

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

Chapter 1: Introduction	9
1.1 Overview	9
1.2 Motivations	10
1.3 Objectives	11
1.4 Problem Statement	11
1.5 Thesis Contribution	12
1.6 Thesis Organization	12
Chapter 2: Background and Related Work	13
2.1 Traditional Networks	13
2.2 SDN Advantages	16
2.3 SDN Architecture	18
2.4 OpenFlow	21
2.5 Challenges	24
2.5.1 Performance	24
2.5.2 Scalability	25
2.5.3 Security	26
2.6 SDN Attacks	29
2.6.1 Distributed Denial of Service (DDoS)	33
2.6.2 DDoS attack types	34
2.6.3 DDoS in SDN	35
2.8 Related Work	37
CHAPTER 3: Proposed Methodology	44
3.1 Machine Learning	45
3.1.1 Supervised Machine Learning	45
3.1.2 Unsupervised Machine Learning	46
3.2 Attack detection Algorithms using Machine Learning (ML) techniques	47
3.2.1 Data Flow	47
3.2.2 Decision Tree	49
3.2.3 Random Forest	50
3.2.4 Random Tree	51
3.2.5 Support Vector Machines (SVM)	52
3.2.6 Navie Bayes	53

3.2.7 Logistic Regression	54
3.3 SDN based NIDS	55
CHAPTER 4: Result and Discussion	56
4.1 Overview	56
4.2 Dataset	56
4.3 Feature Selection	57
4.4 Evaluation Metrics	59
4.5 WEKA	60
4.6 Experiment 1 Results	62
4.7 Experiment 2	64
4.7.1 Decision Tree Results	64
4.7.2 Random Forest Result	66
4.7.3 Random Tree Result	67
4.7.4 Support Vector Machine (SVM) Result	68
4.7.5 Naive Bayes Result	69
4.7.6 Logistic Regression Result	70
4.8 Discussion of Findings	71
CHAPTER 5: Conclusion and Future Work	72
5.1 Conclusion	72
5.2 Future Work	73
References	74

List of Figure

Figure 1. Simplified SDN architecture	19
Figure 2. Software Defined Network Architecture	21
Figure 3. Main components of an OpenFlow switch	23
Figure 4. Security issues in SDN.....	28
Figure 5. DDoS in traditional network	33
Figure 6. DDoS attack types.....	34
Figure 7. DDoS attack in SDN	36
Figure 8. Data Flow Diagram	48
Figure 9. example of a decision tree structure model with three classes	49
Figure 10. Proposed SDN based NIDS	55
Figure 11. Weka explorer interface view	60
Figure 12. Summary of accuracy comparison	63
Figure 13. Decision Tree -J48 summary result	64
Figure 14. Tree diagram of Decision Tree -J48	65
Figure 15. Random Forest summary result	66
Figure 16. Random Tree summary result	67
Figure 17. SVM summary result	68
Figure 18. Naive Bayes summary result	69
Figure 19. Logistic Regression summary result	70
Figure 20. Overall accuracy summary result	71

List of Table

Table 1. SDN and traditional network	18
Table 2. SDN security issues	32
Table 3. Some NSL-KDD Attributes.....	58
Table 4. Performance evaluation metrics	59
Table 5. Summary of accuracy comparison of a different algorithms	62
Table 6. Decision Tree finding	64
Table 7. Random Forest findings	66
Table 8. Random Tree finding	67
Table 9. SVM finding.....	68
Table 10. Naive Bayes finding.....	69
Table 11. Logistic Regression finding.....	70

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