

Packet Length Based Steganography Detection in Transport Layer

Rajeshwari Goudar, Anjali Patil

Department of Computer Engineering
MIT Pune's, Maharashtra Academy of Engineering, Alandi (D)
Pune University, India.

Abstract- Network steganography describe methods which are used for transmitting information over network without being detected. Length of packet is used for sending secret data. In this paper, a network steganographic detection scheme has been proposed which can detect the presence of steganographic content by modifying length of UDP datagrams. Proposed detection scheme can detect network steganography based on packet length with efficient accuracy.

Index Terms- Covert channel, Network security, Steganalysis

I. INTRODUCTION

Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message. Steganography serves as better way of securing information than cryptography. Steganography and cryptography are closely related. In cryptography, message is scrambled to make it extremely difficult for an attacker to put together whereas in steganography, message is embedded in data is visible to the world is the clear and appears as harmless and normal. In modern steganography, different approaches can be used for embedding data in multimedia file (text, image, video, audio) and also in the network packets. Steganography techniques arise and evolve with the development of network protocol and mechanism and are expected to be used in communication. Recent year, its getting popular due to wide spread of information network. e.g multimedia service network and social network.

The traditional approach encrypts the data in the Application layer e.g. HTTP protocol, the most popular and common protocol used over the Internet, uses Secured Socket Layer (SSL) technique for encryption and decryption of data send over the internet. The new method proposes a completely new approach for sending & receiving of encrypted data. Instead of sending encrypted data over Application Layer, it will be hidden in the TCP/UDP header field. The hacker will be deceived, because it will look for data in the application layer. The application layer will contain a fake message e.g. a fake HTML Web Page using HTTP protocol. It will use the TCP Port No. 80 for HTTP protocol. The hacker will be deceived into thinking that it is a genuine HTTP data. The new approach is used which uses length of packet to transfer hidden information in the transport layer, so the detection of packet length based steganography at transport layer is important.

In the network layer, steganography can be achieved through following methods:

- 1) Modifying network packet header and payload
- 2) Modifying the structure of packet streams
- 3) Hybrid scheme

Data hiding can be done by modifying TCP, IP, UDP protocol specific fields [1]. In IP header, identification field can be changed on some firewalls, source address can be changed if data will flow only in one direction and IP options can be modified in certain environment. In case of TCP header, timestamps field can be modified in order to inject secret message whereas in UDP header, source port, data length and checksum can be modified to send secret message across the network. Source port is used in case of dynamic network address translation (NAT). All these techniques have high data hiding capacity that are easily detectable using some steganalytic techniques [4]. There is another method in which both header and payload of packet are modified for hiding data across the network [3]. In hybrid method, the packet header and their time dependencies are changed. Retransmission steganography is the implementation of hybrid scheme. In this method, main idea is to not acknowledge a successfully received packet in order to intentionally invoke retransmission. The retransmitted packet carries a steganogram instead of user data in the payload field [10] and helps attacker to hide message.

Covert channel is used for the transmission of secret data across the network. The concept of covert channel was introduced by Lampson [2]. Covert channel is getting more importance in network steganography. There are some common covert channels which are used for hiding data:

- 1) Steganography - pictures, audio
- 2) Network - various protocols (TCP, IP, UDP)
- 3) Text - words, character substitutions
- 4) File system - hidden files
- 5) Appending data - header, footer

TCP header is used for embedding secret information. NUSHU is an implementation of TCP ISN based passive covert channel [5]. Passive covert channel is a specific kind of carbon copy (CC), which does not generate its own traffic so passive covert channel will be very hard to detect, since the packets used

for carrying the message are beyond any suspicion. Passive covert channel only changes some fields in the packets generated by a legitimate user of the compromised host. Here, ISN field is changed and this new ISN will carry the secret message.

IP TTL field is used for hiding secret information [6]. The sender modify the TTLs of subsequent packets transmitting secret information to the receiver. In the network steganography, new approach is widely used which allows to change the length of packet to transfer secret data across the network.

Steganalysis is the discovery of the existence of hidden information; therefore, like cryptography and cryptanalysis, the goal of steganalysis is to discover hidden information and to break the security of its carriers. Steganalysis is divided into two types: blind steganalysis and targeted steganalysis. The blind steganalysis attempts to detect steganographic data without knowledge about the steganographic system. Current algorithms for blind steganalysis of images are based on two-stages: first, features are extracted in order to reduce dimensionality and to highlight potential manipulations and second, a classifier trained on pairs of cover and stego images detect a decision rule for these features to detect stego images. A targeted steganalysis technique works on a specific type of stego-system and sometimes limited on image format. By analysing the embedding algorithm, it helps to find image statistics that change after embedding. The results from most of targeted steganalysis techniques are very accurate. One of the popular way in steganalysis is to identify embedded features and statistical analysis is done by a supervised learning classifier using those sensitive features. The method used for the detection of steganography in TCP ISN sequence number. In this method, statistical deviations of ISN network packet from the ISN model are discovered and it is considered that this ISN packet is generated by malicious software, which tries to create a covert channel. In case of IP covert channel, inter-arrival time for each packet is observed to detect whether there is any variance in inter-arrival times [7].

