

CONTENTS

ABSTRACT

1. INTRODUCTION	1
1.1 OVERVIEW	1
1.2 DISTRIBUTED DENIAL OF SERVICE ATTACK	1
1.3 METHODS OF FLOODING ATTACKS	4
1.4 MOTIVATION	5
2. LITERATURE SURVEY	6
2.1 DDoS DETECTION STRATEGIES	6
2.2 NETWORK ENTROPY	6
2.3 RENYI'S ENTROPY	7
2.4 F-DIVERGENCE	7
2.5 α -DIVERGENCE	7
2.6 RELATED WORKS	8
3. APPLIED METHODOLOGY	9
3.1 PROBLEM ANALYSIS	9
3.2 DETECTION APPROACH	9
3.3 SYSTEM DESIGN	10
3.4 METHODOLOGY	11
4. EXPERIMENTAL SETUP	13
4.1 DATASETS	13
4.2 ANALYSIS TOOL	14
4.3 SYSTEM CONFIGURATION	14
5. OBSERVATION AND RESULTS	15
5.1 OBSERVATION	15
5.2 THRESHOLD VALUES	20
5.3 COMPUTATIONAL TIME	20
6. CONCLUSION AND FUTURE WORK	21
REFERENCES	22

LIST OF FIGURES

Page No.

FIGURE 1. TYPICAL DISTRIBUTED DOS ATTACK	3
FIGURE 2. TYPICAL DISTRIBUTED REFLECTOR DOS ATTACK	3
FIGURE 3: DETECTION ARCHITECTURE	11
FIGURE 4: BINARY SEARCH TREE FOR STORING PACKET ATTRIBUTES.	13
FIGURE 5: FLOW CHART TO DETECT FLOODING ATTACK BY DETECTOR ENGINE	13
FIGURE 6: A SCREEN-SHOT OF WIRESHSRK	15
FIGURE 7: α -DIVERGENCE BASED ON CONNECTION SIZE FOR UCLA TRACES	17
FIGURE 8: RENYI ENTROPY BASED ON CONNECTION SIZE FOR UCLA TRACES	17
FIGURE 9: α -DIVERGENCE BASED ON SOURCE IP CHANGES FOR UCLA TRACES	18
FIGURE 10: RENYI ENTROPY BASED ON SOURCE IP CHANGES FOR UCLA TRACES	18
FIGURE 11: α -DIVERGENCE BASED ON CONNECTION SIZE FOR CAIDA TRACES	19
FIGURE 12: RENYI ENTROPY BASED ON CONNECTION SIZE FOR CAIDA TRACES	19
FIGURE 13: α -DIVERGENCE BASED ON SOURCE IP CHANGES FOR CAIDA TRACES	20
FIGURE 14: RENYI'S ENTROPY BASED ON SOURCE IP CHANGES FOR CAIDA TRACES	20
FIGURE 15: FILTERING MECHANISM APPLIED TO UCLA MIXED TRAFFIC.	22

LIST OF TABLES

Page No.

TABLE 1: CONSENSUS TABLE	10
TABLE 2: AVERAGE PACKET RATE OF THE DATASETS (PER 5S)	14
TABLE 3: TRAFFIC MIXING STATISTICS	16
TABLE 4: THRESHOLD VALUES FOR THE DATASET	21
TABLE 5: AVERAGE COMPUTATION TIME REQUIRED ON THE DATASET ANALYSIS.	21