International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Email:editorijoer@gmail.com http://www.ijoer.in

Vol.4., Issue.4., 2016
(July-August)

RESEARCH ARTICLE

ISSN: 2321-7758

NETWORK STEGANOGRAPHY USING HICCUPS AND FRAME PADDING TECHNIQUE

SUBHAM CHOURASIA, DISHANTJAGANI, TAPANCHAKRABORTI,
ANINDYA JYOTI PAL
Information Technology Department, Heritage Institute of Technology
Chowbaga Road, Anandapur, P.O. East Kolkata Township, Kolkata, West Bengal, INDIA

ISSN: 2321-7758
IJOER
INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH-ONLINE
www.ijoer.in

ABSTRACT

Network Steganography is a methodology first discovered in 2003 which particularly aims at sending/receiving messages secretly via the use of protocols. Secret messages are put inside these protocols. Popular internet services such as Skype, BitTorrent, Google Suggest, and WLANs are the prime and major targets of information hiding techniques. These days attackers are using carriers for communication that monitors the path of the messages through the protocols. Several methods for hiding data in a network have been proposed, but the main drawback of most of them is that they do not offer a secondary layer of protection.

I. INTRODUCTION

Security on network faces these major problems of covertness, authentication and integrity control. Covertness or confidentiality is used to keep the information at bay from the unauthorized users. That means unauthorized users should not be able to read or understand the information on transfer.

II. PROCEDURE

The following are the existing network steganograhic methods.

A. HICCUPS

HICCUPS stands for Hidden Communication System for Corrupted Networks. It is the steganographic system ded- icated to shared medium networks including WLANs. The freshness of HICCUPS is the use of procure communications network fortified with cryptographic mechanisms to provide steganographic system and proposal of a new protocol with bandwidth allocation based on corrupted frames. It is a steganographic system for hidden group with common knowledge. A station sends a corrupted frame, i.e., a frame with an incorrect checksum. Remaining hidden stations change their mode of operation to the corrupted frame mode. To transmit steganograms, HICCUPS replaces payload of intentionally corrupted frames at the transmitter.

B. PadSteg

PadSteg stands for Padding Steganography. It is the steganographic system for LANs. PadSteg is known to be the first inter-protocol steganography solution. By the term inter-protocol, it means the usage of relation between two or more protocols from the TCP/IP stack to enable secret communication. PadSteg replaces padding bits of the short Ethernet frames with steganograms. The known Etherleak vulnerability makes PadSteg not trivial to detect. Etherleak is caused by ambiguous standardization that makes implementation of padding mechanism vary. In result, some NIC drivers handle frame padding incorrectly and fail to fill it with zeroes [4]. PadSteg utilizes Address Resolution Protocol (ARP) to identify all PadSteg-capable hidden nodes and also to perform so called carrier-protocol hopping during hidden exchange. Carrier-protocol hopping is an ability to negotiate carrier-protocol of the steganograms during hidden communication. PadSteg actually exchanges data with short frames of protocols such as Transmission Control Protocol (TCP), ARP, User Datagram Protocol (UDP) and Internet Control Message Protocol (ICMP).

C. **TranSteg**

TranSteg (Trancoding Steganography) is a middlingly new IP telephony steganographic method. It functions by compressing open data to make space for the steganogram. This is achieved by means of transcoding. It offers high steganographic bandwidth. TranSteg retains good voice quality. It is harder to detect than any other VoIP steganographic methods that exist today. In TranSteg, the hidden information is extracted and the speech data is practically restored to what was originally sent, after the steganogram reaches the receiver. This is a brobdingnagian advantage when TranSteg is compared with the existing VoIP steganographic methods. In all other methods, hidden data can be extracted and removed, but the original data cannot be restored because it was previously erased due to a hidden data insertion process. TranSteg is intended for a broad class of multimedia and real-time applications e.g. IP telephony.TranSteg can be exploited in other applications or services like video streaming, wherever a possibility exists to efficiently compress the overt data. The typical approach to steganography is to compress the covert data in order to limit its size, because it is reasonable in the context of a limited steganographic bandwidth . TranSteg utilizes compression of the overt data to make space for the steganogram. TranSteg for IP telephony is using transcoding of the voice data from a higher bit rate codec - overt codec to a lower bit rate codec - covert codec with the least possible degradation in voice quality. TranSteg operates as follows:

