n^2,\ -1 < x_n < 1$
Chebyshev chaotic map	$x_{n+1} = \cos(g \cdot \arccos x_n),\ -1 < x_n < 1$

In logistic chaotic map □□is a parameter when □□∈ (3.5699,4] the system is in a chaotic state. In Chebyshev chaotic map, g is also a parameter when $g > 2$ the system is in a chaotic state [23].

III. ARCHITECTURE OF MODEL

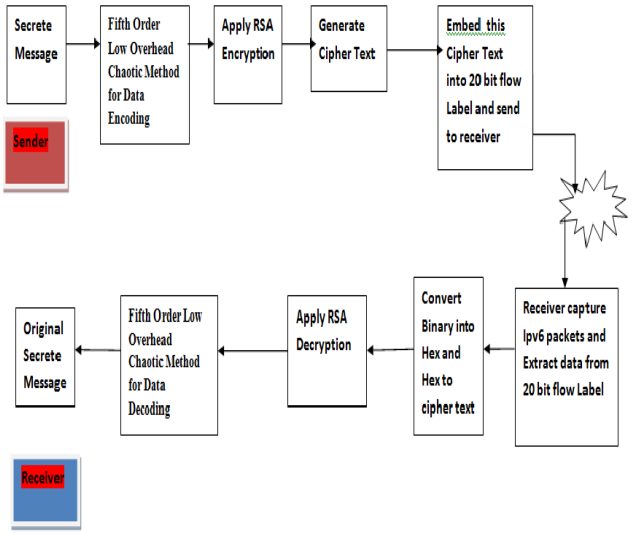

Figure 6. Architecture of Model

3.1 Fifth Order Low Overhead Chaotic Method Encoding Algorithm

Message=M
Define x, λ, sum=0,xmap,key,m,c;
int iteration=1;
x= λ *x*(1-x); logistic chaotic map
sum=sum+x;
x=1-(2*x*x); improved logistic chaotic map
sum=sum+x;
x=cos(5*Math.acos(x)); Chebyshev chaotic map
sum=sum+x;
x=sum/3.0;
Loop until end of message
do
m represents ith character from message
c represents ith character from encoded message
if x>=0 then map=1
else xmap=0
key=xmap ^ iteration
c=m ^ key
Stego_msg=stego_msg+c
x=λ*x*(1-x); //logistic chaotic map
sum=sum+x
x=1-(2*x*x) //improved logistic chaotic m
sum=sum+x
x=cos(5*acos(x)); // Chebyshev chaotic map
sum=sum+x
x=sum/3.0
Iteration++;
done
print encoded text

