Grenze International Journal of Engineering and Technology, January Issue

Developing a Covert Communication Paradigm using TCP's Sequence Number

Shashikant Sukalal Mahajan[1] and Dr. Sunil Arvind Patekar[2]
[1-2] Department of Computer Engineering, Vidyalankar Institute of Technology, Wadala, Mumbai, India
Email: shashikant0320@gmail.com, sapatekar@gmail.com

***Abstract*—In today's digital era, advancement in hardware and software leads to developments in digital communication which results into huge information generation per second. While transmitting information inside LAN or through the Internet it may be exposed to a baleful person and results in to be stolen, altered or damaged represented as real threats to transport process and also to information especially if this information is sensitive. And this information must be accessed by only authorized person. Therefore, data transmission must be secured against such threats. There were many ideas suggested under security concept for protecting data from these threats such as encrypting the content of the message sent which is called as cryptography or the concealment of the important message by existing message which was named steganography. In this paper, covert communication channel is established by using the header field of TCP/IP protocol suit. Source port Number and destination port number field of the TCP protocol is exploited to send the secret message as a sequence number.**

***Index Terms*— steganography, cryptography, covert channel, TCP/IP protocol, hidden data, overt communication, covert communication.**

I. INTRODUCTION

Around 1980, After computer appearance in most institutes like companies, universities, and homes, the Computer Network start to evolve. Since these places had limited hardware resources like printers and having different branches distributed in different places, the individuals really need to communicate and at the same time to exchange important information to do their work. So, the need to connect these institutes by network became necessity [1]. Network in simple case which connects at least two computers for transmitting and sharing information. Network may be built in homogeneous form (i.e. same operating system, Network Interface Card (NIC) … etc for all network computers) like Local Area Network (LAN's) or in heterogeneous form i.e. different operating system running on networked computers, like network of network - Internet. The need for computer networks arose significantly during the 1990s due to several key factors like Expansion of the Internet, Advancements in Technology, Client-Server Architecture, Rise of Personal Computers and Mobile Devices. The necessity for computer networks became especially pronounced during the 2000s due to Internet Expansion, Communication and collaboration, and Entertainment and Media. As a result, these developments in communication lead to exchange huge information. While transmitting information inside LAN or through the Internet it may be exposed to a baleful person and results in to be stolen, altered or damaged represented as real threats to transport process and also to information especially if this information is sensitive. And this information must be accessed by only authorized person. Therefore, data transmission must be secured against

Grenze ID: 01.GIJET.11.1.226

such threats. There were many ideas suggested under security concept for protecting data from these threats such as encrypting the content of the message sent which is called as cryptography [2] or the concealment of the important message by existing message which was named steganography[3].
Around the year 2010, myriad of applications and services like Proliferation of Mobile Devices, Rise of social media, Cloud Computing Boom, Big Data and Analytics, and Advancement in streaming services that had become integral to personal, social, and professional life. These things collectively highlighted the critical role of computer networks in maintaining societal functions during the pandemic, driving their rapid development and deployment to meet emerging demands.
However, sometimes, the onset of communication is sufficient to discover the organizational structure and here cryptography does not prevent the onset of communication activity. Typically, the communication channel can be broadly divided into two distinct categories: Overt communication channel and covert communication channel. Overt communication channel is the legitimate channel intended to carry sensitive information subjected to communication policies. While Covert channels involve using legitimate communication channels (i.e. overt channel) in unintended ways to transmit secret information. Covert channels become useful when the users like Government agency, criminals; terrorist organizations, etc. have an interest to keep their communication secret and want to hide their existence. For these types of user's detection of the onset of activity would be harmful for their secret movement.
This paper shows how network steganography can be implemented by using TCP/IP network protocols to establish covert channel for covert communication. Here TCP protocol header is used for implementation of steganography in the proposed system.