In this paper, a network steganography detection scheme has been presented which can efficiently detect network steganography based on packet length. In the proposed method, a feature set is determined from the packet flow and a supervised classifier is trained for detecting the presence of hidden data. The paper is organized as follows: The concept of packet length based steganography and the related work have been introduced in section II. In section III, a proposed steganography detection scheme is presented.

II. PACKET LENGTH BASED NETWORK STEGANOGRAPHY

Communication in the network happens by transmission of information in the form of packets and the content in each packet gives its length. The pattern of packet length depends on the application as well as the protocol that sends the packet across the network. Maximum size of the packet is used by any file transfer application to send the information. In certain application, packet length varies for sending message. It helps to

change the length of packet to transmit the hidden data. This is called as packet length based steganography. The detection becomes difficult if the packet flow imitates the normal network flow.

A. Related Work

Length based hiding is first proposed by Padlipsky [8]. It uses an embedding scheme which modulates the length of the link layer frames. This technique employs 256 different frame lengths to describe the bytes. In this scheme, frame length distribution is random and it did not imitate the normal network traffic flow. There is another model which used the length of the packets to transfer the secret message. In this scheme, both the sender and the receiver share a secret matrix, and all the cells represent unique length. The sender selects a cell randomly and finds out the length of the message to be send, the receiver picks up the same algorithm to find the random number from the matrix to get the secret message. Liping [9] has proposed another method which uses the length of the messages to transfer the secret data. In this proposal, the sender and the receiver create a reference which is formed by collection of certain lengths of the normal traffic and the values in this reference are used to send secret message. Liping's second scheme created buckets and these buckets contains certain values. The number of buckets created depends on the payload of the secret data per packet. Depending on the secret data, a value from a bucket is taken and the packet of that value is send across the network.

From the above survey it is observed that length based techniques are an important branch of covert channel implementation. There is certain application where the packets are of random sizes and not having specific pattern. It is possible for steganographers to exploit this particular feature to send the secret data by modulating the size of the network packets. In the steganographic scheme, the payload of UDP protocol that sends chat messages across the network can be modulated. When the users chat, the lengths of the messages have a random distribution and it is exploited to transfer the secret message across the network. In proposed work, a new steganalysis scheme depending on the length vector is proposed and using this scheme the steganographic scheme is proved to be detected.

B. Model for Packet Length based Network Steganography

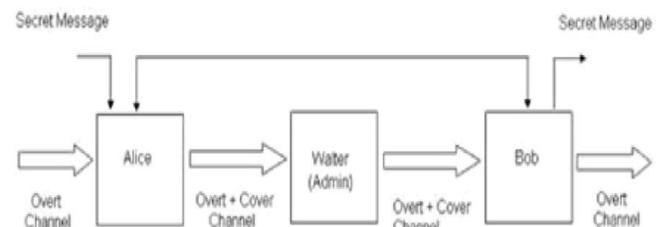


Figure 1: Model of Packet Length Based Network Steganography

Chat application based on UDP can be used for steganography where UDP packet length can be modified to inject secret data.

UDP based application has been used because packet length of UDP datagram are random in nature.

In Figure 1, Alice needs to send secret message to Bob in her chat application and she embeds secret message along with the length of the message to be send. Walter is the administrator who can monitor all the network packets. Bob receives the packets and decode secret message from the length of the packet. Bob also sends messages to Alice so that it appears as a normal chat application running between them.

III. PROPOSED STEGANALYSIS SCHEME

In the packet length based network stenography, packet lengths are modified for embedding secret data. It is possible to detect the presence of secret data by statistical analysis of different packet length. In this proposal, statistical analysis is done in a specific application. The detector observes a large set of packet for a particular application to detect possible trace of steganographic embedding. As seen in section II, the proposed detection scheme is focused on UDP based network steganography. UDP datagram are more suitable for length based steganographic embedding as the distribution of packet length for application is random in nature.

A. Packet Length Analysis

The proposed detector mainly observes length distribution of UDP datagram for the particular application. Packet length distribution for the application is studied. For each packet number, corresponding packet length is determined. Packet length statistics is randomly distributed in UDP datagrams. The existing steganalysis schemes cannot used for the detection of the presence of secret data in the length of packets because of this random distribution.

