*C02029: Doctor of Philosophy*
*Subject Code: 33874*
*February 2020*

*CRICOS Code: 0000*

# *End-to-End IoT Security: Authentication, Vulnerability Exploration and Data Analysis*

*Annie Gilda Roselin Arockia Baskaran*

School of Electrical and Data Engineering
Faculty of Engineering and Information Technology
University of Technology Sydney
NSW - 2007, Australia

# End-to-End IoT Security: Authentication, Vulnerability Exploration and Data Analysis

*A thesis submitted in partial fulfillment of the requirements*
*for the degree of*

Doctor of Philosophy
*in*
Software Engineering

*by*

**Annie Gilda Roselin Arockia Baskaran**

*to*

School of Electrical and Data Engineering
Faculty of Engineering and Information Technology
University of Technology Sydney
NSW - 2007, Australia

February 2020

# Abstract

Wireless 6LoWPAN networks consist of resource-starved, small sensor nodes. Secure sensors' communication is necessary to avoid threats such as a replay attack and a Man-in-the-Middle (MITM) attack. This research has three major parts. The first part of the research focuses on developing a lightweight authentication algorithm and key management of sensors within the 6LoWPAN network. Before transmitting sensible information, sensors must prove that they are the legal transmitting entity to the Edge Router. The second part of the research exploits the vulnerability of CoAP (Constrained Application Protocol) on the application layer of the 6LoWPAN protocol. We also investigate how 6LoWPAN with CoAP protocol withstands the off-path pin code injection threat while the 6LoWPAN sensor communicates with the legacy Internet. The Third part of the research deals with intelligent intrusion detection techniques using deep learning and clustering algorithms.

The first part, Lightweight Authentication Protocol (LAUP), uses the symmetric key method with no pre-shared keys. It comprises four flights to establish authentication and session key distribution between sensors and Edge Router in a 6LoWPAN environment. Each flight of LAUP uses freshly derived keys from existing information such as PAN ID (Personal Area Network Identification) and device identities. The second part involves the CoAP protocol that resides in an application layer protocol of the 6LoWPAN protocol stack. The widely available CoAP implementations failed to validate the remote CoAP clients. We exploit the combination of IP Spoofing vulnerability and cross-protocol vulnerability of CoAP along with the remote server access support to launch the off-path attack. The off-path attack is considered a weak attack on a constrained network, and it receives less attention from the research community. However, the consequences resulting from such an attack cannot be ignored in practice. In the third part, we propose a two-fold network traffic analysis method for anomaly detection with Optimized Deep Clustering (ODC), which involves an optimized deep autoencoder and BIRCH clustering algorithm. We observed that our ODC deep clustering algorithm outperforms the existing deep clustering methods for anomaly detection.

As a result of this research, we achieve an end-to-end secure communication of sensors within the 6LoWPAN constrained network and when the 6LoWPAN network devices interact with the legacy Internet. This research is a concrete contribution to the IoT Cyber Security community. Also, we ensure the secure communication of IoT by investigating the network traffic dataset despite any malfunction caused by an intruder.

Dissertation supervised by Professor Dr.Priyadarsi Nanda

School of Electrical and Data Engineering (SEDE)

# AUTHOR'S DECLARATION

I, *Annie Gilda Roselin Arockia Baskaran* declare that this thesis, submitted in partial fulfillment of the requirements for the award of Doctor of Philosophy, in the *School of Electrical and Data Engineering*, *Faculty of Engineering and Information Technology* at the University of Technology Sydney, Australia, 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 and Commonwealth Scientific and Industrial Research Organisation/Data 61, Australia.

SIGNATURE: Production Note: Signature removed prior to publication.

[Annie Gilda Roselin Arockia Baskaran]

DATE: 28th February, 2020

PLACE: Sydney, Australia

# Dedication

*Dedicated To,*
*My Husband*
*My Loving kids*
*My supportive family*
*My motivating Teachers*

# ACKNOWLEDGMENTS

Firstly, I would like to express my sincere gratitude to Almighty God for guiding me and blessing me with physical and mental strength along this Ph.D. journey. I would like to express my sincere gratitude to my supervisor, Dr. Priyadarsi Nanda, whose expertise, understanding, and patience, added considerably to my graduate experience. He is such a nice, generous, helpful and kind-hearted person. I am greatly indebted to his continuous encouragement, advice, motivation, and invaluable suggestions. I owe my research achievements to his experienced supervision. His guidance helped me all the time with my research and writing of this thesis. Without his support and supervision, I could not have come this far. I want to convey my deepest gratitude to my industrial supervisor Dr.Surya Nepal for his experienced supervision and continuous encouragement throughout my Ph.D. journey. Besides my supervisors, I would like to thank my co-supervisor, Prof. Xiangjian He, for his valued suggestions and constant support, and the numerous conversations with them. Their encouragement has kept me moving ahead at a critical time. Without their help, I would not have been able to complete this thesis. I wish to thank my fellow researchers for assisting in the completion of this research work. I appreciate the financial support of the University of Technology Sydney and an industrial scholarship provided by the Commonwealth Scientific and Industrial Research Organization (CSIRO). Last but not least, I would like to express my love and gratitude to my husband Arockia Baskaran, my kids Aileen Bernice and Abishai Ruiz, especially my parents Alexander and Lilly Joy Thanka Bai, my brother Aji and my in-laws.

# List of Publications

## Journal Papers

J-1 **A. G. R. Arockia Baskaran**, P. Nanda, S. Nepal, and S. He, “Testbed evaluation of Lightweight Authentication Protocol (LAUP) for 6LoWPAN wireless sensor networks," *Concurrency and Computation: Practice and Experience,* vol. 31, no. 23, p. e4868, 2019. https://doi.org/10.1002/cpe.4868 **Impact factor of 1.167**

J-2. **A. G. Roselin**, P. Nanda, S. Nepal, X. He, and J. Wright, “Exploiting the remote server access support of CoAP protocol," *IEEE Internet of Things Journal,* vol. 6, no. 6, pp. 9338-9349, 2019. Digital Object Identifier: 10.1109/JIOT.2019.2942085 **Impact factor of 9.515**

J-3. **A. G. Roselin**, P. Nanda, S. Nepal, and X. He, “Intelligent anomaly detection for large IoT network traffic with Optimized Deep Clustering (ODC) algorithm," *Submitted to IEEE Access Journal, Under review*

## Conference Papers

C-1. **A. G. Roselin**, P. Nanda, and S. Nepal, “Lightweight Authentication Protocol (LAUP) for 6LoWPAN Wireless Sensor Networks," in *2017 IEEE Trustcom/BigDataSE/ICESS. IEEE, 2017,* pp. 371-378.
DOI: 10.1109/Trustcom/BigDataSE/ICESS.2017.260 **(Rank A)**

# TABLE OF CONTENTS

# List of Figures

**Figure** **Page**

# List of Tables