# Survey and Design Approach of Protocol Steganography in IPv6

Sandip Bobade
Research Associate
MITAOE
Alandi,Pune

R.M.Goudar
Research Scholar
MITAOE
Alandi,Pune

## ABSTRACT

Steganography is the process of hiding message in another cover medium such that it is difficult to detect. Cover medium is used as a carrier.this carrier can be Image,video, text or IP packet. Covert Channel is implemented in different header Fields of IPv4 header to send secrete message. A covert channel is the medium that is used to transmit the information such as message, image or file. The fields flow label, traffic class and IPV6 source address of IPV6 header are selected as covert channel in this project. The more security in IPV6 header steganography can be achieved by apply- ing cryptography ie Encryption. Public key algorithm i.e. RSA is selected for cryptography. Message is at first encrypted using RSA algorithm. The ciphertext is embedded in selected fields. The- ses covert channels could be used for a Exploiting the Security rules so hidden Communication can be possible.this can be used for purpose such as pinching encryption key,login information or other secrets from in a way that should not easily detectable, but it could also be used for a good reason such as secret message can be passed under the watchful eyes of passive attacker. The demonstration of covert channel increases information security.

### General Terms:

Network Security

### Keywords:

IPv6,Covert Channel,Steganography,

## 1. INTRODUCTION

There are different Steganographic methods which hides secret data in users normal data transmissions and in good Condition hidden data and existence of hidden communication cannot be noticed by attacker.Various Steganographic methods have been proposed and analyzed. They may be exploiting the network security policies and they can be used as a tool to Secrete information leakage. That is why it is important to identify potential possibilities for covert communication, because knowledge of the information hiding procedure can be used to develop countermeasures. There are various ways of steganography like text, image, audio, video and packet steganography. Secret communication can be achieved by exploiting property of computer network that means by way of packet steganography. Secret communication is done in Protocol steganography by using covert channel. A covert channel refers to the Carrier that is used to communicate the information such as a message, image, or file. A good amount of work has been done in IPv4 packet steganography. But future computer network infrastructure will use IPv6; Internet Protocol Version 6 (IPv6) is the new generation Internet protocol that is set to slowly merge with and ultimately replace IPv4. According to a recent research [1] from Ars Technica, if the world continues at its current rate of adding millions IP addresses per year for new machine that are connected to the Internet, people will exhaust the current address space allowed for by IPv4 in 7.5 years. This is the main reason behind the move forward to switch to IPv6. IPv6 allows 128 to the power of 2 addresses, which shows that the Internet Engineering Task Force.ere are different covert channel in IPv6 header fields like flow label ,traffic class, Source address field which can be used as a Carrier of data. more. Hence we will focus on IPv6 steganography.

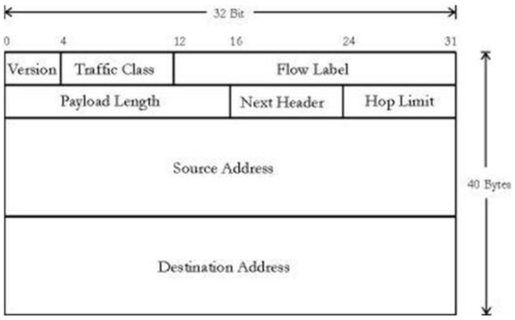

Fig. 1. Format of IPv6 header

### 1.1 IPv6

IPv6 Header Consist of Following Header fields.
Version (4 bits)
The constant 6 is for version Identity ie.bit sequence 0110.
Traffic Class (8 bits)
Traffic class is an 8 bit field.this field used is used by the node to identifiy different priorites and different class of the packet.Supporting node of the Traffic class can change value of this field.The 6 most-significant bits are used for which is used for classify packets The other two bits are used for ECN.

