# A Research Paper on Steganography in IPV6

Lalit Mohan Joshi
M.tech Scholar
BTKIT Dwarahat, Almora
Uttarakhand, India

Amit Yadav
M.tech Scholar
BTKIT Dwarahat, Almora
Uttarakhand ,India

Sumit Sharma
M.tech scholar
BTKIT Dwarahat, Almora
Uttarakhand, India

## ABSTRACT

Steganography is the process to hide a secret message such that it is very difficult to detect the presence of secret message presence. On other way, the existence of secret message is hidden. A covert channel may refer to the actual medium that is used to communicate the information such as a message, image as well as file. This project uses steganography within the source address fields of Internet Protocol Version 6 (IPv6) packets to create a covert channel through which clandestine messages can be passed from one party to another.

A fully functional computer program was designed and written that transparently embeds messages into the source address fields of packets and across IPv6 networks, embedded messages are by these packets. This demonstrates the covert channel possibility within a default Internet protocol. For a malicious purpose such as stealing encryption passwords as well as keys or other secrets from remote hosts in a sequence not easily detectable this channel is used, but it may be used for a noble cause such as secretly passing messages under the watchful eyes of an oppressive regime. The covert channel demonstration in itself the overall information security of society is increased by bringing awareness to the existence of such a steganographic medium.

## Keywords

Steganography, IPV6, MAC Address ,IPV6 Model

## 1. INTRODUCTION

In an increasingly connected world, more and more devices are being networked together than ever before. This trend will continue with not only more laptop and desktop computers needing to be able to talk to one another around the world, but handheld PDAs, cell phones, cars, and, eventually, even fridge, oven and other household things. Most networked devices today are

connected through Internet Protocol version 4 (IPv4), a layer three protocol of the International

Standard Organization's Open System Interconnect (ISO/OSI) model. IPv4 provides for a theoretical possibility of two raised to the thirty-second power or a little over 4 billion possible addresses, but for practical reasons of off-limits address ranges, the actual number of IPv4 addresses available for use to the world is about 3.7 billion, and these are rapidly running out.

Internet Protocol Version 6 (IPv6) is the "next generation" Internet protocol that is set to slowly merge with and definitely replace IPv4. According to Ars Technica article, "If the world continues at its current rate of adding 170 million IP addresses per year for new hosts 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 driving force behind the push to switch to IPv6.

IPv6 allows for astronomically more addresses than people could possibly ever use, which shows that the Internet Engineering Task Force,the group that guides the development of protocols that run the Internet, does not want to run into the "limited address space" problem again in the future. Switching to IPv6 is necessary and inevitable. However, society must also be aware of the risks and otherwise unintended possibilities that accompany the adoption of any new protocol or technology, and IPv6 carries at least one significant unintended possibility of allowing for a covert channel to be created and exploited using the built-in mechanism of the source address of the header.

As in the IPv6 specification along with the privacy extensions for the stateless address auto configuration feature of IPv6 introduce the possibility of embedding a significant amount of secret data into the source address field of an IPv6 packet header that will likely be an uninformed observer which is undetectable. The 128-bit field source address, which is contain the universally originator of the packet with unique Internet address. The privacy extensions proposed for IPv6 rely on the random generation of a 64-bit portion of the 128-bit source address.

The second way the program can embed messages is by explicitly creating IPv6 packets containing the message in the source address field, which are then injected into the network. The packets transmitted in this manner would not be transmitted as part of the normal networking activities of the host and is, therefore, slightly less stealthy, but can, in some cases, be more practical. The way the software decodes the received messages depends upon the way in which the message was transmitted. All parties involved in sending and receiving the secret message ahead of time must know the method of transporting the message.

## 2. FEASIBILITY STUDY

The term feasibility relates to practicality, possibility or convenience. The feasibility study in reference to the software development specifies that whether the given problem is worth the hard work and the time for the software developing team. Feasibility study has 4 major aspects or dimensions regarding the development of software.

### 1. Technical feasibility

The project (Steganography in ipv6) is technically feasible using the applications such as java language features and require basic knowledge of networking for support. Although no special software of frame work is required for the development of the project yet some advanced concepts of the

Socket Programming are used to fulfill the requirements where ever necessary.

## 2. Economical feasibility

The development cost of this software is very low as it can be installed at very reasonable investment, which can be recovered in a very short span of time through the services it provides. The creation of this project requires the java platform which is an open source environment, so it doesn't cost much.

