



**INFORMATICS
INSTITUTE OF
TECHNOLOGY**

INFORMATICS INSTITUTE OF TECHNOLOGY

In Collaboration With

UNIVERSITY OF WESTMINSTER

Enhancing Security in Transport Layer

Dissertation by

Ms. Harshi Prabha Sepala Ratnayake

UoW Student ID: w1867857

IIT Student ID: 20210606

Supervised by

Mr. Geethapriya Liyanage

Submitted in partial fulfilment of the requirements for the MSc in Cyber Security and
Forensics degree at the University of Westminster.

May 2023

Abstract

TCP has been the main protocol contributed towards the evolution of internet for four decades. To start a TCP session, the three-way handshake between the client and the server happens in plain text. As per the literature at the design stage of the TCP, security was not considered. Therefore, TCP has inherent security problems and is subject to many attacks, especially DoS attacks involving SYN floods.

This research intended to find a comprehensive solution that would overcome these problems of TCP. A framework was developed identifying the requirements for a secure transport layer protocol. Then using that framework, a new protocol was designed. The proposed solution is called Alternative Transport Layer Protocol, which could be utilized as a guidance to develop and implement a fully-fledged protocol in future. It has an authentication mechanism, safeguards data confidentiality and integrity, TCP re-transmission problem handled, ensures large scale deployment, and end-to-end communication.

The proposed conceptual protocol was evaluated for its effectiveness in overcoming the security issues of TCP through self-evaluation and through evaluations by technical experts. The evaluation results were positive, and the conceptual protocol was identified as a viable framework to develop a secure transport layer protocol in future.

Keywords— TCP, security, three-way handshake, attacks, DoS, man-in-the-middle, sequence number, countermeasures, framework, alternative, confidentiality, integrity, authentication,