

# Contents

<b>1</b>	<b>INTRODUCTION</b>	<b>1</b>
1.1	Intrusion detection system (IDS) . . . . .	1
1.1.1	IDS types . . . . .	2
1.2	Anomaly Detection . . . . .	3
<b>2</b>	<b>INITIAL STUDY</b>	<b>4</b>
2.1	Analysis of Existing Flow Based Approaches . . . . .	5
2.2	Problem Definition . . . . .	11
<b>3</b>	<b>BACKGROUND</b>	<b>12</b>
3.1	IP Flow . . . . .	12
3.1.1	Flow Definition . . . . .	12
3.1.2	Working of IP Flow . . . . .	13
3.1.3	Flow export Protocols . . . . .	13
3.2	NetFlow . . . . .	14
3.2.1	NetFlow record . . . . .	14
3.3	Holt-Winter's Forecasting . . . . .	15
3.3.1	Multiplicative Seasonal Model . . . . .	15
3.3.2	Additive Seasonal Model . . . . .	16
3.4	Entropy . . . . .	18
3.5	Attacks . . . . .	20
<b>4</b>	<b>THE PROPOSED SYSTEM AND APPROACH</b>	<b>21</b>
4.1	System Architecture . . . . .	21
4.2	Approach . . . . .	22
<b>5</b>	<b>IMPLEMENTATION</b>	<b>23</b>
5.1	Tools used in implementation . . . . .	23
5.1.1	Pmacct(promiscuous mode accounting package) . . . . .	23
5.1.2	Round Robin Database Tool (RRDtool) . . . . .	25
5.2	Flow analysis . . . . .	27
5.3	Anomaly Detection . . . . .	30
5.3.1	Entropy based module . . . . .	30
5.3.2	Holt-winters forecasting based module . . . . .	31

5.3.3 Database Backend . . . . .	33
<b>6 TESTING</b>	<b>36</b>
<b>7 TEST SETUP AND RESULT</b>	<b>38</b>
7.1 Result Analysis . . . . .	41
7.2 Result's Snapshots . . . . .	42
<b>8 CONCLUSION AND FUTURE WORK</b>	<b>44</b>

## List of Figures

1	IDS types . . . . .	2
2	IP Flow architecture . . . . .	13
3	System Architecture . . . . .	21
4	Modular Overview of pmacct . . . . .	24
5	Test Setup . . . . .	38
6	Scan detection . . . . .	43
7	Attack details in database . . . . .	43

## List of Tables

1	NAIDS Types . . . . .	4
2	Summary of Flow Based Anomaly Detection Methods . . . . .	5
3	Attacks Detected . . . . .	20
4	Records used for Feature Extraction . . . . .	28
5	Behaviour of Feature Extracted . . . . .	29
6	Classification of anomalies based on entropy change. . . . .	29
7	Variation of Feature used in HW . . . . .	30
8	Attributes of the alert table. . . . .	33
9	Functional Test Table . . . . .	36
10	Entropy Detection Result . . . . .	39
11	Holt-Winter Detection Result . . . . .	40
12	Result of Further Identification of attacks . . . . .	40
13	Final Result . . . . .	41