CONTENTS

Agreement Page

Originality Statements

ABSTRACT **iv**

PREFACE **v**

Contents **viii**

List of Figures **x**

List of Tables **xi**

1 INTRODUCTION **1**

1.1 Background 1
1.2 Problem Formulation 3
1.3 Objectives 3
1.4 Scope of Works 3
1.5 Research Method 4
1.6 Undergraduate Thesis Organization 4

2 BASIC CONCEPT **5**

2.1 Tranport Layer 5
2.1.1 Transmission Control Protocol (TCP) 5
2.1.2 User Datagram Protocol (UDP) 6
2.2 Raspberry Pi 6
2.3 Client and Attacker Devices 7
2.4 Denial of Service (DoS) Attack 7
2.4.1 SYN Flood Attack 8
2.4.2 UDP Flood Attack 9
2.5 Host Intrusion Prevention System (HIPS) 10
2.6 Snort 10
2.7 RaspAP 11
2.8 Hping3 11

3 SYSTEM PLANNING **12**
3.1 System Design 12
3.1.1 System Description 13
3.1.2 System Requirement 13
3.2 Raspberry Pi Configuration 14
3.2.1 Raspberry Pi as A Router Configuration 15
3.2.2 Snort Configuration 15
3.3 Virtual Machines (VM) installation on VirtualBox 17
3.4 Server's VM Configuration 17
3.5 Client's VM Configuration 18
3.6 Research Scenarios 19
3.6.1 Total Incoming Packets Testing 19
3.6.2 Using Snort Testing 19
3.7 CPU and Memory Usage Testing 19

4 PERFORMANCE EVALUATION **21**
4.1 Total Incoming Packets 21
4.1.1 Client's Connection 21
4.1.2 Total Incoming Packets from Attackers Testing 22
4.2 Using Snort Testing 23
4.2.1 Active Snort Impact for Client Connection 23
4.2.2 Total Packet Processed by HIPS Snort 24
4.3 CPU and Memory Usage Testing 26

5 CONCLUSIONS **27**
5.1 Conclusion 27
5.2 Suggestion 28

Bibliography **29**