Energy-efficient Routing and Secure Communication in Wireless Sensor Networks

A Thesis Submitted for the Degree of

Doctor of Philosophy

By

Mian Ahmad Jan

in

Faculty of Engineering and Information Technology

UNIVERSITY OF TECHNOLOGY, SYDNEY

AUSTRALIA

February 2016

UNIVERSITY OF TECHNOLOGY, SYDNEY

Faculty of Engineering and Information Technology

The undersigned hereby certify that they have read this thesis entitled "**Energy-efficient Routing and Secure Communication in Wireless Sensor Networks**" by Mian Ahmad Jan and that in their opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Doctor of Philosophy.

Principal Supervisor	Co-Supervisor
Dr. Priyadarsi Nanda	Prof. Xiangjian He

CERTIFICATE OF AUTHORSHIP

Date: **3rd February 2016**

Author: Mian Ahmad Jan
Title: Energy-efficient Routing and Secure Communication in Wireless Sensor Networks
Degree: PhD

I certify that the work in this thesis has not previously been submitted for a degree nor has it been submitted as part of requirements for a degree except as fully acknowledged within the text.

I also certify that the thesis has been written by me. Any help that I have received in my research work and the preparation of the thesis itself has been acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis.

_____

Signature of Author

Acknowledgements

Firstly, 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. Besides my supervisor, I would like to thank my co-supervisors, Prof. Xiangjian He and Dr. Ren Ping Liu for their valued suggestions and constant support, and for 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 gratefully acknowledge the useful discussions with Dr. Zhiyuan Tan, Mohammed Ambu Saidi, Thawatchai Chomsiri and Dr. Mahardhika Pratama. I wish to thank my fellow research students and the staff of the school, especially those people listed below for providing assistance for the completion of this research work.

- Hla Myint, M. Usman Khan, Adrian Johannes, Ashish Nanda, Amber Umair, Deepak Puthal, Upasana Nagar, Doan B. Hoang, Soud Nassir, Mohammad Alshehri, Khaled Aldebei, Minqi Li and Chi Yang.

I appreciate the financial support of University of Technology Sydney International Research Scholarship (IRS) and a Top-up scholarship provided by the Commonwealth Scientific and Industrial Research Organisation (CSIRO).

Last but not the least, I would like to express my love and gratitude to my family members, especially my parents, my sister and my brother-in-law. Foremost, I want to thank my late brother for his constant motivation during my studies. In my heart, you will always stay loved and remembered, every day.

Dedicated to my family

Table of Contents

Acknowledgements **iv**

List of Tables **x**

List of Figures **xi**

Abbreviation **xv**

Abstract **xviii**

List of Publications **xx**

1 Introduction **1**

1.1 Background 1

1.1.1 Routing Protocols in WSN 4

1.1.2 Emergence of Internet of Things 7

1.1.3 Security Considerations 8

1.2 Motivation 10

1.3 Research Objectives and Contribution 12

1.4 Research Focus 15

1.5 Structure of the Thesis 16

2 Literature Review **18**

2.1 Overview of Wireless Sensor Network 19

2.2 Hardware Components of a Node 22

2.3 WSN Routing Protocols . . . 26
2.4 Cluster-based Hierarchical Routing Protocols . . . 28
2.4.1 Types of Cluster-based Hierarchical Routing Protocols . . . 28
2.4.2 Congestion Detection in Cluster-based Hierarchical Protocols . . . 35
2.5 Sybil Attack Detection . . . 38
2.5.1 Detection of Sybil Attack in WSN . . . 38
2.5.2 Detection of Sybil attack in a Wildfire Monitoring Application . . . 41
2.6 Internet of Things . . . 44
2.6.1 Constrained Application Protocol . . . 48
2.6.2 Security Challenges in IoT . . . 51
2.7 Summary . . . 55

3 Energy-efficient Communication in Cluster-based Hierarchical Networks 57
3.1 Energy-efficient Cluster-based Routing Algorithm . . . 57
3.1.1 Network Architectural Model . . . 58
3.1.2 Network Operational Model . . . 60
3.1.3 Experimental Results and Analysis . . . 62
3.1.3.1 Lifetime of the Network . . . 63
3.1.3.2 Data Aggregation . . . 64
3.1.3.3 Quality of Data . . . 65
3.2 A Centralized Energy Evaluation Model . . . 66
3.2.1 Network Operational Model . . . 67
3.2.2 Energy Evaluation Model . . . 73
3.3 Summary . . . 77

