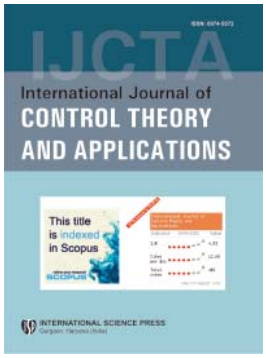

International Journal of Control Theory and Applications

ISSN : 0974–5572

Volume 9 • Number 42 • 2016

Storage Covert Channel Concealment in TCP Field

Pournima More[a] T.N. Shankar[b] and P.T Borse[c]

[a]*Department of Computer Science & Engineering, KL University, Vaddeswaram, Guntur Dist. A.P*

E-mail: pournima.more1@gmail.com

[b]*Department of Computer Science & Engineering, KL University, Vaddeswaram, Guntur Dist. A.P*

E-mail: tnshankar2004@rediffmail.com

[c]*D.Y Patil School of Engineering, Pune*

E-mail: pborse386@gmail.com

Abstract: Covert channel is malicious communication in secured network. Due to absence of inbuilt security mechanism, covert channel is threat in legitimate communication. Covert channel means a channel with 'secret communication technique' employed by two or more parties permitted to interchange information. In this channel, it is assumed that the data channel in use is under surveillance. The content of the genuine low security message is modified, so that the eavesdropper cannot read it from the secret channel. There are two types of Covert Channel; Storage Covert Channel and Timing Covert Channel. Storage covert channel uses header fields of packets like reserved bits of header, timestamp, initial sequence number, packet length etc. for sending data whereas timing covert channel is based on timing of event. In this paper we are storing secret data by using cryptography algorithm and Steganography in TCP Initial sequence number field because this field is of maximum capacity for storage based covert channel. Existence of hidden information in TCP initial sequence numbers field (ISN) is one of the most difficult covert channels to be detected. The proposed algorithm is simple but hard to crack unless one is not familiar with its inner working.

Keywords: *Covert Channel, Steganography, Cryptography, Initial Sequence Numbers, Mean Squared Error, Peak Signal to Noise Ratio.*

1. INTRODUCTION

A covert channel is communication channel exploited by a process to transfer information that violates system security policy [1]. Covert channel is secured communication channel that transmits information in a secret manner. Covert channel is used by trusted parties to share secret key. Cryptography is different from Covert channel. Covert channel hides existence of transmission whereas in cryptography, message transforms into not readable form, it does not hide existence of message.

TCP/IP protocols used in covert channel become new challenge for network security. There are two types of covert channel- storage channel & timing channel [1]. In storage covert channel sender put data into particular data item (packet header) & receiver simply retrieve data from same field. On other hand timing covert channel

depends on order of event & amount of time (packet arrival) of sending process while receiver simply detects delay information. Many field of TCP/IP we can use to hide data, among which Initial Sequence number field & Identification field are more difficult to detect [1]. Many attacks we can avoid if we use covert channel.

How to prevent accessing of data by unauthorized user is interesting topic for information security. There are two common techniques for information security- cryptography & steganography. Cryptography is to secure communication by changing data form so that it cannot understand by unauthorized user. On other hand steganography hide existence of message itself [12].

There are different ways of hiding data such as direct embedding or indirect embedding. For direct embedding LSB bit is used to embed data, but it is not secured because of bit plane attack. Indirect embedding data hiding is based on EDGE algorithm [2] to improve data security.

How to protect sensitive information from unauthorized user access? Answer was cryptography. Cryptography not only provides confidentiality and privacy but also authentication, non-repudiation, integrity etc. Cryptography techniques can be broadly divided into asymmetric key and symmetric key. Asymmetric key uses two keys for the purpose of encryption and decryption. Symmetric key uses single key for purpose of encryption and decryption.

