

Contents

Page no

Chapter 1

Introduction	1
1.1 Aim of work.....	2
1.2 Objectives	2
1.3 Organization of the report	3

Chapter 2

Anomaly Detection: an overview.....	4
2.1 Network anomalies.....	4
2.2 Type of anomalies.....	4
2.3 Anomaly detection mode.....	6
2.4 Various anomaly detection approaches.....	7
2.5 Discussion.....	10

Chapter 3

Dataset Preparation.....	11
3.1 Testbed setup.....	11
3.2 Launching of real life attack.....	12
3.2.1 Port scanning.....	12
3.2.2 DoS attack.....	13
3.2.3 Distributed Denial of Service attack.....	17
3.3 Packet level network traffic capturing and dataset preparation.....	20
3.3.1 Preprocessing.....	22

3.3.2 Feature Extraction.....	22
3.3.3 Correlation of various features.....	27
3.4 Flow level network traffic capturing and dataset preparation.....	27
3.4.1 Network flow capturing.....	28
3.4.2 Preprocessing.....	31
3.4.3 Feature extraction.....	32
3.4.4 Correlation of various features.....	34
3.5 Discussion.....	34

Chapter 4

Supervised and unsupervised algorithms.....	35
4.1 Classification algorithms.....	35
4.1.1 Decision tree.....	35
4.1.2 Decision table.....	36
4.1.3 Naive Bayes Algorithm.....	36
4.1.4 Bayes Network Classifier	38
4.1.5 Sequential minimal optimization (SMO).....	38
4.2 Clustering Algorithms.....	39
4.2.1 k-means.....	39
4.2.2 PAM.....	40
4.2.3 CLARA.....	40
4.2.4 diana.....	40
4.2.5 Fanny.....	41

4.3 Outlier Detection Algorithm.....	41
4.4 Discussion.....	42

Chapter 5

Experimental Study.....	43
5.1 KDD CUP'99 dataset.....	43
5.2 Supervised Technique.....	44
5.3 TUIDS Dataset.....	47
5.4 Unsupervised Technique.....	50
5.5 Discussion.....	53

Chapter 6

Conclusion and Future work.....	54
References	55

List of figures:

Sl no.	Figure Name	Page no.
1	Testbed setup	11
2	A typical synflood attack in networks	18
3	A smurf attack in networks	19
4	A fraggle attack in networks	20
5	Three level hybrid classifier	45
6	Detection rate of different classifiers in DDoS dataset	49
7	Detection rate of different classifiers in Probe dataset	49
8	Outlier score Vs Type of packet	50
9	Cluster Validation Model	51

List of tables:

Table No.	Table Name	Page No.
1	Different anomaly based intrusion detection techniques	7
2	List of DoS attacks present in Targa tool	14
3	some available option in GULP	21
4	Description of basic features	23
5	Description of content based features	24
6	Description of time based features	26
7	Description of connection based features	26
8	Properties of flow	28
9	List of parameters filter out from captured data	31
10	basic features of flow data	32
11	Description of time based features	33
12	Description of connection based features	33
13	Number of attacks in KDD CUP'99 dataset	43
14	Detection rate of different classifiers	44
15	Detection rates of stage-1 classifiers	45
16	Detection rates of stage-2 classifiers	46
17	Detection rates of stage-3 classifiers	46
18	Number of attack instances in DDoS dataset	47
19	Number of attack instances in Probe dataset	47
20	List of attributes of our own real-life dataset	47
21	Internal validation report of different clustering algorithms	52
22	Optimal Scores	52