Efficient and Secure Data Transmission by using Steganography Technique

[1]Basant Sah , [2]Dr. V .K Jha
[1]Research Scholar , [2]Associate Professor
[1,2]BIT Mesra , Ranchi
[1]basantbitmtech2008@gmail.com , [2]vkjha@bitmesra.ac.in

Abstract :Steganography is a digital technique for hiding secret information into some form of media, such as image, audio or video. Steganography has evolved into a practice of concealing data in larger file in such a way that others cannot suspect the presence of a hidden message. In this paper, we design a system, which uses features of both cryptography as well as steganography, where TCP/IP header is used as a steganographic carrier to hide encrypted data.[1] Steganography is a useful tool that allows covert transmission of information over the communications channel.

Keywords: LSB,Steganography, Cryptography, Encryption, TCP/IP Header, Fragmentation.

1. INTRODUCTION

Constantly communicated through the Internet are flows of information generated from many diverse applications such as e-commerce transactions, audio and video streaming or online chatting. The security of such data communication, which is required and vital for many applications nowadays, has been a major concern and ongoing topic of study given that the Internet is by design open and public in nature. Many techniques have been proposed for providing a secure transmission of data. Hence, in order to provide a better security , we propose a data hiding technique called steganography along with the cryptography technique. Steganography is the art and science of hiding data into different carrier files such as text, audio, images, video, etc. In cryptography, the secret message that we send may be easily detectable by the attacker.[6] But in steganography, the secret message is not easily detectable. The persons other than the sender and receiver are not able to view the secret message. The secret message that sender transfers over the network, can be encrypted and hidden into TCP/IP header using Stego object. The Stego object is an encrypted message embedded into carrier file.

II.STEGANOGRAPHY OVER A COVERT CHANNEL

Covert channel is a communication channel through which information transmits by violating security principles. The communication through covert channel is non-obvious manner. TCP/IP Header can serve as a carrier for a steganography through covert channel. As the steganography is data hiding technique, sender embeds the encrypted data by using carrier file.[3-5] At the encoder process encryption algorithm is applied over secret file then it embeds with carrier file, it generates stego object that hides into unused fields of TCP/IP header, which implies covert channel. The carrier files may be text, image, audio or video. In our system, we are using images as carrier. Digital images are very useful and secure carrier for hiding the secret massage. Image is a collection of color pixels. In standard, 24 bit bitmap we have three color components per pixel:

Red, Green and Blue. Each component is 8 bit and have 28 i.e. 256 values. In 3 megapixel image you can hide 9 megabits of information using this technique, which is equivalent of 256 pages of book. If we only change the lowest bits of each pixel, then the numeric values can only change by a small percentage. We can only alter the original pixel color value by ±7. Stego object traverses over a communication channel.[8] Stego object is divided into packets. These packets are hidden in TCP or IP header's unused fields. Many fields from the TCP or IP header are not used for certain situations.

III.STRUCTURE OF TCP HEADER:

Structure of TCP header is shown in Fig 3.1, we can use irrelevant fields namely sequence number and option fields.

a)Sequence number:

It is 32 bit field. Which is use to identify the current position of data byte in the segment. Sequence Information and Acknowledge

number is randomly generated number based on: local host, local port, remote host, and remote port.

b)Options

In order to provide additional functionality several optional parameter may used between a Tcp sender & receiver. The most common option is the maximum segment size option. This option gives the sender

maximum segment size the receiver willing to accept.

Structure of IP header

Structure of IP header is as shown Fig 3.2, irrelevant fields used in IP header are given as follows:

a) Type of service

It is 8 bit field. The type service in IP header is potential for using as steganographic carrier, because many networks never use them.

b)Identification field

It is 16 bit field. When fragmentation of message occur the value of identification field is copied into all fragments. The identification number helps the destination in reassembling the fragments of the datagram.

c)Flags

It is 3 bit field which gives information about Reserved, Do not fragment bit and more fragment bit.

d)Fragmentation offset

This bit is 13 bit field. When the fragmentation of message occurs this field specifies the offset, or position in the overall message, where the data in this fragment goes.

e)Option:

Options are not required for every datagram to be sent. They are used for network testing & debugging purpose.

