國立中正大學

National Chung Cheng University

Department of Computer Science and Information Engineering

College of Engineering

National Chung Cheng University

Doctoral dissertation

Collaborative detection framework for security attacks on the Internet of Things

Nguyen Van Linh

Advisor: Prof. Po-Ching Lin, Ph.D.

Co-advisor: Prof. Ren-Hung Hwang, Ph.D.

Taiwan, R.O.C, Fall 2019

國立中正大學博士學位論文考試審定書

資訊工程學系

研究生 阮文齡 所提之論文

Collaborative detection framework for security attacks on the Internet of Things

經本委員會審查，符合 博 士學位論文標準。

學位考試委員會
召集人 Chi 簽章

委員

Ren-Hung Hwang　　Po-Ching Lin

Wei-Kuo Chiang　　Jian-Jhih Kuo

指導教授 Po-Ching Lin 簽章

中華民國 108 年 12 月 25 日

博碩士論文電子檔案上網授權書

＊106CCU00392111＊

（本聯請隨論文繳回學校圖書館，供國家圖書館做為授權管理用） ID:106CCU00392111

本授權書所授權之論文為授權人在 國立中正 大學(學院) 資訊工程研究所 系所 ______ 組 108 學年度第 二 學期取得 博 士學位之論文。

論文題目： Collaborative detection framework for security attacks on the Internet of Things

指導教授： 林柏青,Po-Ching Lin

茲同意將授權人擁有著作權之上列論文全文（含摘要），提供讀者基於個人非營利性質之線上檢索、閱覽、下載或列印，此項授權係非專屬、無償授權國家圖書館及本人畢業學校之圖書館，不限地域、時間與次數，以微縮、光碟或數位化方式將上列論文進行重製，並同意公開傳輸數位檔案。

☑ 校內外立即開放
□ 校內立即開放，校外於 年 月 日後開放
□ 校內於 年 月 日；校外於 年 月 日後開放
□ 其他

授權人：阮文齡

簽　名：______________________　　　日期：______年______月______日

Acknowledgements

The road to scientific research has never been a flat one, especially to me. After three years of fighting for my dream, being a cybersecurity scientist, finally, I also have a chance to express my sincere gratitude to the people who have given me passion and strength in this fight. I would like to sincerely express the deepest appreciation to my beloved supervisors, Prof. Po-Ching Lin and Prof. Ren-Hung Hwang, who both have encouraged me to surpass the critical points of this research. I could not have imagined, without their valuable assistance and timely encouragement, whether I was on the right track. To me, their insightful comments, tough questions, and particularly thoughtful reviews have certainly motivated me a lot to finish this extremely hard work on time.

I'd like to sincerely thank National Chung Cheng University (CCU) for offering me a full scholarship. Also, the precious and constant sponsorship from Prof.Lin and Prof.Hwang, Department of Computer Science and Information Engineering (CSIE@CCU), and Taiwan Information Security Center in National Sun Yat-sen University (TWISC@NSYSU) is extremely vital for my research and living in Taiwan.

Also, a thank you to my professors at CCU/NSYSU who taught me great courses or worked with me in meaningful projects. A thank you to Ms. Huang and Ms. Chen who have given me exciting Chinese courses, that certainly helped me to forget all tiredness at work and keep fighting. I would like to thank the staff of CSIE@CCU for their great support in the document procedure. Thank all members of Network and System Security Lab, my beloved friends in CCU, Karate club, and Badminton team who are always willing to encourage and cheer with me at the memorable time of my Ph.D. journey.

Finally, thanks to my parents, my darling, and all my friends for their unconditional support and patience during the courses of this work. Last but not least, I would like to thank my life partner, Lan-Huong, for her constant encouragement, sacrifices and endless love in me, that motivated me a lot to firmly pursue the doctoral program till the end. I believe that, without the encouragement and supports, I could never be strong enough to overcome the difficulties and finish this research successfully.

Abstract

A connected world of Internet of Things (IoT) has become a visible reality closer than ever and that is now being fueled by the appearance of 5G and beyond 5G (B5G) connectivity technologies. However, besides bringing up the hope of a better life for the human being through promising applications, at the same time, the complicated structure of IoT and the diversity of the stakeholders in accessing the networks also raises grave concerns that our life may be extremely vulnerable than ever with daily threats of security attacks, disinformation, and privacy violation. The objective of the research presented in this dissertation is to detect the attacks targeting the network availability (e.g., the volume attacks) and data authenticity (e.g., data forgery dissemination attacks) in the perception layer and the network layer of IoT networks. Further, our research targets to exclude responsible attackers, misbehavior nodes and unreliable stakeholders from active network participation or even mitigate the magnitude of such attacks significantly at the edge of the networks in a timely fashion.

