An Overview of Advanced Network Steganography

Maitrik K Shah
Assistant Professor
Indus University, Rancharda,
Gujarat, India

Ankitkumar M. Virparia
Assistant Professor
Indus University, Rancharda,
Gujarat, India

Kamal Sharma
Assistant Professor
Indus University, Rancharda,
Gujarat, India

ABSTRACT
Steganography is the art and science of hiding the information in the carrier object. The main objective of steganography is to hide the existence of data. Lots of advancements has been done in the use of carrier medium, started from image, sound, video and network packets and protocols. Information hiding inside image, audio and video is often called digital steganography whereas if network packets and/or protocols are used then it is called network steganography. Using this technique we can send small amount of information confidentially. Here in this paper, various approaches towards network steganography and current status of research in this field are discussed.

Keywords
Steganography, Network Steganography, Network Protocols, Covert communication, covert channels, information hiding.

1. INTRODUCTION
Cryptography aims to making the information so complex by encrypting it so that the unauthorized user can't understand what is being sent. However it is possible for the attacker to get the existence of the secure channel and can decrypt the information. Steganography, in contrast, hides the existence of the message. The message can be hidden in the carrier medium. Here, the carrier medium can be anything like image, audio, video, network protocols, etc. Network steganography uses network protocols as a carrier medium. Basically network steganography can be classified into 3 main ways:

1. Modify the structure of Network protocols' header and payload
2. Modify the structure/sequence of packet streams
3. Hybrid schemes

The first way uses the structure of network protocols' header. These headers contain number of fields that are required for the correct delivery of the packet from source to receiver. Many of these fields are unused in the normal transmission or used sometimes during specific network conditions. So these fields can be a proper carrier to carry the information in the hidden manner. The very first approach to use protocol header was suggested by Craig H. Rowland [1]. He had used identification field of IP header for covert communication in 1997. He also suggested the use of ISN(Initial sequence number) field of TCP header for hiding the data. Other methods of network steganography which uses network protocols are suggested in [2]. Here the author has used 2 bits of type of service field of IP header and 6 unused bits of TCP header. In [3] author has used the etherleak problem. To maintain the minimum length of frame padding bits are added in the Ethernet header. These padding bits are sequence of 0s but some NICs improperly append random bits which is considered as special case. Author has used this vulnerability to send hidden data in the padding bits. Here author has used ARP and TCP protocols to hide the data. In [4] author has used options field of IP header to hide the data.

The second way makes the use of sequence and structure of packet streams. In [5] author has used oversized data packets to send hidden data. If packet is very big then it will be fragmented. Here, if number of fragments are even then it carries hidden 1 and if number of fragments are odd then it carries 0. So only 1 bit/ packet can be transmitted hiddenly. In another method author has used fragmentation offset field of IP header. If its value is even then hidden bit 1 otherwise 0. The fragmentation offset of first fragment of the packet will always be 0 which will not carry any hidden bit but rest of the fragments will. Here, number of bits per packet that can be send in hidden manner is $n_f - 1$. Where n_f = number of fragments of that packet. In [6] author has used packet payload of packet. Here, based on the number of 1s and 0s of packet payload size of packet will be modified to deliver '0' or '1' of the secret message.

The third way combines previous two approaches. In the following sections we will describe few more and advanced approaches to network steganography.

2. APPROACHES TO NETWORK STEGANOGRAPHY

2.1 PADSTEG (Padding based Steganography)
It is the first interprotocol steganography which uses mere than one protocol from TCP/IP stack. It uses ARP and TCP protocols with etherleak vulnerability to implement secret communication. Few protocols in the protocol stack has restriction on the size of frame/packet. To maintain the size of frame padding bits are appended with the original frame. Generally these padding bits are sequence of 0s and added by NIC or software. Few NICs sometimes add other bit sequence than 0s in padding to maintain the minimum size of the frame. Author has made use of this vulnerability to send hidden data as padding bits and because of etherleak problem this will be considered as normal scenario. It means presence of hidden bits will not be revealed. Padsteg works in 2 phases.

- In first phase nodes advertise themselves as hidden node.
- In second phase actual hidden data transfer occurs.

In the first phase random number is inserted in the Ethernet frame padding and hash value is calculated based on the source MAC to announce its existence as hidden node. In the second phase during connection establishment improper frame padding is inserted during TCP ACK segment as shown in the figure.