Flow Label (20 bits)
this field used for real-time application service The flow label is set by source a non-zero value used as special handing of routers. it is used to identify the flow of the packet.and also improve and Manage the quality of Service.
Payload Length (16 bits)
The size of this field in octets, with any extension headers.if the higher payload required jumbo payload extension header will be Provided.
Next Header (8 bits)
It is used to identify type of the Packet ie UDP or TCP following the IPv6 header.This field usually specifies the transport layer protocol used by a packet's payload.
Hop Limit (8 bits)
for forwading the packet the field is decremented by 1.if the Hop limil field decremented by 0 then the packet is Discarded.
Source Address (128 bits)
The IPv6 address of the Source node.
Destination Address (128 bits)
The IPv6 address of the destination node(s).

### 1.2 Steganography

The aim of steganography is to hide a secret message within a cover-media in such a way that others cannot discern the presence of the hidden message.different steganography methodologies are image Steganography,Text Steganography,Video Steganogra phy, Protocol Steganography.our focus on Protocol Steganography. Hiding information into a media requires following elements.
The cover media(C) that will hold the hidden data
The secret message (M), may be plain text, cipher text or any type of data
The stego function (Fe) and its inverse (Fe-1)
An stego-key (K) may be used to hide and unhide the message.
The stego function operates over cover media and the message (to be hidden) along with a stego-key (optionally) to produce a stego media (S). The schematic of steganographic operation is shown below.
Some of the Objectives are: 1. To detect Covert Channel In IPV6 header. II. To develop a method for embedding a data in field of ipv6 header. III. To secretly share encryption key and stegno key between two communicating parties. Steganography and Cryptography are great partners in spite of functional difference. It is common practice to use cryptography with steganography.

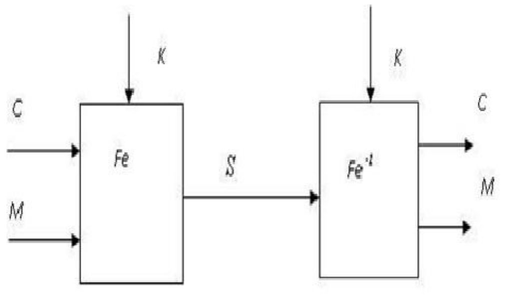

Fig. 2. Steganography Operations

## 2. RELATED WORK

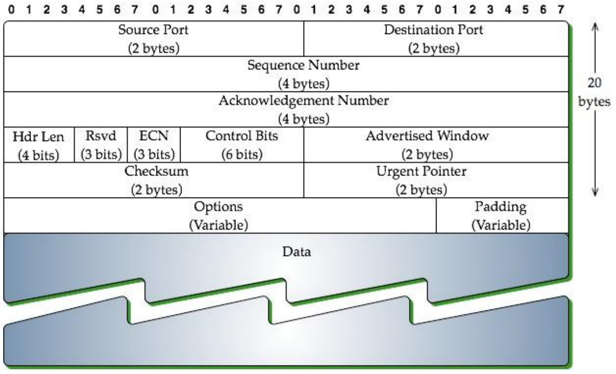

Fig. 3. TCP Header Format

Possible covert channel in TCP header are following:
PAD (padding bits) -bandwidth 31 bits/packet
Usage of chosen ISN (initial SN) -32 bits per connection
Usage of urgent pointer, when URG=0-16 bits/packet
Usage of reserved bits -6 bits/packet
Existence of data, when RST=1

