

# **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 Chemalarri, 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<sup>1</sup> 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)<sup>2</sup> 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)

---

<sup>1</sup> 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](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%).

<sup>2</sup> 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

<b>Certificate of Original Authorship</b> .....	<b>II</b>
<b>Acknowledgement</b> .....	<b>III</b>
<b>Abstract</b> .....	<b>IV</b>
<b>Author’s Publications</b> .....	<b>VI</b>
<b>Table of Contents</b> .....	<b>VIII</b>
<b>List of Figures</b> .....	<b>XI</b>
<b>List of Tables</b> .....	<b>XIII</b>
<b>List of Algorithms</b> .....	<b>XIII</b>
<b>Chapter 1 Introduction</b> .....	<b>1</b>
1.1    Aim and Research Goals .....	2
1.1.1    Network Model .....	2
1.1.2    Security Framework .....	5
1.2    Research Motivation .....	6
1.3    Research Overview .....	8
1.3.1    Methodology.....	8
1.3.2    Contributions .....	9
1.4    Thesis Organization .....	11
<b>Chapter 2 Background Studies and Related Works</b> .....	<b>13</b>
2.1    Research Overview .....	14
2.2    Data Transmission Techniques .....	17
2.2.1    Flooding - Broadcast Technique .....	17
2.2.2    Unicast - Multicast Technique .....	19
2.3    Routing Protocols .....	20
2.3.1    Optimized Link State Routing (OLSR).....	21
2.3.2    Ad hoc On-Demand Distance Vector (AODV) Routing.....	22
2.3.3    Zone Routing Protocol (ZRP).....	23
2.3.4    Destination-Sequenced Distance-Vector (DSDV) Routing.....	24
2.3.5    Dynamic Source Routing (DSR) .....	25

2.3.6	Temporally Ordered Routing Algorithm (TORA).....	26
2.4	Network Models .....	27
2.4.1	The SPAN Project .....	28
2.4.2	The Several Project .....	29
2.4.3	Open Garden: FireChat .....	32
2.4.4	The BRIAR Project .....	34
2.5	Security Concerns in Distributed Networks .....	35
2.5.1	Availability.....	36
2.5.2	Authenticity.....	38
2.5.3	Integrity.....	38
2.5.4	Confidentiality.....	39
2.5.5	Non-Repudiation.....	40
2.5.6	Anonymity.....	40
2.6	Key Security Aspects for Distributed Systems.....	41
2.6.1	Authentication .....	41
2.6.2	Encryption .....	43
2.6.3	Key Management.....	46
2.7	Summary.....	48
<b>Chapter 3 Secure Geo-Location Oriented Routing Network Model.....</b>		<b>50</b>
3.1	Introduction.....	51
3.2	Existing Approaches.....	52
3.2.1	Routing Models.....	53
3.2.2	Legacy Routing Protocols.....	54
3.3	Proposed Geo-Location Oriented Routing Protocol.....	55
3.3.1	Security Framework .....	58
3.3.2	Node Addressing.....	61
3.3.3	Node Registration .....	63
3.3.4	Smart Packets.....	64
3.3.5	Random Waypoint Mobility Model .....	70
3.4	Results and Validation .....	71
3.4.1	Environment Setup .....	72
3.4.2	Simulation and Observation .....	72
3.4.3	Results and Discussion .....	73
3.5	Summary.....	75
<b>Chapter 4 Authentication Mechanism for Distributed Networks.....</b>		<b>76</b>
4.1	Introduction.....	77
4.2	Current Approaches and Problem Statement.....	78
4.2.1	Current Approaches.....	79
4.2.2	Problem Statement.....	80
4.3	Authentication Mechanism .....	81
4.3.1	Full Authentication (Scenario 1) .....	83
4.3.2	Quick Authentication (Scenario 2).....	87

