Network Steganography and its Techniques: A Survey

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

ABSTRACT

With the ongoing increase of threats and vulnerabilities to our information security, the need for a strong, secure and an effective kind of approach is highly required. An approach that fulfills all these parameters is a byproduct of the trending steganography technique. As there is the availability of various types of cover media, but this paper focuses only on one such media, which is a 'network'. Using the network as the cover media for hiding the data for transmission of the secret information safely, is one of the smart moves towards the information security. This approach is known as network steganography. Since the intruders try every bit to take the advantage of that secret information, this concept of network steganography provides the concealment of the secret data by using the covert channel which uses the bandwidth of other permissible communication channels for the transmission purpose. This paper is on network steganography depicting all the proposed methods available for the network steganography along with the process of concealing the secret information in the desired communication protocol.

Keywords

Covert Channel, IDS, Network Steganography, OSI Model, Protocol.

1. INTRODUCTION

Steganography means concealing a secret message in any other file or also called cover file, cover can be audio, video, text or image, etc. Main purpose of steganography is to make the secret message undetectable to ensure that the message reaches the desired person unchanged and undetected. There are various steganographic techniques based on the cover used to conceal the message out of all the most sophisticated and developing is Network Steganography. 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. Network steganography has a vast scope of development. Various new methods are developed in network steganography on the basis of the way of transmitting/concealing the message. Network steganography uses communication protocols and the new network steganography techniques come in existence day by day. One can make this technique more secure and robust by combining other techniques like cryptography along with this technique the secret message can be encoded using the cypher code and then can be transmitted using network steganography.

Network Steganography is a suspicion resistant real time communication tool. In the network, the data flows in between the sender and receiver. So, the transmission depends on the bandwidth of it. This bandwidth varies as per the capacity of the link (channel). This varying feature of bandwidth is the advantage over all other media steganographic techniques because it cannot be modified due to its dependency on the cover object in the latter one. In network steganography the transmission channel used is known as covert channel. This covert channel plays the role of the cover in this case. The secret message is embedded into this cover channel. This channel is classified into two main categories namely- Storage based covert channel and Timing based covert channel. Another different category of covert channel is Hybrid.

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 [10]. 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.

Inter Protocol Network Steganography: In this method multiple network protocol is used

Fig 1 shown below defines the various categories of network steganography with the sub type on which they are based on.

1.1 Attributes of Network Steganography

The main attributes of network steganography that are namely-

- bandwidth,
- undetectability and,
- 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 covers where the stego object is limited by the size of the cover object. Also, extra files are needed to be sent to & fro in media steganography.

- The short life span of steganogram 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).

- In case of Network Steganography, the bandwidth is quite flexible and depends on the type of protocol and network capability. This is contrast to media steganography approach in which bandwidth is limited to cover size.

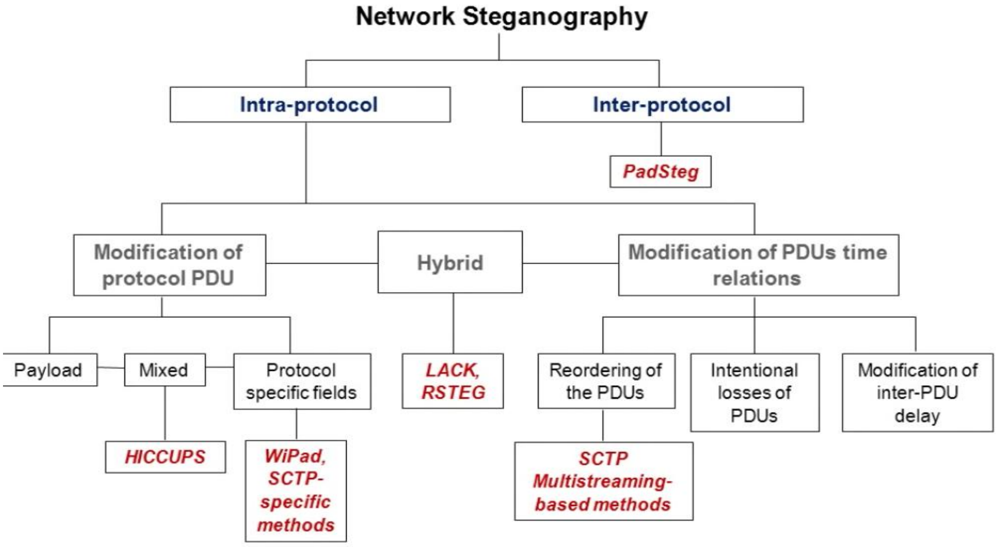
Network Steganography
Intra-protocol
Inter-protocol
PadSteg
Modification of protocol PDU
Hybrid
Modification of PDUs time relations
Payload
Mixed
Protocol specific fields
LACK, RSTEG
Reordering of the PDUs
Intentional losses of PDUs
Modification of inter-PDU delay
HICCUPS
WiPad, SCTP-specific methods
SCTP Multistreaming-based methods

