Research Journal of Applied Sciences, Engineering and Technology 7(10): 2123-2128, 2014
DOI:10.19026/ajfst.7.506
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: July 6, 2013 Accepted: September 02, 2013 Published: March 15, 2014

Research Article

A Multi-level Security Mechanism for Secure Data Transmission in SCTP

[1]P. Venkadesh, [1]Julia Punitha Malar Dhas and [2]S.V. Divya
[1]Department of CSE,
[2]Department of IT, Noorul Islam Centre for Higher Education, Kumaracoil, Tamilnadu, India

Abstract: In this study we propose a multi-level security mechanism to provide secure data transmission in Stream Control Transmission Protocol (SCTP). During the time of TCP/IP protocols the computers were single-homed and nowadays there is a need for mobility, therefore new protocols were designed to support the mobility and multi-homing facilities. SCTP is a newly designed protocol that supports more interesting features such as Multi-homing and Multi-streaming when compared to the existing protocols. Since SCTP is designed for telecommunication its native design does not consider the security issues for data transmission. In this study we analyzed and identified the possibility places for hiding and exchanging of secret information in SCTP and proposed a dynamic encryption algorithm to provide a secure end-to-end data transmission between two nodes by altering the basic structure of the existing SCTP multi-homed protocol so that the attacker does not know the algorithm used since the algorithm is dynamic and the key for the encryption algorithm is hidden in the heartbeat signal of the SCTP and also suggest a method to detect the hacker incase of any attacks against the transmitted packets and finds an alternate path to transmit the remaining packets using the multi-homing options of SCTP.

Keywords: Datagram congestion control protocol, dynamic encryption, hacker, heartbeat chunk, multi-homing, multi-streaming

INTRODUCTION

Transmission Control Protocol (TCP) was developed in the mid of 1970's-1980's. TCP/IP is the intermediate layer between IP and the application below it.

Using TCP, applications can establish a reliable connection to one another and it is a complex protocol; User Datagram Protocol (UDP) is the main alternative to TCP was developed in the 1980's which is an unreliable protocol whereas Datagram Congestion Control Protocol (DCCP) was developed in the year 2004 which is a unicast transport layer protocol that supports unreliable data transfer but does not supports multi-homing. Hence SCTP is introduced. Stewart (2007) had explained the reason behind the development of SCTP, the offered services and the basic concept of SCTP protocol.

SCTP is a message oriented transport layer protocol that provides new services and features to IP Communication. It is originally designed to support PSTN signaling messages over IP Networks. The higher and widely used protocols like TCP, UDP, do not support features like Multi-Homing Multi-Streaming etc. UDP is a simplest connectionless and unreliable protocol.UDP faces some problems like duplicate packets and unordered delivery of packets. TCP is a connection oriented and reliable protocol i.e., connection is established throughout the data transmission. TCP provides strict ordering and reliability. Since TCP uses a strict byte order delivery, it suffers from Head-of-Line blocking (HOL) and it is a stream oriented protocol. TCP-MH is similar to the TCP protocol with connection oriented and reliable features. TCP-MH was originally developed to overcome the problems of TCP to use multiple IP address over a single TCP session. It supports Multi-homing. But it cannot be used for Multi-streaming purpose.

DCCP is an unreliable protocol for the flow of datagrams with acknowledgements mainly used for the purpose of Congestion control and Multi-homing but it does not support flow control, Multi-Streaming and Sequential flow of datagrams. Hence there is a need for new protocols. In the past ten-twenty years, reliable communication is established by TCP and unreliable communication is established by UDP. Neither TCP nor UDP support Multi-Streaming and Multi-Homing facilities. What would happen if there is a new protocol that combines the features of TCP, UDP and DCCP along with some additional features? Therefore, SCTP was introduced. SCTP provides a reliable connection oriented protocol, with unordered message delivery. It

Corresponding Author: P. Venkadesh, Department of CSE, Noorul Islam Centre for Higher Education, Kumaracoil, Tamilnadu, India

