

CONTENTS

| | |
|---|----|
| 1. Introduction | 01 |
| 1.1 Motivation | 03 |
| 1.2 Problem Definition | 04 |
| 1.3 Objectives | 04 |
| 1.4 Work Done | 04 |
| 1.5 Organization of the Dissertation | 05 |
| 2. Background Studies | 06 |
| 2.1 Domain Name System (DNS) | 07 |
| 2.1.1 Vulnerability in DNS | 08 |
| 2.1.2 Why DNS? | 09 |
| 2.1.3 Limitation of DNS Based Detection | 10 |
| 2.2 Botnet Overview | 10 |
| 2.2.1 Life-Cycle of a Botnet | 10 |
| 2.2.2 Botnet Malicious Behaviour | 11 |
| 2.2.3 Command and Control models | 12 |
| 2.2.4 Communication Protocols | 14 |
| 2.2.5 Fast Flux and Domain Flux | 15 |
| 2.2.5 Botnet Detection Approaches | 15 |
| 3. Existing DNS based Botnet Detection Techniques | 18 |
| 3.1 Kulczynski Ratio Similarity Method | 19 |
| 3.2 Jaccard's Ratio Similarity Method | 20 |
| 3.3 Bayesian Bot Detection Method | 21 |
| 3.4 X-means Clustering Method | 25 |
| 3.4.1 Cosine Similarity | 26 |
| 3.4.2 Algorithm for X-means Clustering | 27 |
| 3.4.3 Sequential Probability Ratio Testing (SPRT) | 29 |
| 4 Experimental Study on the Existing Mechanisms | 31 |
| 4.1 Software Used | 32 |
| 4.2 Hardware Used | 32 |

| | |
|--|----|
| 4.3 Data Collection | 32 |
| 4.4 Preprocessing | 33 |
| 4.5 Feature Extraction | 33 |
| 4.5.1 Types of Features | 33 |
| 4.6 Dataset Preparation | 33 |
| 4.7 Experimental Observation | 34 |
| 4.7.1 Kulczynski Ratio Similarity Method | 34 |
| 4.7.2 Jaccard's Ratio Similarity Method | 35 |
| 4.7.3 Bayesian Bot Detection Method | 36 |
| 4.7.4 X-means Clustering Method | 37 |
| 4.7.5 Hybrid Method | 38 |
| 4.8 Comparison Among the implemented methods | 39 |
| 4.9 Limitations | 41 |
| | |
| 5. Conclusion And Future Work | 42 |
| 5.1 Conclusion | 43 |
| 5.2 Future Work | 43 |
| | |
| References | 44 |