II. Literature Review

Rowland used Initial Sequence Number Field (ISN) of TCP for hiding the information. It was done by multiplying ASCII of each character with (65536 * 256) to generate number which was placed as sequence number value for each connection. On the receiver side, opposite process applied to get the character by dividing sequence number's value on (65536 * 256). The big disadvantage, when every character is transferred through a connection, is that many requests was made to connect to the server without receiving SYN/ ACK packet would attract the attention [10].
Joanna implemented steganography by changing the sequence number field in the packet which is generated by compromised the system using NUSHA tool. NUSHA sender did not generate its own packet, but instead it modifies the sequence number and the acknowledgement number that were generated by the operating system by saving the TCP state, so when packet with the modified initial sequence number was sent, the original initial sequence number was stored and when a reply was received which included the acknowledgement number (modified sequence +1), it must be replaced with the original sequence +1. This made NUSHA process complicated since it must store every sequence and acknowledgement numbers. In other side, recipient could be applying a simple sniffer by staying on trusted gateway or using technique that force traffic toward its interface network card to capture all the packets [11].
Ciobanu suggested SCONeP (Steganography and Cryptography Over Network Protocols) and using ISN (Initial Sequence Number) after solving the issue which appeared in [10] by sending RST (Reset) packet to abort a connection instead of ACK packet after 4-bytes will be transmitted. Identification field was also used after DF(Don't Fragment) -bit was assigned to 1 to avoid modifying it by kernel since it must have value (1) when packet do not need fragmentation [12].
Abeer implemented steganography by using source port number and destination port number and both concatenated to form string of 32 bit to generate a sequence number by xor operation with 4 byte data.

III. Motivation

Information exchanged over a Local Area Network (LAN) or the Internet may be vulnerable to theft, alteration, or damage by malicious parties who pose a real threat to the information being transported and its integrity, particularly if the information is critical, sensitive, and should only be accessed by those with the proper authorization. Thus, it is necessary to protect sensitive data from these dangers. Many suggestions were made under the security concept to safeguard data from these hazards, like steganography, which conceals the existence of such messages, and cryptography, which hides the content of conveyed messages.
It was suggested to hide this data in two methods. One of them employed the Transmission Control Protocol (TCP) header's source and destination ports as the Stepgo key. The other method combines the protocol and

version fields of the Internet Protocol (IP) header with the source and source port fields of the Transmission Control Protocol (TCP) header. The application of the exclusive OR (XOR) between the data that must be hidden with the STEGO key serves as a summary of the procedure. The Transmitter Control Protocol (TCP) sequence number field was chosen to be the carrier for hidden data. This field contains four characters, which are transferred in a single connection.
The proposed approaches are not the same as the current approaches. In contrast to the suggested ways, which send four characters, one of them sent just one character over a single connection. Apart from this variation, there was also a variance in the stego key that was utilised. due to the fact that the ASCII character code will be used to collect the constant value. In contrast, the suggested solutions use XOR instead of a collection procedure and variable values. Even if four characters were transferred using the other techniques, their execution required a lot of resources due to the characters' compression and encryption.

IV. Problem Domain

Steganography and Cryptography
From the ancient era, steganography has remained a fascinating and often secretive means of communication, with its techniques evolving alongside advancements in technology and cryptography.
The modern cryptography gets evolved during the 1970s, with significant contributions from researchers. Whitfield, Martin Hellman, and Ralph introduced the concept of public-key cryptography and laid the groundwork for secure key exchange protocols [4].
Recently, with the emergence of computer Networks and Information Technology, hiding information takes another direction by using text, image, audio and video which represents suitable carrier for transferring secret information. Also, the protocol header of TCP/ IP protocol suite can be utilized to hide and transfer the secret message. This is known as Network Steganography [5] and was introduced firstly by Krzysztof Szczypiorski in 2003 through implementing hidden data in HICCUPS (HIdden Communication system for CorrUPted networkS), a steganographic system dedicated to shared medium networks including WLANs with the novelty using cryptographically secure telecommunications network to provide steganographic technique with bandwidth allocation based on corrupted frames [6]. In 1973, a concept of covert channel was introduced by Lampson which provides utilizing unused field of network protocols [7]. This concept enables researchers to create carrier for hiding information. For steganography, a carrier is required to hide information which can be fulfilled by unused field of network protocol to establish covert channel.
In 2017, Abeer Abed articulated three essential elements for articulating data, 1. Carrier also known as cover message, 2. Message, i.e. secret data and 3. Password known as stego-key, known by sender and recipient [8].
Here the aim of research to create a covert channel paradigm or reference model for specific case using the header field of the TCP/IP protocol suite.