4.3.3	New Node Authentication (Scenario 3)	91
4.4	Results and Validation	93
4.4.1	Environment Setup	93
4.4.2	Results and Analysis	93
4.5	Comparative Analysis	97
4.6	Summary	99
<b>Chapter 5</b>	<b>Encryption Techniques for Dynamic Distributed Networks</b>	<b>100</b>
5.1	Introduction	101
5.2	Existing Models	102
5.3	Encryption Techniques	103
5.3.1	Asymmetric (Standard) Encryption Technique	104
5.3.2	Hybrid Encryption Technique	105
5.4	Theoretical Analysis	107
5.4.1	Security Proofs	108
5.4.2	Forward Secrecy	110
5.5	Results and Validation	111
5.5.1	Simulation Environment Setup	111
5.5.2	Simulation and Observation	112
5.5.3	Results and Analysis (Standard Encryption Technique)	112
5.5.4	Results and Analysis (Hybrid Encryption Technique)	116
5.6	Summary	121
<b>Chapter 6</b>	<b>Key Management Scheme for Distributed Networks</b>	<b>122</b>
6.1	Introduction	123
6.2	Assumptions and Notations	125
6.2.1	Network Assumptions	125
6.2.2	Notations Used	126
6.3	Proposed Key Distribution Scheme	127
6.3.1	Initial Contact	128
6.3.2	Key-Pair Generation	128
6.3.3	Key Transmission	130
6.3.4	Key Selection	131
6.3.5	Challenge - Response	132
6.4	Key Distribution Process	133
6.5	Security Analysis	136
6.5.1	Claims & Proof	136
6.5.2	Threat Analysis	138
6.6	Summary	141
<b>Chapter 7</b>	<b>Conclusion and Future Direction</b>	<b>142</b>
7.1	Thesis Summary and Conclusions	143
7.2	Future Work	146
<b>Bibliography</b>		<b>148</b>

# List of Figures

Figure 2.1 Mesh Network Topology .....	14
Figure 2.2 Data Transmission in a Mesh Network.....	15
Figure 2.3 Self-Healing in a Mesh Network .....	15
Figure 2.4 Flooding / Broadcast Technique Sample .....	18
Figure 2.5 Multicast Routing.....	19
Figure 2.6 Generation III Several Mesh Extender [11] .....	31
Figure 2.7 Encryption - Decryption Process.....	44
Figure 2.8 Symmetric and Asymmetric Encryption .....	45
Figure 3.1 Network Scenario .....	56
Figure 3.2 Different Steps of Routing Process .....	57
Figure 3.3 Addressing Scheme (Part 1).....	61
Figure 3.4 Addressing Scheme (Part 2).....	62
Figure 3.5 Sector and Cluster Formation in the Network.....	62
Figure 3.6 Node Registration Process.....	63
Figure 3.7 Packet Format (Omitting TCP/IP Headers) .....	65
Figure 3.8 Next hop calculation .....	67
Figure 3.9 Packet Processing and Forwarding .....	69
Figure 3.10 Default Packet Forwarding .....	70
Figure 3.11 Instance Showing Packet Route Trace.....	73
Figure 3.12 Message Roundtrip Time (+/- 10%).....	74
Figure 4.1 Authentication Scenario Selection .....	83

Figure 4.2 Full Authentication Process .....	84
Figure 4.3 Quick Authentication Process.....	87
Figure 4.4 Registration and New Node Authentication .....	91
Figure 4.5 Scenario 1 Timeline.....	94
Figure 4.6 Scenario 2 Timeline.....	95
Figure 4.7 Memory Consumption.....	96
Figure 4.8 CPU Usage.....	97
Figure 5.1 Hybrid Encryption .....	106
Figure 5.2 Time Taken for the Trip (500-Bytes Data) .....	113
Figure 5.3 Time Taken for the Trip (64000-Bytes Data) .....	114
Figure 5.4 Memory Consumption.....	115
Figure 5.5 CPU Usage.....	115
Figure 5.6 Time Taken for the Trip (500-Bytes Data) .....	117
Figure 5.7 Time Taken for the Trip (64000-Bytes Data) .....	118
Figure 5.8 Memory Consumption.....	119
Figure 5.9 CPU Usage.....	120
Figure 6.1 Multi-Path Data Transmission .....	130
Figure 6.2 MPARK Distribution at a Glance .....	132

## List of Tables

Table 3.1 Components for Next-Hop Calculation.....	67
Table 4.1 List of Components .....	81
Table 4.2 Comparison Between Security Protocols.....	98
Table 5.1 Notations Used.....	104
Table 5.2 Hybrid Encryption Scenarios .....	116
Table 6.1 Types of Key Distribution Approaches.....	124
Table 6.2 Notations Used.....	126

## List of Algorithms

Algorithm 4.1 Scenario-1 Challenge .....	85
Algorithm 4.2 Scenario-2 Challenge .....	88
Algorithm 5.1 Key Management.....	104
Algorithm 5.2 Session Key Management.....	107