Information and Knowledge Management
ISSN 2224-5758 (Paper) ISSN 2224-896X (Online)
Vol 2, No.1, 2012

Secure Data Transmission by using Steganography

R.M. Goudar, Prashant N. Patil, Aniket G.. Meshram*, Sanyog M. Yewale, Abhay V. Fegade

Computer Engineering Department, Pune University, MAE, Alandi

Pune, Maharashtra 412105, India

E-mail: rmgoudar66@gmail.com

Abstract

Steganography is the efficient technique to provide secure data transmission over the network, as the number of users increases effectively. The cryptography is also used to provide security to data over network, but transmission of secured message may be detectable to third party. From security point of view, steganography does not allow to detect the presence of hidden secret other than indeed user, over the communication channel. 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. Steganography is a useful tool that allows covert transmission of information over the communications channel.

Keywords: Steganography, Cryptography, Encryption, TCP/IP

1. Introduction

As people become aware of the internet day-by-day, the number of users in the network increases considerably thereby, facing more challenges in terms of data storage and transmission over the internet, for example information like account number, password etc. Hence, in order to provide a better security mechanism, we propose a data hiding technique called steganography along with the technique of encryption-decryption. 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. 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. In this paper, current trends and technologies are explained in section II. Followed by covert channel is explained in section III. Secure data transmission using steganography in section IV and its applications are discussed in section V. The secret message that the sender transfers over the network can be encrypted first, which creates cipher message. A stego object is generated by embedding the cipher message into any carrier files such as image. This stego object is then hidden in the irrelevant bits of TCP/IP header and hence creates a covert channel. In this way a more secure data is sent over the communication channel. The reverse procedure is carried out on the receiver's end, where decryption is carried out using the key. After decrypting that stego_object receiver is able to extract secret message, that sender sends for him/her.

2. Current trends and practices

Wang Jia-zhen, explained a scheme which uses fourth-order Chebyshev chaotic system to generate chaos sequence which is used to encrypt secret message, and then embeds the modulated message into identification field of IP header. Thus the identification bit of Ipv4 header can be used through PMTUD (Path Maximum Transfer Unit Discovery) and the generation of uncorrelated sequences to send covert information point-to-point. The randomness in the identification field values makes this scheme non-detectable against the detection of secret data through packet filtering and stateful inspection type firewalls. However, this scheme has limitations, when fragmentation occurs, which results in the use of identification field by the message itself as explained by Wang. Implementation of steganography can be done by using two techniques. One is the fragmentation strategy and other is the by using the IP checksum covert channel and hash collision, which is illustrated by Miss Dr. V. R. Ghorpade has the similar approach as suggested by

Jia-zhen. Where he explained an algorithm to show the 4^{th} order Chebyshev chaotic system, how steganography can be implemented. Stego medium can be transferred securely. The most recent application is in the client server architecture wherein several clients make a request to the FTP server, say of a library. A log file can be maintained, for audit purposes, based on the requests sent by various users. Moreover, serving the request by transferring a digital image to the user, say, can have the same user information or library information tied to the content packets. This scenario of tags tied to the content can allow for audit. But the first problem that arises here is of fragmentation occurrence. The second problem that arises is that the internet checksum fails to be a secure method for validating data integrity. Jain Ankit describes in short some steganographic techniques such as: Substitution Technique, Transform Domain Technique, Spread Spectrum Technique, Statistical Techniques and Distortion Techniques. He also gives some steganographic tools such as Blindside, Data Marking Technologies, Digital Picture Envelope, Gifshuffle, Hide4PGP etc. Introducing a new subject altogether called as the "Steganographic file system" where files are neither merely stored, nor stored encrypted, but in which the entire partition is randomized - encrypted files strongly resemble randomized sections of the partition, is also discussed. Another system for data hiding by using the covert channel is the SCONeP (Steganography and Cryptography Over Network Protocols) elaborated by Radu Ciobanu. Here the author proposes an application that reads data from a file and sends it over the covert channel which uses protocols from TCP/IP stack. The author proposes a software application that will have a loadable kernel module that checks incoming or outgoing packets for hidden data. The goal was to test several protocols that are less utilized in steganography, and to compare performances for implemented protocols. Thus SCONeP is used to send hidden data using headers from TCP, IP, UDP and ICMP. Cryptanalysts tries to crack the encrypted data over the network, while the Steganalyst tries detecting messages that are hidden by looking at variances between bit patterns and unusually large file sizes. Encrypted data is more difficult to differentiate from naturally occurring plain text. However there are several techniques to decrypt data from an encrypted one. If we combine the steganography and encryption then we opt for a more secure system Even if the steganography fails the encrypted data might help to protect at least the message. Arvind Kumar also emphasizes few points in this regards.

3. 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. 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 2^8 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. 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.

3.1 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.