V. TCP/IP protocol suite

The TCP/IP suite of protocols can be understood in terms of layers. From the top they are, Application Layer, Transport Layer, Network Layer, Network Interface Layer, and Hardware. TCP/IP work in tandem to transfer a data packet from one computer to another using computer networks. Though it's a collection of many protocols, Transmission Control Protocol (TCP) and Internet Protocol (IP) are the two main foundation protocols.

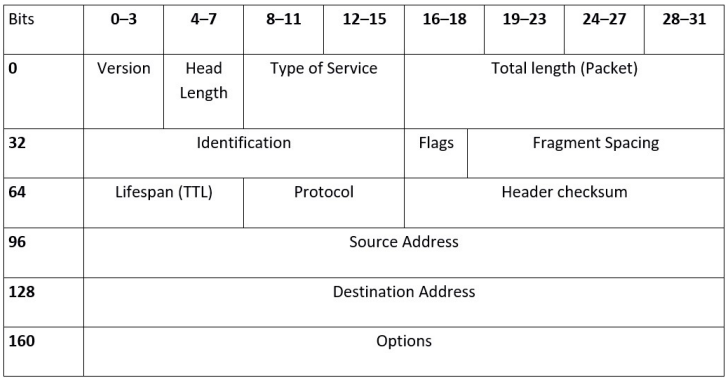

Fig.1- IP Header

The IP protocol and its associated routing protocols are possibly the most significant of the entire TCP/IP suite. IP is responsible for the IP addressing, Host-to-host communications, Packet formatting and Fragmentation [9]. IP is the connectionless protocol which means that before transmitting the data, there was no exchanging control information (known as handshake) to establish end – to end connection. For packet lost or out of order delivery, IP must depends on protocols of the upper layer. Datagram consists of header and payload. The length of header is variable and ranges between 20-60 bytes proportion to the existence of option field. This variation results in variable length datagram. The header of IPv4 is shown in Fig.(1)-IP Header.

TCP Header				
Bits	0-15			16-31
0	Source port			Destination port
32	Sequence number			
64	Acknowledgment number			
96	Offset	Reserved	Flags	Window size
128	Checksum			Urgent pointer
160	Options			

Fig.2-TCP Header

TCP is a connection oriented protocol, means data would be transferred after the connection is established. It uses three-way handshake mechanism to ensure reliable delivery. It uses sequence number to ensure delivery correctness and confirmed no data was lost when network failure occur, so it was considered a reliable protocol. Also, it is stream-orientation because it uses buffer in sending and receiving and this enable application to write very small or an amount of data and divide it into appropriate size. TCP provides a process to process communication, i.e, the transfer of data that takes place between individual processes executing on end systems. This is done using port numbers or port addresses. Port numbers are 16 bits long that help identify which process is sending or receiving data on a host. TCP segment consists of header part and data part as shown in Fig.(2)-TCP Header.

VI. COVERT CHANNEL SCENARIO

A manager from the corporate office is under the radar of a government security agency for illegal activities. But they don't have any evidence against him to take an action. So, they decided to plant their agent in the corporate office as a PA to the suspicious manager and planned to use the covert communication channel for this operation.

As a daily routine the PA (agent) would communicate to his boss (suspicious manager) without any suspicion. During this operation the agent will never communicate to the security agency. He must keep this mission secret. The job of the agent would be collecting the evidence against the manager. And once his job has been done. He must inform his original authorities through covert communication. Once the Agent done with his job, he would execute the program from his desk which would initiate the communication through raw socket to communicate with the government agency office. Here 4 characters are used as secret data which would be XOR with source port number and the destination port number to generate a sequence number of a syn packet of three-way handshake mechanism. And would be send to the security agency to indicate that the mission is successful.

VII. SYSTEM MODEL

The structure of the proposed system for Covert channel scenario is illustrated in Fig.(3). It consisted of two models. The Agent (sender) and the manager (receiver) receiver are the two models respectively.

Practical and Implementation:

The proposed system is implemented using Linux kernel raw sockets. Linux is a good environment provides the easiest access of raw sockets interface. At the both ends Kali Linux operating system is used and the user interface is created using the python programming language. Wireshark can be used to monitor the traffic. The transmission is sent from the host node to the predetermined IP address of the server. Netcat command represent the server that listens and waits for connection request from the client (sender of the hidden data).