Table 1: Comparison of TCP, UDP, DCCP and SCTP

Feature name	TCP	UDP	DCCP	SCTP
Bundling	Yes	No	No	Yes
Built-in heart beat	No	No	No	Yes
Congestion control	Yes	No	Yes	Yes
Connection oriented	Yes	No	Yes	Yes
Data checksum	Yes	Optional	Yes	Yes
Explicit congestion notification support	Yes	No	Yes	Yes
Extensible	No	No	Yes	Yes
Flow control	Yes	No	No	Yes
Full duplex	Yes	Yes	Yes	Yes
Half closed connection	Yes	N/A	No	No
Handshake for connection setup	3-way	No	3-way	4-way
Handshake for shutdown	4-way	No	3-way	3-way
Mobility support	No	No	Yes	Yes
Multi-homing	No	No	No	Yes
Multi-streaming	No	No	No	Yes
NAT friendly	Yes	Yes	Yes	Yes
Ordered date delivery	Yes	No	No	Partially
Packet size	20-60 bytes	8 bytes	12 or 16 bytes	12 bytes
Partially reliable date	No	No	Yes	Optional
Path maximum transmission unit discovery	Yes	No	Yes	Yes
Protection against DOS attack	No	No	Yes	Yes

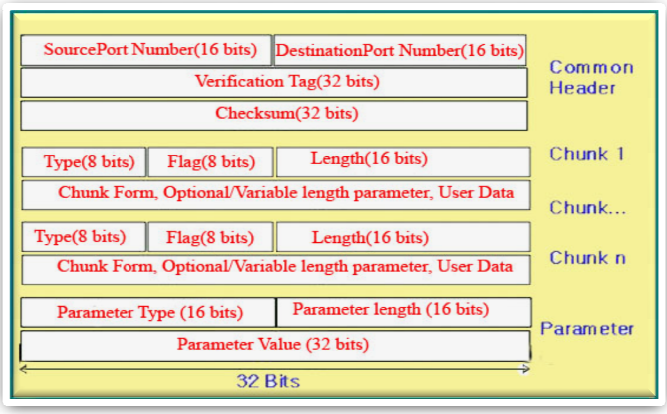

Fig. 1: SCTP packet format

provides acknowledged, error-free and non-duplicate of SCTP packets (messages).

SCTP provides a reliable connection oriented protocol with unordered message delivery. It provides acknowledged, error-free and non-duplicate of SCTP packets (messages). Moreover, it supports two important features: Multi-Homing and Multi-Streaming which is not supported by any other protocols.

Various protocols such as TCP, UDP, DCCP along with their features are compared to SCTP in Table 1.

The Basic structure, Association setups, Tear-downs and the features of SCTP such as Multi-Homing and Multi-Streaming, Security, SCTP authentication, the recent advances in the standardization of IETF process of SCTP protocol is analyzed and moreover, the dynamic address reconfiguration, chunk authentication and partial reliability of the protocol is also addressed by Dreibholz *et al*. (2011).

Packet format of SCTP: The SCTP packet contains a common header which includes Source Port Number, Destination Port Number, Verification Tag and the checksum which is used for protecting the data against transmission errors and guarantees data integrity. The packet structure of SCTP is shown in Fig. 1.

The block of data formatted and embedded in SCTP packet is referred to as chunks. Each SCTP packet contains a data chunk or control chunks which consist of the type used to identify the type of chunks, the flag which is an ordered/unordered bit and length is used to identify the length of the variable.

Even though SCTP has many advanced features, its native design does not consider its security issues. Therefore a secure data transmission technique is necessary for transmitting the data over SCTP. In this study, we focused the interesting features of SCTP and identified the possible information hiding location of SCTP and the basic structure of SCTP is modified and a 4-bit code is added to select one of the three encryption algorithm and hiding the key of the encryption algorithm in the Heartbeat Signal of SCTP thereby providing Multi-Level Security for preventing the information from network attacks.

FEATURES OF SCTP

SCTP is the newest transport layer protocol standardized by IETF. It has more interesting features to transmit data over IP.

Multi-streaming: Unlike TCP, which has only one stream and all the messages delivered on that, SCTP has the property of multi-streaming; it contains multiple streams within a single connection so that if a message in a stream is lost, it doesn't affect the other messages and their delivery. Multi-streaming, where one association can bundle multiple independent streams, is one of the most important features of SCTP. It avoids the Head-of-Line (HOL) blocking problem of TCP and makes SCTP a proper transport for signaling messages. In SCTP, a stream is a unidirectional logical channel established from one to another associated SCTP endpoint.