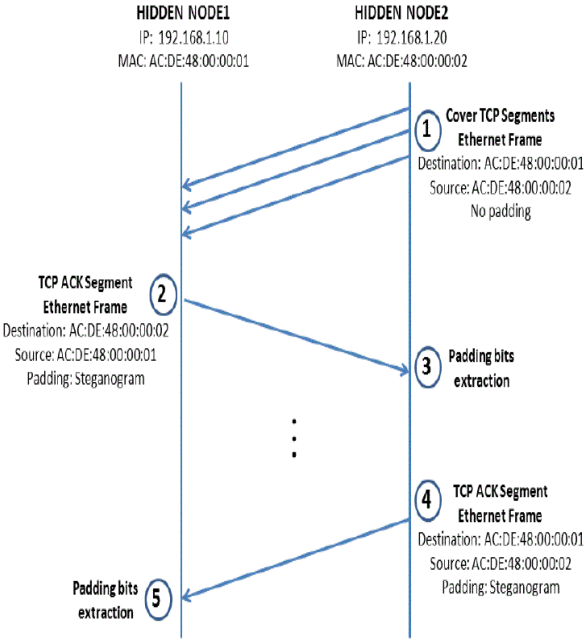

Fig 1: Hidden data exchange [3]

Padsteg can also be called as interprotocol based steganography because it involves more than one protocol(ARP and TCP) for hidden exchange. Here the steganographic bandwidth is 27bits/s which is good as compared to other steganographic approaches.

2.2 HICCUPS: Hidden Communication system for CorrUPed Networks

This steganographic system is intended to shared medium networks including wireless local area networks. It uses telecommunication system with cryptography to provide steganographic system. In particular, wireless area networks use air connection with variable bit error rate (BER) that creates opportunity to inject "synthetic" corrupted frames. Here, the system works with the assumption that the possibility of frame's interception in shared medium. It is possible to create 3 hidden data channels (HDC).

HDC1: Channel based on cipher's initialization vector
HDC2: Channel based on MAC address
HDC3: Channel based on integrity mechanism values

HICCUPS works in 3 phases as shown in the figure.

- The first phase is the system initialization in which all stations included in hidden group establishes secret key for ciphers embedded in cryptographic system. The system can be used in any unicast, multicast or broadcast environment.
- The second phase is the basic mode in which data exchange happens based on cipher's initialization vector (HDC1) and MAC addresses (HDC2).

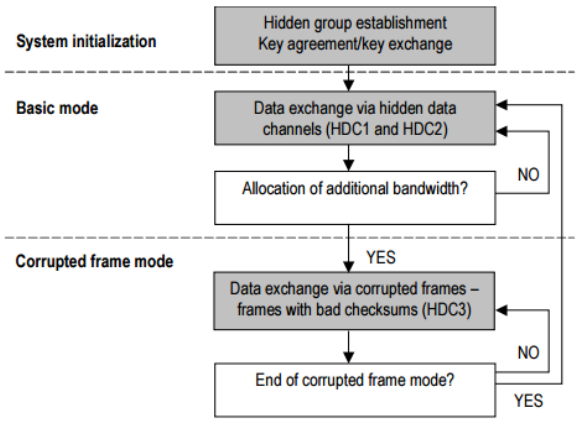

Fig 2: HICCUPS operation scheme [7]

- In the third phase which is corrupted frame mode information is exchanged with intentionally created bad checksums (HDC3). The stations which belong to hidden group accepts bad checksum as hidden data whereas other stations remove the packet because of bad checksum.

This system can be applied to wireless cryptosystems which works in the environment which is susceptible to interception.

2.3 TCP SQN as REFERENCE MODEL

In this technique sequence number field of TCP header is used as a reference to send hidden data. If SYN flag is set this field contains initial sequence number. If the flag is not set then it contains sequence number of accumulated data. Here, sender will not put any data in this field or do not modify the working of this field. Instead sender uses this field as a reference to send hidden message from sender to receiver. As sender does not modify working of this field it will become hard for third party to distinguish overt and covert communication.

TCP SQN field will be filled by the sequence number generated by the system kernel. This will ensure that the ISN generated by the system will look like it is generated by some normal system. To convey covert data TCP payload is used, which contains key. This key can be used to extract hidden data from the TCP SQN field. To make it more secure this key will be divided into number of bytes and it will be places into different positions in the payload which works as data pointers. These pointers contain symbols from the symbol table which can be used in cover communication [8].

2.4 CLACK: Covert channel based on partiaL ACK

It is a storage based covert channel which encodes message in TCP data channel and provides reliable and resilience covert channel to adverse network conditions. Here the messages are encoded in TCP acknowledgement field. Following is the functionality at sender and receiver side. Here, since the message is encoded in the ACK encoder is receiver and decoder is sender.

CLACK Encoder:

Here encoder sets its receiver size equal to effective MSS which limits the number of data segments sent each time to one. Here the assumption is encoder receives single full sized data segment which is shown in fig 3(b)(c).

