# Efficient Secure Network Steganographic Communication over Stream Control Transmission Protocol

May Aye Chan Aung, Khin Phyo Thant
*University of Computer Studies, Mandalay*
*mayayechanaung@gmail.com, khinphyothantucsy@gmail.com*

## Abstract

*As the internet evolves and computer networks become bigger and bigger, network security is one of the most challenging issues in today's world that touches many areas using network communication. Nowadays, there is a need for mobility, therefore new protocols were designed to support the mobility and multihoming facilities. Since SCTP is designed for telecommunication, its native design does not consider the security issues for data transmission. In this paper, an efficient secure network steganographic approach that is able to send, receive, detect and recover encrypted messages hidden in the Initiate Tag of Stream Control Transmission Protocol (SCTP) will be proposed. The main aim of the proposed work is to hide and protect secret data inside user's normal data transmissions without destroying by third parties. Finally, the efficiency of this proposed approach will be compared to other known steganographic tools.*

## 1. Introduction

Network steganography is the art of hiding secret information within normal network transmission. Contrary to typical steganographic methods which utilize digital media such as pictures, audio and video files as a cover for hidden data (steganogram), network steganography utilizes communication protocols' control elements and their basic intrinsic functionality. It is usually done by making the use of fields in network protocol headers that are unused or irrelevant. Although data transmitted through steganography is usually unencrypted, encryption provides an extra level of security in case the convert channel is detected.

Although steganography is applicable to text, images, audio signals and other digital data, this paper chooses network packet headers for this purpose. In this paper, the proposed work will be done that offers additional security to the covert data by encrypting it. The implementation of the proposed work sends, receives, detects and recovers encrypted messages hidden in the Initiate Tag of Stream Control Transmission Protocol (SCTP). The overt data is compressed using Lempel-Ziv-Welsh (LZW) compression algorithm for efficiency, and then encrypted using Vigenère Cipher algorithm before sending it.

The rest of the paper is structured as follows: In the next section, literature review is described. Overview of SCTP protocol is presented in section 3. The architecture of the proposed system is described in section 4.The final conclusion is drawn in section 5.

## 2. Literature Review

In recent year, the security of the sensitive data has become a prime and supreme importance. To protect data or secret information from unauthorized person, the two main data hiding techniques like Cryptography and Stegnography have been used. There are various types of steganography used by many people to send their secret data over communication network. Recently, most of the research works have been proposed and analyzed the developing different methods and techniques for network steganography.

Network steganography was first introduced by Krzysztof Szczypiorski using all information hiding methods that may be used the unused or reserved bits in packet headers, packet padding, or various header fields .The author introduced a data link layer method called Hidden Communication System for Corrupted Networks (HICCUPS) [4]. The main idea is to utilize transmission frames with intentionally wrong checksums.

B. Jankowski, W. Mazurczyk, and K. Szczypiorski presented a steganographic system which is the information hiding solution based on inter-protocol steganography [1]. It may be deployed in LANs and utilized two protocols such as Ethernet and ARP/TCP to enable secret data exchange.

Radu Ciobanu, et.al. [2] proposed the design and implementation of a network steganography application called Steganography and Cryptography over Network Protocols (SCONeP). Moreover, the performance of two scenarios for using SCONeP was developed. Then, the performance and efficiency of these two methods were compared to other known steganography tools. Finally, an active warden was used for steganography prevention and implemented as a Linux kernel module as a proof-of-concept component of SCONeP.

Jasbir Singh and Lalitsen Sharma presented a covert channel framework for network steganography using TCP/IP protocol [3]. The framework provides additional security to the data sent through covert channel by using encryption. Several ways of sending covert information through network using TCP/IP protocol were discussed. Then, the efficiency of the proposed implementation was compared to other known steganography tools and results obtained were comparable to the results of image steganography.

According to Wojciech and Wojciech [13], the various steganographic methods used for hiding information in SCTP was introduced. They also identified the possible places were the hidden information can be exchanged. The possible detection technique and its countermeasure were also analyzed.

Venkadesh et al. [11] had suggested a method for secure data transmission by hiding Digital signature in the modified Heartbeat chunk of SCTP in the sender side and thus provides data authentication in SCTP. Using this method it is only possible to detect the network attack at the end of the transmission.