The connection in the SCTP is called an association. Each association contains multiple channels called streams. Each stream is a logical, unidirectional data flow within an association and it provides an in-sequence delivery of messages in a single stream and not in the different streams and these messages does not have any ordering.

SCTP's multi-streaming helps the infrastructure that contains multiple means of communications simultaneously. For example, stream1 can handle voice communications and stream 2 can handle multimedia messages and so on **(**Fig. 2).

Multi-homing: To provide end-to-end network fault tolerance and redundancy, SCTP provide an additional feature called Multi-Homing mainly at the transport layer. Each pair contains multiple IP address which was bound by the SCTP association.

The connection in SCTP is called as association instead of connection and each association has multiple streams and it provides a four way handshake for connection setup and three way handshake for connection termination.

Multi-Homing is the ability that a single endpoint supports multiple IP address. Figure 3 shows two multi-homed hosts. The sender (Host A) and the receiver (Host B) consists of two addresses A1, A2 and B1, B2 respectively. The SCTP sender chooses one destination address as the primary address and if this primary address fails, it chooses an alternate destination until the primary destination becomes available again. In this case, the host A sends the packets through the primary path (A1-B1) at the beginning. If the primary path fails, the SCTP chooses the alternate path (A2-B2) for data transmission.

Iyengar *et al*. (2004) has evaluated different re-transmission policies with varied constraints with

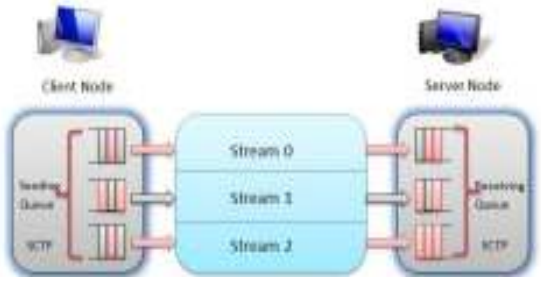

Fig. 2: A scenario for multi-streaming

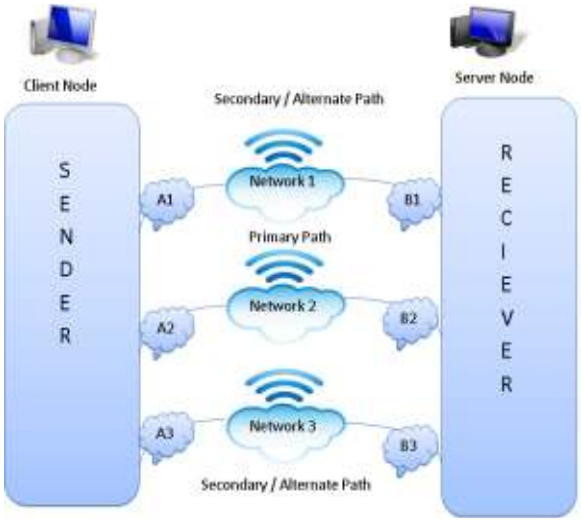

Fig. 3: A scenario for multi-homing

Table 2: Steganographic methods in SCTP and its bandwidth

Steganographic areas of SCTP	Bandwidth in bits/chunk
Initiate tag	32
Number of inbound streams	8
Stream sequence number	16
Payload protocol identifier	32
Advertised receiver window credit	32
Shared key identifier	16
Padding data	Varies
Heart beat info parameter	320
Random number in random parameter	32

receive buffer size for the SCTP re-transmission in case of packet loss for Multi-homed networks.

Daniel and Abdallah (2012) presented a comprehensive review of transport layer multi-homing using the Steam Control Transmission Protocol (SCTP). His main areas of study include: handover management, concurrent multipath transfer and cross-layer activities.

Information hiding in SCTP: There are several important places in which the information can be hidden and exchanged within SCTP. Each method has its own bandwidth/capacity. The various areas in which steganographic techniques that can be used in SCTP and their bandwidth is given in the Table 2.

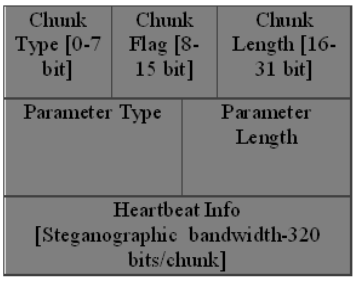

Fig. 4: Heartbeat chunk

Heartbeat chunk of SCTP: The SCTP packet consists of two basic section Common header and data chunks. Chunk is a unit of information within an SCTP packet that contains user and control data. Heartbeat chunk of SCTP is used to verify the reach-ability of the destination addresses.

