IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 12, December 2022

DOI: 10.17148/IJARCCE.2022.111224

Network Steganography for Secure Communication: A Survey

Shraddha Khonde[1], Rutuja Gaikwad[2], Pratiksha Chavan[3], Dnyaneshwari Rakshe[4]

Department of Computer Engineering, MES College of Engineering, Pune [1-4]

Abstract: A steganography is the science of sending secrete messages between the sender and receiver. It is such a technique that makes the exchange of covert messages possible. Each time a carrier plays a major role in establishing covert communication channel. This survey paper has more about network protocols to be used as a carrier. There are a number of protocols available to do so in the networks. TCP/IP protocol suite has been a potential target for network steganography from the very beginning. It has a lot of possibilities for creation of hidden channel that can be used to communicate covertly. This paper depicts the technique that creates a covert channel using the Overflow filed of Timestamp option of Internet protocol, version 4, over a Local Area Network. This technique implements a storage area network steganography that uses the timestamp option which is used to hide information by modifying protocol header fields, such as unused bits of a header, or the data field of a packet.

Keywords: Cryptography, Steganography, Protocol, Steganography, Covert, IP4

I. INTRODUCTION

Information security is the need of every industry today. No organization would want their data to be hacked or intercepted by anyone. One way to secure the data over the networks is through information hiding using steganography. Steganography is the art and science of communicating in a way, which hides the existence of the communication Nowadays almost all people exchange information online, whether Facebook, WhatsApp, mailing, video calling, voice calling, everything is on network each and every information is exchanged on networks, whether P2P, TCP/IP, HTTP everything it is handy though, but intruders always keep an eye on the information exchange, but the best part of network steganography is that we can use any network protocol to transmit message by concealing it in the Headers, packets etc. depends which method we use

• In storage type of covert channel, the storage location for the bits is altered while in timing-based type of covert channel the bits timing is varied. Hybrid covert channel combines the features of both storage and timing based covert channels. Network steganography is categorized into two categories on the basis of Open System Interconnection System Model (OSI RM)

1) Intra Protocol Network Steganography: In this method only single network protocol is used.
2) Inter Protocol Network Steganography: In this method multiple network protocol is used

1.1Attributes of Network Steganography

The three main attributes f network steganography that are namely-

- Bandwidth
- Undetectability
- Robustness

Bandwidth deals with amount of information that a link could handle at a time. Undetectability is the important feature that marks for the fact that the hidden message should go untraceable by the attacker. A good steganographic approach has to have this one.
Robustness marks for the conformity to the error free condition where the secret should not be prone to any kind of failure or error

1.2 Advantages of Network Steganography

It is one of the best suitable methods as the covert channel could be implemented on the layers of the protocol suite. It is better than other media coverts where the stego object is limited by the size of the covert object. Also, extra files are needed to be sent to and from in media steganography.

DOI: 10.17148/IJARCCE.2022.111224

The short life span of steganography is a plus point as compared to other steganographic approaches which have long life span. Steganogram is destroyed after IDS (Intrusion Detection System) discards the embedded steganogram (however exceptions exist).

II. STEGANOGRAPHY

Steganography is a technique of hiding secrete data inside a cover. The most popularly used cover media include images, videos, audios, documents and network protocols. Network Steganography is implemented by creating covert channels as means of communication between a covert sender and a covert receiver.

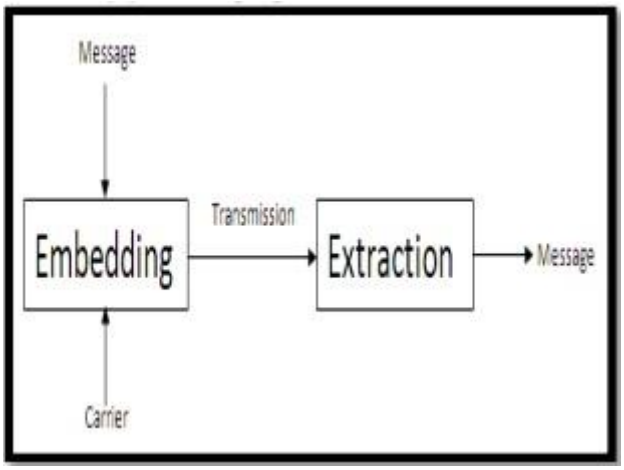

Fig 1: Basic Model of Steganography

2.1 Steganographic Techniques Using Network Protocol

Network steganography is a technique implement steganography using available network protocols. The concept of covert channels was first introduced by Lampson. The OSI RM (Open System Interconnection Reference Model) has 7 layers in it. The 7 layers have different protocols freely available for carrying out steganography.

