UNIVERSITY OF TECHNOLOGY SYDNEY
Faculty of Engineering and Information Technology

SECURING DATA TRANSMISSION IN INTERNET OF THINGS

by

Xuan Zha

A Thesis Submitted
in Partial Fulfillment of the
Requirements for the Degree

Doctor of Philosophy

Sydney, Australia

2019

Certificate of Authorship/Originality

I, Xuan Zha declare that this thesis, is submitted in fulfilment of the requirements for the award of Doctor of Philosophy, in the Faculty of Engineering and Information Technology at the University of Technology Sydney. This thesis is wholly my own work unless otherwise reference or acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis. I certify that the work in this thesis has not been previously submitted for a degree nor has it been submitted as a part of the requirements for other degree except as fully acknowledged within the text. This thesis is the result of a research candidature jointly delivered with Beijing University of Posts and Telecommunications as part of a Collaborative Doctoral Research Degree. This research is supported by the Australian Government Research Training Program.

Production Note:
Signature: Signature removed prior to publication.

Date: 26/09/2019

Dedication

To my dear husband

To my loving parents

To my supportive supervisors

To my wonderful friends

Acknowledgements

I sincerely convey my deepest gratitude to my principal supervisor Prof. Y. Jay Guo for his experienced supervision throughout my doctoral program. I would show my honest and sincere appreciation to my co-supervisor Prof. Ren Ping Liu and Dr. Wei Ni from Commonwealth Scientific and Industrial Research Organisation (CSIRO). Without their consistent support and supervision, I would not have been able to complete this thesis. I would also like to express my honest appreciation to my supervisors at Beijing University of Posts and Telecommunications (BUPT) for their experienced supervision and continuous encouragement.

I thank the University of Technology Sydney (UTS) and the Faculty of Engineering and IT (FEIT) for providing me an IRS Scholarship throughout my doctoral program. I would also like to thank staff members, previous and current colleagues, friends at UTS and CSIRO for their kind help. Special thanks to Dr. Xu Wang, Dr. Bo Song, Dr. Saber Yu, Dr. Ping Yu, Dr. Shangjing Lin, Dr. Chen Qing, Dr. Shoulu Hou, Dr. Xin Yuan, Dr. Zishan Liu, Dr. Xinchen Lyu, Dr. Haihan Sun, Dr. Fangfang Dai, and Dr. Yixun Hu.

Last but not least, I am deeply grateful to my husband Xiaoming Peng, my mother Guiying Zhang, my father Rihui Zha, my aunt Wenfang Zha and the rest of my family for their support and constant encouragement.

Xuan Zha

Sydney, Australia, 2019.

List of Publications

The author has published four journal papers, including two IEEE transaction journal papers, and three international conference papers, as the (co-)first author. The impact factor (IF) of the journal papers is also stated*.

Journal Papers

J-1. **X. Zha**, W. Ni, X. Wang, R. P. Liu, Y. J. Guo, X. Niu and K. Zheng, "The Impact of Link Duration on the Integrity of Distributed Mobile Networks," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 9, pp. 2240-2255, Sep. 2018. (IF: 5.824)

J-2. **X. Zha**, W. Ni, K. Zheng, R. P. Liu and X. Niu, "Collaborative Authentication in Decentralized Dense Mobile Networks With Key Predistribution," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 10, pp. 2261-2275, Oct. 2017. (IF: 5.824)

J-3. X. Wang, **X. Zha**, W. Ni, R. P. Liu, Y. J. Guo, X. Niu and K. Zheng, "Survey on Blockchain for Internet of Things", *Computer Communications*, vol. 136, pp. 10-29, Feb. 2019 (IF: 2.613) **(X. Zha and X. Wang contributed equally to this paper)**

J-4. **X. Zha**, X. Wang, W. Ni, R. P. Liu, Y. J. Guo, X. Niu and K. Zheng, "Blockchain for IoT: the Tradeoff between Consistency and Capacity", *China Journal on Internet of Things*, vol. 1, no. 1, pp. 21-33, 2017

J-5. X. Wang, **X. Zha**, W. Ni, R. P. Liu, Y. J. Guo, X. Niu and K. Zheng, "Game Theoretic Suppression of Forged Messages in Online Social Networks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, Accepted, 2019.

---

*IF: Impact Factor. Refer to http://wokinfo.com/essays/impact-factor/ for details.

J-6. K. Zheng, X. Wang, **X. Zha** and H. Xiao, "A New Network Coding Mechanism Balancing Coding Opportunities, Energy and QoS in WSNs," *China Communications*, vol. 11, no. 6, pp. 108-118, June 2014.