Fig. 1 Types of network steganography [2]

2. STEGANOGRAPHIC METHODS

2.1 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[1]. This method comes under protocol data unit where modification of payload is done as per the requirement[3]. For a detailed and much clearer approach the flowchart for the HICCUPS is shown below in the Fig.2 from which it is clear that 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). FER can be calculated by taking the ratio of data received with errors to total data received if this ratio is too high the connection may drop so for effective HICCUPS the FER should be in a range where the communication should remain continuous in Fig. 3 the FER is shown for a simple communication network and a HICCUPS network.

2.2 LACK (Lost Audio Packets Steganography)

This method also falls under the protocol data unit. In this method the voice packets are generated at the transmitter end and out of those generated voice packets one is delayed intentionally replacing the payload of the selected packet with the delayed steganogram.[1] As soon as the delay timer expires the packet is sent to the receiver's end. Now for a normal receiver the delayed packet is loss and it drops it but LACK receiver extracts steganogram from the delayed voice packet[4].

2.3 RSTEG (Retransmission Steganography)

In this method the retransmission mechanism is used here the receiver intentionally acknowledge that few received packed are not received evoking the need of retransmission now the retransmitted packet’s payload is replaced with the steganogram by the transmitter which is received by the receiver. This method is very hard to detect[6,1]. Below Fig. 4 shows how the process of RSteg works here sender is sending the data #1 to the receiver and receiver is intentionally showing that the data is not received because of which sender does not get the acknowledgment of receipt of data #1 so he retransmits the data by inserting the secret data in the specific payload and acknowledgement is sent for the recipient.

2.4 SCTP (Stream Control Transmission Protocol)

This is a multi-streaming based method in this method the rather sending the complete steganogram together it is sent in parts. As an example a complete steganogram be 10011100 is to be transmitted so we use 4 streams for transmitting it 1,2,3 and 4 for which 10 is sent in stream 3 as it corresponds to it, Similarly 01 in stream 2, 11 in stream 4 and 00 in stream 1. The robustness of this method increases if we use mixed components of UDP and TCP.[7,1]

2.5 PadSteg (Padding Steganography)

PadSteg falls under the category of Inter protocol steganography i.e it uses more than one protocols from TCP/IP. In this method the padding bits of Ethernet frames is replaced with the steganogram. Because of the Etherleak it the normal receiver will not feel important to detect PadSteg reason for the Eatherleak is varying standardization in padding.[5,1]

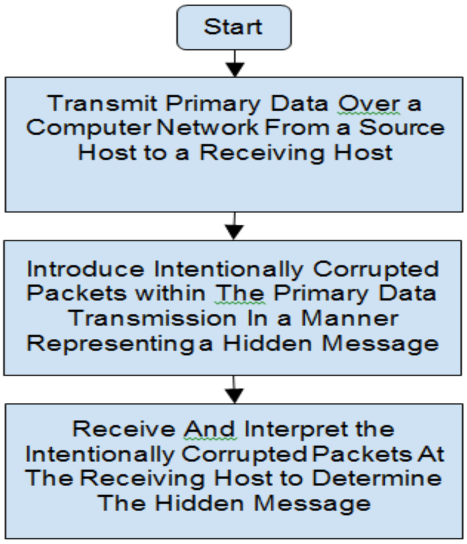
Start
Transmit Primary Data Over a Computer Network From a Source Host to a Receiving Host
Introduce Intentionally Corrupted Packets within The Primary Data Transmission In a Manner Representing a Hidden Message
Receive And Interpret the Intentionally Corrupted Packets At The Receiving Host to Determine The Hidden Message

