Adaptive Secure Network Model for Dynamic Wireless Mesh Network

By

Ashish Nanda

A dissertation submitted to

Faculty of Engineering and Information Technology

University of Technology Sydney

In fulfilment of the requirements for the award of

Doctor of Philosophy – Computer Systems

June 2018

Dedicated To

My Loving Parents

My Artistic Brother

My Supportive Family

My Motivating Teachers and Mentors

My Crazy Friends

And To Everyone That Reads This

Certificate of Original Authorship

I, Ashish Nanda declare that this thesis is submitted in fulfilment of the requirements for the award of Doctor of Philosophy, in the Faculty of Engineering and 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.

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

Signature of Student:

Production Note:
Signature removed prior to publication.

Date: 2/07/2018

Acknowledgement

I would like to convey my deepest gratitude to my principal coordinating supervisor Dr. Priyadarsi Nanda and my honest appreciation to my co-supervisor Prof. Xiangjian He, external supervisor Dr. Aruna Jamdagni from Western Sydney University and mentor Dr. Meenakshi Mahajan from National Informatics Center, India for their experienced supervision and continuous encouragement throughout my PhD study. I would also like to thank the University of Technology Sydney (UTS), Faculty of Engineering and IT (FEIT), staff members, research assistants, previous and current colleagues at UTS for all the help throughout my doctoral program.

To my friends, I thank you for listening, offering me advice, and supporting me through this journey. Special thanks to Dr. Deepak Puthal, Dr. Karthick Thiyagarajan, Vijaya Chemalamarri, Pulkit Rohilla, Jaime Garcia, Ashish Kapoor, Neha Sharma, Madhumita Takalkar, Abhijeet Takalkar, Alina Rakhi, Manisha Pratihast, Ashish Kumar, Chau Nguyen, Tham Nguyen, Sara Farahmandian, Gaurvi Goyal, Umesh Gupta, Aayushi Singh, Abhilash Kalotra, Akanksha Rana, Divya Krishna, Manushree Sharma, Yukti Mangal, Deepa Singh, Harshitha Mysore, Sidhant Sehegal, Saurabh Sachdeva, Shweta Sachdeva.

I am deeply grateful to my parents Arun Kumar Nanda and Meenakshi Nanda, my brother Ayush Nanda, my grandparents Late Shri Jagdish Prasad Nanda, Susheela Nanda, Late Shri Ram Prakash Sharma, Chanchal Sharma and the rest of my family for their support, constant encouragement and guidance. Most importantly, I would like to express my sincere gratitude to Almighty God for guiding me along this path.

Abstract

We as an advanced civilization rely on communication networks for a lot of important tasks. They are used to share information between vital systems, provide us with our pin-point location, access various digital resources and to stay connected with each other. Due to its necessity and enormity, maintaining and securing such a communication medium is an important task. As most communication networks rely on centralized systems, they are bound by the control of a central entity and are unable to keep up with the current growth of the network and advancements in electronic devices. The next step in an inter-connected world requires a decentralized distributed system that can also provide high levels of security. One possible solution is a dynamic distributed wireless mesh network as it provides all the features of a traditional network along with the flexibility of wireless communication and an infrastructure less distributed setup. The network can be created by connecting mobile or stationary devices together using wireless communication devices (such as smartphones, laptops, hot-spots, etc). As the network is created by multiple devices, it would not break-down if some of the devices were disabled. On the contrary, as the network uses hopping for message transmission using dynamic routes, it can self-heal by creating alternate routes if a device was to fail. As the workings and features of a dynamic mesh network differ from the traditional network, it also requires a modified security framework that can provide high levels of security whilst taking benefit of the dynamic mesh network's unique features.