Network steganography is done by using covert channels. Covert channels could be Storage channels: the channels which use the reserved or unused bits of the packet header and payload are called storage channels.

Timing channels: the channels which use the time synchronization of the packets for sending secret bits are called timing channels. Hybrid channels: the channels which use the strategies of storage as well as timing are called hybrid channels.

2.2 Covert Channels

There are a number of covert channel techniques in computer network protocols.

They are described as follows

Unused Header Bits Secret message could be encoded in unused or reserved bits of frame or packet headers. IP header's Type of Service (TOS) field, TCP header's Flags field, IP header's Don't Fragment (DF) bit, TCP Urgent Pointer, TCP Reset segments (RST) and IPv6 header fields could be used to hide secret bits of data.

Checksum Field IP header Checksum field could be used to encode secret information. IP header extension is added with the content such that the modified checksum is correct again. Same technique could be used for TCP Checksum. UDP Checksum is used for providing a signal if any secret information is sent.

Wireless LAN(WLAN) There are various protocols in the IJIRT101379 for applying network steganography. The RC4 initialization vector can be used. Retry bit and More Fragments bit of the Frame Control field and the Duration/ID header fields can also be used for this purpose. The ACK frames or invalid frames are also available.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 12, December 2022

DOI: 10.17148/IJARCCE.2022.111224

Modulating Address Fields and Packet Lengths Any communication protocol uses address fields to identify the address of senders and receivers. The number of bits transmitted depends on the number of different addresses. Also, the packet length fields indicate the length of headers, header extensions or messages (frames, packets). This packet length could be used to send secret bits of data.

2.2.3Structure of IP Timestamp option

The structure of the Timestamp option is shown in Figure 2. The Option Type value for Timestamp option is 68 in decimal (copy flag = 0, option class = 2 and option number = 4). Option Length specifies the number of octets used by the current option including the type, length, pointer, overflow and flag fields

Option Type 8 bits (01000100)	Option Length 8 Bits	Pointer 8 Bits	Overflow 4 Bits	Flag 4 Bits
Internet Address 32 Bits				
Timestamp 32 Bits				

Fig 2: Structure of IP Timestamp option

• Modulating Timestamp Fields IP timestamp header extension can be used to transmit covert data. But it limits a packet to only 24 hops and is no longer used. TCP timestamp header options can also be used to transfer secret information over the network.

III. STEGANOGRAPHIC METHODS

3.1.1 HICCUPS (Hidden Communication System For Corrupted Networks)

In this method a station sends corrupted frame and rest of the stations change their mode as per the corrupted frame here corrupted frame means a frame having incorrect checksum. This method comes under protocol data unit where modification of payload is done as per the requirement.

The primary data is sent with the intentionally corrupted frames to the receiver depicting your secret message which after receipt is fixed to get the message because of the introduction of the corrupted frames an error is introduced in this process known by the name of frame error rate (FER)

3.1.2 Steg Torrent

Steg Torrent is based on peer-to-peer data exchange protocol where a single client shares a file with multiple clients at same time using IP networks. In case of Steg Torrent both sender and receiver of secret information uses IP addresses known to each other.

The sender uses modified bit torrent client for sending the information which is then received by using Steg Torrent client.

3.1.3 Steg Suggest

This method is based on hiding the secret message in the Google suggestions. Whenever we search online for something on Google, Google provides us with suggestions itself the secret message is hidden by inserting a letter suffixed with each word present in the suggestion.

As the google suggestion feature works on Ajax so the data retrieval is asynchronous.

