

Table of Contents

1 Introduction	1
1.1 Problem Statement.....	4
1.2 Overview of the Proposed Model.....	4
1.2.1 Naïve Bayes Classifier	5
1.2.2 Windowing	5
1.2.3 Packet Based Windowing	6
1.2.4 Parameters for Transmission Control Protocol	7
2 DDoS Attack Tools	9
2.1 DDoS Attack Tools	10
2.2 Packet Capturing Tool	12
3 Classification of DoS and DDoS Attacks	14
3.1 DoS Attack Classification	15
3.1.1 Direct Attacks.....	15
3.1.2 Reflector Attack.....	16
3.1.3 Classification Based on Attacked Protocol Level	17
3.2 DDoS Attack Definition and Classification.....	18
3.2.1 Classification by Degree of Automation.....	19
3.2.2 Classification by Attack Rate Dynamics.....	20
3.2.3 Classification by Impact.....	20
3.2.4 Classification by Exploited Vulnerability.....	21
4 DDoS Strategy and Defense Problem	24
4.1 DDoS Strategy.....	25
4.1.1 Steps Involved In a DDoS	26
4.2 DDoS Defense Problem and Classification.....	27

5 DDoS Defense Classification	28
5.1 Intrusion Prevention.....	29
5.2 Intrusion Detection.....	30
5.3 Intrusion Tolerance and Mitigation	31
5.4 Classification by Deployment Location.....	32
6 Working Model	34
6.1 Practical Design Considerations.....	35
6.2 Architecture of the Working Model.....	36
6.3 Algorithm.....	37
6.4 Filtering Algorithm.....	38
6.5 Pseudo Code	38
6.5.1 Algorithm 1: Training Phase Functionality for TCP.....	39
6.5.2 Algorithm 2: Learning Module Algorithm for TCP.....	39
6.5.3 Smoothing and Probability Distribution	40
6.5.4 Band Grouping and Optimal Band Determination.....	40
6.5.5 Probability Updation.....	41
6.5.6 Algorithm 3: Optimal Band Determination Algorithm.....	42
6.5.7 Algorithm 4: Probability Updation Algorithm.....	43
6.6 Thresholding	44
6.6.1 Algorithm 5: Determining Threshold Probability.....	45
6.7 Probability Computation and Attack Detection	46
6.7.1 Algorithm 6: Determining Window Probability	46
6.7.2 Algorithm 7: Attack Detection.....	46
6.8 Tools Used.....	47

7 Observations.....	48
7.1 Graphical Output of Normal Traffic.....	49
7.2 Graphical Output of TCP Flood.....	50
7.3 Output generated by Wireshark.....	50
7.4 Output of Filtering Algorithm.....	51
7.5 Output of Attack Detection Algorithm.....	52
8 Conclusion and Future Work.....	53
References	55