Software Defined Networking: Network Intrusion Detection System

Tuan Anh Tang

Submitted in accordance with the requirements for the degree of

Doctor of Philosophy

The University of Leeds

Department of Electronic and Electrical Engineering

June 2019

Declaration

The work in this thesis is based on research carried out at the Institute of Robotics, Autonomous Systems and Sensing (IRASS), School of Electronic and Electrical Engineering, Leeds University, UK. The candidate confirms that no part of this thesis has been submitted elsewhere for any other degree or qualification and it is all his own work except where work which has formed part of jointly authored publications. The contribution of the candidate and other authors to this work has been explicitly indicated below. The candidate confirms that appropriate credit has been given within the thesis where reference has been made to the work of others. It is to assert that the candidate has contributed solely to the technical part of the joint publication under the guidance of his academic supervisors. The detailed contributions of the authors are as the following:

Author: Tuan Anh Tang
Contributions: Proposed and implemented the SDN-based intrusion detection models. Wrote first and final drafts of the manuscripts.

Co-Author: Dr. Des McLernon
Contributions: Provided overall supervision on the whole project. Provided feedback on technical analyses and final drafts of the manuscripts.

Co-Author: Dr. Lotfi Mhamdi
Contributions: Provided feedback on technical analyses related to SDN aspects and drafts of the manuscripts.

Co-Author: Dr. Syed Ali Raza Zaidi
Contributions: Provided feedback on technical analyses and drafts of the manuscripts.

Co-Author: Professor Mounir Ghogho
Contributions: Provided feedback on technical analyses and drafts of the manuscripts.

This thesis is dedicated to my family.

Acknowledgements

First and foremost, I would like to express my sincere gratitude to Dr. Des McLernon for all of his support in my PhD life from the beginning. His guidance, feedback and encouragement have inspired and motivated me a lot in my PhD journey. But above everything, thank you very much for your caring and kindness. I wholeheartedly appreciate your kindness.

I would like to express my gratitude to Dr Lotfi Mhamdi for guiding me to the field of SDN and continuously supporting me during my research.

I would like to thank Dr. Syed Ali Raza Zaidi for all of his advice and feedback. Thank you very much for your guidance since the beginning.

My appreciation also goes to Professor Mounir Ghogho for his support and guidance. Thank you very much for the constructive talks at the early stage of my research that gave me the right research direction.

I thank my fellow lab-mates in rooms 3.62 and 2.59, School of Electronic and Electrical, for all the fruitful discussions and for all the fun we have had in the last four years. I would like to especially thank Yen, Bao, Asma, Ali, Mohanad, Edmond, Bao and Naveed for all the precious things that we have shared.

Last but not least, I would like to thank my family: my parents, and my sisters for supporting and encouraging me endlessly. Thank you very much for being with me through all the ups and downs. Without you, I would not be here now.

Abstract

Software Defined Networking (SDN) is developing as a new solution for the development and innovation of the Internet. SDN is expected to be the ideal future for the Internet since it can provide controllable, dynamic and cost-effective networking. The emergence of SDN provides a unique opportunity to achieve network security in a more efficient and flexible manner. One key advantage of SDN, as compared to traditional networks, is that by virtue of centralized control, it allows better provisioning of network security. Nevertheless, the flexibility provided by the SDN architecture manifests several new network security issues that must be addressed to strengthen SDN security. The SDN has original structural vulnerabilities, which are the centralized controller, the control-data interface and the control-application interfaces. These vulnerabilities can be exploited by intruders to conduct several types of attacks.

Network Intrusion Detection System (NIDS), which is an important part of network architecture, is used to detect network intrusions and secure the whole network. In this thesis, we propose an SDN-based NIDS (DeepIDS) using Deep Learning (DL) algorithms to detect anomalies in the SDN architecture. Firstly, we evaluate the potential of DL for flow-based anomaly detection with different flow features.

Through experiments, we confirm that the DL approach has the potential for flow-based anomaly detection in the SDN environment. Secondly, we propose a Gated Recurrent Unit Recurrent Neural Network (GRU-RNN) to improve the detection rate of the DeepIDS. Our experimental results show that the proposed GRU-RNN model improves the detection rate significantly without deteriorating network performance. The performance of our system in terms of accuracy, throughput, latency and resource utilization shows that DeepIDS does not affect the performance of the OpenFlow controller, and so is a feasible approach.

Finally, we introduce an unsupervised approach (SAE-1SVM) to solve an unlabeled and imbalanced dataset problem. This approach yields a high detection rate while maintaining a significantly low processing time. Through extensive experimental evaluations, we conclude that our proposed approach exhibits a strong potential for intrusion detection in the SDN environments.

Abbreviations

ACC	Accuracy
AE	Autoencoder
AUC	Area Under the Curve
$DDoS$	Distributed Denial of Service Attack
DoS	Denial of Service Attack
DL	Deep Learning
DNN	Deep Neural Network
$F1$	F1-measure
FP	False Positive
FPR	False Positive Rate
FN	False Negative
GRU	Gated Recurrent Unit
$GRU - RNN$	Gated Recurrent Neural Network
R	Recall
ROC	Receiver Operating Characteristic Curve
RNN	Recurrent Neural Network
$OC - SVM$	One-class Support Vector Machine
P	Precision
IDS	Intrusion Detection System
$LSTM$	Long Short-Term Memory
ML	Machine Learning
NN	Neural Network
$NIDS$	Network Intrusion Detection System
SAE	Stacked Autoencoder
SDN	Software Defined Networking
SOM	Self-Organizing Map
SVM	Support Vector Machine
TP	True Positive
TPR	True Positive Rate
TN	True Negative

Contents

List of Figures

List of Tables