CONTENTS

Abstract *i*

Acknowledgment *ii*

Contents *iii*

List of Figures *vi*

List of Tables *vii*

Chapters **Page No.**

Chapter 1: Introduction **01**

1.1 Overview 01

1.2 Network Security 01

1.2.1 Intrusion Detection System 01

1.2.2 Attack Classification 02

1.3 Machine Learning and its Applications 02

Chapter 2: Literature Survey **05**

2.1 Intrusion Detection Systems 05

2.1.1 Signature Based Detection 05

2.1.2 Statistical Anomaly Based Detection 05

2.2 Machine Learning 05

2.2.1 Supervised Learning 06

2.2.2 Unsupervised Learning 07

2.2.3 Reinforcement Learning 07

2.3 Types of Anomaly Based Detection 08

2.3.1 Statistical Anomaly Detection 08

2.3.2 Data Mining Based Approach 10

2.3.3 Knowledge Based Detection Techniques 11

2.4 Statistical Modeling 12

2.4.1 Markov Models 12

2.4.2 Markov Chains 13

2.4.3 Hidden Markov Models 13

2.4.4 HMM Based Related Work 15
2.5 Naive Bayes Classifier 16
2.5.1 Bayes Theorem 16
2.5.2 Formal Definition and Background 17
2.5.3 Properties of Naive Bayes 18
2.5.4 Advantages and Limitations 19
2.5.5 Recent Research in Network Anomaly Detection using NBC 19
2.6 Proposed System 21
Chapter 3: System Analysis 22
3.1 Requirements 22
3.1.1 Hardware Requirements 22
3.1.2 Software Requirements 22
3.1.3 Functional Requirements 22
3.2 Datasets 23
Chapter 4: System Design 26
4.1 Design Considerations 26
4.1.1 Modules 26
4.1.2 Use Case Diagram 28
4.1.3 Sequence Diagram 29
4.1.4 Data Flow Diagram 30
4.1.5 State Diagram 30
Chapter 5: Implementation 32
5.1 Language Used for Implementation 32
5.1.1 Python 32
5.2 Libraries Used for Implementation 33
5.2.1 NumPy 33
5.2.2 Flask 34
5.2.3 Matplotlib 34
5.3 Procedure Description 35
5.3.1 Determine Optimal Bands Procedure 35
5.3.2 Update Probabilities Procedure 35
5.3.3 Train Procedure 35

5.3.4 Train Phase Procedure 36
5.3.5 Determine Probability Procedure 36
5.3.6 Determine Threshold Probability Procedure 36
5.3.7 Deploy Procedure 36
5.3.8 Parse Procedure 36
Chapter 6: Results **37**
6.1 Screenshots 37
6.2 Results Obtained 41
Chapter 7: Conclusion **42**
Chapter 8: Challenges and Future Work **43**
Appendix **44**
Bibliography **49**