

# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Motivation . . . . .	1
1.2	Aim of the Project . . . . .	2
1.3	Objectives of the Project . . . . .	2
1.4	Organization of the Report . . . . .	2
<b>2</b>	<b>Related Work</b>	<b>3</b>
2.1	Discussion . . . . .	4
<b>3</b>	<b>Application Layer DDoS attack</b>	<b>5</b>
3.1	Types of common Application Layer DDoS attacks . . . . .	6
3.2	Application Layer DDoS methods . . . . .	6
3.3	HTTP GET flooding attack in different attack scenarios . . . . .	7
3.4	Parameter Description . . . . .	8
3.5	Discussion . . . . .	8
<b>4</b>	<b>DDoS attack defense mechanism</b>	<b>9</b>
4.1	Generic architecture for Victim-end DDoS defense mechanism . . . . .	10
4.2	Methods for DDoS attack detection . . . . .	10
4.3	Definition of various attack defense systems . . . . .	11
4.4	Packet level analysis and detection . . . . .	11
4.5	Minimum packet attributes . . . . .	12
4.6	Discussion . . . . .	12
<b>5</b>	<b>Machine Learning approach</b>	<b>13</b>
5.1	Definition . . . . .	13
5.2	Decision Tree learning . . . . .	13
5.2.1	Definition . . . . .	13
5.2.2	C4.5 Algorithm . . . . .	13
5.3	Discussion . . . . .	15
<b>6</b>	<b>Proposed Model</b>	<b>16</b>
6.1	Proposed Algorithm . . . . .	16
6.2	Discussion . . . . .	18
<b>7</b>	<b>Work Done and Results</b>	<b>19</b>
7.1	Various Information . . . . .	19
7.1.1	Details of the sample data-set used in the used in the project . . . . .	19
7.1.2	Sample data-set . . . . .	20
7.2	Attribute selection for splitting . . . . .	20
7.2.1	Sample data-set for attribute selection . . . . .	20
7.2.2	Calculation for attribute selection . . . . .	21
7.3	Detection . . . . .	22

7.4	Tool Developed . . . . .	23
7.5	Discussion . . . . .	24
<b>8</b>	<b>Conclusion and Future Work</b>	<b>25</b>
8.1	Future Work . . . . .	25

# List of Tables

3.1	Attack Parameters for HTTP GET flooding attack for the above attack scenarios . . . . .	8
7.1	A very small sample of 1998 Football World Cup data-set . . . . .	20
7.2	Sample data-set for attribute selection . . . . .	21

# List of Figures

3.1	Distributed Denial of Service Attack . . . . .	5
3.2	(a)Shrew flooding App-DDoS (b)Random flooding App-DDoS and (c)Flash crowds App-DDoS	7
4.1	Architecture with Source-end, Intermediate and Victim-end network . . . . .	9
4.2	Generic architecture for Victim-end DDoS defense mechanism . . . . .	10
6.1	Target Architecture for implementation . . . . .	16
6.2	Algorithm for attack detection and attack minimization . . . . .	17
7.1	1998 Football World Cup Semi-final complete data-set plotting (number of requests per second)	20
7.2	Requests per second before application of the proposed algorithm . . . . .	22
7.3	Requests per second after application of the proposed algorithm . . . . .	23
7.4	Snapshot of the tool developed . . . . .	23