**ACKNOWLEDGEMENT**

I am highly indebted to **Prof. Malashree S** for her guidance and constant supervision as well as for providing necessary information regarding the project and also for her support in completing the project. We also take this opportunity to express our gratitude for her support, valuable information and guidance.

I would like to express my gratitude towards **Dr. K S Shridar** (Principal of PES University), **Dr. Shylaja S S**(HOD of ISE), members of PES University for their kind co-operation and encouragement which help me in completion of this project.

My thanks and appreciations also go to my colleagues in developing the project and people who have willingly helped me out with their abilities.

Abstract

A lot of DDoS attack is happening in the world of networking. SYN flooding is one of the primary and significant one which is basically flooding the server with SYN packets. At the same time we have real time switches coming up, which can be controlled from a remote host to control traffic and analyze the network packets. One such switch is a server switch by Pluribus Networks Company.

Our project basically uses both these information and aims at detecting and preventing these kinds of attack that’s happening in the field of networking. With the help of Pluribus Network Switch, certain commands are run in the switch remotely using Pluribus Netvisor Command Line Interface and the data is retrieved. This data is analyzed to check for possible DDoS attack and if it is found to be such a case then further prevention techniques are used where the IP address that is causing this attack is blocked and an e-mail is sent to the switch admin regarding the same.

**TABLE OF CONTENTS**

Chapter 1 - Introduction..........................................................................................1

Chapter 2 - Motivation and Aim…………………………………………………2

Chapter 3 - Literature Review……………...……………………………………3

* 1. Planes in Telecom Architecture…………..……………………..……..……..3
     1. Control Plane………………………….……………..………....3
     2. Data Plane…………………….………………………………...3
  2. Software Defined Networking…………………………………………………3
     1. Advantage of SDN…………………………...………..…………4
  3. Pluribus Switch…………………………………………………………..…….3
     1. What is Pluribus Switch? ………………………………..……….4
     2. Pluribus Netvisor Analytics Engine…….………………………...4
     3. Pluribus Command Line Interface…………………………...……..4
  4. Distributed Denial of Service-DDoS………………………….………….…....5
     1. DDoS Introduction………………………………………..……...5
     2. SYN flood…………………………………….……………...…..6
        1. Normal TCP 3-Way Hand shake……………...…..6
        2. TCP connection during attack scenario……………..6

Chapter 4 - Design…………………………….………………………….....….8

* 1. DDoS Detection technique………………………………………………….....8
  2. DDoS Prevention technique……………………………………….……….…..8
  3. Program Flow………………………………………………………….…...…..8
  4. Pseudo Code………………………………………………..……..………..…..9

4.4.1 Pseudo Code for Connection to Switch………………..…..9

* + 1. Pseudo Code for Data Retrieval and Detection…..….…..10
    2. Pseudo Code for Prevention……………………………..12

Chapter 5 - Future works and enhancements…………….……………...……..13

Chapter 6 - Snapshots……………….……………………………………..…...14

References……………………………………….…………………………..….17