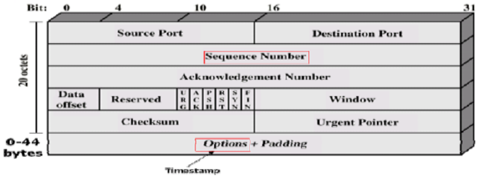

Fig.3.1 TCP header

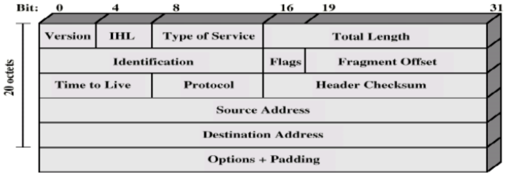

Fig.3.2 IP Header

IV.PROPOSED WORK

In this paper we are focusing on Identification field of the IP header to hide secret encrypted data. Identification field is used only when fragmentation occurs. At the receiver end, to reassemble the packets, identification field tells the right order for that. If fragmentation is not occurred, then identification field will always be unused, so that we can use this 16 bit field to hide secret encrypted message. To avoid fragmentation, we use MTU. Maximum transfer unit decides limit for packet size for transmission over network. Sender and receiver, both should have awareness of MTU unit.[9] For the encryption and decryption we use RSA technique to encrypt the data so that it will be more secure.RSA is a public key cryptography. In public key cryptography each user or the device taking part in the communication generally have a pair of keys, a public key and a private key, and a set of operations associated with the keys to do the cryptographic operations.[11] Only the particular use knows the private key whereas the public key is distributed to all users taking part in the communication. Some public key algorithm may require a set of predefined constants to be known by all the devices taking part in the communication. RSA involves a *public key* and a *private key*. The public key can be known by everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key. The keys for the RSA algorithm are generated the following way:

1. Choose two distinct prime numbers p and q.
   - o For security purposes, the integer's p and q should be chosen at random, and should be of similar bit-length. Prime integers can be efficiently found using a primality test.
2. Compute n = pq.
   - o n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.
3. Compute $\varphi(n) = \varphi(p)\varphi(q) = (p - 1)(q - 1) = n - (p + q - 1)$, where φ is Euler's totient function.
4. Choose an integer e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$; i.e., e and φ(n) are coprime.
   - o e is released as the public key exponent.
   - o e having a short bit-length and small Hamming weight results in more efficient encryption – most commonly $2^{16} + 1 = 65{,}537$. However, much smaller values of e (such as 3) have been shown to be less secure in some settings.[5]
5. Determine d as $d \equiv e^{-1} \pmod{\varphi(n)}$; i.e., d is the multiplicative inverse of e (modulo φ(n)).
   - This is more clearly stated as: solve for d given $d{\cdot}e \equiv 1 \pmod{\varphi(n)}$
   - This is often computed using the extended Euclidean algorithm. Using the pseudocode in the Modular integers section, inputs a and n correspond to e and φ(n), respectively.
   - d is kept as the private key exponent.

V. CONCLUSION AND FUTURE SCOPE

In this work we explored the steganography techniques. We proposed an efficient steganography technique. In steganography,TCP/IP header is used as a carrier for transmission of the secret information or data. The TCP/IP suite along with the covert medium further enhances the security of the system since attackers are more concerned over the "http". The proposed technique will avoid illegal transmission of secret communication on the web and will provide a better secure system in case of Authentication.Only concept based discussed here final implementation will be later.

REFERENCES

[1] R.M. Goudar, Prashant N. Patil, Aniket G.. "Secure Data Transmission by using Steganography" ISSN 2224-5758 (Paper) ISSN 2224-896X Vol 2, No.1, 2012

[2] Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn,"Information hiding- Survey", IEEE, 87(7):1062-1078, 1999.

[3] G. J. Simmons, "The Prisoner's problem and the subliminal channel in Advances in Cryptology", Proc.crypto '83:55–67, 1983.

[4] Udit Budddia and Deepak Kundur, "Digital video steganalysis exploiting collusion Sensitivity",IEEE, 1(4):502-516, 2006.

[5] Furuta, T,.Noda, H., Niimi, M., Kawaguchi E,"Bit-plane decomposition steganography using wavelet compressed video", Joint Conference of the Fourth International Conference, 2(5): 970 - 974, 2003.

[6] V.Karthekayani and kammalakan, "Conversion grayscale image to color image with and without texture synthesis", International journal of omputer science and network security, 7(4):11-16, 2007.

[7] Eiji Kawaguchi and Richard O. Eason, "Principle and applications of BPCS- Steganography", Proc. SPIE ,3528: 464-473 , 1999.

[8] Nameer N. EL-Emam, "Hiding a Large Amount of Data with High Security Using Steganography Algorithm" Jordan Journal of Science publications, 3 (4): 223-232, 2007.

[9] K B Raja, C R Chowdary K R Venugopal, "A Secure Image Steganography using LSB, DCT and Compression Techniques on Images", IEEE, 170-176, 2005.

[10] Naofumi," Technique of lossless steganography", IEICE Transactions on Communications, 90(11):1-4, 2007.

[11] .Nan jiang and wan jiang, "Random oracle model of information modeling", World academy of science, 18:1307-6884, 2006

[12] Steganography [tG. Pulcini, Stegotif,"http://www.geocities.com/SiliconValley/ 9210/gfree. Html, 10/28/2008]