Fig 2 Process followed in HICCUPS[1]

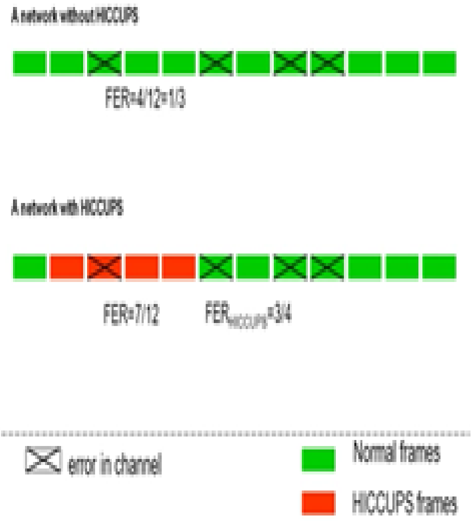

Fig. 3 Influence on frame error rate in HICCUPS[2]

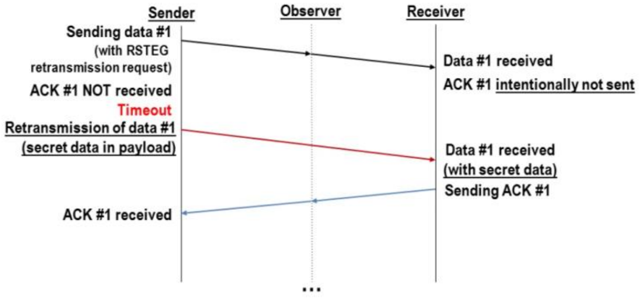
Sender
Observer
Receiver
Sending data #1 (with RSTEG retransmission request)
Data #1 received
ACK #1 intentionally not sent
ACK #1 NOT received
Timeout
Retransmission of data #1 (secret data in payload)
Data #1 received (with secret data)
Sending ACK #1
ACK #1 received
...

Fig. 4 Transmission flow in RSteg[2]

2.6 TranSteg (Transcoding Steganography)

Similiar to LACK this method also uses IP telephony. TransSteg is one of the best available methods out of all VoIP methods this method is really efficient and good because in all other methods the steganogram can be received and extracted at the receiver but the original data in which the steganogram is present cannot be restored but in case of TranSteg the original data is also restored after the extraction of the steganogram. In this method the open data is compressed which makes space for the steganogram and at the receiver end the steganogram is extracted and the original data is restored.[9,1]. In the Fig. 5 below we can see that the voice data content in original voice packet is around 20-30ms which then is compressed during transcoding process to make space for the secret message. Because of the compression of the original data leads to change in the checksum so the secret data is inserted in such a way that the original checksum remains unchanged. After maintaining the same checksum and inserting the secret message/steganogram the transcoded audio packet is to be transmitted to receiver considering Alice as sender/transmitter and Bob as receiver at the sender end the size of RTP payload is intentionally kept greater than the inserted voice payload the transmission process is depicted in the Fig. 6. For extraction of the transcoded message the packet is picked with the transcoded steganogram and the data is extracted as shown in Fig. 7.

