Contents

Contents vii

List of Figures ix

List of Tables x

1 Introduction 1

1.1 Motivation 2

1.2 Objective 2

1.2.1 Problem Definition 2

1.2.2 System Model 3

1.3 Related Works 3

1.4 Work Done 5

1.5 Dissertation Organization 5

2 Intrusion Prevention System 6

2.1 Network Attacks 6

2.1.1 Categories of Attacks 7

2.1.2 Attackers' Perspective 10

2.2 Intrusion Detection 12

2.2.1 Techniques of Intrusion Detection 12

2.2.2 Types of Analysis Techniques 13

2.2.3 Existing Intrusion Detection Systems 15

2.3 Intrusion Prevention 16

2.3.1 Functions of IDPS 16

2.3.2 Requirements of IDPS 18

2.3.3 Common detection Methodologies of IDPS 18

2.3.4 Types of IDPS based on Deployment 19
2.3.5 Components in IDPS technology 21
2.3.6 Risk associated with IDPS 21
2.4 Snort as an IDPS tool 23
2.4.1 Snort Architecture 23
2.4.2 Rules in Snort 24
2.4.3 Writing Rules 24

3 DDoS Attack and Defence 27
3.1 Introduction 27
3.1.1 DDoS Attackers Motives 28
3.1.2 DDoS Attack: Scope and Classification 29
3.2 DDoS Defence Mechanism 30
3.2.1 DDoS Defence: Scope and Classification 30
3.2.2 DDoS defence: Performance Measurement Metrics 30

4 Proposed Framework 32
4.1 Simulation Design 32
4.1.1 Network topology 32
4.1.2 Network Specifications 33
4.1.3 Packet generation 34
4.1.4 An Approach for UDP Flooded DDOS Attack Detection . 35

5 Simulation Results 36
5.1 Environment Used 36
5.1.1 Network Simulator 2 36
5.1.1.1 Basic Architecture 36
5.1.1.2 Running NS2 Simulation 37
5.1.2 Gnuplot 38
5.2 Experimental Results 38
5.2.1 Results (External DDOS attack) 39
5.2.2 Results (External and Internal DDOS attack) 42
5.2.3 Results (Applying Network Tolerance) 45

6 Conclusion and Future Work 47

Bibliography 48

List of Figures

1.1 Network Environment considered for Simulation in NS2 3

2.1 Attack affecting CID 9
2.2 Relationship between the categories and types of attacks 11

3.1 Categories of DDoS attacks and their sub-types 29
3.2 Categories of DDoS defence mechanisms and their sub-types . . . 30

4.1 Network Diagram for study in NS2 32
4.2 Network Structure 34
4.3 Steps in the Detection algorithm 35

5.1 Basic Architecture of NS2 37
5.2 Normal traffic graph 39
5.3 Average bandwidth consumed in normal traffic 39
5.4 Attack traffic graph 40
5.5 Average bandwidth consumed in attack traffic 40
5.6 Graph of traffic after prevention mechanism 41
5.7 Average of bandwidth consumed after prevention 41
5.8 Normal traffic graph 42
5.9 Average bandwidth consumed in normal traffic 42
5.10 Attack traffic graph 43
5.11 Average bandwidth consumed in attack traffic 43
5.12 Graph of traffic after prevention mechanism 44
5.13 Average of bandwidth consumed after prevention 44
5.14 Network Scenario to study Tolerance 45
5.15 Bandwidth Comparison before monitoring node is introduced . . . 45
5.16 Bandwidth Comparison after monitoring node is introduced . . . 46

List of Tables

2.1 Attacks affecting CID of a network 10

2.2 Different IPS systems and their specifications 17

2.3 The Three Major Detection Techniques 20

2.4 Risk Involved in IDS probe 22

2.5 Risk involved in IDS Management Console 22

2.6 Function of Action section of Rules 25

2.7 Function of the Option section of Rules 25

4.1 UDP Traffic Node Specifications 33

4.2 Router Node Specifications 33

4.3 Router Node Specifications 33