It also uses a Heartbeat info parameter field (Fig. 4), which contains the sender-specific heartbeat info field, Steganographic bandwidth used for this method is 320 bits/chunk and dependently implemented. Heartbeat chunk is sent to many other different addresses that are negotiated during the initial setup of association to find out if they are all up. SCTP chunks use a self-describing Tag-Length-Value (TLV) format. This stegnographic bandwidth is used to hide the key for our encryption algorithm.

BACKGROUND MATERIALS

Even though many features were introduced in SCTP, no mechanism for End-to-End (E2E) security provision is offered. Therefore Anna (2009) recommended to implement the End-to-End security either in IP security layer (IPSec) or Transport Layer Security (TLS). IPsec Over SCTP is the easiest way for secure communication in SCTP. But still, there exists some drawbacks such as inefficiency for Multi-Homing association and not offering differentiation in security while implementing IPSec over SCTP and Dynamic Address Reconfiguration is not possible in IPsec. The TLS was introduced by Dierks and Rescorla (2006) in which various security methods in Transport layer has been proposed. But the disadvantage of TLS over SCTP is that the control chunks of SCTP are highly unprotected during the exchange between two peer nodes during implementation.

The SCTP Aware Datagram Transport Layer Security (DTLS) introduced by Tüxen *et al*. (2011) is the advanced version of TLS for unreliable transport protocols. This method includes changes in the calculation of HMAC and allows each message to be independently verified. The drawback of DTLS is that DTLS cannot protect the control chunks which would be the target of attacks. Hence some adaptations are still necessary.

According to Wojciech and Wojciech (2012), 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*. (2013) 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.

Therefore, we 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 suggest a method to detect the hacker and choosing an alternative path to transmit the remaining packets using multi-Homing options.

PROPOSED METHODOLOGY

We proposed a dynamic encryption algorithm along with the information hiding techniques in SCTP to provide a secure end-to-end data transmission between two nodes by altering the basic structure of the existing SCTP packet format so that the attacker does not know the algorithm used since the algorithm is dynamic and the key for the encryption algorithm is hidden in the heartbeat signal of SCTP it is feasibly impossible for the attacker to hack the packets. In Case of detecting a hacker we are also proposing a new technique by efficiently utilizing the multi-homing facility of SCTP to choose the next network path when an attacker is detected in the primary path. The overall system architecture of our proposed method is shown in the Fig. 5.

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 relationship 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 the Fig. 6.

After the connection is established, the files or data is selected by the server or sender. In order to enhance security, three different encryption algorithms namely RSA, AES and DES were used. Based upon the file size, confidentiality/importance of the file, the appropriate encryption algorithm is chosen. If the file size is less and the confidentiality/importance of the file is low, then AES or DES encryption algorithm is used. For larger file size and high confidential files, RSA encryption algorithm is chosen by default. The key is