Table 1 Comparison among different methods of network steganography

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 12, December 2022

DOI: 10.17148/IJARCCE.2022.111224

S.NO	METHOD	CARRIER/COVER	TYPE
1.	Hidden Communication System For Corrupted Networks	Corrupted Frames	Intra Protocol / WLAN
2.	Lost Audio Packets Steganography	Delayed Audio Packets	Hybrid Intra Protocol
3.	Retransmission Steganography	Intentionally Retransmitted Packet	Hybrid Intra Protocol
4.	Stream Control Transmission Protocol	Multiple Streams	Modifies PDU's time relation
5.	Padding Steganography	Bits Of Ethernet	Inter Protocol
6.	Transcoding Steganography	Space After Overt Data Compression	IP telephony
7.	Skype Hide	Silent Packets	P2P
8.	StegTorrent	IP address	Inter Protocol
9.	StegSuggest	Word Suffixing	Intra Protocol

IV. CONCLUSION

These Network Steganography techniques are versatile and are really reliable as compared to that of other steganography techniques that is the reason network steganography is in more practice as compared to others day by day many new network steganography techniques are coming in to influence which clarifies that this is very wide field for concealing and sending secret information safely. Steganography could be done using various carriers in which using network protocols is the latest and newest approach. Numerous protocols and the unused bits are available to attain steganography. It is been said that if 1 bit per packet data is used to transfer secret messages, a genuine website could lose 26 GB of data

REFERENCES

[1] Avish Dhamade, Krunal Panchal Computer Science Engineering Department, L. J. Institute of Engineering Technology, Gujarat Technological University 2019.
[2] Namrata Singh Dept. of CSE ABES Engg. College Ghaziabad, India, Jayati Bhardwaj Dept. of CSE ABES Engg. College Ghaziabad, India, Gunjan Raghav Dept. of CSE ABES Engg. College Ghaziabad, India 2020.
[3] K. Szczypiorski, HICCUPS: Hidden Communication System for Corrupted Networks, In Proc. of: The Tenth International Multi-Conference on Advanced Computer Systems ACS'2003, pp. 31-40, October 22-24, 2003.
[4] Punam Bedia, Arti Duab * a, Department of Computer Science, University of Delhi, Delhi 110007, India 2020.
[5] B. Jankowski, W. Mazurczyk, K. Szczypiorski, Information Hiding Using Improper Frame Padding - 14th International Telecommunications Network Strategy and Planning Symposium (Networks), 2010.
[6] Amritha Sekhar 1, Manoj Kumar G.2, Prof. (Dr.) M. Abdul Rahiman3 Student, Department of CSE, LBS Institute of Technology for Women, Thiruvananthapuram, India 1 Associate Professor, Department of CSE, LBS Institute of Technology for Women,
[7] Thiruvananthapuram, India 2 Pro Vice Chancellor, Kerala Technological University, Thiruvananthapuram, India 3 2018.
[8] Amritha Sekhar 1, Manoj Kumar G.2, Prof. (Dr.) M. Abdul Rahiman3 Student, a. Department of CSE, LBS Institute of Technology for Women, b. Thiruvananthapuram, India
[9] Hamza Khaddar*, Merouane Bouzid** *(Department of Telecommunication, LCPTS Lab USTHB University, Algeria) ** (Department of Telecommunication, LCPTS Lab USTHB University, Algeria)
[10] Associate Professor, Department of CSE, LBS Institute of Technology for Women, Thiruvananthapuram, India 2 Pro Vice Chancellor, Kerala Technological University, Thiruvananthapuram, India 3 2018
[11] Sun Microsystems (2014) System Administration Guide Volume 3, chapter 15" Transition from IPv4 to IPv6" homepage. [Online]. Available: www.docs. oracle.com/cd/E19455-01/806 0916/index.html.

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 12, December 2022

DOI: 10.17148/IJARCCE.2022.111224

[12] W. Fraczek, W. Mazurczyk, K. Szczypiorski, Stream Control Transmission Protocol Steganography, Second International Workshop on Network Steganography (IWNS 2010) co-located with the 2010 International Conference on Multimedia Information Networking and Security (MINES 2010), November 2010.

[13] T. G. Handeland, M. T. Sandford. Hiding Data in the OSI Network Model. USA, Weapon Design Technology Group, Los Alamos National Laboratory, 1996

[14] D. Llamas, Covert channel analysis and data hiding in the TCP/IP protocol suite. Honours Project Thesis. UK, Napier University, 2004.

[15] Berg, Glossary of Computer Security Terms. USA, National Computer Security Centre, 1998.

[16] (2014) the ns-3 website. [Online]. Available.

[17] C. G. Girling, Covert Channels in LAN's. USA, IEEE Transactions on Software Engineering, 1987 [18] Deepa Kundur and Kamran Ahsan. "Practical Internet Steganography: Data Hiding in IP", In Proceedings of Texas Workshop on Security of Information Systems, April 2003.