

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.

Production Note:

SIGNATURE: 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/Big-DataSE/ICSS. IEEE, 2017*, pp. 371-378.
DOI: 10.1109/Trustcom/BigDataSE/ICSS.2017.260 **(Rank A)**

TABLE OF CONTENTS

List of Publications	ix
Table of Contents	xi
List of Figures	xv
List of Tables	xvii
1 Introduction	1
1.1 Basics of sensor	1
1.2 Research Motivation	3
1.3 Research Questions	4
1.4 Research Objective	5
1.5 Hardware and Software Platform	7
1.6 Structure of thesis	8
I Lightweight Authentication Protocol (LAUP) for 6LoWPAN Wireless Sensor Networks	11
2 Literature Review	13
2.1 Security issues with IoT	13
2.2 Communication protocols of wireless sensor network	15
2.3 Overview of 6LoWPAN network Architecture	16
2.4 Need for Lightweight algorithms / Header Compression Techniques	17
2.5 Anomaly detection using machine learning	20
3 Lightweight Authentication for 6LoWPAN WSN	23
3.1 Introduction	23
3.2 Existing lightweight authentication algorithms	25

TABLE OF CONTENTS

3.3	Proposed work	26
3.3.1	Architectural Environment	27
3.3.2	Basic assumptions of proposed work	28
3.3.3	Proposed LAUP Scheme	29
3.4	Summary	34
4	Evaluating Lightweight authentication algorithm	35
4.1	Introduction	35
4.2	Existing formal verification methods	36
4.3	Formal Verification of LAUP Algorithm	37
4.4	Security Analysis based on threat scenarios:	44
4.4.1	Threat model:	44
4.4.2	Security aanalysis:	45
4.5	Validation and Evaluation of Proposed LAUP Algorithm	47
4.5.1	Evaluation using COOJA simulator	47
4.5.2	Hardware Evaluation	51
4.6	Summary	54
 II Exploring the vulnerability of CoAP protocol and a mitigation technique: a case study of smart door keypad lock		 55
5	Exploring the vulnerabilities of WSN while interacting with Internet	57
5.1	Introduction	57
5.2	6LoWPAN protocol stack with CoAP	59
5.3	CoAP message format and its functionality	60
5.4	Potential attacks on CoAP	62
5.5	Existing Work	63
5.6	Our Testbed Architecture	64
5.6.1	Construction of Testbed	65
5.6.2	Two Factor Authentication (2FA) for the CoAP user	68
5.7	Our off-path attack	70
5.7.1	Off-path attack scenario	70
5.7.2	Packet analysis with off-path attack	72
5.8	Limitations of existing IoT security protocol and IoT user authentication .	74

5.8.1	Limitations of DTLS	74
5.8.2	Limitations of user authentication	76
5.8.3	Limitations of firewall	76
5.9	Summary	77
6	Countermeasure techniques for identified vulnerabilities	79
6.1	Introduction	79
6.2	Existing open-source intrusion detection system	80
6.3	Mitigation technique	80
6.3.1	Dataset	81
6.3.2	Training phase: Building ML models	81
6.3.3	Testing phase: Threat Prediction	84
6.4	Summary	85
III	Intelligent anomaly detection for a large network traffic with Optimized Deep Clustering (ODC) algorithm	87
7	IDS using unsupervised deep clustering algorithm	89
7.1	Introduction	89
7.2	Deep Autoencoder	91
7.3	BIRCH Clustering Algorithm	92
7.4	Existing deep clustering techniques	93
7.5	Proposed deep clustering method	94
7.5.1	Enhanced deep autoencoder	95
7.5.2	Optimized deep clustering with BIRCH	96
7.5.3	ODC outlier handling	98
7.6	Experimental evaluation	99
7.7	Summary	104
8	Conclusion and Future Directions	105
8.1	Summary of the thesis	105
8.2	Contribution of the research	106
8.2.1	Testbed development	107
8.3	Future Directions	107
	Bibliography	109

LIST OF FIGURES

FIGURE	Page
1.1 Wireless Sensor Network	2
1.2 Security challenges in IoT based applications	3
1.3 Schematic mapping of Research Objectives	5
1.4 Protocol stack of a WSN connected to Internet	6
2.1 IoT attacks Taxonomy [150], [8], [9]	15
2.2 Network layer comparison of WSN protocols	16
2.3 6LoWPAN Protocol Stack	17
2.4 IEEE 802.15.4 frame with IPv6 and UDP fixed headers	17
2.5 AH security extension headers for 6LoWPAN frame	18
2.6 ESP security extension headers for the 6LoWPAN frame	18
2.7 Security at the Link Layer	19
2.8 LoWPAN_NHC extension header and AH	19
2.9 Compressed UDP with AH	20
2.10 NHC header for ESP	20
2.11 Compressed UDP with ESP	20
3.1 Proposed Lightweight Authentication Algorithm (LAUP)	27
3.2 System architecture of LAUP	28
3.3 Flow chart of Edge Router Process	32
3.4 Flow chart of 6LoWPAN sensor Process	33
4.1 Sycther tool results for LAUP Protocol verification	37
4.2 Symbols and its Explanations	38
4.3 Simulation using COOJA: motes set up	42
4.4 Computational overhead	43
4.5 Power consumption	43

LIST OF FIGURES

4.6	Processing Time	44
4.7	LAUP Threat model	45
4.8	Hardware setup for LAUP	47
4.9	Uploading Border Router of LAUP to Wismote Hardware using MSP430 USB-Debug-Interface(MSP-FET430UIF) device	49
4.10	Uploading UDP client of LAUP to Wismote Hardware using MSP430 USB- Debug-Interface(MSP-FET430UIF) device	50
4.11	Test bed results-Comparison - simulation and hardware	51
4.12	Test bed results-Comparison of LAUP process time	52
4.13	Test bed results-Processing time of LAUP	53
5.1	Off-path attack model on CoAP protocol	60
5.2	6LoWPAN protocol stack with abstract layering of CoAP	60
5.3	CoAP packet	61
5.4	Our testbed architecture	65
5.5	Smart door keypad lock prototype and its process flow	66
5.6	Software components of smart door keypad lock	67
5.7	Two-factor authentication process for CoAP user	69
5.8	Off-path attack scenario	71
5.9	Actual user's CoAP request packet captured by Wireshark	73
5.10	The attacker's CoAP request packet captured by Wireshark	75
6.1	Training phase: performance comparison of different ML classifiers	82
6.2	Testing phase: Prediction accuracy comparison of different ML models	84
7.1	Enhanced deep clustering (enhanced deep autoencoder + BIRCH clustering)	94
7.2	Comparing the Training Reconstruction Error (Train RE) of deep autoencoder with various combinations of activation and optimization functions	97
7.3	Comparing the Testing Reconstruction Error (Test RE) of deep autoencoder with various combinations of activation and optimization functions	97
7.4	CoAP Accuracy	100
7.5	CoAP NMI	100
7.6	MNIST Accuracy	101
7.7	MNIST NMI	101
7.8	ACC and NMI of CoAP off-path dataset based on Branching factor of BIRCH	103
7.9	ACC and NMI of CoAP off-path dataset based on Threshold value of BIRCH	103

LIST OF TABLES

TABLE	Page
1.1 Sensor Categories	2
3.1 Theoretical comparison of LAUP with other similar protocols	24
3.2 Key Derivation Process	29
4.1 Memory usage of the sensor and an Edge Router	48
5.1 Potential attacks on CoAP	62
7.1 Optimization of Deep Autoencoder	96
7.2 Comparing the accuracy of various deep clustering techniques	98

