Table of Contents

1. Introduction **1**

1.1 Intrusion & Its Types 1

1.1.1 Categories of Intrusions 2

1.2 Intrusion Detection Systems & Its Types 3

1.3 IDS Based on Application 5

1.4 State-of-the-Art 7

1.5 Problem Definition 9

1.6 Aim of the Work 9

1.6.1 Objectives 10

1.7 Organization of the Dissertation 10

2 Anomaly Network Intrusion Detection System (ANIDS) Preliminaries **11**

2.1 ANIDS: A Generic Architecture 11

2.2 Description of the Modules 12

2.3 Anomaly & Its Types 13

2.4 Proximity Measures 14

2.5 Anomaly Score 15

2.6 Discussion 15

3. Related Works on ANIDS **16**

3.1 Supervised Approaches 16

3.2 Semi-Supervised Approaches 18

3.3 Unsupervised Approaches 19

3.4 Hybrid IDS 23

3.5 General Comparison 24

3.6 Discussion 25

3.7 KDD-99 Dataset 26

4. Network Anomaly Detection Using Clustering Approach 30

4.1 Intrusion Detection with Unlabeled Data Using Clustering 30

4.1.1 How to Cluster 31

4.1.2 Normalized model 31

4.1.3 Intrusion detection 32

4.2 Y-MEANS: A Clustering approach for intrusion detection 32

4.2.1 Splitting Clusters 33

4.2.2 Merging Clusters 33

4.2.3 How to Detect 34

4.3 ADWICE - Anomaly Detection with Real-time Incremental Clustering ..34

4.3.1 The Anomaly Detection Algorithm 35

4.3.2 Detection 36

4.3.3 Adaptation of the Normality model 37

4.3.4 Scalability and Performance 37

5. Proposed Work 38

5.1 Background of Work 38

5.1.1 Attribute Frequency Vector of categorical Attribute 39

5.1.2 Centroid Frequency Vector 40

5.1.3 Distance Measurement 40

5.2 Clustering Process 41

5.2.1 Modified k-mean algorithm 42

5.2.2 How modified k-means algorithm works 44

5.3 Labeling Process 45

5.3.1 Outlier detection Process 45

6. Experimental Results **47**

6.1 Performance Measure 47

6.2 Dataset Preparation 47

6.3 Results 48

7. Conclusion and Future works **50**

References **51**