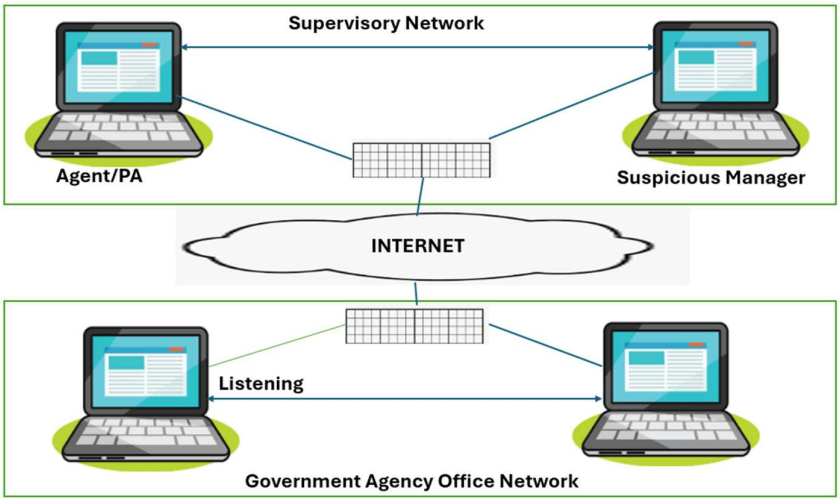

Fig.(3)- Covert communication Scenario

VIII. RESULTS

At the sending host on the network, the tcp/ip packet has been crafted using the raw socket. The execution of the program for the method (described above) is shown below. Fig.(4) shows a packet with the hidden data at the sending host. The sender hides the secret data "done" in a sequence number field of the syn-packet of 3-way handshake mechanism. The sequence number can be generated using the XOR operation of the hidden data with the source and destination ports fields of TCP header.

```
Administrator: Command Prompt

C:\Users\shash\Networking\17June24>python SendingHost.py -s="192.168.0.103" -sp=12333 -d="192.168.0.107" -dp=80 -t=2
Message to be hide: done
Source Port: 0011000000101101, Destination Port: 0000000001010000
Concatinating Source and destination: 00110000001011010000000001010000
Converting the message to binary: 01100100011011110110111001100101
Performing XOR operation on above two to get binary seqience number
Binary sequence no is: 01010100010000100110111000110101

Hex seq number with hidden data is 0x54426e35


Summary:
Source IP : 192.168.0.103
Destination IP : 192.168.0.107
Source Port : 12333
Destination Port : 80

----IP header & bytes----
IP Header : 45000028abcd000040064ce0c0a80067c0a8006b
IP Bytes : bytearray(b'E\x00\x00(\xab\xcd\x00\x00@\x06L\xe0\xc0\xa8\x00g\xc0\xa8\x00k')

----TCP header & bytes----
TCP Header : 302d005054426e350000000050027110c9ba0000
TCP Bytes : bytearray(b'0-\x00PTBn5\x00\x00\x00\x00P\x02q\x10\xc9\xba\x00\x00')

****************************************
```

Fig.4 – hiding the message

At the receiving host the fig.5 shows the output. At the receiving end using scapy tool available in python, the hidden message can be extracted. Here the captured "SYN" packet is stored in the variable a. Using the command a[0][TCP].seq, the sequence number can be extracted from the captured packet. Here the sequence number is in the hexadecimal format which would be converted into 32-bit binary format. One should make note here the data is hidden in this sequence number. To extract the hidden data, we need to extract source port number and destination port number which is in hexadecimal format. We get the 32 bit binary string binsrcdst by concatenating 16 bit source and destination port by using similar process.