## 3. Operational feasibility

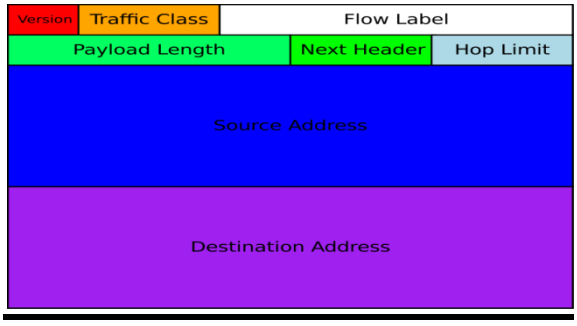
The scope of operation is to fetch the user's message and transmit it into the safe environment to another connected user. Thus it is easily operable and fulfills the requirements of the user in a much more efficient and convenient manner for the sake of easy usability.

## 4. Organizational feasibility

The proposed software will be useful only if provided the proper environment i.e. it will be applicable only at JVM enabled computer systems. As most of the organizations work on various java programs so it will be easy to implement by organization.

## Architecture of IPV6 Packet

An IPv6 Packet Header consists of the fields shown below in Figure IPv6 packet. The exact use of all the different fields is unimportant for a full understanding of project, but it is useful for the reader to be able to visualize the packet header. Important fields are the destination and source address fields, which allows routers to direct the packet to its destination and provide a return address to that destination. In addition, there is a version field indicating IPv4 or IPv6 and the next-header field, which specifies the layer above the current IP layer, such as TCP or UDP.




## Address format

An IPv6 address is represented by 16-bit values of 8 groups, each group represented as like 4 hexadecimal digits and separated by colons (:). For example:

2001:0db8:0000:0000:0000:ff00:0042:8329

The hexadecimal digits are case-insensitive; e.g., the groups 0DB8 and 0db8 are equivalent.

## 3. STEGANOGRAPHY

Steganography literally refers as "covered writing" in Greek language, and there are many ways to perfome steganography, in which there may or may not involvement of using a computer.

For example, a commonly known form of steganography is performed with juice of lemon and simple paper. A pen dipped in lemon juice is capable of writing an invisible message that can only be made visible again with the application of heat to the paper. The secret message existence written in such a fashion that it would have to be seemed to the intended recipient ahead of time, and the main purpose of this secrecy is to protect the trusted parties those are participating against any third party that may intercept the message in transit. With the message secretly embedded into the cover medium, the participating parties can be reasonably secure in the knowledge that any third party is unlikely to discover the hidden message. In the case of the lemon juice on paper, the secret message might be written in between lines of a message written in normal ink that is meant to be seen. The ink message could be innocent or deliberately wrong information designed to lead an enemy down a false path of disinformation.

Steganography can also be combined with cryptography for an extra layer of security in the case that the existence of the secret becomes known to a third party. Sometimes, Steganography is desirable in place of or on top of cryptography for the simple fact that cryptography itself arouses suspicion. The assumption is made that it must be something worth hiding and therefore in the case if data is encrypted, valuable.

## 4. Environmental Characteristics

## 1. Hardware Specifications:-

- Operating System
  → Any with JVM
- CPU
  → Pentium 200MHz or above
- Memory
  → 32 MB or above
- HDD Space
  → 28 MB or above

## 2. Software Specifications

Front End of the mini-Project is supported by the object oriented programming language "java" .

Back End is supported by the Network interface and some algorithms based upon the cryptography

## 5. DESIGN

**1. Encoding Messages through MAC Addresses (Passive Injection):**

MAC addresses are composed of 48 bits (six 8-bit bytes) and can be represented by six octets (two hex digits each) separated by colons such as in the following:

AA:BB:CC:11:22:33

Using the MAC address method, a list of MAC addresses is created from the bytes in the original message. when a network host has not elected to use the privacy extensions of IPv6, the interface identifier portion of IPv6 addresses is created using the MAC address of the interface on the IPv6 network. For this reason, when the MAC address of an interface is changed, the interface identifier portion of the interface's IPv6 address is automatically changed. As long as the MAC is set to one of the entities representing a piece of the secret message, this piece of the message will be embedded implicitly into the interface identifier portion of the source address of all packets leaving the interface of the host