3.1.1 Sequence number:

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

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

3.1.2 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.

3.2 Structure of IP header:

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

3.2.1 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.

3.2.2 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.

3.2.3 Flags:

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

3.2.4 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.

3.2.5 Option:

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

4. Proposed Work

In this paper we are more 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. For the encryption and decryption we use Elliptic curve cryptography. Elliptic Curve Cryptography 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. 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. Domain parameters in ECC are an example of such constants. Public key cryptography, unlike private key cryptography, does not require any shared secret between the communicating parties but it is much slower than the private key cryptography.

The mathematical operations of ECC is defined over the elliptic curve

$$y = x^3 + ax + b,$$

where $4a + 27b \neq 0$. Each value of the 'a' and 'b' gives a different elliptic curve. All points (x, y) which satisfies the above equation plus a point at infinity lies on the elliptic curve. The public key is a point in the curve and the private key is random number. The public is obtained by

multiplying the private key with the generator point G in the curve. Generator point G, parameters 'a', 'b' and some another constants constitutes with domain parameter of ECC. For the secure file transfer by using Steganography, we propose a conceptual scheme. Consider Alice as sender and Bob is a receiver. Alice wants to transfer secrete file for Bob over a network. Fig.4.1 and Fig.4.2 describe the flowchart of ECC algorithm for encryption and decryption.

5. Application:

5.1 A client server architecture wherein several clients make a request to the FTP server, say of a library. A log file can be maintained, for audit purposes, based on the requests sent by various users. Moreover, serving the request by transferring a digital image to the user, say, can have the same user information or library information tied to the content packets. This scenario of tags tied to the content can allow for audit. A logging process for the above application scenario based on the user or application specific information completes the picture (i.e. logging of valid user), maintaining the record of user requests based on user information and ultimately serving the user requests by having either the user information or the server I source (library) information tied to the content packets to avoid unlawful use such as copyright violation.

5.2 Steganography is used by some modern printers, including HP and Xerox brand color laser printers. Tiny yellow dots are added to each page. The dots are barely visible and contain encoded printer serial numbers, as well as date and time stamps.

6. Conclusion and Future Scope

Secure data transfer by using steganography provides an efficient technique for data hiding by using covert channel. Covert channel is a subject which can be seen in many areas. Hiding the medium itself has a strong impact on the network communication providing high level of security and a more secure system respectively. 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.

Acknowledgment:

We would like to express our gratitude towards a number of people whose support and consideration has been an invaluable asset during the course of this work.

References:

Xu Bo, Wang Jia-zhen, Peng De-yun, "Practical Protocol Steganography : Hiding Data in IP Header" ,2007.

Miss D. D. DhobaJe Dr. V. R. Ghorpade Mr. B. S. Patjj Mrs. S. B. Patil "Steganography By Hiding Data In Tcp/Ip Headers",2010.

D. K. Kamran Ahsan. "Practical Data Hiding in TCP/IP", Workshop on Multimedia Security at ACM Multimedia, 2002. Jain Ankit, "Steganography : A solution for data hiding"

Arvind Kumar Km. Pooja "Steganography- A Data Hiding Technique",2010.

Steven J. Murdoch and Stephen Lewis , "Embedding Covert Channels into TCP/IP",2005.

Radu Ciobanu, Ovidiu Tirsa, Raluca Lupu, Sonia Stan, "Steganography and Cryptography Over Network Protocols",2011.

Vishal Bharti, Itu Snigdh "Practical Development and Deployment Of Covert Communication In IPv4".

Enrique Cauich, Roberto Gómez, Ryouske Watanabe "Data Hiding in Identification and Offset IP fields"

ZHANG lie etc. "Information hiding in TCP/IP based on chaos". Journal on Communication.voJ.26 NO. I A January

2005.

