Contents

Page no.

1. INTRODUCTION 1

1.1 Intrusion 1

1.2 Intrusion Detection 2

1.3 Intrusion Detection System 3

1.4 Types of Intrusion Detection Systems 4

1.5 Intrusion Detection Approaches 5

1.6 Elements of a generic Anomaly Network Intrusion Detection System 6

1.7 Issues in existing Intrusion Detection Systems 7

1.8 What is DDoS attack? 8

1.8.1 Causes of DDoS attacks 8

1.8.2 Symptoms and Manifestations 8

1.8.3 Working of DDoS attacks 9

1.9 Existing methods for DDoS attack detection 9

1.10 Motivation 10

1.11 Contribution 10

1.12 Organization of Report 11

2. FUNDAMENTALS OF DDOS ATTACKS 12

2.1 DDoS attack overview 12

2.2 DDoS attack strategy 13

2.3 DDoS goals 13

2.4 DDoS attack architecture 13

2.4.1 The Agent Handler Model 13

2.4.2 Internet Relay Chat (IRC) based model 14

2.5 DDoS attack parameters 14

2.6 Taxonomy of DDoS attacks 16

2.7 Discussions 22

3. RELATED WORK 23

3.1 Statistical Methods 23

3.2 Soft - Computing Methods 24

3.3 Knowledge – based Methods 25

3.4 Data Mining – based Methods 25

3.5 Ensemble - based Methods 26

3.6 Discussions 26

4. DATASET DESCRIPTION 28

4.1 Dataset used 28

4.2 Characteristics of Dataset 29

4.3 DDoS attack Categorization in CAIDA Dataset 30

4.3.1 Low – Rate attack 30

4.3.2 Constant – Rate attack 30

4.3.3 Increasing - Rate attack 31

4.3.4 Intermittent - Rate attack 31

4.4 Description of Tools Used 32

4.5 Discussions 35

5. PROPOSED MODELS 36

5.1 Detection of Predictable and Non Predictable Rates of DDoS attacks 36

5.1.1 Description of Work 40

5.2 Source IP segregation method for DDoS attack detection 42

5.2.1 Description of Work 42

5.3 Detection of Protocol Flooding attack 45

5.3.1 Description of Work 46

6. EXPERIMENTATION & RESULT 47

6.1 Environment worked on 47

6.2 Detection of Predictable and Non Predictable Rates of DDoS attacks 47

6.2.1 Data Analysis 54

6.2.2 Results & Discussions 57

6.3 Source IP based segregation method for DDoS attack detection 58

6.3.1 Data Analysis 58

6.3.2 Discussion 62

6.4 Detection of DDoS Protocol Flooding 63

6.4.1 Data Analysis 63

6.4.2 Results 67

6.4.3 Discussions 68

7. Conclusion 69

7.1 Future Work 70

8. References 71

List of figures:

	Page no.
Figure 1: Intrusion Detection System	03
Figure 2: Taxonomy of IDS	04
Figure 3: A generic architecture of ANIDS	07
Figure 4: DDoS attack	12
Figure 5: Agent Handler attack model	14
Figure 6: IRC-based attack model	15
Figure 7: A comparison between normal traffic and CAIDA DDoS traffic	16
Figure 8: CAIDA traffic profile	29
Figure 9: Increasing rate DDoS attack	31
Figure 10: Pulsing rate DDoS attack	31
Figure 11: Constant rate DDoS attack	32
Figure 12: Subgroup rate DDoS attac	32
Figure 13: Rawcap interface	32
Figure 14: Traffic client and server	33
Figure 15: Wireshark interface	34
Figure 16: Splitcap	34
Figure 17: Proposed test bed for the future	70

List of Tables:

Page no.

Table 1: Correlation of 5 minute interval (25th – 30th min) 48 - 49

Table 2: Correlation of 5 minute interval (30th – 35th min) 50 - 51

Table 3: Correlation of 5 minute interval (45th – 50th min) 52 - 53

Table 4: Packet rates of the samples of a 5 sec window 58

Table 5: Sorted packet rates and IP address of the sample of the 5 sec window 58

Table 6: Packet rates from 1 second window from (45th – 50th min) time interval 60

Table 7: Packet rates from 1 second window from (45th – 50th min) time interval 61

Table 8: Protocol Flooding 1 for 5 minute window 63 – 65

Table 9: Protocol Flooding 2 for 5 minute window 65 – 66

List of Graphs:

Page no.

Graph 1: Correlation vs Time graph (25th to 30th min) 54

Graph 2: Correlation vs Time graph (30th – 35th min) 55

Graph 3: Correlation vs Time graph (45th – 50th min) 56

Graph 4: Increasing rate DDoS attack graph 59

Graph 5: Constant rate DDoS attack graph 60

Graph 6: Pulsing rate DDoS attack graph 61

Graph 7: ICMP Flooding graph 67

Graph 8: TCP/ICMP Flooding graph 67