Conference Papers

C-1. **X. Zha**, X. Wang, W. Ni, R. P. Liu, Y. J. Guo, X. Niu and K. Zheng, "Analytic Model on Data Security in VANETs", *Int. Symposium on Communications and Information Technologies*, pp. 1-6, Sep. 25-27, 2017

C-2. **X. Zha**, K. Zheng, D. Zhang, "Anti-Pollution Source Location Privacy Preserving Scheme in Wireless Sensor Networks,", *Proc. IEEE Int. Conf. on Sensing, Communication, and Networking (SECON)*, pp. 1-8, Jun. 27-30, 2016

C-3. **X. Zha**, W. Ni, R. P. Liu, K. Zheng and X. Niu, "Secure Data Transmission and Modelling in Vehicular Ad Hoc Networks", *Proc. IEEE Int. Conf. on Globecom Workshop*, pp. 1-6, Dec. 6-10, 2015.

C-4. X. Wang, **X. Zha**, G. Yu, W. Ni, R. P. Liu, Y. J. Guo, X. Niu and K. Zheng, "Attack and Defence of Ethereum Remote APIs", *Proc. IEEE Int. Conf. on Globecom Workshop*, Dec. 9-13, 2018

C-5. G. Yu, X. Wang, **X. Zha**, J. A. Zhang, R. P. Liu, "An Optimized Round-Robin Scheduling of Speakers for Peers-to-Peers-based Byzantine Faulty Tolerance", *Proc. IEEE Int. Conf. on Globecom Workshop*, Dec. 9-13, 2018

Contents

List of Figures

Abbreviation

IoT: Internet of Things

VANET: Vehicular Ad hoc Network

WSN: Wireless Sensor Network

GEV: Global Encoding Vector

LEV: Local Encoding Vector

2D: Two-dimensional

3D: Three-dimensional

4D: Four-dimensional

CSMA/CA: Carrier Sense Multiple Access/Collision Detection

DCF: Distributed Coordination Function

MAC: Message Authentication Code

ACK: Acknowledgement

NACK: Non-acknowledgement

ABSTRACT

SECURING DATA TRANSMISSION IN INTERNET OF THINGS

by

Xuan Zha

The Internet of Things (IoT) is poised to transform our lives and unleash enormous economic benefit. With the rise in the number of connected IoT devices, the potential vulnerabilities in IoT increase as well. The IoT security faces severe challenges arising from its specific characteristics. This thesis studies the location privacy protection and secure data transmission issues in IoT to ensure the data confidentiality, integrity, non-repudiation and availability. Markov models are proposed to analyse the network performance of secure data transmission mechanisms, providing quantified criteria for selecting appropriate secure transmission protocols in various network environments. The main contributions of this thesis are as follows,

(1) An anti-pollution source-location privacy scheme is proposed to tackle the conflict between the source-location protection and authentications. The proposed protocol consists of key predistribution mechanisms and a homomorphic signature algorithm, for filtering out polluted and dummy packets at intermediate nodes while concealing the packet trajectory. The proposed protocol improves the message delivery rate and saves energy as compared with previous works.

(2) A probabilistic encrypted data transmission protocol is proposed to transmit messages in confidentiality in an adaptive manner. It avoids the communication overhead caused by handshaking in previous data encryption protocols. In addition, a three-dimensional (3D) Markov model is constructed to analyse the impact of wireless communication collisions and key predistributions on the performance of encrypted data transmissions. The analysis and simulation results prove the accuracy of the 3D Markov model.

(3) An authentication protocol is proposed in opportunistic routing based IoT networks. In order to improve the authentication efficiency, the proposed protocol generates authentication information based on the combination of the new message and previous non-conflict but unauthenticated messages while attempting different keys. A new 3D Markov model is designed to accurately capture the interaction process among non-coordinated transmissions, key selections and packet lifetime. The proposed protocol substantially improves the tolerance against changing topologies and resistance against collusion attacks, as compared to the prior art.

(4) A four-dimensional (4D) Markov model is designed to analyse the impact of dynamic topology on opportunistic authentication protocols. Three cross-layer data authentication protocols are proposed with opportunistic authentication and channel access coupled to different extent. According to the simulation results, the 4D model is general and accurate. The analysis results prove that opportunistic data authentication protocols significantly improve the authentication rate, reduce authentication delay and enhance scalability to dense mobile distributed networks.

Dissertation directed by Professor Y. Jay Guo
Faculty of Engineering and Information Technology