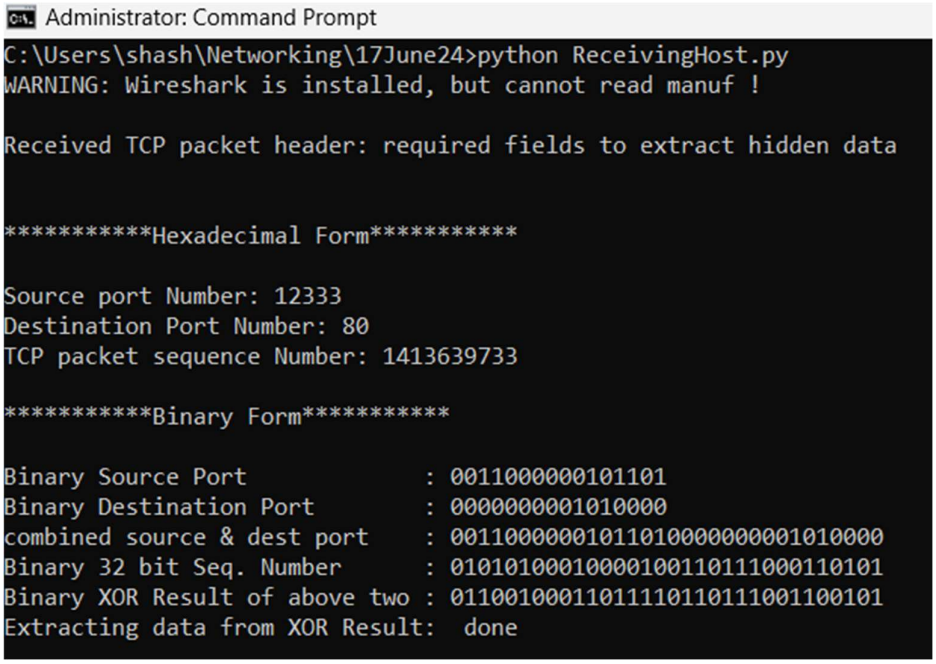

Fig.5 – Extracting the hidden message

Now we get the hidden data as 32 bit binary string by executing the XOR operation as:

Data=(bin(int(binsrcdst,2)^int(binseq,2))[2:].zfill(32)

Since data is 4 byte and each byte represent the character, we got the output as expected, i.e. we got the output : "done".
In this way we are able to send the secret message using the tcp sequence number.

IX. CONCLUSION

In this paper, a network steganography technique using TCP/IP's sequence number is implemented. How the header field of the TCP/IP protocol suit is used to hide the secret message is described. A good mixture for network programming was shown through python as a modern programming language and Linux. TCP/IP header fields were found as a good carrier for sensitive data to be hided. With few minor operations with the field's contents, a secure carrier can be constructed. Due to restrictions of the field size only 4 characters can be transmitted as a hidden data. This limitation restricts the size of data in turn.

REFERENCES

[1] Tanenbaum A. S., Wetherall D. J., "COMPUTER NETWORKS", 4 Ed., Pearson Education, Inc, 8-13, 2003.
[2] Stallings W., "Network Security Essentials: Applications and Standards", 4 Ed., Pearson Education, Inc., 8-12, 2011.
[3] Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn, "Information Hiding - A Survey", Proceedings of the IEEE, special issue on protection of multimedia content, 87(7):1062{1078, July 1999
[4] Whitfield Diffie And Martin E. Hellman, Member, IEEE, New Directions in Cryptography, IEEE Transactions on Information theory, Vol. IT-22, No.6, Nov 1976
[5] Singh J., Sharma L., "Framework for Efficient Secure Steganographic Communication over Network Protocols", International Journal of Advanced Computer Research, 3 (4), Issue 13,146- 150, Dec. 2013
[6] Krzysztof Szczypiorski, HICCUPS: Hidden Communication System for Corrupted Networks, ACS '2003: Proceedings of The Tenth International Multi-Conference on Advanced Computer Systems, 31- 40, 2003.
[7] Rohankar N, D., Deorankar A. V., Chatur, Dr. P. N., "A Review of Literature on Design and Detection of Network Covert Channel", International Journal of Engineering Science and Innovative Technology (IJESIT), 1, Issue 2, Nov.2012

[8] Abeer E. Abed, Steganography Using TCP / IP's Sequence Number, Journal of Al-Nahrain University, Vol.20 (4), December, 2017, pp.102-108
[9] Peter L Dordal, An Introduction to Computer Networks, Release 2.0.11. Jul 20, 2023
[10] Rowland C. H., "Covert Channels in the TCP/IP Protocol Suite", First Monday Journal on the Internet, 2(5), 1997.
[11] Joanna Rutkowska, The Implementation of Passive Covert Channels in the Linux Kernel, Chaos Communication Congress, December 2004
[12] Radu-Ioan Ciobanu; Mihai-Ovidiu Tirsa; Raluca Lupu; Sonia Stan; Mugurel Ionut Andreica, SCONeP: Steganography and Cryptography approach for UDP and ICMP, RoEduNet International Conference 10th Edition: Networking in Education and Research, 2011.