Research Paper

Volume : 4 | Issue : 5 | May 2015 • ISSN No 2277 - 8179

An Improved Network Steganography for Hiding data in IP header

Engineering

KEYWORDS : Network steganography, IP header, Packet watermarking

Maitrik Shah Assistant Professor,Indus University,rancharda.

ABSTRACT

Network Steganography is the way of hiding data in the innocent network transmission. It can be carried out by simply embedding information in payload, header or else without embedding any information in which the way the packet is send, length of packets, length of fragments of packets will actually convey the information in the hidden manner. In this paper we will suggest the approach to hide data in the options field of IP header.

INTRODUCTION

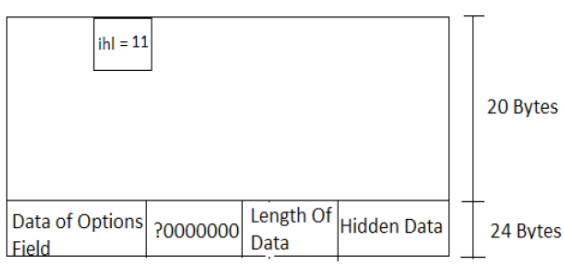
Steganography is a very old technique which basically hides data in the innocent looking carrier object. Now this carrier object can be anything like image, sound, video, network packet etc. Digital steganography is used since many years to send the secret information in the hidden manner. Media files are ideal places to embed the data because of their larger size.

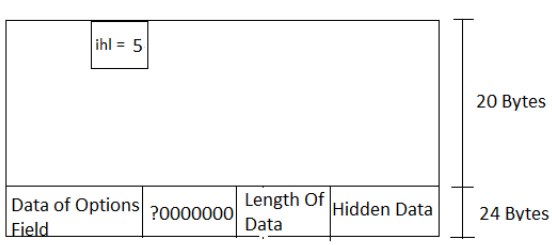
In the past few years new ways of steganography has emerged which is network steganography. It embeds the information in the network transmission. Here the cover object can be anything like protocol header of packets. TCP/IP packets have several fields which are of no use or little use. These fields can be used as a cover object to send data hiddenly. This is sometimes called packet watermarking also[1].

Several approaches has been suggested for network steganography[2][3]. In past many scientists have worked on it and successfully transmitted hidden data. Here in this paper we will analyse the problems in the previous approaches and give a new way to hide the data in the options field of IP header.

RELATED WORK:

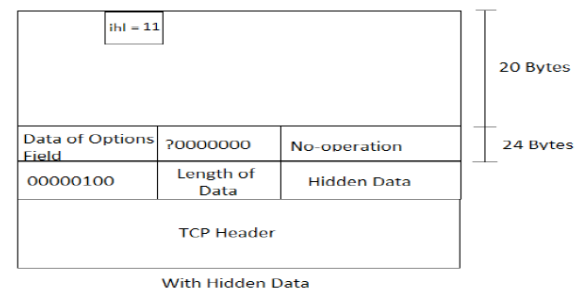
Many approaches has been suggested to hide data using networks steganography. Here in this section we analyze every approach and identify the problems in the same and in the next section we will give our approach.



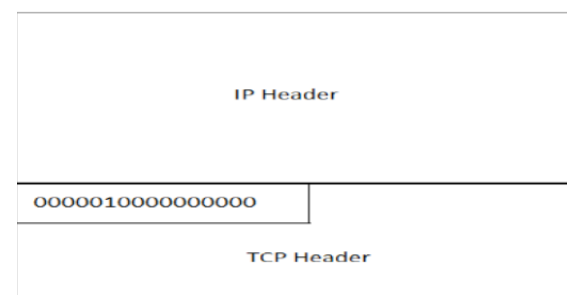


In the second approach of method –I we suggested to use wrong value of ihl (IP Header Length) field to fool the intruder. But in this case intermediate routers will not be able to read the options data in the packet because of wrong ihl value.

Method – II : Use of specific bit sequence



With Hidden Data



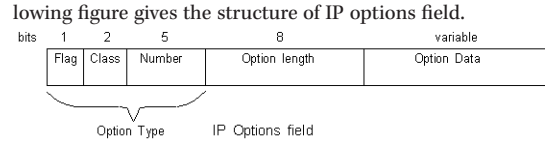
Without Hidden Data

Receiver must be able to distinguish which packet contains hidden data and which packet does not. To make receiver understand we have used specific bit pattern which is 00000100. It means if this pattern is there immediately after IP header it means hidden data is there otherwise TCP packet is there. But the problem with this approach is that if TCP header starts with the same sequence 00000100 then receiver will incorrectly consider that packet as a packet containing hidden data as shown in the second figure.