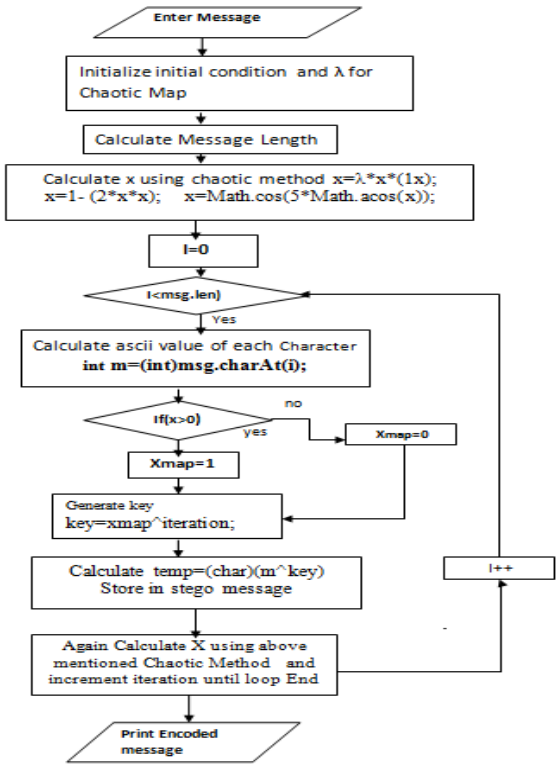

Figure 7. Flow Chart of Algorithm

3.2 IPv6 Flow Label Steganography

At Sender site
Step 1. Enter Message and Apply Fifth Order Chaotic Encoding algorithm. Encoded Message Generated.
Step 2. Apply RSA Encryption Algorithm on Encoded Message. Cipher text Generated.
Step 3.Convert Cipher text in Ascii Value and convert into Hex Value.
Step 4. Convert Hex into Binary
Step 5.Embed binary in 20 bit flow label.
Step 6.binary data divided into 20 bit and store 20 bit binary data in each ipv6 Packet. As per data size packets are created.
Step 7.Send Number of IPv6 Packet.
Step 8.Reciever capture Ipv6 number of Ipv6 packet and apply Decoding algorithm and Receive original packet

IV. IMPLEMENTATION AND RESULT

Implementation of this work is completed in UBUNTU 12.04 LTS and using java Language.