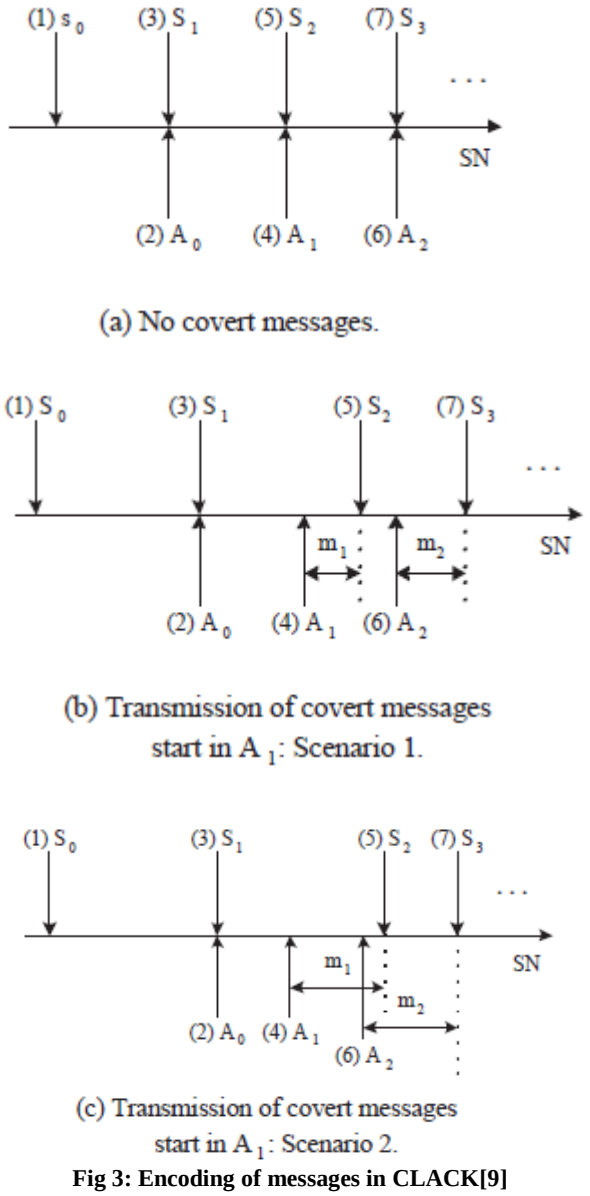

Fig 3: Encoding of messages in CLACK[9]

Figure 3(a) shows the scenario when no covert message is transmitted. Partial ACks can be given by $a_i = s_{i+1} – m_i$ where, a_i is the value of A_i, s_i is the sequence number of S_i and m_i is the value of M_i. After receiving partial ACK sender sender sends new data segment to fill up the sender window.

CLACK Decoder:

Here, the decoder keeps track of SND.NXT and SND.UNA variables which are the sequence number of next data segment to be sent and oldest unacknowledged sequence number respectively. By examining the SN and packet length decoder is required to update the value of first variable. In case of partial ACk decoder extracts the covert message from SND.NXT – a_i.

2.5 RSTEG: Retransmission based STEGanography

This technique works on the concept of retransmission in TCP. It is basically a hybrid approach which uses modification to payload and sequencing of packets. After sending the segment if acknowledgement /cumulative acknowledgement is not received of that segment then sender is required to retransmit the segment. Author has used this property of TCP protocol to send the hidden data. Even after receiving the segment successfully the receiver intentionally does not generate the acknowledgement due to which sender's clock for that segment gets expired and sender is expected to retransmit the segment. In RSTEG instead of sending original segment again sender replaces it with the segment which contains hidden data.

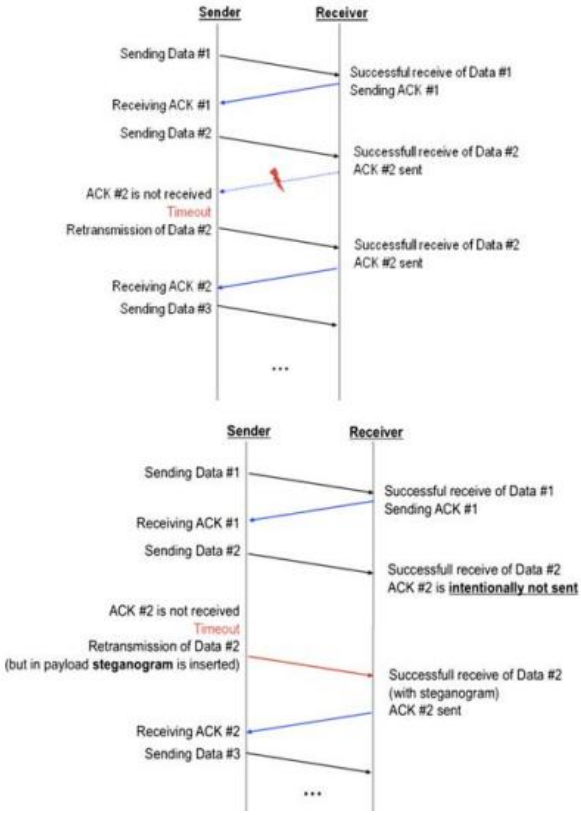

Fig 4: Normal retransmission vs Stegno retransmission[10]