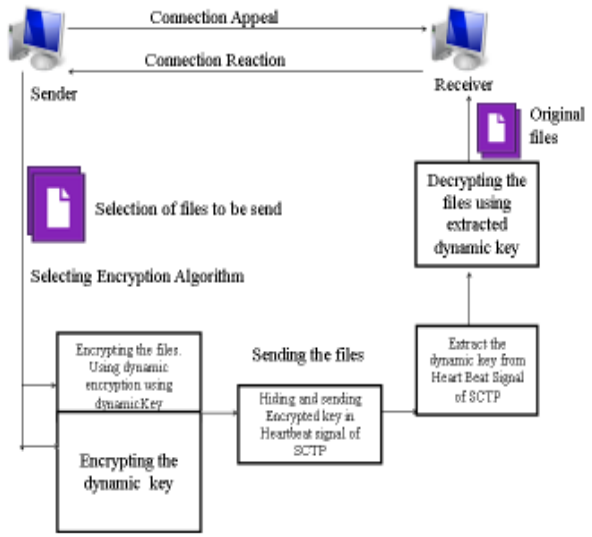

Fig. 5: System architecture

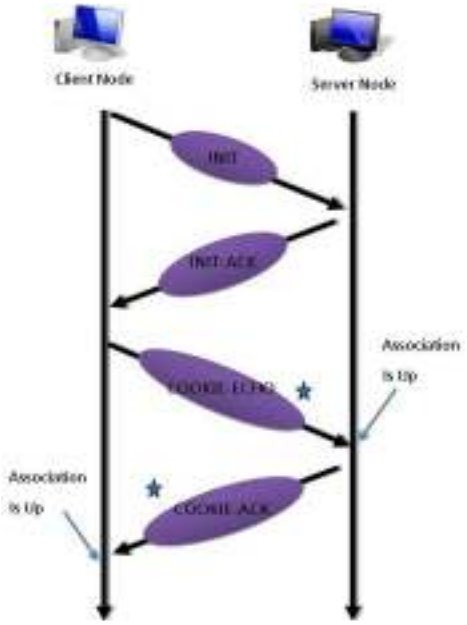

Fig. 6: Connection establishment

then encrypted by means of an encryption algorithm and sent it to the receiver by hiding the key in the