P. Venkadesh, Julia Punitha Malar Dhas and S.V. Divya, proposed a Multi-level security mechanism to provide secure data transmission in Stream Control Transmission Protocol (SCTP) by providing various security levels in terms of dynamic encryption algorithms, hiding the key in the heartbeat signal of SCTP and also suggested a method to detect the hacker and choosing an alternative path to transmit the remaining packets using multi-Homing options [7].

## 3. Overview of SCTP

SCTP stands for Stream Control Transmission Protocol. It is a new reliable, message-oriented transport layer protocol that combines the best features of TCP and UDP. It lies between the application layer and the network layer and serves as the intermediary between the application programs and the network operations. It eliminates the limitations of TCP, which are more onerous in many applications.

Each SCTP connection which is called association in SCTP can use one or more streams, which are unidirectional logical channels between SCTP endpoints [9]. Order-of-transmission or order-of -arrival delivery of data is performed within each stream separately and globally. If one of stream is blocked, it does not affect other streams. Benefit of using multiple streams is illustrated in figure 1.

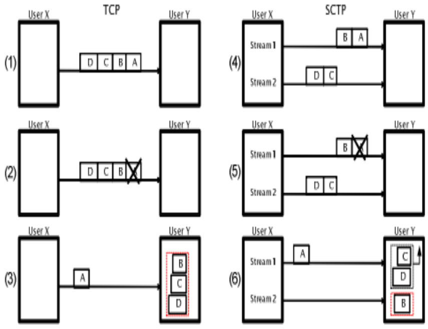
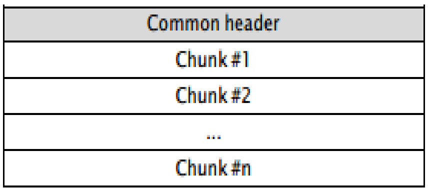
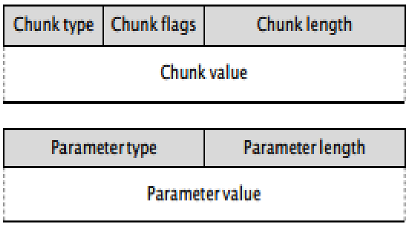


**Figure 1. Comparison of TCP and SCTP data transport using multiple streams**



| Common header |
|---|
| Chunk #1 |
| Chunk #2 |
| ... |
| Chunk #n |

**Figure 2. SCTP Packet Format**



| Chunk type | Chunk flags | Chunk length |
|---|---|---|
| Chunk value | | |

| Parameter type | Parameter length |
|---|---|
| Parameter value | |

**Figure 3. SCTP Chunks and Parameters Format**

Another SCTP feature is the provision of protocol extensibility [9]. Each SCTP packet consists of main header and one or more chunks as shown in figure 2. There are two types of chunks: data chunks, which contain user data and control chunks, which are used to control data transfer. Each chunk consists of fields and parameters specific to chunk type as shown in figure 3. Fields are mandatory, and parameters can be either mandatory or optional. SCTP packet structure allows defining not only new chunk types but also broadening functionality of the existing chunk types through defining new parameters.

SCTP supports multi-homing. Multi-homing in SCTP is used to provide more reliable data transfer. If there are no packets losses, all messages are transmitted using one source address and one destination address (primary path). If chunk is retransmitted, it should be sent using different path (different source and destination addresses) than primary path. Another advantage of SCTP multi-homing in SCTP is the ability to failover data transfer if primary path is down.

SCTP uses a four-way handshake with cookie which provides protection against synchronization attack (type of Denial of Service attack) known from TCP. In SCTP, user initiates an association with INIT chunk. In response, he/she receives INIT chunk with cookie contained information that identifies proposed connection. Then, he/she replies with a COOKIE ECHO with copy of received cookie. Reception of this chunk is acknowledged with COOKIE ACK chunk. After successful reception of COOKIE ACK association is established. Afterwards, connected users can send data using DATA chunks and acknowledge reception of them with SACK chunks. Aside from described features, SCTP also provides built-in path MTU discovery, data fragmentation mechanism and it is considered more secure than TCP [12].