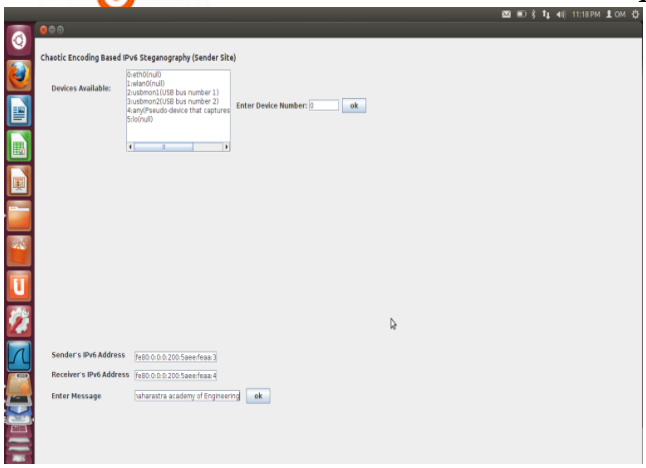

Figure 8(a). Sender site

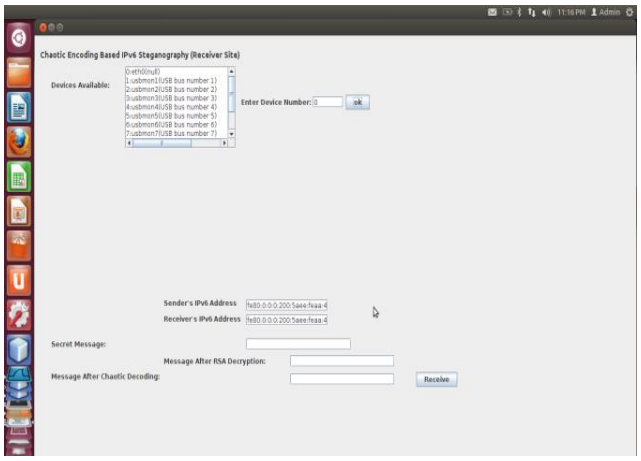

Figure 8(b). Receiver site

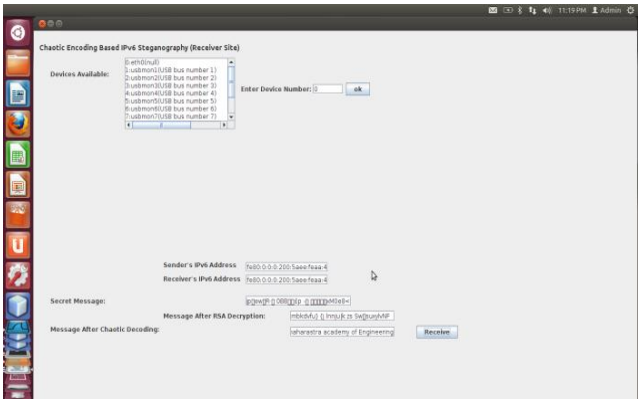

Figure 8(c). After receiving Message

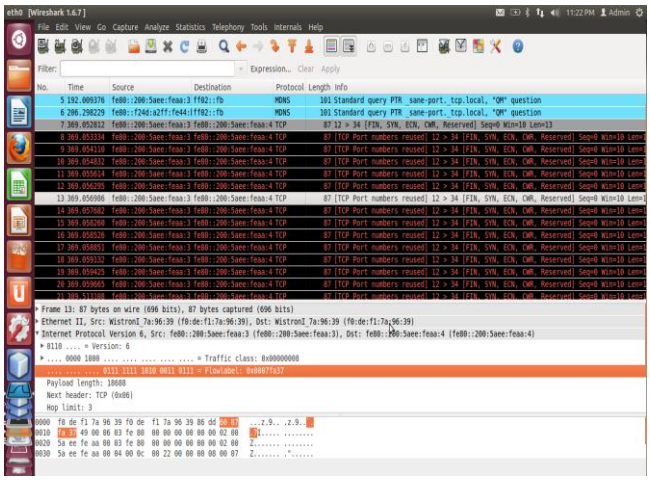

Figure 8(d). Wire shark IPv6 packet Capture

Table 2.Data Size w r t Encoding Time

Sr. No	Data size (byte)	Fifth order Low overhead Chaotic Encoding Time(m/s)	Long Mac Encoding Time(m/s)
1	1	0.71	1.24
2	5	0.77	1.68
3	10	0.79	1.91
4	15	0.85	2.32
5	20	0.91	2.45
6	25	0.92	2.72
7	30	0.93	3.00
8	35	0.95	3.24
9	40	1.00	3.61

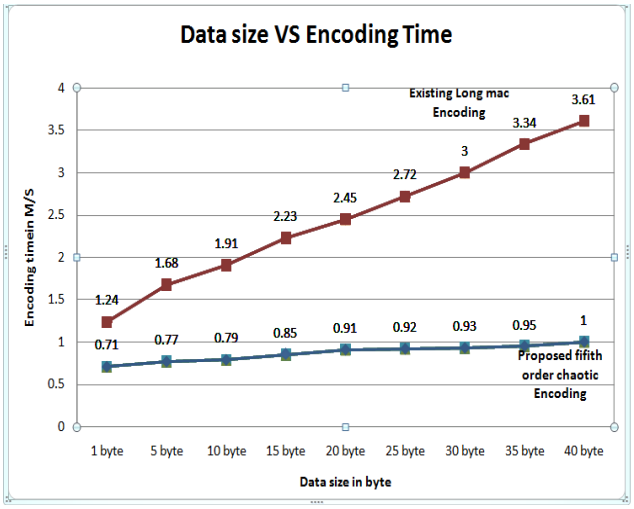

Figure 8. Data Size Vs Encoding Time

In Proposed method less Encoding time is required as compared with existing Encoding Technique.

V. CONCLUSION

Storage covert channel are more capacity to hide a data than timing covert channel. In IPv6 flow label field can be used as covert channel for Steganography. This channel is more secure to secrete communications where high confidential data need to be transferred. In future other covert channel in IPv6 needs to analyze.

REFERENCES

[1] M. Owens, "A Discussion of Covert Channels and Steganography" SANS (SysAdmin, Audit, Network, Security) Institute, 2002.
[2] Norka B. Lucena, Grzegorz Lewandowski, and Steve J. Chapin "Covert Channels in IPv6" Syracuse University, Syracuse NY 13244, USA 147–166, 2006._c Springer-Verlag Berlin Heidelberg 2006.
[3] Szczypiorski K., Steganography in TCP/IP Networks.State of the Artand a Proposal of a New System – HICCUPS, In Institute of Telecommunications' seminar, Warsaw University of Technology,Poland,November,2003 URL:http://krzysiek.tele.pw.edu.pl/pdf/steg-seminar 2003.pdf
[4] T. Sohn, J. S. , and J. Moon, "A study on covert channel detection of TCP/IP header using support vector machine," in Proc. 5th Int. Conf. Information and Communication Security (ICICS 2003),Oct. 2003,pp.313–324.
[5] Sellke, S.H., Wang, C., Bagchi, S., Shroff, N.B.: TCP/IP Timing Channels: Theory to Implementation, pp. 2204–2212 (2009),
[6] W. Mazurczyk, M. Smolarczyk, K. Szczypiorski, Retransmission steganography and its detection, Soft Computing, ISSN: 1432-7643 (print version), ISSN: 1433-7479 (electronic version), Journal no. 500 Springer, November 2009