To overcome problems of these two approaches we suggest a novel approach to hide data in the options field of IP header in the next session.

PROPOSED APPROACH:

Our proposed approach uses Code bits of IP options field. Following figure gives the structure of IP options field.



Description:

Flag: This 1 bit flag specifies whether to copy data of options field in case fragmentation to all the fragments. A 1 indicates it should be copied.

Class: This 2 bit value specifies that option belongs to which class. Currently all the options can be categorized into 2 classes. 0(00) – Control class and 2(10) – Debugging and management.

Other two values 1(01) and 3(11) are not used.

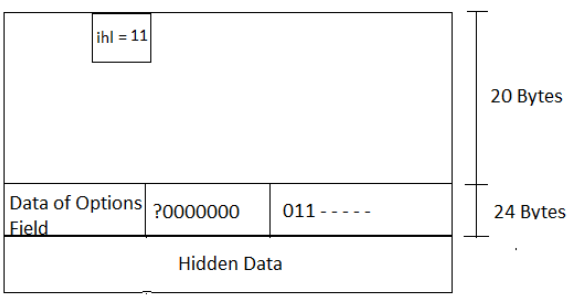
Number: This 5 bit value is used to identify one of the many options.

#	Option	Description
0	End of the option	Indicates end of the option field.
1	No operation	Generally used for padding
2	Security	Length is 11 octets
3	Loose Source Routing	IP routing based on information supplied by the source station
4	Internet Timestamp	Used for debugging and management purpose
7	Record Route	Records the route that datagram takes.
8	Stream ID	Length of 4 octets.
9	Strict Source Routing	IP routing based on information supplied by the source station

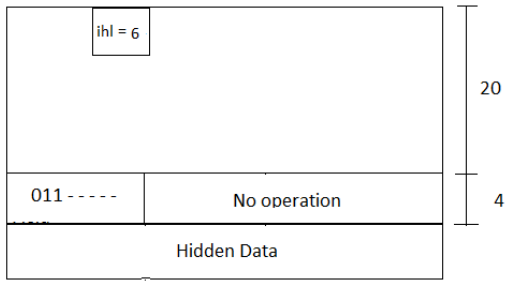
Option Length: This 8 bit field specifies the length of options field.

Options Data: It is the actual options data which is of variable length.

Here in our approach we have used class field. 2 bits of options class field specifies 4 values out of which only 2 values are currently used. We can utilize any of the other unused value of this field. We have used 11. So first 8 bits of IP options field will be either 011----- or 111-----. So the hidden data will start from (ihl*4+1)st byte of IP header as shown in the following figure.



With Data of options field



Without Data of options field

The first figure shows the approach if sender wants to send options data along with the hidden data. Suppose sender wants to send 24 bytes of data in the options field of IP header. So total length of IP header will become 44 which includes 20 bytes of standard IP header and 24 bytes of options field. So value of ihl field will be 11. So as said hidden data will start from (ihl*4+1) = (11*4+1) = 45th byte.

The second figure shows the approach if sender does not want to send hidden data though 4 bytes will be occupied which we can consider as overhead and hidden data will start from (ihl*4+1) = (6*4+1)th byte. In any case whether sender sends options data or not hidden data will always start from (ihl*4+1)th byte.

CONCLUSIONS AND FUTURE WORK

We had suggested the method to hide data using IP header. This is a novel approach. This can be clubbed with cryptography to encrypt the data to provide more security. The proposed approach removes the problems which were faced by its previous approaches. Furthermore this approach can be tested against many attacks which intruder may try to get the hidden data and based on the results this approach can be modified in future to have more secure and safe implementation

REFERENCE

[1] Maitrik K. Shah, Samir B. Patel,: Network Based Packet Watermarking using TCP/IP | Protocol Suite, 978-1-4577-2168-7/11:IEEE Transaction December 2011. | [2] K. Ahsan and D.Kundur,"Practical data hiding in TCP/IP",Proc. | ACM Workshop on Multimedia Security, 2002 | [3] W Bender "Covert Channels in the TCP/IP protocol suite", Techniques for Data Hiding | IBM Systems Journal Vol 35, 2003. | [4]Maitrik Shah, Jignesh Patel, Roshni Patel: "Network Steganography for hiding data in IP", International Journal of Scientific Research (IJSR), DEC 2012, vol 1 issue 1. |