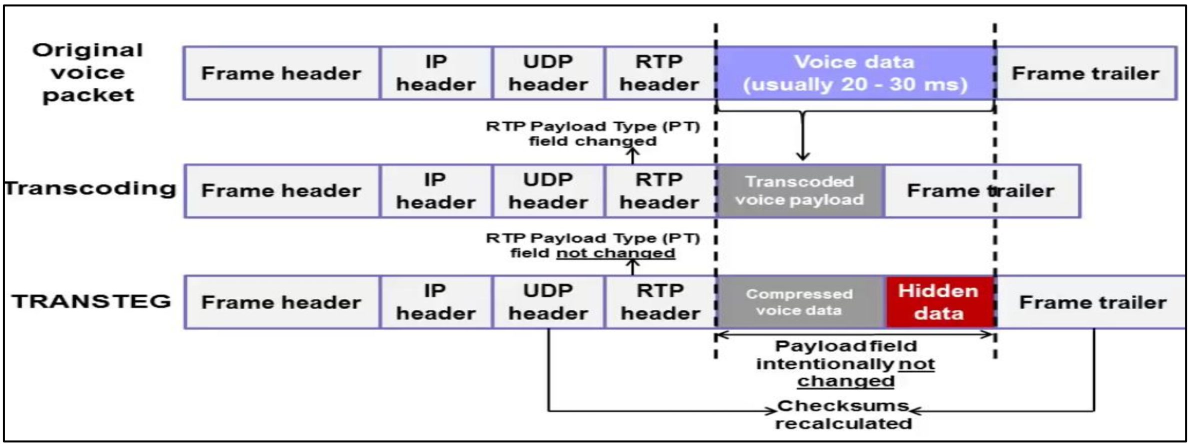

Fig.5 Step 1 in TranSteg[2]

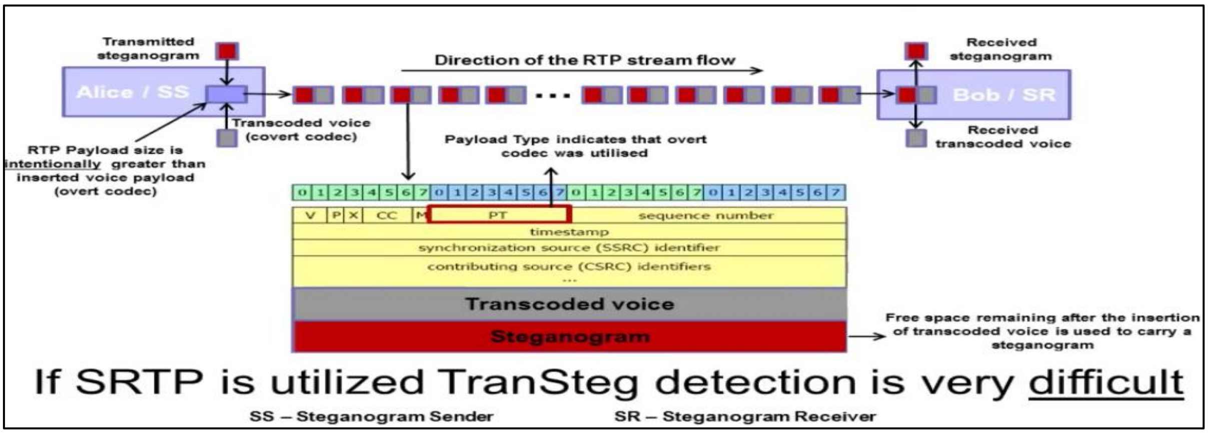
Transmitted steganogram
Direction of the RTP stream flow
Received steganogram
Alice / SS
Bob / SR
Transcoded voice (covert codec)
Received transcoded voice
RTP Payload size is intentionally greater than inserted voice payload (overt codec)
Payload Type indicates that overt codec was utilised
0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7
V P X CC M PT sequence number
timestamp
synchronization source (SSRC) identifier
contributing source (CSRC) identifiers
...
Transcoded voice
Steganogram
Free space remaining after the insertion of transcoded voice is used to carry a steganogram
If SRTP is utilized TranSteg detection is very difficult
SS – Steganogram Sender
SR – Steganogram Receiver

Fig.6 Step 2 in TranSteg[2]

