List of Tables

4.1 Short hand notations and names used in chapter 4 45
4.2 Details of a FTT record 50

5.1 Code distribution of different schemes for mwest monitoring point . 68
5.2 Node distribution of SEM scheme for different topologies 85

6.1 Short hand notations and their meanings 94
6.2 Interpretation of the mark of an outgoing packet by a router 97
6.3 The fields of a traceback *Query* 99
6.4 FPR vs Memory needed to store $N = 10^7$ flow information for Bloom filter 105
6.5 $E(visited\ nodes)$ per SFT traceback query 106

7.1 Strengths and limitations of the proposed techniques against different types of DDoS attack traffic 116

A.1 Comparison of attacking tools 126

List of Figures

1.1 Different types of DDoS attacks based on attack rate dynamics . . . 3
1.2 Indirect attack 4
1.3 Reflection/Amplification attack 5
1.4 Google's unusual traffic message. 6

2.1 Packet capturing arrangement of AUK-VIII and WAIK-VIII network traces. 23
2.2 Anatomy of CAIDA-2007 DDoS attack trace 24

3.1 The binary search tree used in the VSC 29
3.2 Architecture of VSC 30
3.3 Different possible placement locations of VSC 30
3.4 Normal traffic characteristics 35
3.5 Result of VSC on low rate attack scenario 36
3.6 Result of VSC on DARPA dataset 37
3.7 Result of VSC on small size BOT 38
3.8 Result of VSC on CAIDA attack trace 39

4.1 DDoS attack and its variants 43
4.2 Topology of a protected network 44
4.3 Incoming vs outgoing TCP and UDP traffic for normal traces . . . 46
4.4 unidirectional traffic present in the normal traces 47
4.5 Demonstration of the working of a *bi-agent* 49
4.6 Defense system architecture 52
4.7 *Experiment*1 result 56
4.8 *Experiment*2 result 57
4.9 Arrival rate of SIP/interval 59
4.10 Modified FU 60
4.11 *Experiment*3 result 61
4.12 Entries in the GL over time 62

5.1 Identification mark based anti-spoofing technique 66
5.2 Demonstration of XORID marking scheme 69

5.3 FNR comparison of XORID with StackPI and ANTID 71
5.4 FNR comparison of XORID with ANTID 72
5.5 Incremental deployment Analysis of XORID, StackPi and ANTID . 74
5.6 General architecture of source identification mark based spoofing attck defense system 75
5.7 Different deployment locations of the anti spoofing defense system . 78
5.8 SEM enabled routers in a network 80
5.9 SEM enabled routers in a network 82
5.10 Pictorial representation of the experimental arrangement 86
5.11 FNR comparison of SEM with StackPI, ANTID and XORID 87

6.1 Comparison of number of $< S, D >$ pairs vs number of packets per 10 minutes in CAIDA network trace. 93
6.2 An example of transit flow 93
6.3 Demonstration of Lemma1 95
6.4 Demo 95
6.5 Incoming packet processing 97
6.6 Outgoing packet processing 97
6.7 Demonstration of flow recording 98
6.8 Traceback query processing at a router 101
6.9 Demonstration of traceback mechanism 102
6.10 Demonstration of Lemma2 103
6.11 Pictorial representation of preprocessed skitter topology 107
6.12 hopcount distribution of SKITTER dataset 108
6.13 RTT distribution of SKITTER dataset 109
6.14 degree distribution of SKITTER dataset 110
6.15 Distribution of visited nodes by a traceback query in SKITTER dataset 111

A.1 TUCANNON attack traffic generation strategy 124
A.2 GUI of TUCANNON server program. 125
A.3 Selecting packet rate of an attack thread 128
A.4 Selecting the on/off period of a pulse attack 129
A.5 The testbed setup for TUCANNON experiments experiments. . . . 129
A.6 Parameter specification for attack scenario 1 130
A.7 Wireshirk snapshot of the attack packets in attack scenario 1 131
A.8 Attack scenario 1 packet rate 132
A.9 Parameter specification for attack scenario 2 133
A.10 Packet rate decomposition for different protocol in attack scenario 2 133
A.11 New SIP rate in attack scenario 2 134
A.12 New SIP rate in attack scenario 3 134
A.13 Parameter specification for attack scenario 4 135

A.14 New SIP rate in attack scenario 4 135

List of Acronyms

AS	Autonomous System
AUK-VIII	Auckland Network Trace
BGP	Border Gateway Protocol
CPU	Central Processing Unit
CUSUM	Cumulative Sum
DDM	DDoS Detection and Mitigation
DDoS	Distributed Denial of Service
DNS	Domain Name System
DPM	Deterministic Packet Marking
DRDoS	Distributed Reflection Denial of Service
HCF	Hop Count Filtering
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IoT	Internet of Things
IP	Internet Protocol
LAN	Local Area Network
NTP	Network Time Protocol
OSI	Open Systems Interconnection
PPM	Probabilistic Packet Marking
QoS	Quality of Service
SDN	Software Defined Network
SEM	Source End Marking
SFT	Singleton Flow Traceback
SIP	Source IP
SNTP	Simple Network Time Protocol
TCP	Transmission Control Protocol
TTL	Time To Live
UDP	User Datagram Protocol
VOIP	Voice Over IP
VSC	Violating Source Count
WAIK-VIII	Waikato Network Trace