- For a chosen RTP voice stream, find a codec that will result in a similar voice quality but smaller voice payload size than the originally selected.
- Then, transcode the voice stream.
- At this step, the original voice payload size is intentionally unaltered and the change of the codec is not indicated. Instead, after placing the transcoded voice payload, the remaining free space is filled with hidden data. If Secure Real-time Transport Protocol (SRTP) is utilized for RTP streams, TranSteg detection is very difficult to perform.

D. StegTorrent

StegTorrent is a new network steganographic method. It is intended for the popular P2P file transfer service - BitTorrent. StegTorrent is developed for encoding classified data or information in transactions via BitTorrent. It works on the basis of reordering data packets in the peer to peer data exchange protocol. Some of the existing steganographic methods also reorder packets, but they need synchronization. StegTorrent doesn't. BitTorrent is a P2P file sharing system that allows its users to distribute large amounts of data over IP networks. A BitTorrent user shares a file or part of a file with so many recipients at once. This is the advantage taken up by StegTorrent. . In the clandestine communication scenario, both the secret data senders and receivers are in control of a number of BitTorrent clients and their IP addresses are known to each other. It is not at all necessary to have any knowledge about the topology of the network. The hidden data sender uses the modified BitTorrent client, i.e., the StegTorrent client. This client then shares a resource downloaded by another StegTorrent client. And that consists of a controlled group of BitTorrentclients .

III. **APPLICATIONS IN PROTOCOL FIELDS**

Fig. 1 shows the IP header. In the IP header, the 8 bit ToS field is not used by many of the network systems. The 16 bit ID field helps the receiver in reassembling the datagram fragments. The value in the ID field is copied to all fragments when a fragmentation occurs. The Flag field has 3 reserved bits – X (Reserved), DF (Do not Fragment) and MF (More Fragments). The use of DF bit in covert communication requires prior knowledge about the MTU. In Fig. 1 a method of covert communication by manipulating the lower order bits of the TCP timestamp field has been presented.

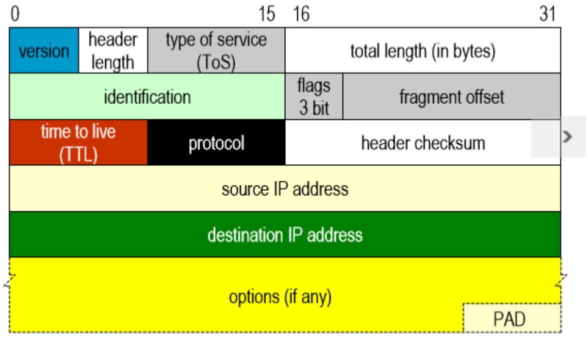

Fig. 1 IP Header

From the analysis made in, it is concluded that the use of most of these header fields in carrying out network steganography, can be easily detected. Therefore, it is necessary to have new systems that are capable for the effective transmission of secret information across the network.

IV. ALGORITHM

Given below are few techniques applied to achieve various conclusions on Network Steganography.