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

[7] Mazurczyk ,W., Szczypiorski, K., Steganography of VoIP Streams, In: R. Meersman and Z. Tari (Eds.): OTM 2008, Part II – Lecture Notes in Computer Science (LNCS) 5332, Springer-Verlag
[8] Kundur, D., Ahsan, K.: Practical internet steganography: Data hiding in IP. In: Proc. TexasWorkshop on Security of Information Systems (College Station, Texas) (April 2003)
[9] Gianvecchio, S., Wang, H.: Detecting covert timing channels: an entropy-based approach.In: CCS 2007: Proceedings of the 14th ACM conference on Computer and communicationssecurity, pp. 307–316. ACM, New York (2007)
[10] Servetto, S.D., Vetterli, M.: Communication Using Phantoms: Covert Channels in theInternet. In: Proc. IEEE International Symposium on Information Theory, p. 229 (2001)
[11] B. W. Lampson, "A Note on the Confinement. Volume 16 Issue 10, Oct. 1973 ACM New York, NY, USA
[12] Steven 1. Murdoch and Stephen Lewis, "Embedding Cover Channelsinto TCP/IP". Information Hiding Workshop 2005 proceedings on, 2005
[13] Henry, P.A., Corporation, C., Rowland, C.H.: Covert channels in the tcp/ip protocol suite
[14] Ahsan, K., Kundur, D.: Practical data hiding in TCP/IP. In: ACM Workshop on Multimedia and Security (2002), http://ee.tamu.edu/deepa/pdf
[15] D. D. DhobaJe, V. R. Ghorpade B. S. Patjj, S. B. Patil, "steganography by hiding data in tcp/ip headers", 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE), 2010.
[16] Hong Zhao, Senior Member, IEEE, and Yun-Qing Shi, Fellow, IEEE" Detecting Covert Channels in Computer Networks Based on Chaos Theory" IEEE transactions on information forensics and security, vol. 8, no. 2, february 2013
[17] B. Jankowski, W. Mazurczyk, K. Szczypiorski, "Information Hiding Using Improper Frame Padding", In Proc. of 14th International Telecommunications Network Strategy and Planning Symposium (Networks 2010), 27-30.09.2010, Warsaw, Poland
[18] Zander, S., Armitage, G., Branch, P. (2007) "A Survey of Covert Channels and Countermeasures in ComputerNetwork Protocols", IEEE Communications Surveys & Tutorials, 3rd Quarter 2007, Volume: 9, Issue:3, pp. 44-57, ISSN: 1553-877X
[19] K. Szczypiorski, "Steganography in TCP/IP Networks. State of the Art and a Proposal of a New System HICCUPS" Institute of Telecommunications Seminar [Online].Available: http://www.tele.pw.edu.pl/krzysiek/pdf/steg-seminar-2003.pdf, Retrieved Jun. 2010 [20]G.
[20] Fisk, M. Fisk, C. Papadopoulos, and J. Neil. "Eliminating steganography in Internet traffic with active wardens." In Proc. IH, 2002.
[21] R.J.Anderson and F.A.P.Petitcolas,"On the limits of steganography,"IEEE J. Sel. Areas Commun., vol. 16, no. 4, pp. 474–481, May1998.
[22] Norka B. Lucena, Grzegorz Lewandowski, and Steve J. Chapin "Covert Channels in IPv6" Syracuse University, Syracuse NY 13244, USA 147–166, 2006._c Springer-Verlag Berlin Heidelberg 2006.
[22] K. Ramakrishnan, S. Floyd, and D. Black, "The Addition of Explicit Congestion Notification (ECN) to IP-RFC 3168, Sep. 2001.
[23] *Guangxian Xu*1, *Xiao Fu*2 *and Wei Wu*3 Low-overhead "Secure Network Coding based on Chaotic Sequence" Appl. Math. Inf. Sci. **7**, No. 2L, 605-610 (2013)

BIOGRAPHIES

Sandip Bobade, PG student, Computer Engineering Department, MIT Academy of Engineering.

Rajeshwari Goudar, is presently working as a Associate Professor in Computer Engineering Department, MIT Academy of Engineering.Alandi, Pune.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)