**DETECTION OF DDoS ATTACK IN SDN ENVIRONMENT**

*Report submitted to the SASTRA Deemed to be University*

*as the requirement for the course*

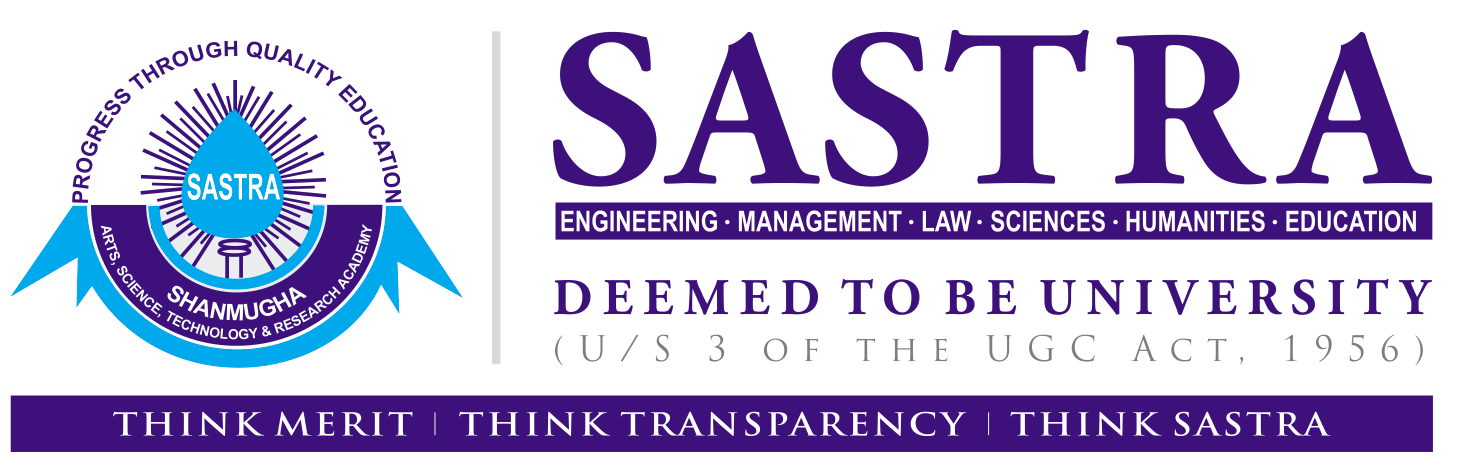
**CSE302: COMPUTER NETWORKS**

*Submitted by*

**JAISAIARUN P SRINIVASAN**

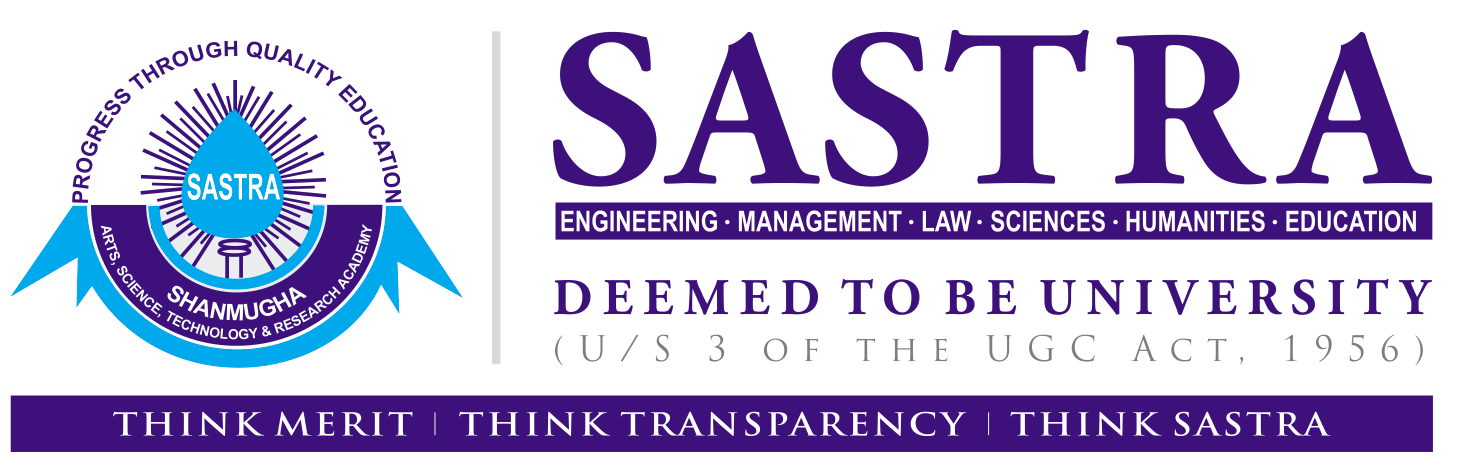
**Reg. No.:122003096, B.Tech COMPUTER SCIENCE**