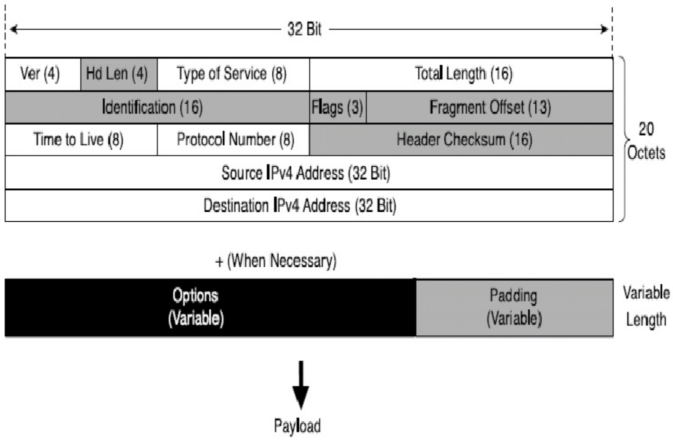

Fig. 4. IPv4 Header Format

steganography within TCP/IP is easily achieved by embedding data in header field seemingly filled with random" data, such as the IP identification,TCP initial sequence number (ISN) or the least significantcant bit of the TCP timestamp[1].Possible covert channel in IPv4 header are following.
PAD (padding bits) -bandwidth 31 bits/packet
IP identification -16 bits/packet
Fake source IP address -32 bits/packet
Usage of IP destination address as a flag -8 bits/packet
Usage of the unnecessary fields (ToS, options, some flags for example don't Fragment - DF for the fragmented packet) -various bandwidth
internet protocol(IPv4) header manipulation and packet ordering

Table 1. Covert Channel in IPv6

| Field | Covert Channel | Bandwidth |
|---|---|---|
| Traffic class | Set a false traffic class | 8b/p |
| Flow Lable | Set a false Flow lable | 20 b/p |
| Hop Limit | Increase or decrease a val | 1b/p |
| Source Address | a false source address | 16b/p |

are the different senario for data hiding. in which 16 bit Identification field and data fragmentation Stratergy is used,in fragmentation Stratergy flag field is used. [2].There are 22 covert channel in IPv6.which are network storage Covert Channel.Covert Channel are Classified as Storage or Timing Covert Channel. Timing Channel Involve a signalling Mechanism based on the Modulation of Resources such as CPU or time in a way Response time is Observed.Possible covert channels in IPv6 basic header can be following.IPv6 Traffic class can be used as a covert channel.as this is a 8 bit field.by setting a false bit can be used as a covert channel.differntiate service user can modify the traffic classes passes through it.because IPv6 specification agree to change the value of Traffic class by Intermediate node.

[3].The Privacy Extension is Propose to use instead of Fixed MAC Address based Interface identifier but when Protocol use pseudo random field they can be used as a Covert Channel.[4].The 20 bit header field of IPv6 ie flow label could be used as a covert data channel, since it seems that pseudo-random flow label values could, consist of covert data.flow label can be fabricated so 20 bits can be used as covert data.means by setting false flow label covert communication can bepossible.[NSA].Still flow lable is in Experimental phase.flow label is most probably used to achive quility of Service.flow classification depend on three touple which are flow label,source address and destination address. [5]. Steganography with a passive adversary is perhaps best illustrated by Simmons' Prisoners' Problem" [Sim84]. Alice and Bob are in jail and wish to plan an escape plan. All their communication is observed by the opponent (the custodian), who will spoil their plan by transferring them to a high-security prison as soon as he detects any sign of a hidden message. Alice and Bob succeed if Alice can send information to Bob such that Eve does not become doubtful [6].in IPv6 the duplicate address detection can be use for covert channels is possible because the interface identifier part of the address can be chosen in random. In IPv6 enabled Ethernets, the 64 bits of the 128 bit IPv6 address are reserved for the interface identifier.[7].IP fragmentation mechanism involves using the following fields of the IPv4 header Identification, Fragment Offset fields, along with the MF (More Fragments) and DF (Don't fragment) flags. It also needs to adjust values in Total Length and Header Checksum fields for each fragment to represent correct values[8].Cabuk et al. present in "IP Covert Timing Channels: Design and Detection" how adjusting the sending of IP packets can be used as a covert channel even though the Internet Protocol is an unreliable packet delivery service where the packet arrival times are not guaranteed [9].