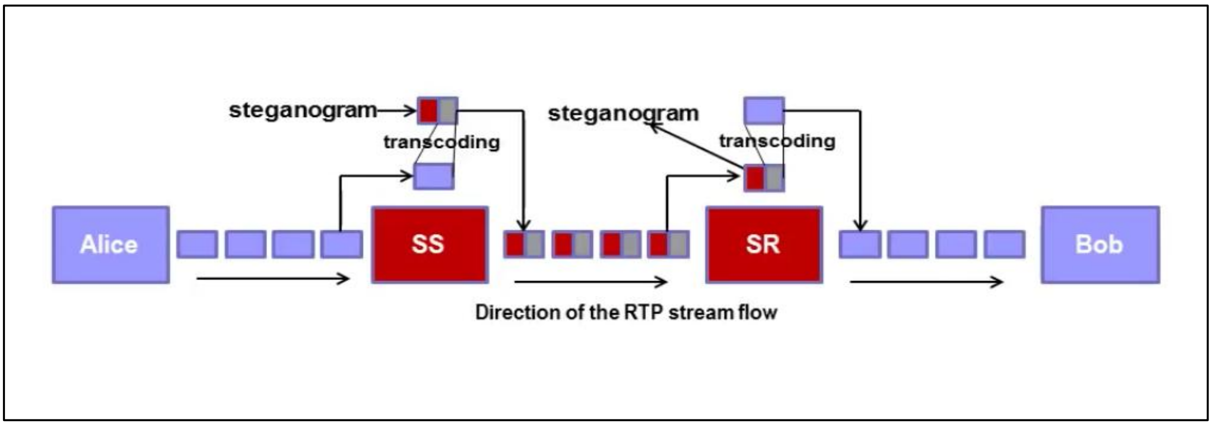

Fig.7 Step 3 in TranSteg[2]

2.7 SkyDe(Skype Hide)

Skype is a P2P service which uses IP telephony in this transmission there are various silent packets or packets not having any voice signals in them SkyDe replaces those silent packets with the secret message with a very minimal distortion the transmission. This method is really hard to detect and also provide a very good bandwidth for the data transmission.

2.8 StegTorrent

StegTorrent 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 StegTorrent both sender and receiver of secret information uses IP addresses known to each other. The sender uses modified bittorrent client for sending the information which is then received by using StegTorrent client.

2.9 StegSuggest

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[8]. Whenever we type any search term in the google text bar it sends HTTP GET request every time to fetch the suggestion so those suggestions can be used for transmitting the secret information by suffixing a letter after each word in the suggestion this process works as shown in Fig. 8. It is clear from Fig. 8 that for each letter the google client sends HTTP GET request to the google server to send the suggestion based on that word. During this process of sending and receiving the HTTP GET ,an steganogram sender and receiver is in introduced as shown in Fig. 9. The google suggest server is used as the carrier of the hidden/secret information. for this the network node must be same for both SS and SR. To use this process every time the SR searches a term SS transmits a word with every suggestion sending a complete message.

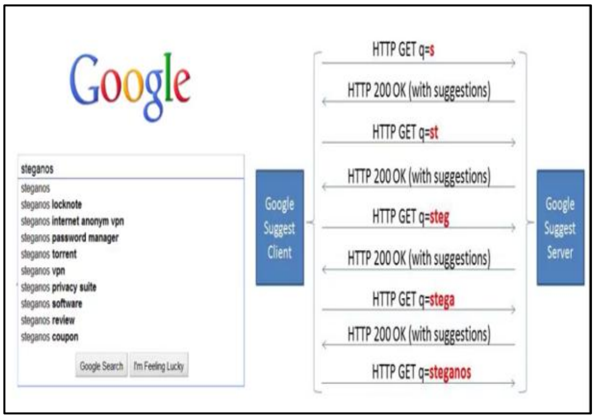

Fig.8 StegSuggest method[2]