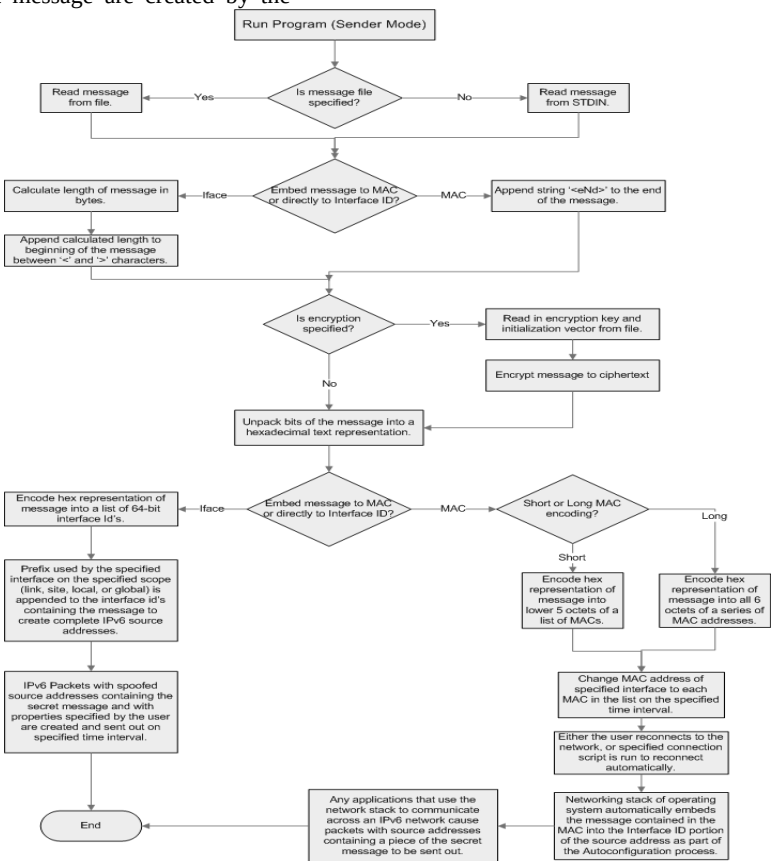
on the network. This happens regardless of the details, such as source and destination ports and destination addresses, that the application or higher level protocol uses as long as the interface containing the piece of the message as its MAC address is used.

**2. Encoding Messages through Packet Creation (Active Injection):**

Another method used to send messages in the source-address covert channel of IPv6 is called Active Injection. This method is referred to as active because packets with spoofed source addresses containing the secret message are created by the program and injected into the network solely for the purpose of sending the secret message, whereas in the passive mode, no packets are actually created by the program at all. However, in the passive mode, packets are created by other applications that simply use the IPv6 source addresses with the embedded message set by the stego program for an interface. In active mode, the actual address of the interface connected to the network never changes at all.

