Detection of DDoS Attacks in Software Defined Networks

A thesis submitted in partial fulfilment of the requirements for the degree of

Master of Science in Network Security

By:

Mansour Sulaiman Alrajhi

B.Sc. in Information Systems

Under Supervision of:

Prof. Dr. Mostafa G. M. Mostafa

Naif Arab University for Security Sciences

Submitted to Department of Network Security, Computer and Information Security College,

Naif Arab University for Security Sciences.

2019

Acknowledgement

I would like to take this opportunity to express my special feeling and say thanks to my advisor Prof. Dr. Mostafa G. M. Mostafa for his patient guidance, advice and encouragement which also help me in doing a lot of research to come up with a lot of information in addition to a skill of reading and writing that I have gained during the thesis period.

Also, I would like to thank all members of college of computer and information security. I really appreciate their support.

Finally, I would like to thank my mother, father and the rest of my family, and my friends for their encouragement and usual support.

Table of Contents

List of Figure

List of Table

List of Abbreviations

AI	Artificial Intelligence
API	Application Programming Interface
ASIC	Application Specific Integrated Circuit
CBU	Completely Built Up
CNN	Convolutional Neural Networks
DDoS	Distributed Denial of Service
DNN	Deep Neural Networks
DoS	Denial of Service
DR	Detection Rate
FC	Flash Crowd
FN	False Negative
FP	False Positive
FPGA	Field Programmable Gate Rate
FPR	False Positive Ratio
Gbps	Gigabit Per Second
GPP	General Purpose Processor
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IoT	Internet of Things
IP	Internet Protocol Address
IPv4	Internet Protocol Address version 4
IPv6	Internet Protocol Address version 6
KNN	K Nearest Neighbors
LOA	Lion Optimization Algorithm
ML	Machine Learning
NBI	Northbound Application Interface
NFP	Near-field Proximity

NFV	Network Function Virtualization
NIDS	Network Intrusion Detection System
NPU	Network Processor
ONF	Open Networking Foundation
OSI	Open Systems Interconnection Model
PCA	Principal Component Analysis
PLD	Programmable Logic Device
QoS	Quality of Service
SBI	Southbound Application Interface
SDN	Software Defined Network
SIEM	Security Incident and Event Management
SOM	Self Organizing Map
SVM	Support Vector Machine
TCAM	Table Content Address Memory
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TN	True Negative
TP	True Positive
TPR	True Positive Ratio
UDP	User Datagram Protocol