## 4. Architecture of Proposed System

This section describes the architecture of the proposed work. A graphical representation of the architecture can be presented in figure 4. Two communication parties will be denoted as Sender and Receiver. The initial connection is established between the sender and the receiver by sending a request to the client, where the server will response for the client request. The connection is successfully established after receiving an acknowledgement from the client. The communication between the sender and the receiver is known as an association. As SCTP is a connection-oriented protocol, the association has three phases: connection establishment, data transfer, shut down as shown in figure 5.

After the connection is established, the files or data is selected by the sender. In order to enhance efficiency, LZW compression algorithm will be used**.** In this paper, any files will be compressed. Text and PDF files will be input files. According to LZW compression algorithm, a dictionary of frequently used groups of characters will be built. Before the file is decoded, the compression dictionary must be sent to the receiver. This method is good at compressing text files because text files contain ASCII characters [5]. If the transmitted message is: ababacdcdaaaaaaef,

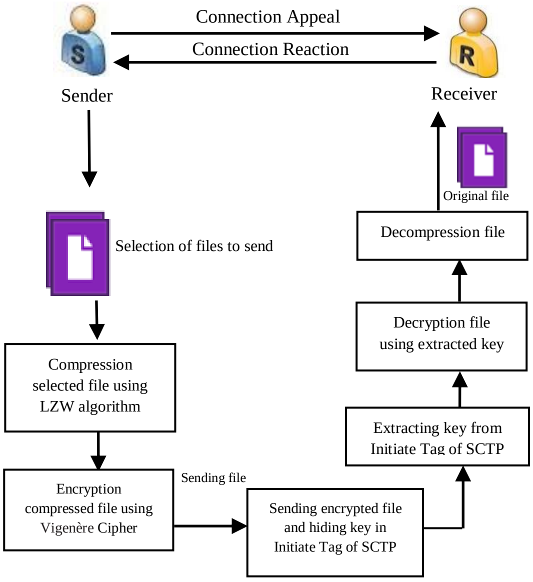

Connection Appeal
Connection Reaction
S
R
Sender
Receiver
Original file
Selection of files to send
Decompression file
Decryption file using extracted key
Compression selected file using LZW algorithm
Extracting key from Initiate Tag of SCTP
Sending file
Encryption compressed file using Vigenère Cipher
Sending encrypted file and hiding key in Initiate Tag of SCTP

**Figure 4 . Architecture of Proposed Work**

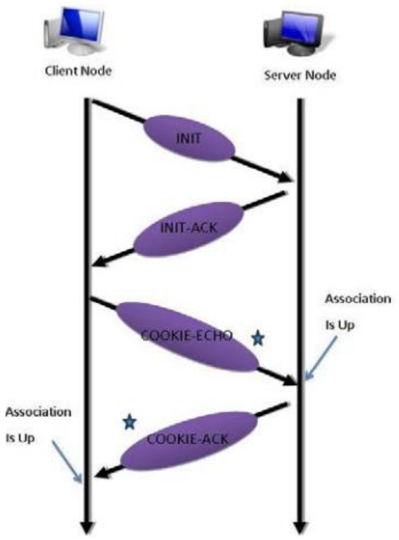


**Figure 5. Connection establishment**

then the sender and receiver would initially add the following to 16 entry dictionary:

0000 ‘a’
0001 ‘b’
0010 ‘c’
0011‘d’
0100 ‘e’
0101 ‘f’
0110–1111 empty

First the ‘a’ character is sent with 0000, next the ‘b’ character is sent and the sender checks to see that the ‘ab’ sequence has been stored in the dictionary. As it has not, it adds ‘ab’ to the dictionary, to give:

0000 ‘a’
0001 ‘b’
0010 ‘c’
0011‘d’
0100 ‘e’
0101 ‘f’
0110 ‘ab’
0111–1111 empty

The receiver will also add this to its table. Next the sender reads the ‘a’ character and checks to see if the ‘ba’ sequence is in the code table. As it is not, it transmits the ‘a’ character as 0000, adds the ‘ba’ sequence to the dictionary, which will now contain:

0000 ‘a’
0001 ‘b’
0010 ‘c’
0011‘d’
0100 ‘e’
0101 ‘f’
0110 ‘ab’
0111 ‘ba’
1000–1111 empty

0000 0001 0000 0110 0010
↑ ↑ ↑ ↑ ↑
‘a’ ‘b’ ‘a’ ‘ba’ ‘c’

Next, the sender reads the ‘b’ character and checks to see if the ‘ba’ sequence is in the table. As it is, it will transmit the code table address which identifies it, i.e. 0111. When this is received, the receiver detects that it is in its dictionary and it knows that the addressed sequence is ‘ba’.