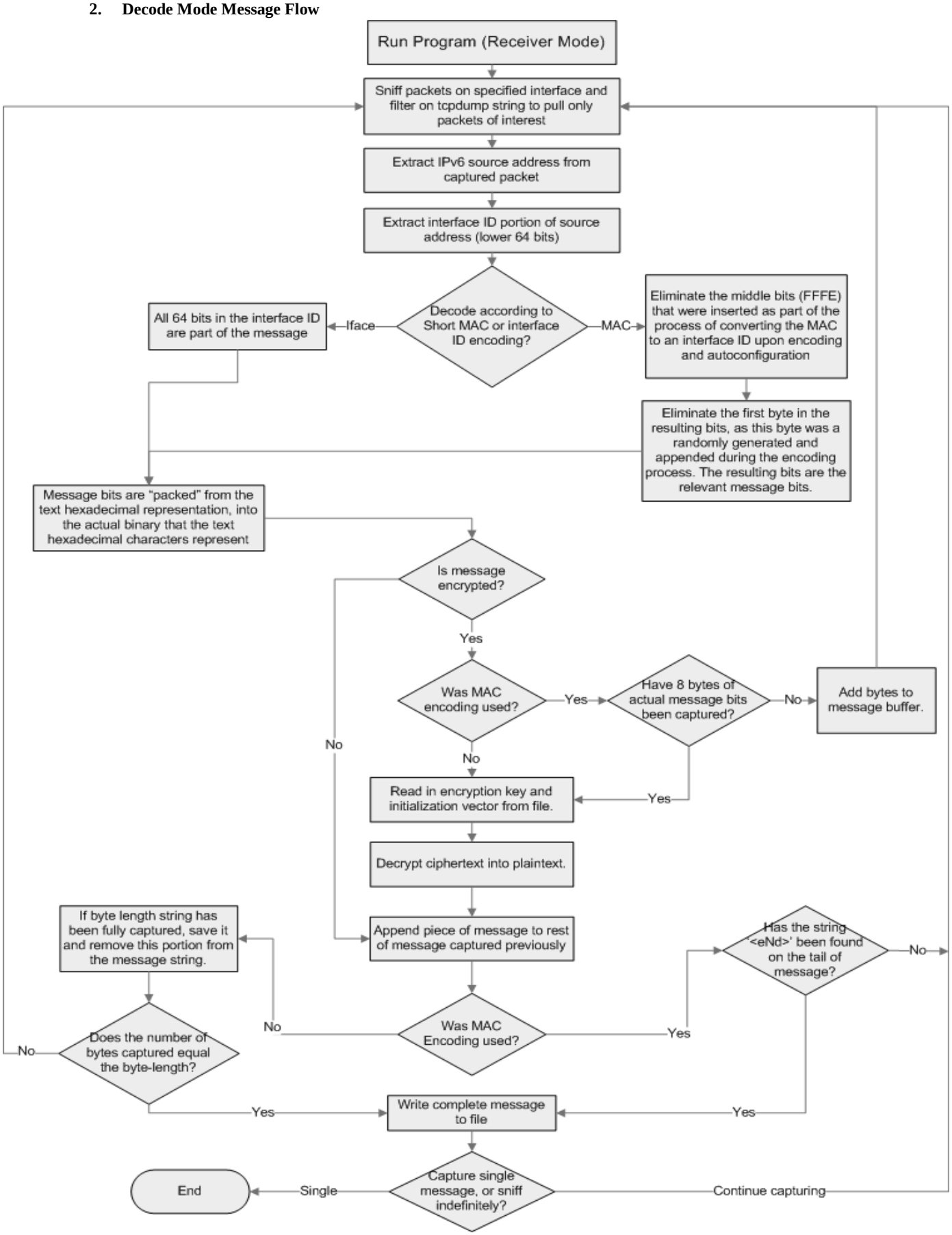
# 6. IMPLEMENTATION

**1. Message mode process flow**




IPv6 packets are constructed by the program in pieces from the link-layer to the application layer, with most properties of these packets configurable by the user, and injected into the network on a time interval set by the user. An example of a property not directly configurable by the user in these packets is the IP source address, which will obviously be set to a piece of the secret message specified by the user. Other properties, however, such as source and destination port, destination address, data for the layer-seven data portion, and much more can be specified by the user in many different configurations that can help to make the packet look more legitimate on the network the user is connected to.

**2. Decode Mode Message Flow**



world wishes to responsibly implement a system on such a wide scale as IPv6 that will affect the lives of over one billion users whether they are aware of it or not, then it is the duty of the implementers and maintainers of such a system to fully understand it. Full understanding is not hard to come by in an open system such as the Internet Protocol version 6, where anyone from the community that has a desire may closely inspect the inner workings. This thesis demonstrates the community acting responsibly to increase awareness and understanding of protocol that will soon be used by billions.

## 8. REFERENCES

[1] B. Dunbar. A detailed look at Steganographic Techniques and their use in an Open-Systems Environment, Sans Institute, 1[2002].

[2] Christian. An Information-Theoretic Model for Steganography,Proceedings of 2nd Workshop on Information Hiding, MIT Laboratory for Computer Science. 1998.

[3] H. Wu, H. Wang, C. Tsaiand C. Wang, Reversible image steganographic scheme via predictive coding. 1 (2010), ISSN: 01419382, 35-43.

[4] J, Corporation, Steganography. http://www.webopedia.com/TERM/S/steganography.html. 2005.

[5] M. D. Swanson, B. Zhu and A. H. Tewfik, Robust Data Hiding for Images, IEEE Digital

[6] Signal Processing Workshop, University of Minnesota, September 1996 ( 37-40). N Ghoshal, J K Mandal .A steganographic scheme for colour image authentication (SSCIA), Recent Trends in Information Technology ICRTIT 2011 International Conference on (2011), 826-831.

[7] N. Johnson, Survey of Steganography Software, Technical Report, January 2002.

[8] N. Johnson, Digital Watermarking and Steganography: Fundamentals and Techniques , The Computer Journal. (2009)

[9] P. Fabien, J. Ross. Anderson, and Markus G. Kuhn. "Information Hiding – A Survey." Proceedings of the IEEE, 87:7. 1062-1078. 1999.

[10] W, Peter. Disappearing Cryptography: Information Hiding: Steganography & Watermarking (second edition). San FranciLi, B., Biswas, S., & Blasch, E. P. (2007, 9-12 July 2007).

[11] Li, L.-d., Guo, B.-l., & Guo, L. (2008). Rotation, scaling and translation invariant image watermarking using feature points. The Journal of China Universities of Posts and Telecommunications, 15(2), 82-87. doi: 10.1016/s1005-8885(08)60089-8

[12] Martin, A., Sapiro, G., & Seroussi, G. (2005). Is image steganography natural? Image Processing, IEEE Transactions on, 14(12), 2040-2050. doi: 10.1109/tip.2005.859370

[13] Marvel, L. M., Retter, C. T., & Boncelet, C. G., Jr. (1998, 4-7 Oct 1998). Hiding information in images.Paper presented at the Image Processing, 1998. ICIP98. Proceedings. 1998 International Conference on.

[14] McBride, B. T., Peterson, G. L., & Gustafson, S. C. (2005). A new blind method for detecting novel steganography. Digital Investigation, 2(1), 50-70. doi: 10.1016/j.diin.2005.01.003

[15] Min-Jen, T., & Jung, L. (2011, 6-9 Nov. 2011). The quality evaluation of image recovery attack for visible watermarking algorithms.Paper presented at the Visual Communications and Image Processing (VCIP), 2011 IEEE.