The following section describes features which are used to train steganalytic classifier that is used in the detection of packet length based steganography.

1) Packet Length Vector X:

A first order statistic is obtained from the UDP (IP) packets and is called as Packet Length Vector (X). This vector contains the number of packets for each of the valid packet lengths. It represents the relative frequency of specific packet length in the series of packets. The range of packet lengths is from [0....L-1] and is represented by the following discrete function

$$X(r_k) = \frac{n_k}{n} \quad (1)$$

Where r_k is k^{th} packet length in the time series, n_k is the number of packets with the packet length and n is the total number of packets.

Packet Length Vector (X) is given as

$$\rightarrow X = [X(r_0), X(r_1), X(r_2), X(r_3), \dots, X(L-1)] \quad (2)$$

Or it can also be represented as,

$$\rightarrow X = [X(0), X(1), X(2), X(3), \dots, X(L-1)] \quad (3)$$

2) Effect of Embedding on Packet Length Vector (X) :

Packet Length Vector (X) is altered due to embedding. There can be hidden communication, if different pattern is observed from this alteration of the Packet Length Vector (X) due to embedding. Due to embedding, smoothness for normal packet stream gets reduced.

The effect of embedding on statistic of the cover in case of image steganography is given by Harmsen [12]. In this scheme, steganographic embedding is done on LSB of image that smoothens the image histogram and this smoothens can be quantified. In the proposed scheme, steganography based on packet length reduces the smoothness of Packet Length Vector(X). This reduction can also be quantified by performing Discrete Fourier Transform (DFT) on X. The Center Of Mass (COM) of X_{dft} is then determined to detect the effect of embedding. The Center Of Mass (COM) of X_{dft} can be calculated as

$$COM = \frac{\sum_{i=0}^{N-1} iX_{dft}}{\sum_{i=0}^{N-1} X_{dft}} \quad (4)$$

Where N is length of the X_{dft} vector.

In packet length based network steganography, it is observed that COM (Stego) is usually grater that COM (Cover) where Stego is the embedded message in UDP packet stream and Cover is UDP packet stream without embedded data. Embedding process distorts the packet length vector (X), the number of local maxima, minima of packet length vector is also increased due to embedding. Distortion metric can be defined as,

$$\partial = |2X(\lambda) - X(\lambda - 1) - X(\lambda + 1)| \quad (5)$$

where n is the number of bins in the packet length vector (X) and λ is the position of maxima or minima. In case of packet length based network steganography, ∂ (Stego) is usually greater than ∂ (Cover) where Stego is the UDP packet stream with embedded message and Cover is innocent UDP packet stream.

B. Feature Extraction and Classification

In proposed scheme, a steganalytic classifier is trained using two dimensional features. The packet length vector (X) is first determined for a UDP stream. First, the Fisher Linear

Discriminant (FLD) is used. FLD are the methods used in statistic, pattern recognition and machine learning to find linear combination of features which characterize or separates two or more classes of events. Resulting combination may be used as linear classifier or for dimensionality reduction before classification. Then the Linear Discriminant Analysis (LDA) classifier [11] is trained using this single dimension feature. Linear Discriminant Analysis easily handles the case where the within-class frequencies are unequal and their performance has been examined on randomly generated test data.

IV. PERFORMANCE EVALUATION

Proposed scheme provides various parameters that are used to detect the presence of hidden data. First, Packet Length Vector (X) is calculated for normal network traffic , the center of mass(COM) of resultant Packet Length Vector (X) and distortion metric (δ) are also calculated for normal traffic flow. Then center of mass (COM) of resultant Packet Length Vector (X) and distortion metric (δ) are also calculated for stego traffic. Fisher Linear Discriminant (FLD) is used to reduce the two dimensional feature space to single dimension. Using this reduced feature space, a Linear Discriminant Analysis (LDA) classifier has been trained.

To evaluate the performance of the proposed scheme, ROC curve is used. In signal detection theory, a receiver operating characteristic (ROC) or simply ROC curve, is a graphical plot of the sensitivity, or true positive rate, vs. false positive rate (one minus the specificity or true negative rate), for a binary classifier system as its discrimination threshold is varied. A ROC is used to evaluate the performance of the classifier. The ROC can also be represented equivalently by plotting the fraction of true positives out of the positives (TPR = true positive rate) vs. the fraction of false positives out of the negatives (FPR = false positive rate). The ROC is also known as a Relative Operating Characteristic curve, because it is a comparison of two operating characteristics (TPR & FPR) as the criterion changes. Detection accuracy (P_{detect}) is computed using equations (6) and (7).

$$P_{detect} = 1 - P_{error} \quad (6)$$

$$P_{error} = \frac{1}{2} \sum P_{FP} + \frac{1}{2} \sum P_{FN} \quad (7)$$

Where P_{FP} , P_{FN} are the probabilities of false positive and false negative respectively. A value of $P_{detect} = 1.0$ shows a classification with 100% accuracy. The Figure 2 shows ROC graph.