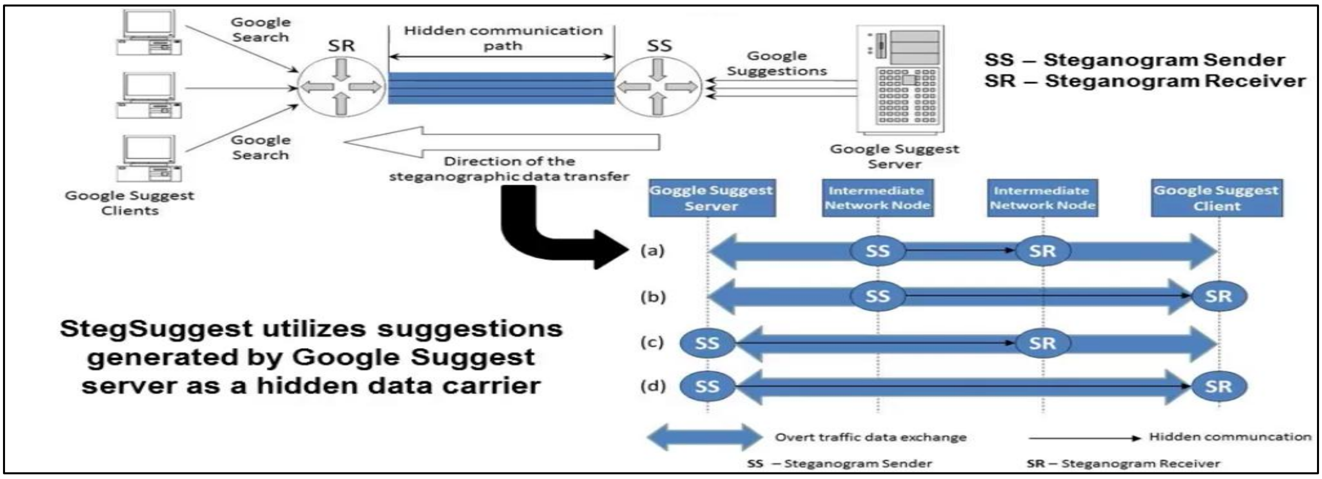
Google Search
SR
Hidden communication path
SS
Google Suggestions
SS – Steganogram Sender
SR – Steganogram Receiver
Google Search
Google Suggest Server
Direction of the steganographic data transfer
Google Suggest Clients
Goggle Suggest Server
Intermediate Network Node
Intermediate Network Node
Google Suggest Client
(a)
SS
SR
(b)
SS
SR
(c)
SS
SR
(d)
SS
SR
StegSuggest utilizes suggestions generated by Google Suggest server as a hidden data carrier
Overt traffic data exchange
Hidden communcation
SS – Steganogram Sender
SR – Steganogram Receiver

Fig.9 Process involved in StegSuggest method[2]

Table1 Comparison among different methods of network steganography.

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

3. RELATED WORK

In [11] Jun O Seo et.al. gave the concept for the design of network steganography. Design contained cyclic model of three processes- location identification, steganogram concealment and Validation. Location identification defines how to have the insight of the protocol and its related areas to be exploited as cover channel. Second step is bifurcated into storage and timing based types categories. It defines embedding mechanism or altering mechanisms for a steganogram. Third step of validation checks whether the applied technique of steganography conforms to the attributes of the network steganography.

3.1 Storage Based Covert Channel

StegBlock [12] approach defined by Wojciech Fraczek and Krzysztof Szczypiorski for an undetectable communication. Their work exploits the main attribute of undetectability. StegBlocks are the carriers that carry objects (identifiers) but the number of identifiers are limited. Identifiers are merged in sequences called blocks. Blocks are assigned values depending on last bits of the number of objects in that block. Value of block indicate hidden message bits. Perfect undetectability for the StegBlock concept is taken from Cachin[13]. But this approach has limited practical applications.

In the work of paper [14], the proposed technique can cope up with anomaly detection methods in a traffic without traffic overhead. It uses parity of payload, count the number of zeroes and ones of packet and then alter their size to either even or odd count. The payload parity bit covert channel was found to be infeasible. For that purpose two different covert channels are introduced- Packet Payload Byte Parity and Alternative Packet Payload Bit Parity. These covert channel use byte or bit count respectively. Results show resilience to detection instead of low bandwidth.

