

Contents

1	Introduction	5
1.1	DDoS attack detection and its significance	6
1.2	Motivation	6
1.3	Objective	7
1.4	Our contribution	7
1.5	Organization of report	7
2	Overview of DDoS attack	9
2.1	DDoS attack	9
2.2	DDoS attack architecture	9
2.2.1	Agent-Handler model	9
2.2.2	Internet Relay Chat (IRC) model	10
2.3	Types of DDoS attack	10
2.3.1	Direct DDoS attack	10
2.3.2	Indirect DDoS attack	11
2.4	DDoS attack strategy	12
2.4.1	Selection of zombies	13
2.4.2	Compromise phase	13
2.4.3	Communication phase	13
2.4.4	Attack phase	14
2.5	DDoS taxonomy	14
2.5.1	Constant rate attack	14
2.5.2	Increasing rate attack	16
2.5.3	Pulsing rate attack	16
2.6	Challenges in detecting DDoS detection	16
3	Related works	18

3.1	Detection approaches	18
3.1.1	Packet-based approach	18
3.1.2	Flow-based approach	19
3.2	Existing research methodology	19
3.2.1	Statistical method	20
3.2.2	Machine learning method	21
3.2.3	Knowledge-based method	22
4	Proposed method	24
4.1	Problem statement	24
4.2	Attack traffic generation	24
4.2.1	Increasing rate attack	25
4.2.2	Constant rate attack	25
4.2.3	Pulsing rate attack	26
4.3	Feature selection	27
4.4	Mathematical model	28
4.5	Proposed algorithm	30
4.6	Performance analysis	34
4.6.1	Size of the split window analysis	34
4.6.2	Selection of minimum feature	34
4.6.3	δ threshold analysis	34
4.6.4	θ analysis	35
4.6.5	<i>PCC</i> analysis	35
4.6.6	Peak analysis	36
5	Experimental results	37
5.1	Performance analysis using CAIDA dataset	37
5.2	Performance analysis using real-life data	40
5.2.1	Test-bed used	40
5.2.2	Environment used	41
6	Conclusion and future work	44
6.1	Conclusion	44
6.2	Future work	44

List of Figures

2.1	Direct DDoS attack	11
2.2	Indirect DDoS attack	12
4.1	Increasing rate attack	25
4.2	Constant rate attack	26
4.3	Pulsing attack (regular)	26
4.4	Pulsing attack (irregular)	27
4.5	Packet delay with respect to the timestamp of first packet	28
4.6	Rate of packet in time interval of 0.1	28
4.7	Limiting values of coefficient of variation	29
4.8	Illustration of pulsing traffic pattern	36
5.1	Constant rate traffic pattern in CAIDA DDoS dataset	38
5.2	Increasing rate traffic pattern in CAIDA DDoS dataset	39
5.3	Pulsing traffic pattern to victim in CAIDA DDoS dataset	39
5.4	Pulsing traffic pattern from victim in CAIDA DDoS dataset	40
5.5	test-bed used for attack generation	41
5.6	Constant rate traffic pattern in generated attack data	42
5.7	Increasing rate traffic pattern in generated attack data	42
5.8	Pulsing traffic pattern to victim in generated attack data	43

List of Tables

2.1	Taxonomy of DDoS attack by Mirkovic	15
4.1	Symbols used in detection algorithm	31
5.1	Detail information of detection result in CAIDA data	38
5.2	Detail information of detection result in generated attack data	43