

Table of Contents

Abstract	I
Acknowledgments	III
Table of Contents.....	IV
List of Figures.....	VIII
List of Tables	X
List of Equations.....	XII
List of Symbols and Abbreviations.....	XIII
Chapter 1 Introduction	2
1.1 Research Motivation	2
1.2 Literature Review	3
1.3 Aim of the work	4
1.4 Contributions	5
1.5 Thesis Outline	6
Chapter 2 Intrusion detection systems	10
2.1 Basic Intrusion detection terminology	10
2.1.1 Intrusion	10
2.1.2 Intrusion detection	10
2.1.3 Intrusion Detection System.....	11
2.1.4 Firewall	14
2.2 Intrusion detection systems and firewalls	15
2.3 Intrusion taxonomy.....	16

2.3.1 Attack type.....	17
2.3.2 Number of connections involved in attacks	24
2.3.3 Source of Computer Attacks	24
2.4 Intrusion detection taxonomy.....	24
2.4.1 Environment	25
2.4.2 Detection Engine.....	28
2.4.3 Overall architecture	30
2.4.4 Time.....	31
Chapter 3 Machine learning and neural networks	33
3.1 Machine learning	33
3.2 Machine learning techniques.....	35
3.2.1. K-nearest neighbor	37
3.2.2. Support vector machines	39
3.2.3. Artificial neural networks.....	41
3.2.4. Self-organizing maps.....	42
3.2.5. Decision trees	43
3.2.6. Bayes networks.....	43
3.2.7. Genetic algorithms.....	44
3.2.8. Fuzzy logic.....	44
3.3 Neural networks	45
3.4 Multilayer perceptrons.	46
3.4.1 Strengths of BP Learning	49

3.4.2 Deficiencies of BP Learning	50
3.5 Back propagation learning algorithm	51
3.5.1 Incremental mode.....	51
3.5.2 Batch mode.....	52
3.6 Radial basis function	53
3.7 Radial basis function learning algorithm	55
3.7.1 The first learning algorithm.....	55
3.7.2 The second learning algorithm.....	56
3.7.3 The third learning algorithm	57
Chapter 4 The DARPA 98 KDD99 benchmark data set.....	59
4.1 Overview.....	59
4.2 KDD Cup 1999 Data files	64
Chapter 5 The proposed system architecture	66
5.1 Overview.....	66
5.2 Data Preprocessing Stage.....	68
5.2.1 Adding columns headers:-	68
5.2.2 Sampling:-.....	68
5.2.3 Encapsulating the 22 attacks:-	76
5.2.4 Encoding the symbolic features:-	76
5.3 Building Neural network IDS (two engines):-.....	77
5.4 Metrics used to analyze the results:-	77
5.4.1 Detection rate (DR)	77

5.4.2 False positive alarm rate (FPR)	77
5.4.3 A confusion matrix (CM)	77
Chapter 6 Experimental results.....	80
6.1 Overview.....	80
6.2 Five categories system using 10% version of KDD Cup 99 (FCS 10 KDD) ..	80
6.3 Five categories system using the proposed reduced data set (FCS P KDD)	85
6.3.1 Comparing Performance under the two sets (FCS).....	87
6.4 Two categories system using 10% version of KDD Cup 99 (TCS 10 KDD) .	88
6.5 Two categories system using the proposed reduced data set (TCS P KDD)	92
6.5.1 Comparing Performance under the two sets (TCS)	94
6.6 Alternative approach	95
6.6.1 Five categories system using the proposed reduced data set and RBF (FCS P KDD).....	95
Chapter 7 Conclusions and future work	100
7.1 Conclusions.....	100
7.2 Future work	102
Publication.....	105
References.....	107