Network Steganography for Hiding Data in IP

Engineering

KEYWORDS : Internet Streganography, Streganography, Option field, hiding data, IP option

Jignesh. S. Patel	18 Dhanjinagar Society,B/h eye hospital,unjha, Dist-mahesana,Gujarat
Roshni Patel	18 Dhanjinagar Society,B/h eye hospital,unjha, Dist-mahesana,Gujarat
Maitrik Shah	18 Dhanjinagar Society,B/h eye hospital,unjha, Dist-mahesana,Gujarat

ABSTRACT

Internet streganography is the exploitation of internet element and protocols for the purpose of covertly communication supplementary data. Stregonography is defined as the art and science of hiding data it take one piece of information and hides it within another. The pieces more used to hide data are the digital images. TCP/IP packets are transmitted over a network in large quantity within TCP/IP header. There are number of field that are no used for normal transmission or are "optional". In this paper we propose to use unused option field of IP header for hiding data

I. INTRODUCTION

Stregonography is the process of discreetly hiding data in a given host carrier for the purpose of enhancing value or subliminally communication information. Intruder is always tried to forge our data while data is transit. It may be possible that they may reveal the information to other modify it to misrepresent individual or organization or use it to launch an attack or change the ownership ,make the copy of it and distribute it to the other one solution to this problem is through the use of internet stregonography.

Stregonography works by replacing bits of useless or unused data in regular computer files (such sound,graphic,text)with bits of different invisible information. This hidden information can be plain text cipher text, or even images, The Technique used have the intention to make impossible to detect that there is anything inside the innocent file, but the recipient must obtain the hidden data without any problem,

Many scientific works has been made in order to create software and methods to hide information into digital images. Our approach take advantage of the unused option field of the IP header packet, as mentioned earlier we not all the fields of an IP packet are always used, These field

are used to hide the information we want to send without raising any suspicion.

For IP fragmentation mechanism there are two stenographic Method .Each of methods may be utilizes for IPv4 and IPv6 protocols for each scenario. However, for IPv4 fragmentation and fragments reassembly may be performed by intermediate nodes as well as by sender and/or receiver.

a. Steganographic Method –F1

In this method SS (steganogram sender) must be the source of the fragmentation.SS inserts single bit of hidden data by dividing original IP packet into predefined number of fragments. For example, if the number of the fragments is even then it means that binary "0"is transmitted and in other case binary "1"

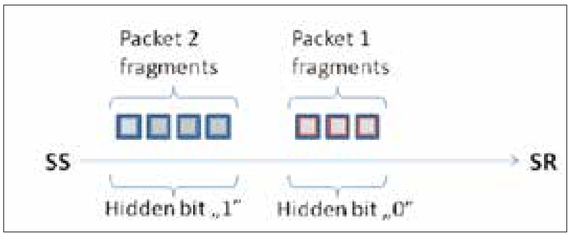
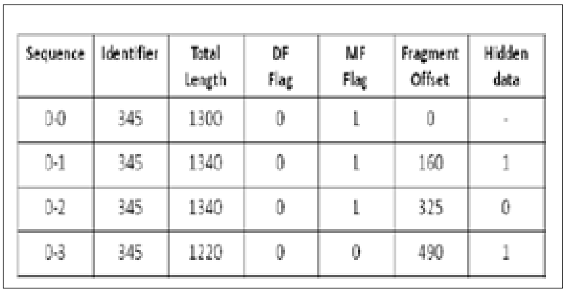


Figure 1 about Steganographic Method –F1

After reception of the fragments SR uses the number of the fragments of each received IP packet to determine what hidden data was sent.

Potential streganographic bandwidth for this method is PRBR=1 bit/packet

b. Steganographic Method –F2



Sequence	Identifier	Total Length	DF Flag	MF Flag	Fragment Offset	Hidden data
0-0	345	1300	0	1	0	-
0-1	345	1340	0	1	160	1
0-2	345	1340	0	1	325	0
0-3	345	1220	0	0	490	1

Fig. 2 about Steganographic Method –F2

The main idea of this method is to divide a packet into fragments and insert hidden information by modulating the values that are inserted into Fragment Offset field. In above method proposed inserting steganogram directly into Fragment Offset field and modulate the size of the fragment to match this value. Such approach can cause high irregularities in fragments sizes which may be easily detected.

F2 method works as follows .SS must be the source of the fragmentation.SS inserts single bit of hidden data by intentionally modulating the size of each fragment of the original packet in order to obtain fixed values in Fragment offset, For example even offset means transmitting binary '1',odd offset–binary '0'"streganographic" fragmentation of the exemplary IP packet which was introduced in figure .