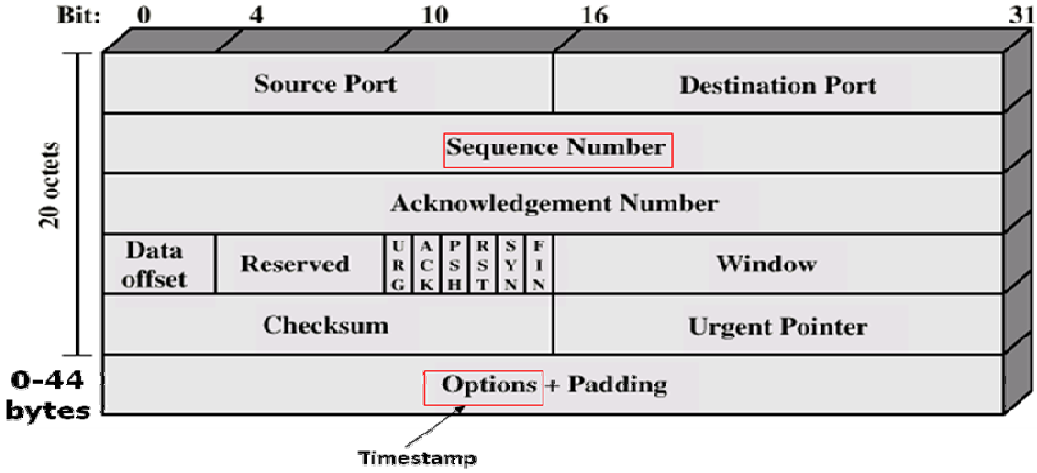

Fig.3.1 TCP header

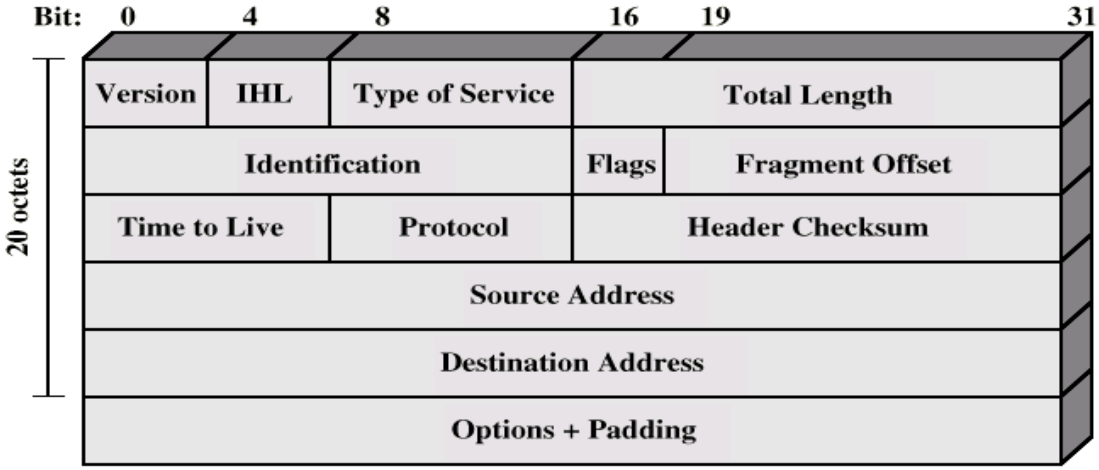

Fig.3.2 IP Header