Covert channels can be considered as one of the main sub disciplines to hide data. In data hiding, based on the security policy of the system two communicating parties are permitted to communicate with each other while using the features as associated with covert channel. A covert channel is primarily used for information transmission. [3]

Hybrid covert channel is combination of more than one channel, which can be active at same time or at different time. We are implementing hybrid covert channel which is combination of subliminal channel & steganography channel.

In this paper, a new covert channel is presented. The following section explains previous work on covert channel. In section III we introduce method of covert channel by using sequence number field. We conclude in section IV.

2. RELATED WORK

Construction of covert channel is done by utilizing the TCP and IP header checksum field, padding field, timestamps, initial sequence number field, acknowledgement number field, Identification field and TTL field. This paper implemented noisy covert channel. The bandwidth varies depending upon the field which we are going to send data. Among above fields, a TTL field is used in this paper due to which false positive numbers and time complexity is reduced [1].

The TCP sequence number field is used as primary field in the storage based covert channel. Limiting the bandwidth of covert communication is main purpose and not the detection. This approach uses three way handshaking for network packets. The result shows that when the intended receiver receives contents, almost all the original contents are blocked [4].

Data compression and arithmetic division operation schemes are used in this paper for covert communication. Using compression algorithm secret data is first compressed, then using an arithmetic division operation data is embedded into LSB position of the image. To evaluate results of embedded image, image quality parameters are calculated [5].

There are three techniques to embed data into image: LSB, RLSB and ELSB. Among these three techniques, attacker can easily identify presence of hidden message in LSB and RLSB. But in ELSB technique, the data is hidden in edge pixel. The technique is also applicable to all kinds of images and can be used in covert communication to hide secret information [2].

In this paper, hash based LSB technique is used secret data or information is hidden within a video. Eight bits among the secret information is divided into 3, 3, 2 and then embedded into respective RGB pixel values. The position of insertion in LSB bits is selected using various parameters such as PSNR, MSE and IF the results are encouraging [6].

If the information is hidden in TCP initial sequence number (ISN), then it is most difficult covert channel to detect. The information hiding in TCP/IP protocol is analyzed in this paper and new effective method is proposed for hidden information detection. A statistical model is proposed for detecting covert channels in TCP initial sequence number. Based on this model, in order to identify the existence of information hidden in ISN a classification algorithm is developed. Results have shown that this method has high detection accuracy and reduced computational complexity [8].

Hybrid covert channel is combination of noisy channel and subliminal channel. It is co-existence of homogeneous or heterogeneous network covert channel at same time or at regular instance of time. This paper explains detection of intra LAN covert activities. Also, a detection engine is developed to detect or analyzed hybrid covert channel. This paper suggested that padding bit, initial sequence number, acknowledgement number and reserved field can be used for covert data placement. To provide more security RSA, DES and DSA algorithm can be used. We can detect covert channel using three ways: signature based, protocol based and behavior based [7, 11].

3. DATA HIDING METHODS

Covert channel in TCP/IP protocols: TCP/IP header structure allows number of covert channel options in packet header fields which are normally unused field or hold random number. There are many fields for hiding information among these we can use sequence number field, acknowledge number field, 8 bit flag, option & padding field from TCP & Identification field, unused bits, types of services & TTL from IP.

Data hiding methods can be used by intruders to communicate over data channels and to overcome firewalls. In fact, most detection systems can identify hidden data in the payload but struggle to deal with data hidden in the IP and TCP packet headers or in the protocol session layer [10].

In designing data hiding approaches, functional interfaces required in all IP implementations are considered. In this way, we avoid detecting covert channels related to particular TCP/IP software implementations which are not available for general use. The layered structure of networks requires the IP datagram to confine information received from the transport layer. Like IP headers encapsulate ICMP messages, IGMP report and query messages. Covert channels in the IPv4 header can be associated with those identified in the TCP, ICMP or IGMP headers [9].

We present three data hiding techniques in this section. Each technique makes use of some redundancy in the representation of information in the Internet Protocol for effective data hiding.