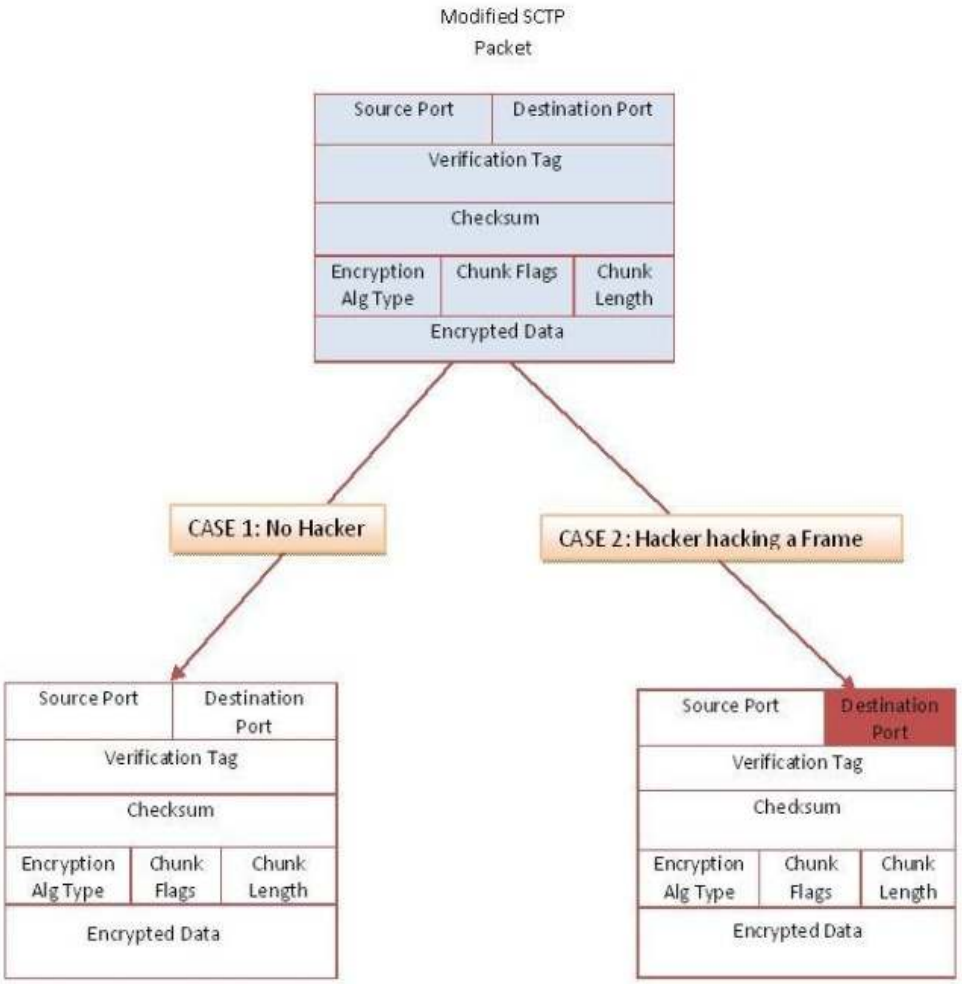

Fig. 7: Method to detect the hacker

Table 3: 4-bit code for selecting the algorithm

4-bit code	Algorithm used
0000	AES
0001	DES
0010	RSA

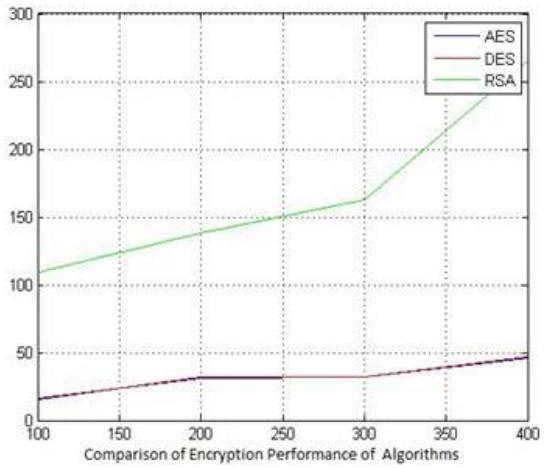

Fig. 8: Performance analysis of algorithms

heartbeat signal of SCTP. The algorithm in the receiver side is choosen from the modified SCTP packet which uses a 4-bit code for the notification of the algorithm to the receiver. The 4 bit code and the appropriate algorithm is shown in the Table 3.

The receiver on the other side extracts the key from the modified heartbeat signal of SCTP and decrypts the key by means of a decryption algorithm indicated by the 4-bit code in the encryption Type field of the modified SCTP packet. In case of a network attack we also suggest a method in which the attacker's address is stored in the destination address of the SCTP packet when an unauthorized user tries to hack the packet or access the packet and intimated to the sender. In Case of detecting a hacker the sender stops the transmission immediately and the selects the alternate/secondary path by efficiently utilizing the multi-homing facility of SCTP to transmit the remaining packet. The modified SCTP packet and scenario of the proposed method is shown in the Fig. 7.

RESULTS AND DISCUSSION

The modified SCTP packet contains an Encryption Algorithm Type which consists of 4 bit value from which the receiver can identify which encryption algorithm is chosen so that the appropriate decryption algorithm is selected to decrypt. The performance of the three encryption algorithms used in our proposed method is analyzed and the simulation graph for the Number of packets vs. Encryption time is shown in Fig. 8. Our simulation result shows that overall time taken to transmit the packets from the source to the destination yields better results when compared to the basic SCTP and provides Security in Multi-level than the basic SCTP.

CONCLUSION

Our proposed method yields a multilevel security by means of:

- Dynamic encryption algorithm
- By hiding the key in the heartbeat signal of SCTP
- By recording the IP address of the unauthorized user thereby detecting the attacker
- By efficiently utilizing the multi-homing facility of SCTP to choose the next network path when an attacker is detected in the primary path

Simulation result of our proposed method show that our method is highly secure to transmit data in SCTP when compared to the existing basic SCTP. This work can also be extended with other recent encryption algorithms for secure data transmission in SCTP.

REFERENCES

Anna, B., 2009. Reliable and secure communication in SCTP. Proceedings of the 1st International Workshop on Security and Communication Networks (IWSCN). Trondheim, pp: 1-6.

Daniel, T.W. and S. Abdallah, 2012. A review of multi-homing issues using the stream control transmission protocol. IEEE Commun. Surv. Tutorials, 14(2): 565-578.

Dierks, T. and E. Rescorla, 2006. The Transport layer Security (TLS) Protocol Version 1.1. RFC 4346. Retrieved from: http://www.rfc-base.org/rfc-4346.html.

Dreibholz, T., E.P. Rathgeb, I. Rüngeler and R. Seggelmann, 2011. Stream control transmission protocol: Past, current and future standardization activities. IEEE Commun. Mag., 49(4): 52-788.

Iyengar, J., P. Amer and R. Stewart, 2004. Retransmission policies for concurrent multipath transfer using SCTP multi-homing. Poceeding of the IEEE International Conference on Network, 2: 713-719.

Stewart, R., 2007. Stream Control Transmission Protocol. RFC 4960. Retrieved from: http://www.rfc-base.org/rfc-4960.html.

Tüxen, M., R. Seggelmann and E. Rescorla, 2011. Datagram transport layer security for stream control transmission protocol. IETF RFC 6083. Retrieved from: http://tools.ietf.org/html/rfc6083.

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.

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