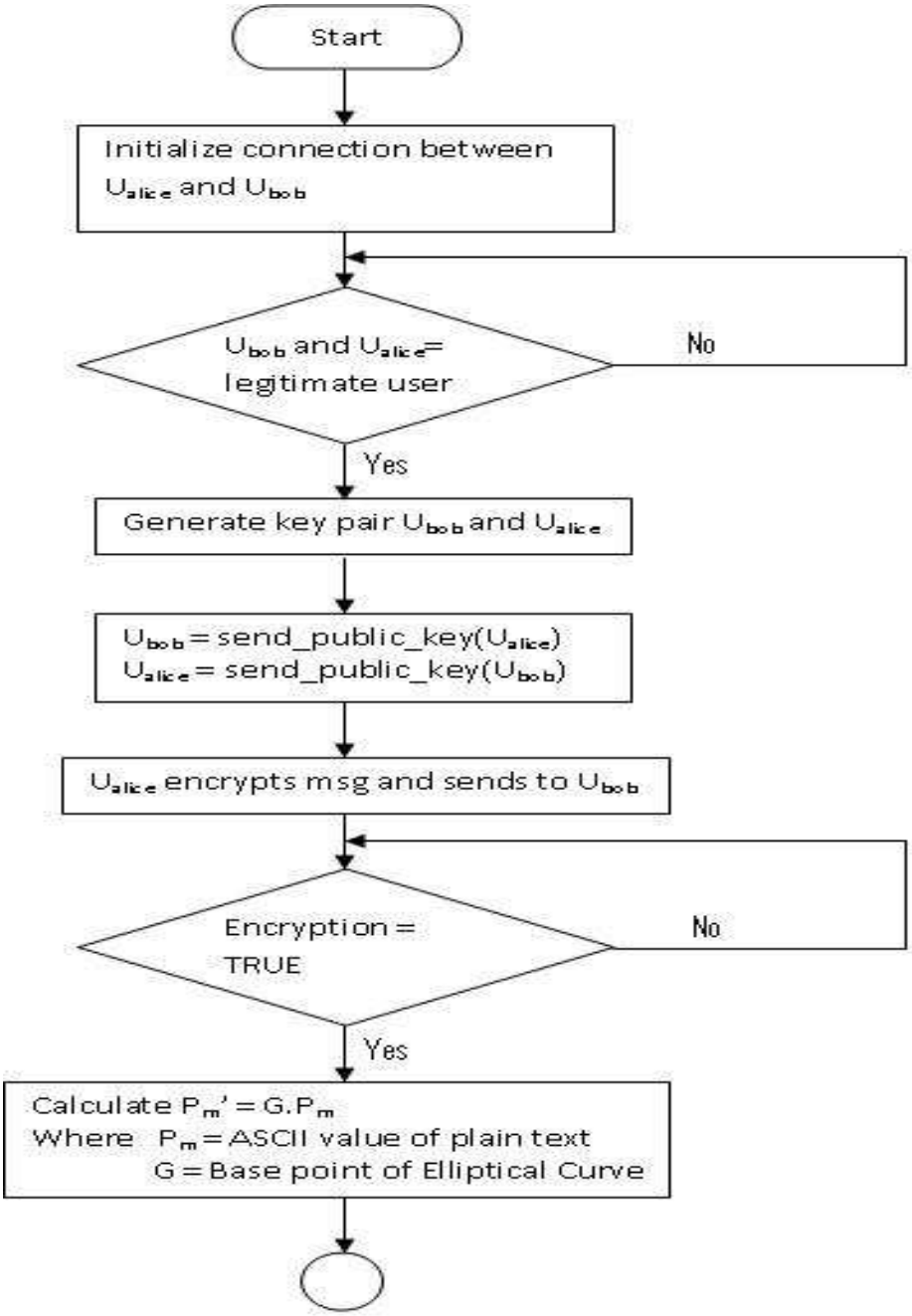

Fig.4.1 ECC Algorithm

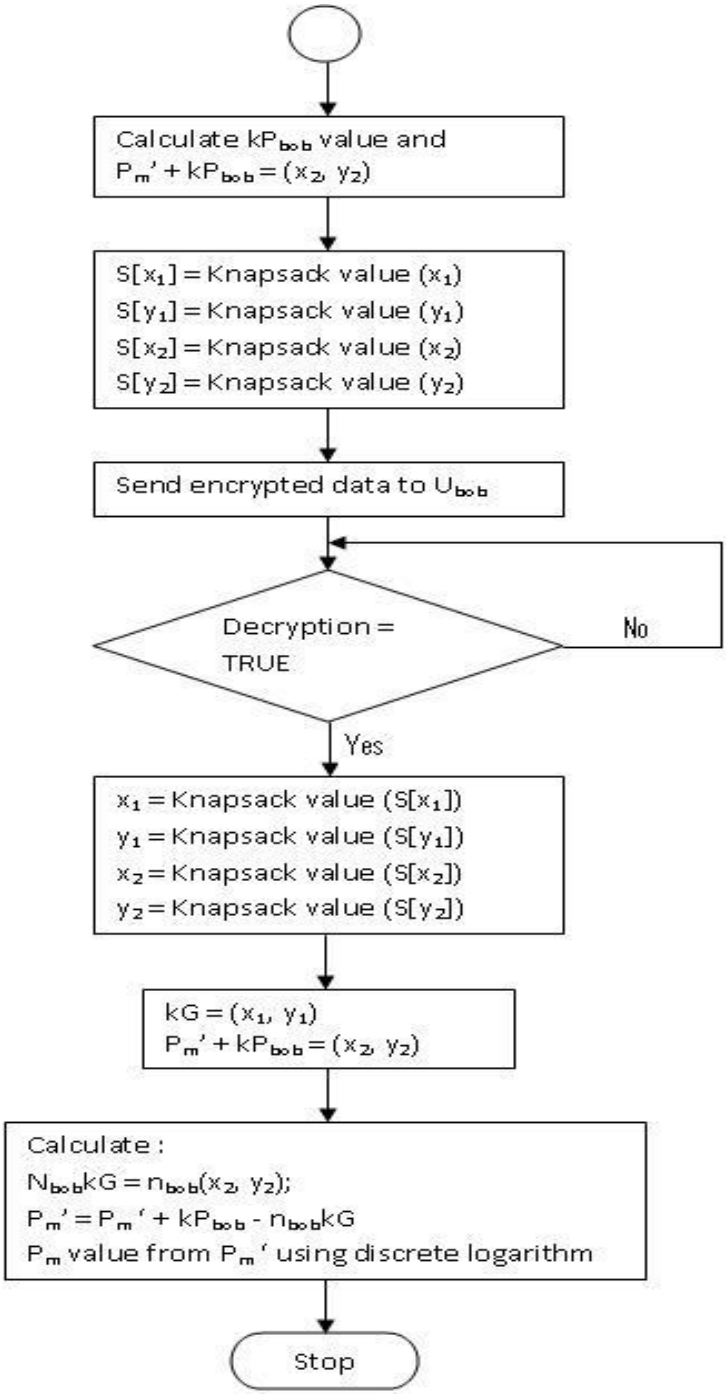

Fig.4.2 ECC Algorithm(cont.)