Contents:

1 Introduction

1.1 Intrusion Detection....................1

1.1.1 Signature-based approach....................2

1.1.2 Classification-based approach....................2

1.1.3 Anomaly-based approach....................2

1.2 Intrusion Detection System....................2

1.2.1 Host-IDS....................2

1.2.2 Network-IDS....................3

1.3 DDoS....................3

1.4 DDos Detection Approaches....................3

1.4.1 Statistical Approach....................4

1.4.2 Soft-Computing approach....................4

1.4.3 Knowledge-based approach....................4

1.5 Motivation....................4

1.6 Objective....................5

1.7 Organisation of the Report....................5

2 Background....................6

2.1 DDoS Attack Fundamentals....................6

2.1.1 Direct DDoS....................6

2.1.2 Reflective DDoS....................7

2.2 DDoS Attack Architecture....................8

2.2.1 Agent Handler Model....................9

2.2.2 Internet Relay Chat Model....................10

2.3 Attack Classification....................11

2.4 Tools Used....................11

2.4.1 Wireshark....................11

2.4.2 Matlab....................12

2.5 Information Theoretic Measure....................13

2.5.1 Entropy....................13

2.6 Discussion....................15

3 **Related Work**..16

4 **Proposed Work**..18

4.1 DDoS Detection: Two Class Problem...18

4.2 DDoS Detection-Four Class Problem.. 19

4.3 Algorithm to detect and classify the attack pattern................ 19

5 **Implementation**..24

5.1 Dataset Used... 24

5.1.1 CAIDA DDoS ATTACK 2007 Dataset........................ 24

5.2 Experiment Methodology 24

5.3 Results and Analysis 24

5.3.1 Results for 2-class problem.................................... 24

5.3.2 Results for Protocol Specific Attack........................... 26

5.3.5 Results for Four Class Attack Detection...................... 27

6. **Conclusion And Future Work**.................................. 31

6.1 Conclusion... 31

6.2 Future Work...31

References

List of Figures

2.1 Direct DDoS Attack.. 7

2.2 Reflective DDoS Attack.. 8

2.3 Agent Handler Attack Network.. 9

2.4 IRC Attack Network.. 10

2.5 Snapshot of Wireshark.. 12

4.1 Conceptual framework of attack Detection... 18

4.2 Flowchart of Proposed Algorithm... 19

5.1 Entropy evaluation for Normal Dataset... 25

5.2 Entropy evaluation for Attack Dataset... 25

5.3 Protocol attack comparision... 26

5.4 Constant rate attack entropy variation.. 29

5.5 Subgroup attack entropy variation... 29

5.6 Entropy variation for Increasing Rate attack...................................... 30

5.7 Entropy variation for Pulsing attack.................................... 30

List of Tables

5.1 Results of Protocol Specific Attack.. 26

5.2 Increasing Rate Attack Type... 27

5.3 Sub-Group Attack Type... 27

5.4 Pulsing Attack Type... 28

5.5 Constant Rate Attack Type... 28