

# Contents

<b>1</b>	<b>An Overview of DDoS Attacks</b>	<b>1</b>
1.1	Introduction	1
1.2	How to Launch DDoS Attacks	3
1.3	Challenges in DDoS Related Research	5
1.3.1	Malicious Networks	6
1.3.2	Data Collection of Malicious Networks	8
1.3.3	Topology Modelling of Malicious Networks	9
1.3.4	Dynamics of Malicious Networks	10
1.3.5	Concealed Malicious Activity Detection	11
1.3.6	Forensics of Malicious Networks	11
	References	12
<b>2</b>	<b>Malicious Networks for DDoS Attacks</b>	<b>15</b>
2.1	Introduction	15
2.2	The Fast Flux Mechanism and Detection	16
2.2.1	The Fast Flux Mechanism	16
2.2.2	Fast Flux Detection	17
2.3	The Domain Flux Mechanism and Detection	19
2.3.1	The Domain Flux Mechanism	19
2.3.2	Domain Flux Detection	20
2.4	Modelling Malicious Networks	23
2.4.1	The SI Model	25
2.4.2	The SIS Model	25
2.4.3	The SIR Model	26
	References	27
<b>3</b>	<b>DDoS Attack Detection</b>	<b>31</b>
3.1	Introduction	31
3.2	Feature Based Detection Methods	32
3.2.1	Profile Based Detection	32
3.2.2	Low Rate DDoS Attack Detection	35
3.3	Network Traffic Based Detection	36

3.4	Detection Against Mimicking Attacks .....	39
3.4.1	Similarity Metrics .....	40
3.4.2	Flow Correlation Based Discrimination .....	42
3.4.3	System Analysis on the Discrimination Method .....	44
	References .....	51
<b>4</b>	<b>Attack Source Traceback .....</b>	<b>55</b>
4.1	Introduction .....	55
4.2	Probabilistic Packet Marking Based Traceback .....	56
4.3	Deterministic Packet Marking Based Traceback .....	59
4.4	Marking on Demand Traceback Scheme .....	61
4.4.1	The Framework of Marking on Demand Scheme .....	62
4.4.2	System Analysis of the MOD Scheme .....	63
4.5	Network Traffic Based IP Traceback .....	68
4.5.1	System Model for IP Traceback on Entropy Variations .....	69
4.5.2	System Analysis on the Model .....	71
	References .....	74
<b>5</b>	<b>DDoS Attack and Defence in Cloud .....</b>	<b>77</b>
5.1	Introduction .....	77
5.2	Defeat DDoS Attacks in Cloud .....	80
5.2.1	System Model in General .....	81
5.2.2	Approximation of the Model .....	82
5.2.3	Resource Investment Analysis .....	83
5.2.4	System Analysis for Non-attack Cases .....	84
5.2.5	System Analysis for Attack Cases .....	85
5.3	A Cloud Firewall Framework Against DDoS Attacks .....	87
5.3.1	Dynamic Resource Allocation for Cloud Firewall .....	90
5.3.2	Single Chain vs Multiple Parallel Chains .....	90
	References .....	92
<b>6</b>	<b>Future Work .....</b>	<b>95</b>
	References .....	96

Distributed Denial of Service Attack and Defense

Yu, S.

2014, X, 97 p. 16 illus., 8 illus. in color., Softcover

ISBN: 978-1-4614-9490-4