Anand S. Nair et.al. [15] proposed a more secure scheme which modifies the length of UDP datagram and then embed the secret data into it. This algorithm tries to overcome the limitations of all existing length

based embedding algorithms. It exploits the random pattern feature of UDP datagram length, which makes it apt for steganographic purpose. Result findings show that the scheme follow normal traffic flow after embedding.

Aoki[19] introduced enhanced Packet Loss Concealment(PLC) feature to VoIP protocol as network steganographic technique. Forward packet pitch variations are embedded into the current packet. Dropped packets are kind of recovered by the approximation analysis of forward packet from current packet.

In paper [20] Miao and Huang suggested that the LSB (Least Significant Bit) technique is not suitable for flat blocks of voice samples, but could be considered for sharp blocks. Flat blocks LSB embedding decreases sound quality and could be easily detected. On the contrary, manipulations in the LSB of high amplitude voice could be more frequent and secure.

To resist detectability in limited bandwidth is an important aspect in network steganography. This work idea is implemented by Mazurczyk et.al. [21] through transcoding. Transcoding replaced original codec with another codec which seems like the original codec. This technique allows more storage of information as compared to other techniques.

Frczek [23] proposed steganography approach for SCTP (Stream Control Transmission Protocol) by using two features as- multihoming and multistreaming. In multihoming, packet from a specific IP address is addressed as'0' while from another IP is addressed as'1'. In multistreaming, one bit is associated with each stream for encoding purpose. After embedding streams are altered.

Many other approaches [23][24][25] proposed steganographic method to hide secret message into the identification field of IP packet header. This allows to add 16 bits per packet. Drawback of the approaches include loss of data due to fragmentation or repetition of secret data due to same IP Id of fragments. These drawbacks result in errors in steganography.

3.2 Timing Based Covert Channel

In this type, the packet timings are varied in order to create covert channel. These channels are more complex than storage type covert channel [10].

The predetermined time limit based technique[16], in which the packet has to be received within the defined time. Presence and absence of packet is mentioned in the form of '1' and '0' respectively. The approach is effective but lacks channel synchronization which makes the network condition unpredictable. Also, carrier capacity is low.

[17] defines multipath embedding scheme. This scheme is an improvement over all existing problems in timing covert channels. Problems are found to be with channel capacity (low), error rate (high) and covertness. The approach defines two different paths i.e. a location or a port. On modifying either location or port, the secret message could be conveyed.

[18] suggested a timing based type covert channel by employing a passively working physical device named Jitter Bug. This keylogging device is implanted on to connections and keystrokes are recorded. Secret message is sent by expanding delays in each keystoke.

4. CONCLUSION

Network Steganography is one of the most sophisticated and vast steganography method having ample number of ways to transmit the secret information without any specific need of physical cover objects like Image, Video etc. These 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. In fact as compared to other techniques where only the message is retrieved at the receiver's end and cover is distorted and destroyed it is possible to retrieve both message and carrier in case of the network steganography TransSteg is the most efficient technique for doing so. This paper clarifies the various methods along with the survey of different approaches being used for steganography using network as covert channel. This proves that the technique is quite impressive and has significant advantages over other cover objects. The concepts of concealment, robustness imperceptibility are conformed in the network steganography.

5. REFERENCES

[1] Amritha Sekhar, Manoj Kumar G., Prof. (Dr.) M. Abdul Rahiman, A Study on Network Steganography Methods, International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), International Conference on Recent Trends in Computing and Communication (ICRTCC 2015), Cochin College of Engineering & Technology, Vol. 4, Special Issue 1, June 2015.

[2] Network Steganography http://stegano.net/network-steganography.html (last accessed 6 august 2017).

[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] W. Mazurczyk and K. Szczypiorski, Steganography of VoIP Streams, In: Robert Meersman and Zahir Tari (Eds.): OTM 2008, Part II - Lecture Notes in Computer Science (LNCS) 5332, Springer-Verlag Berlin Heidelberg, Proc. of On The Move Federated Conferences and Workshops: The 3rd International Symposium on Information Security (IS'08), November 9-14, 2008, pp. 1001-1018.

