Intelligent Machine Learning Architecture for Detecting DDoS attacks in IoT networks

by

Yahya Sulaiman Al-hadhrami

Thesis submitted in fulfilment of
the requirements for the degree of

Doctor of Philosophy

Under the supervision of **Dr. Farookh Khadeer Hussain**

University of Technology Sydney
Faculty of Engineering and Information Technology

September-2020

Certificate of Authorship/Originality

I, Yahya Al-Hadhrami declare that this thesis, is submitted in fulfilment of the requirements for the award of Doctor of Philanthropy (C02029), in the computer science school/faculty of engineering and information technology at the University of Technology Sydney.

This thesis is wholly my own work unless otherwise referenced or acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis.

This document has not been submitted for qualifications at any other academic institution.

This research is supported by the Australian Government Research Training Program.

Production Note:

Signature: Signature removed prior to publication.

Date: 16/09/2020

ABSTRACT

Intelligent Machine Learning Architecture for Detecting DDoS attacks in IoT networks

by

Yahya Sulaiman Al-hadhrami

The Internet of Things (IoT) is growing rapidly across a wide range of applications; one example of such an application is the smart city, in which a city's infrastructure, such as road management, building automation, and people and crowd surveillance, is connected to the Internet. Such applications are being extended to factories, smart agriculture, and even smart devices, which are becoming very common. The rapid growth in the IoT has driven other technologies, such as 5G networks, to grow rapidly to adjust to the sheer number of devices connected to the Internet, and these technologies are expected to further expand the spread of the IoT. However, the existing IoT deployment does not come without challenges, including the large number of connected devices, security issues, and a variety of new standards. From a security perspective, IoT faces a growing threat when it comes to the availability of networks. Distributed denial of service (DDoS) attacks are one well-known threat. However, investigation of the literature shows a lack of solutions with which to tackle DDoS attacks in the IoT.

To address this gap in the literature, this thesis proposes an intelligent machine-learning-based platform that can detect denial-of-service attacks, termed IDD-IoT. The proposed platform consists of several components, including building a real-time dataset generation framework to generate IoT-based datasets (IoT-DDoS) to detect malicious attacks in the IoT, allowing scientists and researchers in the field to further enhance intrusion detection systems with an up-to-date dataset. The

platform then builds on the dataset generation framework, developing an intelligent machine-learning-based framework for detecting three kinds of IoT-DDoS attacks: blackhole, selective forwarding, and flooding attacks. We utilize this framework to build a novel advanced intrusion detection system (IDS) for IoT networks capable of analyzing and detecting DDoS attacks. The IDS consists of a real-time monitoring and analysis unit capable of monitoring traffic in real time with the assistance of an IDS agent that works as a communication link between the IDS and IoT network. We show that our proposed intelligent framework can efficiently detect malicious attacks in respect to security goals such as confidentiality, privacy, and availability, by building an emulated smart IoT environment using the Cooja simulation platform, and we evaluate its performance. Finally, we present the simulation and evolution results to highlight the proposed platform's efficiency, taking into consideration the limitations associated with resource-constrained devices.

thesis directed by Associate Professor Farookh Hussain
School of Computer Science
Faculty of Engineering and Information Technology (FEIT)

Dedication

I dedicate this thesis to my family, friends and all who supported me through this journey.

Acknowledgements

I would like to humbly extend my utmost gratitude and thankfulness to the hands that helped craft my academic endeavours throughout my PhD journey. This journey has been blessed by the Almighty Allah and such blessings were bestowed upon me in the form of people guiding me to the light. One person to whom I must express my sincere appreciation is my superior and principal advisor, Associate Professor Farookh Khadeer Hussain for his endless support. His critical vision and leadership contributed greatly to my work ethic and the outlet it took. You shaped my academic character which will be of great value to me as I begin my career. My journey was also blessed by the encouragement of my family, friends and colleagues to whom I owe my deep gratitude. May Allah give you back the light you brought into my journey. Thank you.

Yahya Al-Hadhrami

Sydney, Australia, 2020.

List of Publications

The following is a list of my research papers produced during my PhD study.

Journal Papers

J-1. **Yahya Al-hadhrami**, and Farookh Khadeer Hussain, "Real time dataset generation framework for intrusion detection systems in IoT," *Future Generation Computer Systems*, 08:414 – 423, 2020, doi:"doi.org/10.1016/j.future.2020.02.051".

J-2. **Yahya Al-hadhrami**, and Farookh Khadeer Hussain, "DDoS attacks in IoT Networks: A ComprehensiveSystematic Literature Review," *World Wide Web Journal*, 2020 (Minor Revision).

Conference Papers

C-1. **Yahya Al-hadhrami**, Nassser Al-hadhrami and Farookh Khadeer Hussain: Data Exportation Framework for IoT Simulation Based Devices. *International Conference on Network-Based Information Systems*, pp.212-222 , Springer, 2019

C-2. **Yahya Al-hadhrami**, and Farookh Khadeer Hussain :A Machine Learning Architecture Towards Detecting Denial of Service Attack in IoT. *Conference on Complex, Intelligent, and Software Intensive Systems*, pp.417-429, Springer, 2019

Contents

List of Figures

List of Tables