4 Energy-efficient Cluster-based Congestion Control Algorithm 79
4.1 The PASCCC Protocol . . . 80
4.2 Framework of PASCCC . . . 81
4.3 PASCCC Operational Mechanism . . . 82
4.3.1 PASCCC: An Application-specific Protocol . . . 82
4.3.2 PASCCC: Congestion Detection and Mitigation . . . 84
4.3.3 PASCCC: Queuing Model . . . 86
4.4 Experimental Results and Analysis . . . 88

4.4.1 Lifetime of the Network . . . 89
4.4.2 Residual Energy . . . 89
4.4.3 Data Transmission . . . 90
4.4.4 Causes of Congestion . . . 92
4.5 Summary . . . 93

5 Sybil Attack Detection Scheme for a Cluster-based Hierarchical Network 95
5.1 Network Assumptions . . . 96
5.2 Sybil Attack Detection . . . 98
5.3 Centralized Cluster-based Hierarchical Network . . . 101
5.4 Experimental Results and Analysis . . . 106
5.4.1 Detection of Sybil Nodes . . . 106
5.4.2 Total Number of Candidates and Cluster Heads . . . 107
5.4.3 Network Lifetime . . . 108
5.4.4 Energy Consumption with Sybil Nodes . . . 109
5.4.5 Packet Loss Rate . . . 110
5.4.6 Packet Acceptance Ratio . . . 111
5.5 Summary . . . 112

6 Detection of Sybil Attack in a Wildfire Monitoring Application 113
6.1 Design Considerations . . . 114
6.1.1 Characteristics of Burning Wildfire Scenario . . . 114
6.1.2 Network Parameters and Design Consideration . . . 115
6.2 Sybil Attack Detection in a Forest Wildfire . . . 117
6.2.1 Network Architectural Model . . . 117
6.2.2 Network Deployment Model . . . 118
6.2.3 Detection of Sybil Attack . . . 120
6.2.3.1 RSSI-based Sybil Attack Detection . . . 121
6.2.3.2 Residual Energy-based Sybil Attack Detection . . . 122
6.2.4 Cluster-based Hierarchical Network . . . 124
6.2.4.1 Set-up Phase . . . 124
6.2.4.2 Steady-state Phase . . . 127
6.3 Experimental Results and Analysis . . . 130

6.3.1 Detection of Sybil Attack 131
6.3.2 Accuracy of Wildfire Monitoring Application 132
6.3.3 Lifetime of the Network 134
6.3.4 Average Size of the Clusters 135
6.4 Summary 137

7 A Lightweight Authentication Scheme for the Internet of Things Objects 139
7.1 Problem Statement 140
7.2 Payload-based Mutual Authentication 143
7.3 Detection of Replay Attacks and their Mitigation 150
7.4 Experimental Results and Analysis 154
7.4.1 Authentication 154
7.4.2 Handshake Duration 155
7.4.3 Average Response Time 157
7.4.4 Average Memory Consumption 158
7.4.5 Detection of Replay Attacks 159
7.5 Summary 159

8 Conclusion and Future Work 161
8.1 Future Work 165

Bibliography 170

List of Tables

2.1 Usage of CoAP Messages 49

2.2 CoAP vs. HTTP 51

7.1 Pre-Shared Secrets Table 144

7.2 Format of the Authentication Options 149

7.3 Number of Detected Replay Attacks 159

List of Figures

1.1 Research Focus 15

2.1 Wireless Sensor Network 20

2.2 Applications of WSN 23

2.3 Hardware Architecture of a Node 24

2.4 WSN Protocol Stack 25

2.5 Drawbacks of Flooding 26

2.6 Randomly Distributed Cluster-based Hierarchical Routing 32

2.7 Different Levels of Hierarchy 33

2.8 Hop-by-Hop Communication vs. End-to-End Communication 36

2.9 Sybil Attack in WSN 39

2.10 Integration of Physical Objects with Internet-IoT 46

2.11 Protocol Stack at the Nodes 47

2.12 Exchange of CoAP Messages 50

2.13 A Vulnerable IoT Architecture 53

3.1 Radio Communication Model 59

3.2 Sensing Similar Events 62
3.3 Lifetime of the Network 63
3.4 Data Aggregation 64
3.5 Quality of Data 65
3.6 Frame Format of a Status Message 68
3.7 Candidate Nodes and Cluster Heads 69
3.8 Cluster Head Selection 70
3.9 Data Transmission to a Base Station 71
3.10 Flowchart of Set-up and Steady-state Phases 72
3.11 Energy Consumption in different Scenarios 76
4.1 Framework of the Proposed Protocol 82
4.2 Congestion Detection and Mitigation 85
4.3 Queuing Model of a Sensor Node 87
4.4 Flowchart for the Queuing Operation 87
4.5 Lifetime of the Network 89
4.6 Residual Energy Consumption (in Joules) 90
4.7 Data Transmission to Cluster Heads and Base Station 91
4.8 Congestion Detection and Mitigation 93
5.1 A Single Sybil Node Forming Multiple Clusters 97
5.2 High Energy Nodes Collaboration for Sybil Attack Detection 99
5.3 Cluster formation and Data Transmission 103
5.4 Detection of Sybil Nodes and their Forged Identities 107