Next, the sender reads a ‘c’ and checks for the character in its dictionary. As it is included, it transmits its address, i.e. 0010. When this is received, the receiver checks its dictionary and locates the character ‘c’. Then, this continues with the transmitter and receiver maintaining identical copies of their dictionaries. A great deal of compression occurs when sending a sequence of one character, such as a long sequence of ‘a’.

After the data is compressed, this compressed data will be encrypted by using a symmetric encryption scheme, Vigenère Cipher algorithm. Vigenère Cipher algorithm is one of the simplest and best known polyalphabetic ciphers [14]. In this scheme, the set of related monoalphabetic substitution rules consists of the 26 Caesar ciphers with shifts of 0 through 25. Each cipher is denoted by a key letter, which is the ciphertext letter that substitutes for the plaintext letter a. Thus, a Caesar cipher with a shift of 3 is denoted by key value. A general equation of the encryption process is

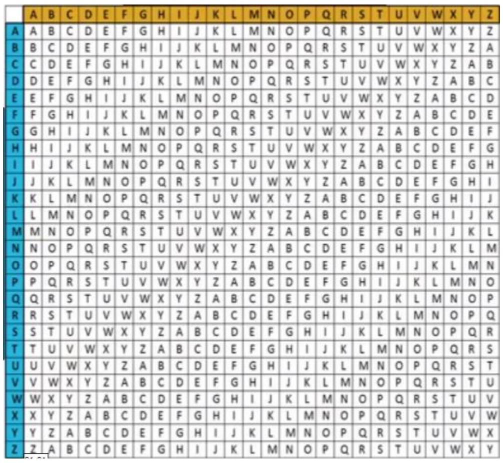
$$Ci = (pi + ki \bmod m) \bmod 26 \tag{1}$$

Similarly, decryption is a generalization of

$$pi = (Ci - ki \bmod m) \bmod 26 \tag{2}$$

To encrypt a message, a key is needed that is long as the message. Usually, the key is a repeating keyword. In this paper, the length of key will have 20 characters. Using longer keyword will be difficult for the third person to crack this key. All 26 characters (A to Z) will be assigned that A → 0, B → 1, ……., Z → 25. An encrypted message with spaces will help a third person to decode this encrypted message with the keyword. So, the message must always be written without any space. Firstly, a single-line message will be written no space between words. Secondly, on the line below, the keyword will be written by repeating the letters of the keywords until the end of the message to encrypt. And then, the message will be encrypted according to the equation 1.

On the receiver side, using the Vigenère table (26 letters x 26 letters) as shown in figure 6, the letters of the message with the one from the keyword will be crossed. Starting with the keyword column (vertical) to the message line (horizontal), the recipient will reverse the process to decrypt the message. The final result will be found at the top of the column of these letters.



| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| B | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A |
| C | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B |
| D | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C |
| E | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D |
| F | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E |
| G | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F |
| H | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G |
| I | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H |
| J | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I |
| K | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J |
| L | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K |
| M | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L |
| N | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M |
| O | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
| P | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
| Q | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P |
| R | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q |
| S | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R |
| T | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S |
| U | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T |
| V | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U |
| W | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V |
| X | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W |
| Y | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X |
| Z | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y |

**Figure 6 . Vigenère table**

There are several important places in which the information can be hidden and exchanged within SCTP. Each method has its bandwidth/capacity. Initiate Tag is a 32 bit value of the Verification Tag field [13]. This tag must be inserted into each SCTP packet, which is sent to the originator of INIT or INIT ACK chunks within this association. The Initiate Tag can be any value except 0 and thus may be used for steganographic purposes, as shown in figure 7. The maximum bandwidth of this channel is 32 bits/chunks (fewer bits of this field should be used to limit the chance of detection). In this paper, the key will be hidden in the Initiate Tag of SCTP. The receiver on the other side will extract the key from the Initiate tag of SCTP and decrypt the compressed and encrypted files by a decryption algorithm according to the reverse order.