This thesis investigates the problems and limitations linked to secure dynamic wireless mesh networks and how they can be improved upon. In addition to the routing protocols used and how they can be improved upon, the thesis also elaborates on the various security concerns with such networks. As distributed networks aren't dependent on a central entity, enabling various security features such as authentication are a major challenge. In addition to the decentralized nature of the networks, a single security scheme would not be able to cover the various types of requirements a given scenario in the network might have. Along with authentication, providing end-to-end encryption is also an important component towards ensuring the data travelling through the network is secure and not tampered with. Encryption is also essential in a dynamic wireless mesh network as the data transmitted travels through multiple devices on the network before reaching the destination node and can be easily compromised if not secured. With such an importance of encryption, the network also requires a key management and distribution framework. As traditional network uses a centralized system for maintaining and distributing cryptographic keys in the network, it is a big challenge to implement the same in a distributed network with minimal dependence on a central entity. The key exchange must consider the nature of the network and accordingly incorporate improvements to be able to function in a distributed network. This thesis explores the above areas to propose a new network model for a secure dynamic wireless mesh network including a new routing scheme and a security framework comprising a hybrid encryption scheme, a hybrid authentication scheme and an improved key exchange and management scheme. This thesis demonstrates that our solutions not only strengthen and secure the dynamic wireless mesh networks but also significantly improve the performance and efficiency as compared to existing approaches.

Author's Publications

The author has published five refereed papers including one ERA ranked A[1] journal paper, two ERA ranked A conference papers and two ERA ranked B conference paper. The publications including one ERA ranked B conference paper that is under review are listed below in detail. The impact factor (IF)[2] of the journal paper is also stated.

Journal Article:

1. **Ashish Nanda**, Priyadarsi Nanda, Xiangjian He, Aruna Jamdagni, and Deepak Puthal, 2018, 'A hybrid encryption technique for Secure-GLOR: The adaptive secure routing protocol for dynamic wireless mesh networks', *Future Generation Computer Systems* (FGCS), https://doi.org/10.1016/j.future.2018.05.065, 2018 (ERA tier A, Impact Factor 4.639)

[1] ERA ranking is a ranking framework for publications in Australia. Refer to http://www.arc.gov.au/era/era_2010/archive/era_journal_list.htm for detailed ranking tiers. The 2010 version is used herein. For journal papers: A* (top 5%); A (next 15%). For conference papers (no A* rank): A (top 20%).

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

Conference Papers:

2. **Ashish Nanda**, Priyadarsi Nanda, Xiangjian He and Deepak Puthal, 2018, 'A Novel Hybrid Authentication Model for Geo Location Oriented Routing in Dynamic Wireless Mesh Networks', 51st Hawaii International Conference on System Sciences(HICSS-51) Hawaii, 3rd-6th January 2018 – Published, (ERA tier A)

3. **Ashish Nanda**, Priyadarsi Nanda, Xiangjian He, Aruna Jamdagni, and Deepak Puthal, 2017, 'Secure-GLOR: An Adaptive Secure Routing Protocol for Dynamic Wireless Mesh Networks', 16th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-17) Sydney, Australia, 1st-4th August 2017 – Published in IEEE Conference Proceedings by IEEE CS CPS, (ERA tier A)

4. **Ashish Nanda**, Priyadarsi Nanda and Xiangjian He, 2016, 'Geo-Location Oriented Routing Protocol for Smart Dynamic Mesh Network', 18th IEEE International Conference on High Performance Computing and Communications (HPCC-2016), Sydney, Australia, 12th-14th December 2016 – Published in IEEE Conference Proceedings by IEEE CS CPS, (ERA tier B)

5. **Ashish Nanda**, Priyadarsi Nanda, Xiangjian He and Aruna Jamdagni, 2016, 'A Secure Routing Scheme for Wireless Mesh Networks', 12th International Conference on Information Systems Security (ICISS-2016), Jaipur, India, 16th-20th December 2016 – Published in Springer Verlag series of Lecture Notes in Computer Science, (ERA tier B)

Table of Contents

List of Figures

List of Tables

List of Algorithms