CONTENTS

1. Introduction 1-3

1.1 Network security 1
1.2 SYN Flooding 1
1.3 Aim 2
1.4 Proposed work and objectives 2
1.5 Outline of the project 2
1.6 Organization of the Dissertation 3

2. Background 4-15

2.1 Intrusion Detection System 4
2.1.1 IDS Terminology 4
2.1.2 Types of Intrusion Detection Systems 5
2.1.3 Anomaly based IDS- Modes of Operation 5
2.1.4 Reporting of anomalies 6
2.2 Syn Flooding Attack 7
2.2.1 How the attack works 7
2.2.2 Backlog Queue 11
2.3 Some Built-In mechanisms to overcome Syn Flood Attacks 11
2.4 Launching syn flood attack 13
2.5 Observed effect of syn flooding attack 13
2.6 Detection of syn flood attack 14
2.7 Discussion 15

3. Intrusion Detection System algorithms 16-19

3.1 Adaptive threshold algorithm 16
3.2 CUSUM (Cumulative SUM) algorithm 17
3.3 Advantage of CUSUM over Adaptive Threshold Algorithm 18
3.4 Anomaly Detection with Real Time Incremental Clustering 18
3.5 Discussion 19

4. **Network traffic capture** 20-27

4.1 Introduction 20

4.1.1 Promiscuous Mode 20

4.1.2 Port Mirroring and Mirror Port 20

4.2 Packet Capture 23

4.3 Traffic Analysis tool 23

4.4 Test Bed 25

4.5 Discussion 27

5. **Feature extraction and dataset preparation** 28-42

5.1 Traffic capture 28

5.2 Dataset preparation 30

5.3 Feature construction 34

5.3.1 Content based features 35

5.3.2 Time based features 37

5.3.3 Connection based features 40

5.4 Combining time based and connection based features 41

5.5 Discussion 42

6. **Data classification** 42-49

6.1 Clustering analysis 42

6.1.1 Clustering algorithms 42

6.1.1.1 Hierarchical Methods 42

6.1.1.2 Partitioning Relocation 43

6.2 Discriminative analysis 45

6.2.1 Knn 45

6.3 Classification of dataset using k-means and knn algorithm 48

6.4 Challenges of accurate classification 49

6.5 Discussion 49

7. **Conclusions and future work**

7.1 Conclusion 50

7.2 Future work 50