## 3. PROGRAMMER'S DESIGN

Existing system perform communication between two parties using covert channel. If by some means third party extracted data then message will be directly exposed to intruder; hence more level of security is required. That can be achieved by using cryptography. Therefore steganography followed by cryptography approach is powerful. For cryptography public key algorithm i.e. RSA is selected [15]. As cryptanalysis of RSA algorithm is difficult. Public key algorithm is more suitable for steganography because it not necessary to exchange key (in private key algorithm key need to be exchanged secretly).

Table 2. Comparison of Cryptographic algorithm

| Algorithm | Type | Security |
|---|---|---|
| RC4 | Private | Medium |
| Blowfish | Private | Medium |
| AES | Private | High |
| DES | Private | High |
| RSA | Public | High |

Traffic class, flow label and source IPv6 address from Ipv6 header are identified as covert channel. Let Alice and Bob are secretly communicating. Alice will generate public-private key pair and will share public key with Bob. Similarly Bob will generate public-private key pair and will share public key with Alice. Input at Alice End: Cover medium(C): IPv6 packet Public Key: Public key of Bob Secret Message(M) Output at Bob End Cover Medium(C): IPv6 packet Secret Message(M)

### 3.1 Architecture of System

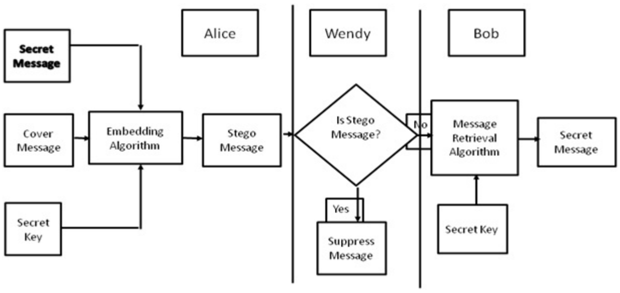

Fig. 5. Architecture of System

Traffic class, flow label and source IPv6 address from Ipv6 header are identified as covert channel. Let Alice and Bob are secretly communicating. Alice will generate public-private key pair and will share public key with Bob. Similarly Bob will generate public-private key pair and will share public key with Alice. Input at Alice End: Cover medium(C): IPv6 packet Public Key: Public key of Bob Secret Message(M) Output at Bob End Cover Medium(C): IPv6 packet Secret Message(M)

### 3.2 Sender and Receiver Site Algorithm

Sender Site Algorithm
1. Accept message from user(Plaintext).
2. Accept covert channel choice from user
a) Traffic class (8 bit i.e 1 char)
b) Flow Label (20 bits i.e. approx. 2 chars)
c) IPv6 Source address (14 byte i.e. 14 characters)
3. Apply RSA algorithm on plaintext to produce ciphertext.(Public key of receiver will be used for encryption)
4. Depending on choice given by user calculate number of IPv6 packet need to be sent.
5. Split ciphertext to fit into corresponding packets.
6. Create IPv6 packet(s)
7. Hide the ciphertext in covert channel

8. Send all packets to receiver.

Receiver Site Algorithm
1. Accept covert channel choice from user(choice should be same as sender)
a. Traffic class (8 bit i.e 1 char)
b. Flow Label (20 bits i.e. approx. 2 chars)
c. IPv6 Source address (14 byte i.e. 14 characters)
2. Generate public key and private key pair for RSA algorithm.
3. Announce public key.
4. Receive packets; and collect them according to sequence number.
5. Analyze packet one by one. Fetch data of that field which is choice of user. This is encrypted data.
6. Collect all these encrypted data to form ciphertext.
7. Apply RSA algorithm on ciphertext to produce plaintext.(Private key of receiver will be used for decryption)
8. Display message(plaintext) to receiver

### 3.3 Mathematical Model

Set Theory:
We consider Alice, Bob, Eva are the Object. Alice wants to send message to Bob without knowing to Eva. We are showing secure model of Crypto-Steganography.
Crypto-Stego system Consist of

i Key Generation(RSA) for crypto-steganography ($S_k$ )
ii Message Encoding by encryption ($S_E$ )
iii Message Decoding by decryption ($S_D$ )