3.1. Manipulation of the IP Identification Field

The re-assembly of packet data by remote routers and host systems can be carried out using the identification field of the IP protocol. It gives a distinctive value to packets so if fragmentation occurs along a route, they can be accurately re-assembled. In this encoding method, IP identification field is replaced by the numerical ASCII representation of the character that is to be encrypted. This allows for easy transmission to a remote host which reads the IP identification field and converts the encoded ASCII value to its original value.

3.2. Initial Sequence Number Field

A client is able to establish a reliable protocol negotiation with a remote server using the Sequence Number field of the TCP/IP protocol suite. In this method, the sender generates an ISN corresponding to actual covert data. Covert receiver extracts this field and does not give an ACK for it. Covert sender keeps on sending the same packet with different covert data embedded in ISN. This is the simplest form of using this field for placement of covert data.

3.3. The TCP Acknowledge Sequence Number Field Bounce

This method depend on basic spoofing of IP addresses to allow a sending machine to "bounce" a packet of information from a remote site and have that site return the packet to the actual endpoint address. This has the benefit of identifying the sender of the packet; it looks as to come from the "bounce" host. Thus an unidentified one-way communication network can be set up using this method that would be challenging to detect specifically if the bounce server is very busy. This method depend on the characteristic of TCP/IP where the destination server replies to an initial connect request (SYN packet) with a SYN/ACK packet having the original initial sequence number plus one (ISN + 1).

4. QUALITY MEASURES

Assessing the error between images is a very important task after an embedding process. The commonly used measures are

4.1. Mean squared Error (MSE)

$$\text{MSE} = \frac{1}{x * y}\sum_{i=1}^{x}(\text{O}(i\,,\,j) - \text{E}(i,\,j))^2$$

Where, MSE is Mean Square error, x and y are height width and O(i, j) represents original image and E(i, j) represents corresponding embedding image.

4.2. Peak Signal to Noise Ratio (PSNR)

The Peak Signal to Noise Ratio (PSNR) is the ratio between signal and corrupting noise which affect representation of image. PSNR is usually measured in decibel scale. The PSNR is commonly used as measure of quality reconstruction of image. In this case the noise is the error introduced and the signal is original data. High value of PSNR indicates the high quality of image. Peak Signal to Noise Ratio is defined via the Mean Square Error (MSE) and corresponding distortion matric.

$$\text{PSNR} = 10\log_{10}\frac{\text{P}^2}{\text{MSE}}$$

Where, PSNR is peak signal to noise ratio, P is peak signal level for a grey scale image it is taken as 255.

5. PROPOSE ALGORITHM

Propose technique first encrypts data using encryption algorithm. After generating cipher text we will embed data into image using EDGE based method and using digital signature concept we will encrypt data.

Algorithm

1. Take input data
2. Encrypt input data using cryptographic algorithm
3. Use either one option
   a) Generate digital signature of encrypted message
   b) b.1) Load cover image
      b.2) Find edge using EDGE algorithm
      b.3) Embed data into edges of image

c) c.1) Generate digital signature of encrypted message

c.2) Load cover image

c.3) Find edges using EDGE algorithm

c.4) Embed data into edges of image

4. Calculate mean square error (MSE) & PSNR of *i/p* image & steganography image
5. Lay data into sequence number field then send to receiver and reverse algorithm apply on receiver side

6. RESULTS

Figure 1 below shows two cover images used in our tests.

