

# Contents

<b>Chapters</b>	<b>Page No.</b>
<b>1. Introduction.....</b>	<b>1</b>
1.1. DDoS – An overview.....	1
1.2. Motivation.....	2
1.3. Aim of the work.....	2
1.4. Contribution.....	3
1.5. Organization of the report.....	3
<b>2. Background.....</b>	<b>4</b>
2.1. Classification Based on Target Layer.....	5
2.1.1. Network/Transport Level DDoS Attack.....	5
2.1.1.1. Flooding Attacks:.....	5
2.1.1.2. Protocol exploitation flooding attacks.....	5
2.1.1.3. Reflection-based flooding attacks.....	5
2.1.1.4. Amplification-based flooding attacks.....	5
2.1.2. App-DDoS Attack.....	6
2.1.2.1. Reflection/amplification based flooding attacks .....	6
2.1.2.2. HTTP flooding attacks .....	7
<b>3. Existing Defence Mechanisms and Related Works.....</b>	<b>10</b>
3.1. Destination Based Mechanisms.....	10
3.1.1. Defense against Reflection/Amplification attacks:.....	10
3.1.2. DDoS-Shield.....	11
3.1.3. Anomaly detector based on hidden semi-Markov model .....	11
3.1.4. DAT (Defense Against Tilt DDoS attacks).....	12

3.2.	Hybrid Mechanisms.....	12
3.2.1.	Speak-up.....	12
3.2.2.	DOW (Defense and Offense Wall) .....	12
3.2.3.	Differentiate DDoS flooding bots from human .....	13
3.2.4.	Hybrid detection based on trust and information theory based metrics .....	14
3.2.5.	Admission control and congestion control .....	14
3.3.	Discussion.....	15
<b>4.</b>	<b>Slowloris Attack.....</b>	<b>16</b>
4.1.	HTTP Request and Response Mechanism.....	16
4.2.	Vulnerability in HTTP Protocol.....	18
4.3.	Mechanism of Slowloris Attack.....	18
<b>5.</b>	<b>Existing Mitigation Techniques and their Problems... 20</b>	
5.1.	GESNIC for web Server Protection :.....	20
5.2.	Disadvantage of GESNIC.....	20
5.3.	<i>mod_antiloris</i> by Apache.....	21
5.4.	Disadvantage of <i>mod_antiloris</i> .....	21
<b>6.</b>	<b>Adaptive Time-out and Our Approach..... 22</b>	
6.1.	Adaptive Time-Out.....	22
6.2.	Detection Mechanism.....	22
6.2.1.	Suspect Determination Module.....	24
6.2.2.	Attacker Verification Module.....	25
6.2.2.1.	Monitoring of Suspects (Potential Attacker).....	25
6.2.2.2.	Confirming Suspect as an Attacker.....	27
<b>7.</b>	<b>Experimental Results..... 28</b>	
<b>8.</b>	<b>Conclusion and Future Work..... 35</b>	
	<b>Bibliography..... 36</b>	

## List of Figures

<b>Figure No.</b>	<b>Caption</b>	<b>Page No.</b>
<b>2.1</b>	Components of Botnet based DDoS attack	<b>4</b>
<b>6.1</b>	Flowchart for Proposed Detection Mechanism	<b>23</b>
<b>6.2</b>	Suspect Monitor Flowchart	<b>26</b>
<b>7.1</b>	False Positive Rate w.r.t. Threshold value	<b>30</b>
<b>7.2</b>	False Positive Rate w.r.t. No. of Slow Request	<b>31</b>
<b>7.3</b>	False Positive Rate w.r.t. No. of Slow Request	<b>32</b>
<b>7.4</b>	False Positive Rate w.r.t. No. of Slow Request	<b>33</b>

## List of Tables

<b>Table No.</b>	<b>Caption</b>	<b>Page No.</b>
<b>7.1</b>	False Positive w.r.t. Threshold Value	<b>29</b>
<b>7.2</b>	False Positive Rate w.r.t. No. of Slow Request	<b>30</b>
<b>7.3</b>	False Positive Rate w.r.t. No. of Slow Request	<b>31</b>
<b>7.4</b>	False Positive Rate w.r.t. No. of Slow Request	<b>32</b>
<b>7.5</b>	Test Case 1 Results	<b>33</b>
<b>7.6</b>	Test Case 2 Results	<b>34</b>
<b>7.7</b>	Test Case 3 Results	<b>34</b>