After successfully reception of the fragments SR extracts hidden data based on the values from fragment offset field

Steganographic bandwidth for this method is PRBR=Nf -1 [bit/packet]

Nf=number of fragments of the packet.

Steganoanalysis in case of F2 is harder than in case of method proposed by Murdoch but hidden communication still can be uncovered, because usually all the fragments except last one have equal sizes. In this case the hidden communication may not be detected at all as this fragmented packet will be similar to other ones.

II. PREVIOUS WORK

Our proposal is to make use of option fields. There are few existing methods to use field IP header related.

In [1] Rowland proposed multiplying each byte of the hidden data by 256 and inserts in directly into Identification header field.

In [2] author has used Do Not Fragment Bit of IP header to send the hidden In this work the problem is the size of data we can use to send our data. Do not Fragment field is of one bit only so here we can transmit only one bit for each datagram. Suppose our packet doesn't carry anything in payload. It contains only data. Since IP header is of 20 bytes if options field is unused than the ratio useful information to total data is 1:160, it means that if you want to transmit the phrase "hello India" then there will be overhead of almost 2 Kb for just 11 bytes.

Cauich et al[3] described how to use Identification and Fragment Offset fields to carry hidden data between intermediate nodes but under condition that the packet is not fragmented. Additionally in selected packet reserved flag is used to mark packet so that the receiver can distinguish between real and convert fragments.

In [4] one approach they have made the use of type-of service field of IP packet which is of 8 bit to send data. In those 8 bits 2 bits are unused and that 2 bits can be used to transmit the hidden data. In another approach they have made the use of reserved bits of TCP header for the transmission of the hidden data. 6 bits of the TCP header are reserved. So they have made the use of those 6 bits. So if we combine these two approaches we can transmit one byte of hidden data per packet transmitted Ahsan and Kundur [5] proposed steganographic methods that use IP fragmentation fields. It utilizes high eight bits of the IP Identification to transmit covert data and the low eight bits are generated randomly.

Murdoch et al. [6] proposed transmitting hidden information by modulating the size of the fragments to match the hidden data inserted into Fragment offset field.

III. PROBLEMS

The main problem is the Packet Fragmentation. There are two possibilities:

1. Packet will be fragmented
2. Packet will not be fragmented

The first case occurs if the packet pass from one network to another network and MTU (Maximum Transmission Unit) of the second is smaller than the first. In that case we can't use Identification field and Do Not Fragment field of IP header.

In second case packet will not be fragmented. In this case we can transmit our hidden data in Identification field and Do Not Fragment field of IP header. But another problem is the size of data. With the use of these fields we can transmit very few bits of data. i.e. if we want to transmit header only then there will be a huge overhead [8]

IV. OUR APPROACH

TCP/IP is the protocol used in Internet. TCP /IP were developed by a Department of Defense (DOD) research project to connect a number different networks designed by different vendors into a network of networks (the "Internet"). IP (Internet Protocol) is responsible for moving packet of data from node to node, and TCP (Transmission Control Protocol) is responsible for verifying the correct delivery of data from client to server. The basic unit of data transfer is Packet. At sender side the data is partitioned into IP packets and packets are transmitted over the network. At receiver side packets are reassembled to get the data. Each packet begins with a header containing addressing and system control information. The header packet is divided into The IP packet header consists of 20 bytes (if options field not used) of data divided in several fields. Each field has a special purpose, depending on the type of data contained in the packet payload. Fig. Shows the structure of the IP header.

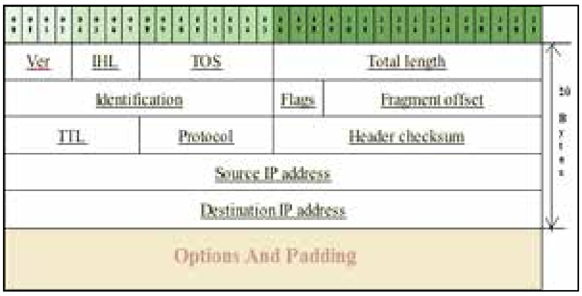


Fig. 3 about IP Header: the options field which we will use

TABLE I
OPTIONS FIELD

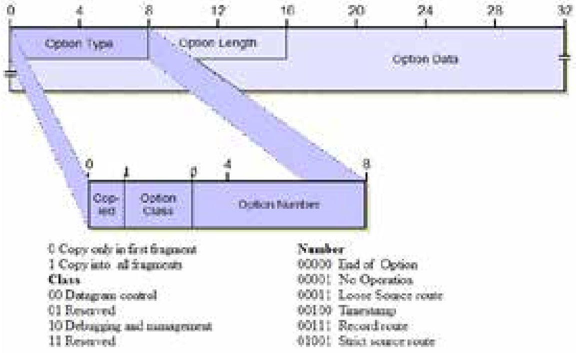


Fig.4 about the options field contain of option field [8]

