

Contents

Acknowledgements	i
Abstract	ii
Contents	iii
List of Figures	v
List of Tables	vi
1 Introduction	1
1.1 DDoS attack	1
1.2 Types of DDoS Attack	1
1.3 Security Issues for defense of DDoS attack	5
1.4 Defense Goals	7
1.5 Location Point of Defense	8
1.5.1 Autonomous Defense	8
1.5.2 Victim-End Defense	8
1.5.3 Intermediate Network Defense	9
1.5.4 Source-End Defense	9
1.6 Motivation	10
1.7 Contribution	11
1.8 Organization	11
2 Related Work	12
2.1 General Approach	12
2.2 Filtering Approach	15
2.3 Discussion	18
3 Proposed Work	19
3.1 Problem Definition	19
3.2 Proposed frame of work	19
3.3 Random attack generation procedure	21
3.4 Prevention procedure	22
4 Experimental Results	23
4.1 Environment Used	23
4.2 Results	23

4.3 Discussion	31
5 Conclusion and Future Work	32
Appendix	32
Bibliography	33

List of Figures

1.1	DDoS Attack Scenario	2
1.2	Different DDoS attack and their Vulnerabilities	2
1.3	DWARD deployment	10
3.1	Main frame of simulation	20
4.1	Simulation of main frame of work	24
4.2	Showing legitimate CBR connection	24
4.3	Showing a non registered node as Node17	25
4.4	Showing result while having a non legitimate connection	25
4.5	Showing normal traffic flow	26
4.6	Graph for normal traffic flowing	26
4.7	Showing an attack scenario	27
4.8	Graph for a simple attack	27
4.9	Graph for a random attack by one attacker	28
4.10	Graph for random attacks by two attacker	28
4.11	Graph for average of random attacks by two attacker	29
4.12	Graph for prevention of attacks	29
4.13	Zoom view of the Graph for prevention of attacks	30
4.14	Graph for prevention of average of attacks	30

List of Tables

1.1	Vulnerabilities cataloged in recent years.	4
2.1	Different General Approaches	14
2.2	Different Filtering approaches	17
3.1	Details about external nodes	20
3.2	Details about internal nodes	20
3.3	Details about routers	21
3.4	Details about attachments	21
3.5	Details about Bandwidth	21