A. 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)); Chebyshevchaotic 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
```

B. 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.

V. FUTURE APPLICATIONS

Network Steganography has a lot of future applications for malicious software. The application of the aforementioned network steganographic methods leads to more sophisticated malware. The covertness of malevolent programs on smart phones can be increased in the future. This possibility is dramatically doubled in smart phones because the multimedia capability lets to create and use a video range of carriers e.g. audio, video, images or QuickResponse (QR) codes. Another reason is the availability of a full featured TCP/IP stack. It gives the possibility to interact with desktop-class services, thereby completely utilizing all the already available network methods for computing devices. Also, covert channels can be made exploitable based on VoIP and P2P, since the plethora of the adopted OS allows developing sophisticated applications. Network Steganography has been emerging into new and new domains. The stealthiness of illegal data exchange can be increased. Network Steganography can have tremendous influence to industrial espionage when it comes to data leakage.

VI. CONCLUSIONS

Due to the constantly increasing complexity of communication protocols, there is a growing need for network steganography. There is no doubt that new, more sophisticated techniques will be created and, in effect, the risk that they will be used for malicious purposes will increase. This concern adds new challenges to the difficult issue of providing network and information security. A deep understanding of the susceptibility of communication protocols to all types of manipulation (not only for steganographic purposes) becomes an extremely important issue. Research in the area of network steganography may be helpful in this respect. Research results should be used as guidelines for a methodology of designing a new generation of robust communication protocols. This is not only an engineering "must" but also an ethical obligation.In order to minimize the potential threat of inter-protocol steganography to public security identification of such methods is important. Equally crucial is the development of effective countermeasures. This requires an in-depth understanding of the functionality of network protocols and the ways in which they can be used for steganography. However, considering the complexity of network protocols being currently used, there is not much hope that a universal and effective steganalysis method can be developed. Thus, after each new steganographic method is identified, security systems must be adapted to the new, potential threat.

REFERENCES

[1]. *SandipBobade, RajeshawariGoudar,* "Secure Data Communication using Protocol Steganography in IPv6". International Journal of Engineering and Advanced Technology (IJEAT) Vol 16/15.

[2]. *Krzysztof Szczypiorski,* "Performance Analysis of HICCUPS – a Steganographic System for WLAN". Nowowiejska Vol.15/19, 00-665 Warsaw, Poland.

[3]. *Bartosz Jankowski, WojciechMazurczyk, Krzysztof Szczypiorski,* "PadSteg: Introducing Inter-Protocol Steganography Telecommunication Systems: Modelling, Analysis, Design and Management", Vol. 52, Iss. 2, pp.1101-1111, 2013

[4]. Zishuai Li ,Xingming,Sun Baowei Wang ,Xiaoliang Wang, A Steganography Scheme in P2P Network,Intelligent Information Hiding and Multimedia Signal Processing, 2008. IIHMSP '08 International ,15-17 Aug. 2008

[5]. WojciechMazurczyk, Krzysztof Szczypiorski, Steganography of VoIP Streams3rd International Symposium on Information Security (IS'08), Monterrey, Mexico, November 10-11, 2008

[6]. *Mrs. Dhanashri D. Dhokate, Dr. Vijay R. Ghorpade* "Data Hiding With Multiple Network Protocol Usage", International Journal of Advanced Research in Computer and Communication EngineeringVol. 4, Issue 7, July 2015.

[7]. J. Lubacz, W. Mazurczyk, K. Szczypiorski, "Principles and Overview of Network Steganography", IEEE Communication Magazine, vol. 52, no. 5, May 2014.

[8]. Guangxian Xu, Xiao Fu and Wei "Secure Network Coding based on Chaotic Sequence" Appl. Math. Inf. Sci. 7, No. 2L, 605-610 (2013).

[9]. Anderson, R. (Ed.): Proceedings of: Information Hiding First International Workshop, Cambridge, U.K., May 30 June 1, 1996, vol. 1174 of Lecture Notes in Computer Science, Springer-VerlagInc.

[10]. Baker, M. Steven. 1992. "Network Delivers." Windows Tech Journal", Volume 1 (August 1992): 22-29.

[11]. Mazurczyk W., Smolarczyk M., Szczypiorski K.: "Retransmission steganography and its detection, Soft Computing", ISSN: 1432-7643 (print version), ISSN: 1433-7479 (electronic version), Journal no. 500 Springer, November 2009.