

**UNIVERSITI TEKNOLOGI MARA**

**DDoS DETECTION AND DEFENSE  
MECHANISM BASED ON PACKET  
ANALYSIS AND MACHINE  
LEARNING**

**MOHD AZAHARI BIN MOHD YUSOF**

Thesis submitted in fulfillment  
of the requirements for the degree of  
**Doctor of Philosophy**  
**(Computer Science)**

**Faculty of Computer and Mathematical Sciences**

**November 2019**

## ABSTRACT

DDoS attacks are one of the most serious threats nowadays. It is an attack launched by an attacker using various source of IP addresses to disrupt a network or IoT environment. There are several types of DDoS attacks such as TCP SYN flood, UDP flood, ICMP/Ping flood, Ping of Death, Smurf, Slowloris, HTTP flood, Zero-day attack and SIDDoS which can be launched by attackers for a specific purpose. Therefore, this research is aimed at overcoming high false positive rate to improve detection accuracy against several DDoS attacks. This research focused on four types of DDoS attacks, namely TCP SYN flood, UDP flood, Ping of Death and Smurf. Packet Threshold Algorithm (PTA) was introduced in this research, where the technique can detect incoming packets either normal packets or DDoS attacks. The packet class detected by the PTA is based on the specified packet threshold. All types of DDoS attacks that have been detected by the PTA will be dropped and will be stored in the log of packets. Meanwhile, normal packets that have been detected by PTA are allowed into the network or IoT environment. Then, this technique is coupled with four machine learning, namely SVM, Naïve Bayes, Logistic Regression and KNN. Finally, they are evaluated based on detection accuracy, FP rate, TP rate, TN rate, FN rate, precision, recall, f1-score and total of running time to see the efficiency of feature selection methods for reducing false positive rate in DDoS attack reduction. Based on performance comparison, it shows that PTA-KNN technique has achieved 99.83% detection accuracy with only 0.02% FP rate, which is considered the best technique to reduce false positive rate problem.

## **ACKNOWLEDGEMENT**

Firstly, I wish to thank God for giving me the opportunity to embark on my PhD and for completing this long and challenging journey successfully. My gratitude and thanks go to my supervisor Dr. Fakariah Hani Binti Mohd Ali and Dr. Mohamad Yusof Bin Darus for valuable guidance, constant support and intuitive supervision.

I also do not forget to thank the lecturers, officers and staff of Faculty of Computer and Mathematical Sciences (FSKM) and Institute of Graduate Studies (IGS) of Universiti Teknologi MARA (UiTM) Shah Alam for their assistance during this research.

I would also like to thank my fellow friends who had given encouragement and support to me. Finally, I would like to convey thanks to my parents, wife and siblings who have supported me in the process of completing this thesis.

# TABLE OF CONTENTS

	<b>Page</b>
<b>CONFIRMATION BY PANEL OF EXAMINERS</b>	<b>ii</b>
<b>AUTHOR'S DECLARATION</b>	<b>iii</b>
<b>ABSTRACT</b>	<b>iv</b>
<b>ACKNOWLEDGEMENT</b>	<b>v</b>
<b>TABLE OF CONTENTS</b>	<b>vi</b>
<b>LIST OF TABLES</b>	<b>x</b>
<b>LIST OF FIGURES</b>	<b>xii</b>
<b>LIST OF ABBREVIATIONS</b>	<b>xiv</b>
<b>CHAPTER: ONE INTRODUCTION</b>	<b>1</b>
1.1 Introduction	1
1.2 Research Background	1
1.3 Problem Statement	4
1.4 Research Questions	5
1.5 Research Objectives	5
1.6 Research Contributions	5
1.7 Scope of Research	6
1.8 Significance of the Study	7
1.9 Thesis Outline	8
<b>CHAPTER TWO: LITERATURE REVIEW</b>	<b>10</b>
2.1 Introduction	10
2.2 Overview of Popular Network Attacks	11
2.3 DDoS Attacks and Its Effects	12
2.4 Types of DDoS Attacks	14
2.4.1 Volume-Based Attack	14
2.4.2 Protocol Attack	16
2.4.3 Application Layer Attack	19
2.5 DDoS Attacking Tools	21

2.5.1	Canon Low Orbit Ion (LOIC)	21
2.5.2	XOIC	22
2.5.3	HTTP Unbearable Load King (HULK)	22
2.5.4	Layer 7 DDoS Simulator (DDOSIM)	22
2.5.5	R-U-Dead-Yet (RUDY)	22
2.5.6	Hping3	23
2.6	Applying Intrusion Detection and Prevention System (IDPS)	23
2.7	Machine Learning	24
2.7.1	Logistic Regression	25
2.7.2	Naive Bayes	26
2.7.3	K-Nearest Neighbor (KNN)	27
2.7.4	Decision Tree	28
2.7.5	Random Forest	29
2.7.6	Support Vector Machine (SVM)	30
2.8	Packet Threshold	31
2.9	Current DDoS Detection and Defense Techniques	33
2.9.1	Dendritic Cell	34
2.9.2	Packet Marking	35
2.9.3	Canny Edge Detector	35
2.9.4	Consensus Algorithm	36
2.9.5	Interface Based Rate Limiting	36
2.9.6	Cumulative Sum	36
2.9.7	Genetic Based Dynamic Growing Self Organizing Tree	37
2.9.8	Dynamic Security Level Changing Strategy Algorithm	37
2.9.9	Multi-Queue Algorithm	38
2.9.10	Message Authentication Code	39
2.9.11	Hop Count Inspection - Support Vector Machine	39
2.9.12	Support Vector Machine	40
2.9.13	Worldwide SYN Flooding Attack Detection	40
2.9.14	IP Address Feature Value and Correlation	40
2.9.15	Lightweight Detection	40
2.9.16	Entropy-Based Lightweight DDoS Flooding Attack Detection	41
2.9.17	Modified K-Means	41
2.9.18	Logistic Regression	42