Sender will mark the segment after which it will send the segment with hidden data. This marking is done by the following equation.

$$IS = H(SK||SN||Checksum||CB)$$

SK = the stegkey which is assumed to be with sender and receiver secretly.
SN = sequence number
Checksum = TCP checksum
CB = Control bit, 1 if sender wants to mark it otherwise 0
IS = Identifying sequence

All IS bits are distributed in the payload in predefined fashion. Receiver calculates IS for each incoming segments for CB=0 and CB=1 and checks it with the IS value in payload. If it matches with IS value when CB=0 then normal transmission will occur otherwise stegnographic transmission will occur where receiver intentionally does not send ACK for that

segment. Author has also given solution to the problem if the segment which is marked is lost. This method can be detected if intentional retransmission occurs frequently and in excessive manner. It should be kept at reasonable level.

3. SUMMARY

The following table gives summary of all the approaches presented in this paper along with their limitations. Here, the class is the method in which particular approach belongs. Classification of approaches to network steganography is given in the introduction part of this paper.

Approach	Class	Description	Limitation
PADSTEG	I	• Uses vulnerability in the ethernet padding which is known as Etherleak • Uses ARP and TCP protocols	• This method can be used in LAN only • If all NICs generate sequence of 0s in the padding then this method can not be used
HICCUPS	I	• Uses 3 different channels • Uses frames with bad checksum for bandwidth allocation	• Limited to corrupted networks in which generation of bad checksum in frame is normal
TCP SQN as Reference	I	• Uses TCP SQN field as reference • Payload will contain key which tells which bits form SQN gives hidden data	• Here the key is distributed in the payload. • Sharing of these positions of key in payload is assumed.
CLACK	II	• Uses TCP ACK field	• Difficulty of keeping states about the connection
RSTEG	III	• Uses retransmission concept of TCP • Intentionally invokes retransmission	• Can be detected if statistical steganalysis is done on network
		by not sending acknowledgement	retransmission rate

4. CONCLUSION

In this paper we have presented a summary of different network steganographic approaches. These advanced approaches presents good steganographic bandwidth and security. Network steganography is evolved in recent years which gives new ways to hide the data and provide covert communication. This can be a threat to the network security if these techniques are used for malicious activities like distribution of confidential information to the unauthorized party. It can also be used for tools to inject warms and viruses to the system. In addition to that current security systems do not provide sufficient countermeasures.

4. REFERENCES

[1] C. Rowland 1997. Covert channels in TCP/IP protocol suite. Peer reviewed journal on Internet, January 1997.

[2] Theodore G. Handel, Maxwell T Sanford, "Data hiding in the OSI Network model", First International workshop on Information Hiding,

[3] Bartosz Jankowski, Wojciech Mazurczyk, Krzysztof Szczypiorski. Information Hiding Using Improper Frame Padding. Telecommunications Network Strategy and Planning Symposium (NETWORKS), 2010 14th International

[4] Shah, M.K. and Patel, S.B, "Network based packet watermarking using TCP/IP protocol suite," NUiCONE, Nirma University, IEEE 2011

[5] IWojciech Mazurczyk and Krzysztof Szczypiorski, "Steganography in Handling Over- sized IP Packets". Proc. Int. Conf. Multime. Inf. Network Security MINS-2009.

[6] Osamah Ibrahiem Abdullaziz, Vik Tor Goh,Huo-Chong Ling and KokSheik Wong, Network Packet payload parity based Steganography, 2013 IEEE conference on sustainable utilization and development in Engineering and Technology

[7] K. Szczypiorski, "HICCUPS: Hidden Communication System for Corrupted Networks," Proc. 10th Int'l. Multi-Conf. Advanced Computer Systems, Oct. 2003, pp. 31–40.

[8] Dhananjay M Dakhane, Dr Prashant R Deshmukh, "New approach towards covert communication using TCP SQN reference model", International journal of innovative research & development, September 2014, Vol 3 Issue 9.

[9] X. Luo, Edmond W. W. Chan, and Rocky K. C. Chang, "CLACK: A network covert channel based on partial acknowledgment encoding," IEEE International Conference on Communications, pp. 1-5, 2009.

[10] Mazurczyk, W., Smolarczyk, M., Szczypiorski, K. (2009) Retransmission steganography and its detection. vSoft Computing, Journal no. 500 Springer, ISSN: 1432-7643 (print version), ISSN: 1433-7479 (electronic version), November 2009