Contents

1 Introduction 1

1.1 Introduction 1

1.1.1 Types of DDoS Attack 2

1.2 The Strength of DDoS Attackers 5

1.3 Motivation 6

1.4 Desired Features of a DDoS Attack Defense System 8

1.5 Objectives of the Research 8

1.6 Thesis Contribution 9

1.7 Thesis Organization 10

2 Related work and Background 12

2.1 Introduction 12

2.2 Types of DDoS Defense Mechanisms 13

2.3 Related Work 14

2.3.1 Statistical Approaches 14

2.3.2 Supervised Machine Learning Based Approaches 16

2.3.3 Unsupervised Machine Learning Based Approaches 17

2.3.4 Packet Marking and IP Traceback Based Approaches 17

2.3.5 Rate Limiting Based Approaches 19

2.3.6 SDN and Cloud Based approaches 20

2.3.7 Surveys 20

2.4 Background 20

2.4.1 Cryptographic Hash Function 21

2.4.2 Hash Table 21

2.4.3 Bloom Filter 22

2.4.4 Datasets Used in the Research 22

2.5 Discussion 25

3 A Light Weight DDoS Attack Detection Mechanism 26

3.1 Introduction 26

3.2 Violating Source IP Count(VSC)- a Light Weight DDoS Detection Mechanism . . . 28
3.2.1 Overview of Violating Source IP Count . . . 29
3.2.2 Theory Behind VSC . . . 31
3.3 Performance Evaluation . . . 34
3.3.1 VSC Under Normal Condition . . . 34
3.3.2 Detection of Low Rate DDoS Attack . . . 34
3.3.3 Detection of Randomly Spoofed Source IP Attack . . . 34
3.3.4 Detection of DDoS Attack From a Small Size Botnet . . . 40
3.3.5 Detection of DDoS Attack in CAIDA-2007 Dataset . . . 40
3.4 Discussion . . . 40

4 A DDoS Detection and Mitigation System Based on Bidirectional Nature of Internet Communications 41
4.1 Introduction . . . 41
4.2 DDoS Detection and Mitigation System (DDM) . . . 44
4.2.1 Agent-based Bidirectional Information . . . 48
4.2.2 Deployment of the Defense System At An Edge Router . . . 49
4.2.3 Implementation Details of DDM . . . 52
4.3 Experiments and Results . . . 55
4.3.1 Experiment 1 . . . 55
4.3.2 Experiment 2 . . . 57
4.3.3 Experiment 3 . . . 59
4.3.4 Experiment 4 . . . 60
4.4 Discussion . . . 61

5 Packet Marking Based Anti Spoofing Techniques 64
5.1 Introduction . . . 64
5.2 Motivation . . . 66
5.3 XORID . . . 69
5.3.1 Analysis of XORID . . . 70
5.4 A General Architecture of Source Identification Mark Based Spoofing Attack Defense System . . . 75
5.4.1 Deployment Location of The Defense System . . . 77
5.5 Limitations of Path Encoding Schemes . . . 78
5.5.1 Source End Marking(SEM) . . . 79
5.5.2 How SEM is Different From Path Based Marking Schemes . 84
5.5.3 Experimental Evaluation of SEM . . . 86
5.6 Discussion . . . 87

6 A Logging Based IP Traceback Mechanism 89

6.1 Introduction 89
6.2 Singleton Flow Traceback(SFT)-The Proposed Traceback Mechanism 92
6.2.1 Flow Recording Process At Intermediate Routers By SFT . 94
6.2.2 Tracing Back a Flow 98
6.2.3 Implementation Details of the Log Tables 100
6.3 Analysis of SFT 102
6.3.1 Analysis of False Negative Rate of SFT 102
6.3.2 Analysis of False Positive Rate of SFT 104
6.3.3 Computational Overhead At Intermediate Routers 112
6.3.4 Traceback Time 113
6.3.5 Storage Requirement 113
6.4 Discussion 113

7 Conclusion and Future Work 114
7.1 Thesis Contribution 114
7.2 Discussion 115
7.3 Future Research 117
7.3.1 Software Defined Network(SDN) Based DDoS Solution . . . 118
7.3.2 DDoS Attack in Cloud Computing Environment 118
7.3.3 DDoS Mitigation System Against IoT Based Botnet 119
7.3.4 DDoS Mitigation System Against Critical Infrastructure Systems 120

A TUCANNON: A DDoS Attack Generation Tool 122
A.1 Introduction 122
A.2 Basics of TUCANNON 124
A.2.1 Server Program 125
A.2.2 Client Program 131
A.3 Demonstration of TUCANNON 131
A.3.1 Attack Scenario 1 132
A.3.2 Attack Scenario 2 133
A.3.3 Attack Scenario 3 134
A.3.4 Attack Scenario 4 135
A.4 Discussion 136