Contents

Abstract

1. Introduction 01

1. Overview 02

1.1 DDoS Characteristics 03

1.2 Types of DDoS attacks 03

1.3 Different approaches to DDoS attacks 05

1.4 Motivation 06

1.5 Problem definition....................................07

2: Literature Survey 08

2. Related work 09

3. Applied Methodology 11

3. Detection approach 12

3.1 F-Divergence....................................12

3.1.1 Kullback-Leibler Distance (KL).................................... 12

3.1.2 Hellinger Distance.................................... 13

3.1.3 Total Variation Distance (TVD).................................... 13

3.1.4 α-Divergence.................................... 13

3.2 System Design.................................... 14

3.3 Methodology.................................... 17

4. Experimental Setup 20

4.1 Network traffic analysis tool.................................... 21

4.2 System configuration 21

4.3 Datasets 22

5. Observation and Analysis.................................... 23

5.1 Observation.................................... 24

5.2 Threshold values.................................... 32

5.3 Computational time 32

6. Conclusion and Future Work.................................... 33

6. Conclusion 34

References.................................... 35

List of Figures

Figure 1: Architecture of DDoS attacks.......... 02

Figure 2: Direct DDoS attack.......... 04

Figure 3: Reflector DDoS attack.......... 04

Figure 4: Classification of DDoS attack detection methods.......... 05

Figure 5: Detection Architecture.......... 14

Figure 6: TCP SYN flooding attack 16

Figure 7: UDP flooding attack.......... 16

Figure 8: Binary tree for ICMP.......... 18

Figure 9: Binary tree for UDP.......... 18

Figure 10: Binary tree for TCP 18

Figure 11: Flow chart to detect flooding attack by filter engine.......... 19

Figure 12: A screenshot of Wireshark.......... 21

Figure 13: α-divergence based on connection size for CAIDA 2013.......... 26

Figure 14: α-divergence based on connection size for CAIDA (2013+2007).......... 26

Figure 15: F-divergence based on connection size for CAIDA 2013 27

Figure 16: F-divergence based on connection size for CAIDA (2013+2007).......... 27

Figure 17: α-divergence based on SYN, ACK count for MIT packet traces.......... 28

Figure 18: α-divergence based on SYN, ACK count for MIT mix traces.......... 28

Figure 19: F-divergence based on SYN, ACK count for MIT packet traces.......... 29

Figure 20: F-divergence based on SYN, ACK count for MIT mix traces.......... 29

Figure 21: α-divergence based on destination port change count for UCLA packet trace.......... 30

Figure 22: α-divergence based on destination port change count for UCLA mix traces.......... 30

Figure 23: F-divergence based on destination port change count for UCLA packet traces.......... 31

Figure 24: F-divergence based on destination port change count for UCLA mix traces.......... 31

List of Tables

Table 1: Symbols used.. 12

Table 2: CAIDA traffic mixing statistics.. 24

Table 3: MIT traffic mixing statistics.. 25

Table 4: UCLA traffic mixing statistics.. 25

Table 5: Threshold values for the datasets.. 32

Table 6: Average computational time required on the dataset analysis....................................... 32