While most existing solutions in the context of security detection in IoT are based on data-driven learning and plausibility checks on the traffic near the victim or a single network hop, we propose in this dissertation a collaborative security defense framework, so-called TrioSys, which primarily relies on three main approaches. First, the system evaluates the behavior of traffic/nodes based on learning cooperatively accumulated information, e.g., traffic request distribution targeting a specific address over a time interval, and fusing the trustworthiness of post-detection results from multiple layer trusted engines such as the edge-based(regional)/cloud-based (global) detection systems. Second, by largely targeting at filtering malicious traffic/bogus messages directly at/near the source/nodes/edge, our system provides an extremely effect protection approach with low latency response to the attacks, particularly before their malicious traffic have a chance to pour into the networks or affect to the decision of the unsuspecting nodes such as the control system of an autonomous vehicle. Finally, in each specific case of the application deployment, i.e., in IoT eMBB or IoT uRRLC, we propose a proper strategy to implement the detection mechanisms for the platform. For example, in the autonomous driving case (IoT uRRLC), we propose a novel method to exploit passive source localization techniques from physical signals of multi-array beamforming antennas in V2X-supported vehicles and motion prediction to verify the truthfulness of the claimed GPS location in V2X messages without requiring the availability of many dedicated anchors or a strong assumption of the honest majority rule as in conventional approaches.

In summary, this work has been developed that consists of two main contributions: (1) TrioSys, a robust and effective platform for detecting and filtering the attacks in IoT, particularly compatible with 5G applications and network models; (2) a novel near-source detection for DDoS defense in IoT eMBB slice and two physical signal-driven verification schemes for V2X (i.e., IoT uRLLC). Also, besides our comprehensive survey on the state-of-the-art attacks against network availability/data authenticity and countermeasure approaches, our findings on relevant security issues can certainly provide useful suggestions for future work.

Keywords – Internet of Things Security, 5G/B5G Security, Distributed Denial-of-service defense, Misbehavior Detection in 5G V2X

Overview of publication

The following articles are peer-reviewed and accepted publications with results included in/achieved during this dissertation:

Journal Papers

1. Van-Linh Nguyen, Po-Ching Lin and Ren-Hung Hwang, “Multi-array relative positioning for verifying the truthfulness of V2X messages,” IEEE Communication Letter, Vol. 23 , No. 10, pp. 1704-1707, Oct. 2019.
2. Van-Linh Nguyen, Po-Ching Lin, and Ren-Hung Hwang, “Energy depletion attacks in Low Power Wireless networks,” IEEE Access, Vol.7, Apr. 2019.
3. Van-Linh Nguyen, Po-Ching Lin and Ren-Hung Hwang, “MECPASS: Distributed Denial of Service Defense Architecture for Mobile Networks,” IEEE Network, Vol 32, No 1, pp. 118-124, Jan.-Feb. 2018.
4. Van-Linh Nguyen, Po-Ching Lin, and Ren-Hung Hwang, “Web Attacks: beating monetisation attempts,” Network Security Journal (Elsevier), No.5, pp. 1-20, May 2019.
5. Ren-Hung Hwang, Min-Chun Peng, Van-Linh Nguyen, and Yu-Lun Chang, “An LSTM-Based Deep Learning Approach for Classifying Malicious Traffic at the Packet Level,” Applied Sciences, Vol. 9, No. 16, pp.3414-3428 , Aug. 2019.
6. Van-Linh Nguyen, Po-Ching Lin and Ren-Hung Hwang, “Enhancing misbehavior detection in 5G Vehicle-to-Vehicle communications,” submitted to IEEE Transactions on Vehicular Technology (major revision).
7. Ren-Hung Hwang, Min-Chun Peng, Chien-Wei Huang, Po-Ching Lin and Van-Linh Nguyen, “PartPack: An unsupervised deep learning model for early anomaly detection in network traffic,” submitted in Aug. 2019 to IEEE Transactions on Emerging Topics in Computational Intelligence.

Conference Papers

1. Ren-Hung Hwang, Van-Linh Nguyen, and Po-Ching Lin, “StateFit: A security framework for SDN programmable data plane model,” The 15th International Symposium on Pervasive Systems, Algorithms and Networks (ISPAN), Yichang,

China, Oct 2018.

2. Po-Ching Lin, Ping-Chung Li, and Van-Linh Nguyen,“Inferring OpenFlow rules by active probing in software-defined networks,” The 19th International Conference on Advanced Communications Technology (ICACT), Pyongchang, South Korea, Jan. 2017.

3. Van-Linh Nguyen, Po-Ching Lin and Ren-Hung Hwang, “Physical signal-driven fusion for V2X misbehavior detection,” IEEE Vehicular Networking Conference, Los Angeles, USA, 2019.

Projects that I have contributions on

1. Po-Ching Lin and Van-Linh Nguyen “Security protection system for V2X in 5G networks,” a three-year granted MOST project, 2019/08/01 - 2022/07/31.

Contents