

# Contents

<b>1</b>	<b>Introduction</b>	<b>4</b>
1.1	Anomaly: An Introduction . . . . .	4
1.1.1	Types of anomaly detection techniques . . . . .	4
1.2	Intrusion Detection System (IDS): An Introduction . . . . .	4
1.2.1	Types of IDSs . . . . .	4
1.3	Anomaly Based Network Intrusion Detection Techniques . . . . .	5
<b>2</b>	<b>Background Study</b>	<b>7</b>
2.1	About Denial of Service attacks (DoS Attacks) . . . . .	7
2.2	Detecting Compromised Routers via Packet Forwarding Behaviour in Large Network. . . . .	9
2.3	Anomaly Detection in IP Networks . . . . .	10
2.4	An Improved Intrusion Detection System Based On Agents. . . . .	11
2.5	Network Intrusion and Fault Detection: A Statistical Anomaly Approach. . . . .	12
2.6	Early Statistical Anomaly Intrusion Detection of DOS Attacks Using MIB Traffic Parameters. . . . .	13
2.7	Proactive Anomaly Detection Using Distributed Intelligent Agents . . . . .	14
2.8	A SNMP based Platform for Distributed Stateful Intrusion Detection in Enterprise Networks . . . . .	15
2.9	Three Level Network Analysis for Anomaly Detection . . . . .	16
2.10	Intrusion Prevention System Design . . . . .	17
2.11	Intrusion Detection Based on One Class SVM and SNMP MIB data . . . . .	17
2.12	Parameterized Anomaly Detection System With Automatic Configuration . . . . .	17
<b>3</b>	<b>Proposed Algorithm</b>	<b>19</b>
3.1	Algorithm . . . . .	19
<b>4</b>	<b>Experiment</b>	<b>22</b>
4.1	Preparing of Training and Treatment Data Sets . . . . .	23
<b>5</b>	<b>Conclusion</b>	<b>26</b>