Consider Set C($S_k$ , $S_E$ , $S_D$
)
Coverttext C be the distribution on a set C

i) $S_k$
Input: randomly generate p and q which are prime and p!=q
Output:Crypto-Stegokey

ii) Crypto-Steganographic Encoding Algorithm ($S_E$ )
Input: Stegokey $S_k$ , Secret Message converted into hex and then converted into binary (0, 1) Output: Crypto-Stego Message

C-Random Variable Represent Cover Message
E-Random Variable Represent Embedding Message
S-Random Variable Represent Crypto-Stego Message.
Idea is Sk=Ck,
Eva Learning what alice transmitted measured by Entropy

$$\Delta = \frac{(H\,(S^k/Z^n\,))}{(H\,(S^k))} \qquad (1)$$

$S^k$ Bits Alice sent
$Y^n$ Bits Bob Received
$Z^n$ Bits Eva Taps.
If Eva determine what Alice sent.
Then all probabilities are 0 or 1

$$H = \frac{S^k}{Z^n} = 0 \text{ and } \Delta = 0 \text{ this is a worst cast of Secrecy} \qquad (2)$$

Case-2
If Eva learn nothing about the Distribution of $S^k$
from knowing $Z^n$

$$\Delta{=}1 \text{ this is the Best Case of Secrecy} \qquad (3)$$

## 4. CONCLUSION

Following covert channels are identified from IPv6 basic packet header for secured communication
a)Traffic class (8 bit)
b)Flow Label (20 bit)
c)Source IPv6 address( 14 byte)
Therefore in a single IPv6 packet basic header max 140 bits (i.e. around 17 bytes) of secret data can be hidden. Stegano analysis if applied by third party then these fields are susceptible for vulnerability due to property of packet format. Stronger security is provided by applying RSA public key algorithm (cryptography). IPv6 packet steganography combined with cryptography gives lowest probability for hijacking of data. The project can be applied to various fields where security is major concern for ex. to share private key in bank application, military, confidential matters etc.

## 5. REFERENCES

[1] Rowland, C. (1997). Covert channels in the TCP/IP protocol suite, first Monday. Peer viewed Journal on the Internet, July 1997.

[2] Zander, S., Armitage, G Branch, P. (2007). A survey of covert channels and untermeasures in computer network protocols. IEEE Communications Surveys Tutorials

[3] Petitcolas, F., Anderson, R., Kuhn, M. (1999). Information hidinga survey. IEEE Special Issue on Protection of Multimedia Content, July 1999.

[4] S. J. Murdoch and S. Lewis, ”Embedding covert channels into TCP/IP,” in 7th Information Hiding Workshop, June 2005.

[5] Request for Comments: 6437 IPv6 Flow Label Specification

[6] S. Deering, R. Hinden, RFC::2460,Internet Protocol, Version 6 (IPv6) Specification.

[7] Neil Johnson, Stefan Katzenbeisser, A survey of steganographic techniques, Information hiding techniques for information hiding and digital steganography.

[8] K. Ahsan and D. Kundur, ”Practical Data Hiding in TCP/IP,” in Proceedings of the Multimedia and Security Workshop at ACMMultimedia, Dec. 2002.

[9] Wojciech Mazurczyk, Miosz Smolarczyk Retransmission steganography applied 2010 International Conference on Multimedia Information Networking and Security

[10] Wojciech Mazurczyk,Krzysztof Szczypiorski, Evaluation of steganographic methods for oversized IP packets Telecommunication Systems,2012

[11] Miller, Steganography in IPv6

[12] Thomas Narten, Neighbor discovery and stateless auto reconfiguration in IPv6 IEEE, 1999.

[13] Mohit Wadhwa, Manju Khari, Velnurability of IPv6 Type 0 routing header and its prevention algorithm International journel of advanced engineering science and technologies, 2011.