(*a*) (*b*)

Figure 1. Cover images *a*) House.jpg *b*) Jetplane.jpg

The stego images generated by our steganographic method are seen in figure 2

(*a*) (*b*)

Figure 2: Stego images *a*) House.jpg *b*) Jetplane.jpg

PSNR were used to evaluate the performance of the proposed algorithm. The results are as shown in table 1

Table 1
PSNR values of stego images

S.No	*Cover image*	*PSNR (Base System)*	*PSNR (Proposed System)*
1.	Lena	69.95 db	76.0018 db
2.	Baboon	69.79 db	74.5299 db
3.	House	–	81.9419 db
4.	Jetplane	–	82.0224 db

The results as seen in the tables above make it clear that good stego images are consistently produced. The PSNR values produced too are better than that as seen produced by Aisha Fernades [5] algorithm. It is also seen that the secret image has a good PSNR value, greater than 70 db, thus indicating robustness. Various statistical tests were carried out comparing the original and stego images and results were found to be promising. In stego images however no visible changes were seen.

7. CONCLUSION

In this paper, a new technique for information security is proposed. We used data hiding methods based on cryptography algorithm and steganography. To detect existence of hidden information in TCP Initial sequence number field is very difficult so; it is secured way of transmitting data. It may be detected but not possible to hack data. This algorithm delivers confidentiality, authentication, non-repudiation, integrity. Proposed algorithm provides data and information security at various levels. Our future work will be we can use various arithmetic operations & various algorithms for embedding data.

8. ACKNOWLEDGEMENT

We extend our appreciation to all the anonymous reviewers for their valuable feedback and comments.

REFERENCES

[1] Haipeng Qu, Purui Su, Dengguo Feng, *A Typical Noisy Covert Channel In The IP Protocol*, 2004 IEEE

[2] K. Naveen BrahmaTeja, Dr. G. L. Madhumati, K. Rama Koteswara Rao, *Data Hiding Using EDGE Based Steganography*, International Journal of Emerging Technology and Advanced Engineering ISSN 2250-2459, Volume 2, Issue 11, November 2012

[3] Pournima More, R Goudar, *Hybrid Covert Channel an obliterate for Information Hiding*, Proceedings of the Third International Conference on Trends in Information, Telecommunication and Computing ,Volume 150 of the series Lecture Notes in Electrical Engineering, pp 609-613

[4] Dhananjay M. Dakhane, Prashant R. Deshmukh, *Active warden for TCP Sequence Number base Covert Channel*, International Conference on Pervasive Computing (ICPC), 2015 IEEE

[5] Aisha Fernandes, Wilson Jeberson, *Covert Communication Using Arithmetic Division Operation*, International Conference on Advanced Computing Technologies and Applications (ICACTA-2015),Elsevier , procedia computer science vol 45,2015, Pp 354-360

[6] KousikDasgupta, J.K. Mandal and Paramartha Dutta, *Hash Based Least Significant Bit Technique For Video Steganography(HLSB)*, International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, No 2, April 2012

[7] Mrs.Mamatha.V.Jadhav, Mrs.Suvarna.L.Kattimani, *Effective Detection Mechanism for TCP Based Hybrid Covert Channels in Secure Communication*, 2011 IEEE

[8] Hong Zhao,Yun-Qing Shi, *Detecting Covert Channels in Computer Networks Based on Chaos Theory*, IEEE Transactions On Information Forensics And Security, Vol. 8, Issue. 2, February 2013

[9] Vishal Bharti, Itu Snigdh, *Practical development and deployment of covert communication in IPV4*, Journal of Theoretical and Applied Information Technology, 2005

[10] Kamran Ahsan, Deepa Kundur, *Practical data hiding in TCP/IP*, Workshop Multimedia and Security at ACM Multimedia'02, December 6, 2002

[11] Koundinya Anjan ,Jibi Abraham, *Behavioral analysis of transport layer based hybrid covert channel*, recent trends in network security and application , communication in computer and information science, vol 89, pp 83-92

[12] Abhishek Anand, Abhishek Raj, Rashi Kohli, Dr. Vimal Bibhu, *Proposed symmetric key cryptography algorithm for data security*, Innovation and challenges in cyber security (ICICCS-INBUSH), 2016 international conference on Innovation and Challenges in Cyber Security (ICICCS 2016).