**February 2021**



**SCHOOL OF COMPUTING**

**THANJAVUR, TAMIL NADU, INDIA – 613 401**



**SCHOOL OF COMPUTING**

**THANJAVUR– 613 401**

**Bonafide Certificate**

This is to certify that the report titled **“Detection Of DDoS Attack in SDN Environment”** submitted as a requirement for the course, **CSE302: COMPUTER NETWORKS** for B.Tech. is a bonafide record of the work done by **Shri Jaisaiarun P Srinivasan (Reg. No. 122003096,Computer Science)** during the academic year 2020-21, in the School of Computing

Project Based Work Viva voce held on \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Examiner-1 Examiner -2**

|  |  |  |
| --- | --- | --- |
| **Figure No.** | **Title** | **Page No.** |
| 2.1.1 | Network topology | 4 |
| 2.2.1 | Network Topology in SDN Emulator | 8 |
| 3.1.1 | Entropy vs Time Graph (No attack | 9 |
| 3.1.2 | Distance of Y vs Time graph (No attack) | 9 |
| 3.1.3 | Standard Deviation vs Time graph (No attack) | 10 |
| 3.1.4 | Entropy vs Time Graph (No attack) | 10 |
| 3.1.5 | Distance of Y vs Time graph (Attack) | 11 |
| 3.1.6 | Standard Deviation vs Time graph (Attack) | 11 |
| 3.1.7 | Entropy vs Time Graph (Attack) | 12 |
| 3.1.8 | Distance of Y vs Time graph (New Attack) | 12 |
| 3.1.9 | Standard Deviation vs Time graph (New Attack) | 13 |

**List of Figures**

**Abbreviations**

|  |  |
| --- | --- |
| SDN | Software Defined Networking |
| DDoS | Distributed Denial of Service |
| TCP | Transmission Control Protocol |
| OD | Origin Destination |
| PCA | Principal Component Analysis |
|  |  |

**Notations**

The student must explain the meaning of special symbols and notations used in the thesis. Define English symbols, Greek symbols, and Miscellaneous symbols separately. Some examples are presented below.

**English Symbols (in alphabetical order)**

|  |  |
| --- | --- |
| *p* | OD flows in a network |
| ***t*** | time intervals of interest |
| ***X*** | time series of all OD flows |
| ***Xi*** | ith ­OD flow |
| ***Xj*** | OD flows at time j |

**Greek Symbols (in alphabetical order)**

|  |  |
| --- | --- |
| ***λi*** | Eigen value |
| ∑ | Summation |
| ∞ | Infinity |

**Miscellaneous Symbols (in alphabetical order)**

|  |  |
| --- | --- |
| |x| | Absolute value of x |
| arg x | Argument of x |
| XT | Transpose of matrix X |

**Abstract**

Software defined networking (SDN) is a new emerging networking architecture, it fixes the needs of shortage of needs the traditional network does not support such as dynamic and scalable computing and storage needs for more computing environment. However, SDN also faces security problems, it is vulnerable to DDos attack. Distributed Denial of service (DDos) is a well know attack, but unlike in traditional networks, DDos not only damages the targeted server but also the SDN network by taking advantage of the devices limited buffer space and disturbing the resource allocation. Therefore it is very important have a rea-time detection system to identify the attack in the early stages.

In this report we start with basics of routing in SDN environment and identify the state of the network during a DDoS attack, it also introduces the new type of DDoS attack which is not possible in the traditional network. We discuss two different methodologies of identifying the attacks – Entropy and Principal Component Analysis (PCA), the pros and cons of these methodology and end the report with the discussion regarding which methodology is suited for the new type of DDoS attack.

**KEY WORDS:** Software Defined Networking (SDN), DDos Attack,

**Table of Contents**

|  |  |
| --- | --- |
| **Title** | **Page no.** |
| Bonafide Certificate | ii |
| List of Figures | iii |
| Abbreviations | iv |
| Notations | v |
| Abstract | vi |
| CHAPTER 1 |  |
| 1.1 Introduction | 1 |
| 1.2Existing System | 3 |
| CHAPTER 2 |  |
| 2.1Proposed System | 3 |
| 2.2 Implementation | 6 |
| CHAPTER 3 |  |
| 3.1 Result | 8 |
| 3.2 Discussion | 13 |
| Source Code | 14 |
| Snapshots | 51 |
| Conclusion and Future Plans | 53 |
| Reference | 54 |