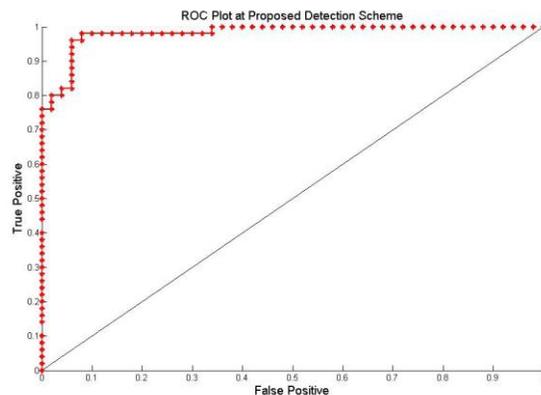


Figure 2: The ROC Curve for evaluating the detection performance of the proposed scheme

V. CONCLUSION AND FUTURE WORK

In this paper, the network packet length based steganography detection scheme has been proposed. Steganographic classifier is trained using two dimensional feature space so as to detect the difference between the normal traffic and stego traffic. The proposed detector can detect the presence of steganography with high accuracy. The proposed scheme is used for moderate payload and also for different payload. There is no comparison with the existing steganalysis techniques as there is no such detection technique based on packet length steganography is available.

ACKNOWLEDGMENT

My heartfelt thanks to my guide, Prof. R. M. Goudar, Asst Professor, College of Maharashtra Academy of Engineering, Pune, who offered her whole hearted guidance and invaluable suggestions throughout the preparation of this paper. Above all I must and do thank God Almighty from the depth of my heart for the being with me at each and every stage assuring hope, confidence and courage to get the task accomplished in time

REFERENCES

- [1] K. Ahsan and D. Kundur, "Practical data hiding in TCP/IP" In: ACM Workshop on Multimedia and Security, 2002, <http://ee.tamu.edu/deepa/pdf/acm02.pdf>.
- [2] B. W. Lampson, "A note on the confinement problem" *Common.ACM*, 16: (10):613-615
- [3] K. Szczypiorski, "A Performance Analysis of HICCUPS Steganographic System for WLAN", in *CoRR*, vol. abs/0906.4217, 2009, <http://arxiv.org/abs/0906.4217>.
- [4] S. J. Murdoch, J. Steven and Lewis, "Embedding Covert Channel into TCP/IP", University of Cambridge Computer Laboratory, Cambridge, UK. July 29, 2005.
- [5] Rutkowska, J., "The implementation of passive covert Channels in Linux kernel" In: *Chaos Communication Congress*, Chaos Computer Club e.V., 2004, http://www.ccc.de/congress/2004/fahrplan/event/176_En.html
- [6] S. Zander, G. Armitage and P. Branch, "Covert Channels in the IP Time To Live Field", Centre for Advanced Internet Architectures, Swinburne University of Tech, Melbourne Australia.

- [7] S. Cabuk, C. E. Brodley and C. Shields, "IP covert timing channels: design and detection", in Proceedings of the 11th ACM conference on Computer communication survey, October 25-29, 2004, Washington DC, USA
- [8] M. A. Padlipsky, D. W. Snow and P. A. Karger, " Limitations of endtoend Encryption in secure networks", Tech.Rep.ESD-TR-78-158, Mitre Corporation
- [9] L. Ji, W. Jiang, B. Dai and X. Niu, "A Novel Covert Channel Based on Length of Messages", International Symposium on Information Engineering and Electronic Commerce, 16-17 May 2009, Page(s):551-554
- [10] W. Mazurczyk , M. Smolarczy and K Szczypiorski, Hiding information in retransmissions ", CoRR, abs/0905.0363, 2009.
- [11] J. Fridrich, "Feature - Based Steganalysis for JPEG Images and its Implications for Future Design of Steganographic Schemes", in Proc. 6th Int. Workshop on Information Hiding, Toronto, Canada, pp. 67-81, 23-25 May 2004.
- [12] J. Harmsen and W. Pearlman, "Steganalysis of additive noise modelable information hiding", in Proc. Security and Watermarking of Multimedia Contents V, vol. 5020, pp. 131-142, June 2003.

AUTHORS

First Author – Prof.R.M.Goudar, M.E Computer Engg.
Maharastra Academy of Engineering, Pune.
rmgoudar66@gmail.com

Second Author – Anjali Patil, ME (2nd year), Maharashtra of
Academy of Enggneering, Pune.
anjalimpatil21@gmail.com