5.5 Candidates vs. Cluster Heads 108
5.6 Lifetime of the Network 109
5.7 Energy Consumption in Presence of Sybil Nodes 110
5.8 Packet Loss Rate 110
5.9 Packet Acceptance Ratio 111
6.1 Network Architectural Model 118
6.2 Base Station Mobility 119
6.3 RSSI-based Sybil Attack Detection in a Forest 122
6.4 Residual Energy-based Sybil Attack Detection 123
6.5 Types of Queries 126
6.6 Data Collection within a Forest 128
6.7 Detection of Sybil Attack 131
6.8 Accuracy of the Wildfire Monitoring Application 133
6.9 Lifetime of the Network 134
6.10 Coverage of a Geographical Region 136
7.1 A Vulnerable Internet of Things Connected Environment 141
7.2 Four-way Authentication Handshake 145
7.3 The Replay Attack in an IoT Environment 150
7.4 Flowchart for the Replay Attack Detection 152
7.5 The Authentication Process 155
7.6 The Handshake Duration 156
7.7 The Average Response Time 157

7.8 The Average Memory Consumption 158

Abbreviations

Abbreviations	Descriptions
6LoWPAN	IPv6 over Low-power Wireless Personal Area Network
AAP	Anonymous Authentication Protocol
ADC	Analog-to-Digital Converter
AES	Advanced Encryption Standard
AIMD	Additive Increase and Multiplicative Decrease
ARQ	Automatic Repeat reQuest
BER	Bit Error Rate
CoAP	Constrained Application Protocol
CODA	COngestion Detection and Avoidance
DoS	Denial-of-Service
DTLS	Datagram Transport Layer Security
EFMP	Energy-efficient Fire Monitoring Protocol
ESRT	Event-to-Sink Reliable Transport
FCFS	First-Come-First-Served
FND	First Node Dies
HTTP	Hypertext Transfer Protocol
IANA	Internet Assigned Numbers Authority
ICE	Indisputable Code Execution
IETF	Internet Engineering Task Force

Abbreviations	Descriptions
IoE	Internet of Everything
IoT	Internet of Things
IP	Internet Protocol
LEACH	Low-Energy Adaptive Clustering Hierarchy
LEACH-C	Low-Energy Adaptive Clustering Hierarchy-Centralized
LLNs	Lower-power and Lossy Networks
LoS	Line-of-Sight
LND	Last Node Dies
MAC	Medium Access Control
MEMS	Micro-Electro-Mechanical Systems
MTU	Maximum Transmission Unit
NLoS	Non-Line-of-Sight
PASCCC	priority-based application-specific congestion control clustering
RAM	Random-access memory
REST	REpresentational State Transfer
RFC	Request For Comments
RFID	Radio Frequency IDentification
ROM	Read-only memory
RRM	Registration Request Message
RSSI	Received Signal Strength Indicator
RTT	Round Trip Time

Abbreviations	Descriptions
SCUBA	Secure Code Update By Attestation
TCP	Transport Control Protocol
TDMA	Time Division Multiple Access
TLS	Transport Layer Security
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
WSN	Wireless Sensor Network
DEEC	Distributed Energy-efficient Clustering
HEED	Hybrid Energy-efficient Distributed

Abstract

Wireless Sensor Networks (WSNs) consist of miniature sensor nodes deployed to gather vital information about an area of interest. The ability of these networks to monitor remote and hostile locations has attracted a significant amount of research over the past decade. As a result of this research, WSNs have found their presence in a variety of applications such as industrial automation, habitat monitoring, healthcare, military surveillance and transportation. These networks have the ability to operate in human-inaccessible terrains and collect data on an unprecedented scale. However, they experience various technical challenges at the time of deployment as well as operation. Most of these challenges emerge from the resource limitations such as battery power, storage, computation, and transmission range, imposed on the sensor nodes.