[5] B. Jankowski, W. Mazurczyk, K. Szczypiorski, Information Hiding Using Improper Frame Padding - 14th International Telecommunications Network Strategy and Planning Symposium (Networks), 2010.

[6] W. Mazurczyk, M. Smolarczyk, K. Szczypiorski, RSTEG: Retransmission Steganography and Its Detection, In: Soft Computing in 2010, ISSN: 1432-7643 (print version) ISSN: 1433-7479 (electronic version), Journal no. 500 Springer.

[7] 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.

[8] P. Białczak, W. Mazurczyk, K. Szczypiorski, Sending Hidden Data via Google Suggest, In Proc. of: Third

International Workshop on Network Steganography (IWNS 2011) co-located with The 2011 International Conference on Telecommunication Systems, Modeling and Analysis (ICTSM2011), 2011.

[9] W. Mazurczyk, P. Szaga, K. Szczypiorski, Using Transcoding for Hidden Communication in IP Telephony - In: Computing Research Repository (CoRR), November 2011.

[10] Jun O Seo, Sathiamoorthy Manoharan, Aniket Mahanti; network Steganography and Steganalysis- A Concise review; 2nd International Conference on Applied and Theoritical computing and Communication Technology (iCATccT), 2016 IEEE.

[11] Jun O Seo, Sathiamoorthy Manoharan, Aniket Mahanti; A Discussion and Review of Nwtwork Steganography; 14th Intl. Conf. on Dependable Autonomic and Secure Computing, 14th Intl. Conf. on Pervasive Intelligence and Computing, 2nd Intl. Conf. on Bigdata Intelligence and Computing and Cyber Science and Technology Congress, IEEE 2016.

[12] Wojciech Fraczek, Krzysztof Szczypiorski; StegBlocks: ensuring perfect Undetectabilityof Network steganography; 10th conference on Avialability, Reliability and Security,IEEE 2015.

[13] Cachin C; An Information Theoratic model for Steganography, In proc. Of 2nd Intl. Workshop on Information Hiding,1998,pp 306-318.

[14] Osamah Ibrahim Abdullaziz et.al.; Network Packet Payload Parity Based Steganography ; IEEE Conference on Sustainable Utilisation and Development in Engineering and Technology ;2013.

[15] Anand S nair et.al.; Length Based Network Steganography using UDP Protocol;3rd International Conference on Communication Software and Networks, IEEE 2011.

[16] S. Cabuk, C. E. Brodley, C Shields; IP Covert Timing Channels:Design and Detection" In Proceedings of 11th ACM conference on Computer and Communications Security CCS '04, 2004.

[17] H. Hovhannisyan, K Lu , J Wang; A Novel High Speed IP- timing Covert Channel: Design and evaluation; in Communications (ICC) 2015 IEEE, pp7198-7203.

[18] G Shah, A. Molina, M Blaze; Keyboards and Covert Channels; In proceedings of 15th Conference on Security Symposium, USENIX –SS'06, 2006.

[19] N. Aoki; A Packet Loss Concealment Technique for VoIP using Steganography; Citeseer.

[20] R. Miao, Y. Huang; An approach of Covert Communication based on th Adaptive Steganography Scheme on Voice over IP in Comunications(ICC) IEEE proceedings, 2011.

[21] W. Mazurczyk et.al. ; Using Transcoding for Hidden Communication in IP Telephony, Multimedia Tools and Applications, 2012.

[22] W. Frczek et.al.; Hiding Information in a stream Control Transmission Protocol; Elsevier, 2012.

[23] C H. Rowland ;Covert Channel in the TCP/IP Protocol Suite; Peer reviewed journal on internet, 1997.

[24] D.D Dhobaje et.al.; Steganography by Hiding Data in TCP/IP headers; PVPIT pp 61-65, 2010.

[25] R.M. Goudar et.al.; Secure Data Transmission using Steganography based Data Hiding in TCP/IP; International Conference and Workshop on Emerging Trends in Technology, 2011.