Most of the times IP options field is not used. But there could be times when packets require additional information in the protocol header for diagnostics purposes or if packet's path across the internet is specified before it is sent. In that case options field will include.Following two approaches that can consider

Approach-I: Use End of Options Field
Approach-II: Use Of Specific bit sequence

Approach-I Use End of Options field:

In this case we have set value of ihl field to its actual values

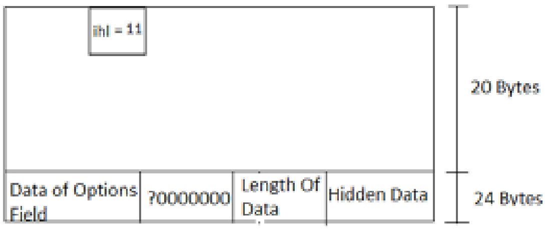


Fig.5 about Use End of Options field with ihl values 11

Receiver will search for the sequence 0/10000000 .After this sequence hidden data will be there. In hidden data receiver analysis first eight bit data that is length of the hidden data remain all are contain of the hidden data

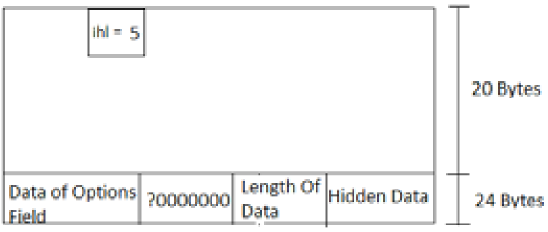


Fig. 6 about Use End of Options field with ihl values 5

In second case we have set value of ihl field to 5.In this case

Approach-I: Use Of Specific bit sequence

In this approach we have used specific bit sequence as shown in the above figure. Here, intermediate routers will be able to read header correctly. We will use specific (e.g 00000100).So that receiver can understand by reading this sequence that there is hidden data in the header

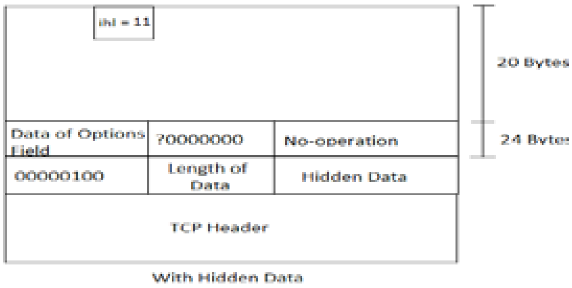


Fig. 7 about Use of Specific bit sequence

V. CONCLUSION

We have presented a new another technique to hide data in option field of IP header. The experiments shown some limitations but they also presented some advantages over similar steganographic techniques.

As we mention above; it is not possible to send information point to point because we cannot assure that the IP datagram will be not fragmented. Furthermore we do not know exactly which way the packet will take, so is not possible to be sure in our information will arrive to destiny or the datagram will take another way that never pass thought our destination. That is caused because the owner of the datagram is not ours.

Another limitation is that in presence of Intrusion detection System (IDS), and depending the configuration of, it is possible that the datagram can be identified as a malicious one.

We have identified the challenging facts in this work with respect to loss of packets, Initially our primary focus is on text files, later the same approach could be extended for multimedia data

REFERENCE

1. Rowland, C.: Covert Channels in the TCP/IP Protocol Suite, First Monday, Peer Reviewed Journal on the Internet, July 1997 | 2. W Bender “Covert Channels in the TCP/IP protocol suite”, Techniques for Data Hiding IBM Systems Journal Vol 35, 2003. | 3. Cauich, E., Gomez Cardenas R.: Data Hiding in Identification and Offset IP Fields, Proc.5th Int’l. School and Symp. Advanced Distributed Systems (ISSADS), January 2005, pp. 118–25. | 4. Theodore G. Handel, Maxwell T Sanford, "Data hiding in the OSI Network model”, First International workshop on Information Hiding, | May-June 1996 | 5. Ahsan, K. and Kundur, D.: Practical Data Hiding in TCP/IP, Proc. ACM Wksp. Multimedia Security, December 2002 | 6. Murdoch S.J., Lewis S., Embedding Covert Channels into TCP/IP. Information Hiding (2005) 247-26 | 7. K. Ahsan and D.Kundur,"Practical data hiding in TCP/IP",Proc. ACM Workshop on Multimedia Security, 2002, | 8. 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.