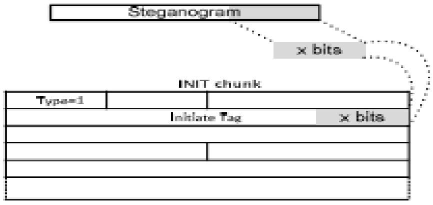


**Figure 7 . Method based on the Initiate Tag field**

## 5. Conclusion

In this paper, an efficient secure network steganographic approach that is able to send, receive, detect and recover encrypted messages hidden in Stream Control Transmission Protocol (SCTP) has been proposed. This proposed work will provide additional security to the data sent through covert channel by using encryption. The implementation of this proposed work will send, receive compressed and encrypted messages. And then, the key will extract in Initiate Tag of SCTP protocol. Convert data will be compressed using LZW compression algorithm for efficiency, and then encrypted using Vigenère Cipher algorithm before sending it. The efficiency of the proposed work will also be compared to other known steganographic tools.

## References

[1] B. Jankowski, W.Mazurczyk, and K. Szczypiorski, “Information Hiding Using Improper Frame Padding”, CoRR, abs/1005.1925, 2010.

[2] Ciobanu R.-I., Tirsa M., Lupu R. and Stan S., “Steganography and Cryptography over Network Protocols”, 10th Roedunet International Conference (RoEduNet), 23-25 June 2011, pp.1-6, ISSN: 2068-1038, Print ISBN: 978-1-4577-1233-3, INSPEC Accession Number: 12193979, IEEE, Lasi.

[3] Jasbir Singh and Lalitsen Sharma, “Framework for Efficient Secure Steganographic Communication over Network Protocols”, International Journal of Advanced Computer Research (IJACR), Volume-3 Number-4, Issue-13, December 2013, ISSN (print): 2249-7277, ISSN (online): 2277-7970.

[4] K. Szczypiorski, "HICCUPS: Hidden Communication System for Corrupted Networks”, In ACS ’2003: Proceedings of The Tenth International Multi-Conference on Advanced Computer Systems, pages 31–40, October 22-24 2003, Miedzyzdroje, Poland.

[5] Lempel-Ziv-Welch, “online at http:// en.wikipedia.org wiki/ Lempe-Ziv-Welch”, December, 2012.

[6] Mrs. Dhanashri D. Dhokate1 and Dr. Vijay R. Ghorpade, “Data Hiding with Multiple Network Protocol Usage”, International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), Vol.4, Issue 7, July 2015, ISSN (Online) 2278-1021, ISSN (Print) 2319-5940.

[7] P. Venkadesh, Julia Punitha Malar Dhas and S.V. Divya, “A Multi-level Security Mechanism for Secure Data Transmission in SCTP”, Research Journal of Applied Sciences, Engineering and Technology 7(10): 2123-2128, March 15 2014, ISSN: 2040-7459; e-ISSN: 2040-7467 © Maxwell Scientific Organization, 2014.

[8] R.M. Goudar, Prashant N. Patil, Aniket G. Meshram, Sanyog M. Yewale and Abhay V. Fegade, “Secure Data Transmission by using Steganography”, International Institute for Science, Technology and Education (IISTE), www.iiste.org , Vol. 2, No.1, 2012, ISSN (Paper) 2224-5758, ISSN(Online) 2224-896X.

[9] R. Stewart, M. Ramalho, Q. Xie, M. Tuexen and P. Conrad, “Stream Control Transmission Protocol (SCTP) Partial Reliability Extension”, RFC 3758, May 2004.

[10] R. Stewart and Q. Xie, “Stream Control Transmission Protocol (SCTP)”, A Reference Guide. Addison-Wesley, 2002.

[11] Venkadesh, P., M.D. Julia Punitha and S.V. Divya, 2013. A framework model for secure key management and hidden digital signature method to enhance security in SCTP. Arch. Sci., 66(5): 236-247.

[12] W. Fraczek, W. Mazurczyk and 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 4-6, Nanjing, China.

[13] Wojciech, F. and M. Wojciech, 2012. Hiding information in a stream control transmission protocol. Comput. Commun., 35(2): 159-169.

[14] William Stalling, - Cryptography and network security: Principles and practices, fifth Edition.