Energy conservation is one of the key issues requiring proper consideration. The need for energy-efficient routing protocols to prolong the lifetime of these networks is very much required. Moreover, the operation of sensor nodes in an intimidating environment and the presence of error-prone communication links expose these networks to various security breaches. As a result, any designed routing protocol need to be robust and secure against one or more malicious attacks.

This thesis aims to provide an effective solution for minimizing the energy consumption of the nodes. The energy utilization is reduced by using efficient techniques for cluster head selection. To achieve this objective, two different cluster-based hierarchical routing protocols are proposed. The selection of an optimal percentage of cluster heads reduces the energy consumption, enhances the quality of delivered data and prolongs the lifetime of a network. Apart from an optimal cluster head selection, energy consumption can also be reduced using efficient congestion detection and mitigation schemes. We propose an application-specific priority-based congestion control protocol for this purpose. The proposed protocol integrates mobility and heterogeneity of the nodes to detect congestion. Our

proposed protocol uses a novel queue scheduling mechanism to achieve coverage fidelity, which ensures that the extra resources consumed by distant nodes are utilized effectively.

Apart from energy conservation issue, this thesis also aims to provide a robust solution for Sybil attack detection in WSN. In Sybil attack, one or more malicious nodes forge multiple identities at a given time to exhaust network resources. These nodes are detected prior to cluster formation to prevent their forged identities from participating in cluster head selection. Only legitimate nodes are elected as cluster heads to enhance utilization of the resources. The proposed scheme requires collaboration of any two high energy nodes to analyse received signal strengths of neighbouring nodes. Moreover, the proposed scheme is applied to a forest wildfire monitoring application. It is crucial to detect Sybil attack in a wildfire monitoring application because these forged identities have the ability to transmit high false-negative alerts to an end user. The objective of these alerts is to divert the attention of an end user from those geographical regions which are highly vulnerable to a wildfire.

Finally, we provide a lightweight and robust mutual authentication scheme for the real-world objects of an Internet of Thing. The presence of miniature sensor nodes at the core of each object literally means that lightweight, energy-efficient and highly secured schemes need to be designed for such objects. It is a payload-based encryption approach which uses a simple four way handshaking to verify the identities of the participating objects. Our scheme is computationally efficient, incurs less connection overhead and safeguard against various types of replay attacks.

List of Publications

Journal Papers

1. Mian Ahmad Jan, Priyadarsi Nanda, Xiangjian He, Ren Ping Liu, PASCCC: Priority-based application-specific congestion control clustering protocol, **Computer Networks**, vol. 74, pp.92-102, 2014. (Published-Tier **A**)
2. Mian Ahmad Jan, Priyadarsi Nanda, Xiangjian He, Ren Ping Liu, A Lightweight Mutual Authentication Scheme for IoT Objects, Journal of Network and Computer Applications (**JNCA**), (Under Review-Tier **A**)
3. Mian Ahmad Jan, Priyadarsi Nanda, Xiangjian He, Ren Ping Liu, A Sybil Attack Detection Scheme for a Forest Wildfire Monitoring Application, Future Generation Computer Systems (**FGCS**), (Under Review-Tier **A**)

Conference Papers

1. Mian Ahmad Jan, Priyadarsi Nanda, Xiangjian He, Energy Evaluation Model for an Improved Centralized Clustering Hierarchical Algorithm in WSN., Wireless and Wired international Conference **WWIC**, pp.154-167, 2013, Springer. (Published-Tier **B**)
2. Mian Ahmad Jan, Priyadarsi Nanda, Xiangjian He, Ren Ping Liu, Enhancing lifetime and quality of data in cluster-based hierarchical routing protocol for wireless sensor network, 10th International Conference on High Performance Computing and Communications & International Conference on Embedded and Ubiquitous Computing (**HPCC_EUC**), pp.1400-1407, 2013, IEEE. (Published-Tier **B**)
3. Mian Ahmad Jan, Priyadarsi Nanda, Xiangjian He, Ren Ping Liu, A robust authentication scheme for observing resources in the internet of things environment, 13th

International Conference on Trust, Security and Privacy in Computing and Communications (**TrustCom**), pp.205-211, 2014, IEEE. (Published-Tier **A**)

4. Mian Ahmad Jan, Priyadarsi Nanda, Xiangjian He, Ren Ping Liu, A Sybil Attack Detection Scheme for a Centralized Clustering-based Hierarchical Network, 14th International Conference on Trust, Security and Privacy in Computing and Communications (**TrustCom**), 2015, IEEE. (Accepted-Tier **A**)