



***SECURE GEOGRAPHIC FORWARDING PROTOCOLS FOR WIRELESS
SENSOR NETWORKS***

ALI IDAROUS ADNAN

FSKTM 2019 89



UPM
UNIVERSITI PUTRA MALAYSIA
BERILMU BERBAKTI

**SECURE GEOGRAPHIC FORWARDING PROTOCOLS FOR WIRELESS
SENSOR NETWORKS**

By

ALI IDAROUS ADNAN

**Thesis Submitted to the School of Graduate Studies, Universiti Putra
Malaysia, in Fulfilment of the Requirements for the Degree of Doctor of
Philosophy**

November 2017

All material contained within the thesis, including without limitation text, logos, icons, photographs and all other artwork, is copyright material of Universiti Putra Malaysia unless otherwise stated. Use may be made of any material contained within the thesis for non-commercial purposes from the copyright holder. Commercial uses of material may only be made with the express, prior, written permission of Universiti Putra Malaysia.

Copyright ©Universiti Putra Malaysia

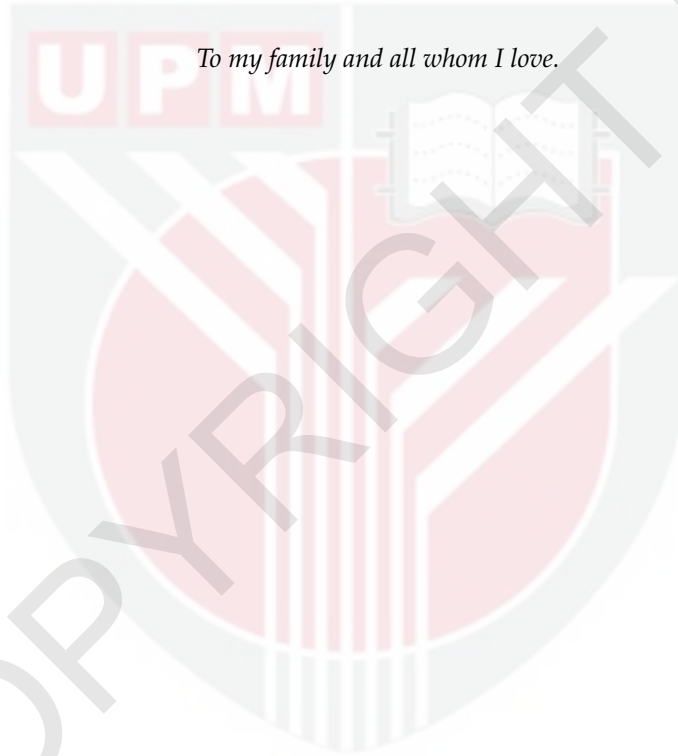


DEDICATIONS

*I would like to dedicate this thesis to my beloved motherland
"Zanzibar-Tanzania".*

&

To my family and all whom I love.



Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfillment of the requirement for the degree of Doctor of Philosophy

SECURE GEOGRAPHIC FORWARDING PROTOCOLS FOR WIRELESS SENSOR NETWORKS

By

ALI IDAROUS ADNAN

November 2017

Chairman: Zurina Mohd Hanapi, PhD
Faculty: Computer Science and Information Technology

The Advancement of the micro-electro-mechanical system (MEMS), wireless communication, and low-power electronic devices has facilitated the development of multipurpose and low-cost sensor devices. These devices are deployed in a target region, in hundreds or thousands with an objective of gathering information and transmit that information through multi-hops, to remote users/computer using a special pattern of communication known as routing protocol.

Indeed, the overall performance of WSNs' routing protocol is significantly influenced by the deployment of security techniques in the routing procedures that intend to prevent routing attacks. Although, WSNs have been used in many sensitive applications, the development of reliable security techniques to safeguard the transmitted information are still a great challenge and unable to adapt to the resource constraints of the sensor nodes. This is because the existing security tools such as cryptographic and key management schemes are too expensive in term of computational resources to be directly integrated into sensor nodes. Furthermore, the multi-hop communication and the absence of centralized administration increase WSN vulnerabilities against routing failures and complexities. For this reasons, inefficient secure routing protocols would cause extreme performance degradation when subjected to attackers in the communication processes.

In order to enhance network performance and improve the ability of secure routing protocol on dealing with the existence of attackers, this research work proposes a Bound collection Geographic Forwarding (BCGF) protocol designed for WSN. The BCGF helps in reducing the participation of an attacker in the communication process as well as prevent retransmission of control packets. Thereafter,

extensive simulation experiments are carried out to evaluate the performance of the proposed BCGF compared to the existing secure implicit geographic routing protocols. The results demonstrate that the BCGF improve network performance when the protocol is subjected to no attacker and increases packet delivery to the destination when a single attacker is of concerned.

Furthermore, the Secure Region-based Geographic Routing (SRBGR) protocol is proposed to increase the number of legitimate responders in the communication process when the number of Sybil virtual nodes increase in the forwarding allocated area, in which the number of attacker selection is high and packet drop is very common. SBRGR proposes an extension of forwarding area beyond allocated sextant for security purposes. Extensive simulation experiments show that the proposed protocol achieves a higher performance in minimizing attacker selection contrary to the other secure protocols.

Moreover, to build a trust communication between neighbouring nodes, during the routing processes and prevent malicious nodes in dropping packets, a Light-weight Trust-based Scheme (LTBS) is proposed. LTBS allows each node to monitor and determine the trustworthiness of its neighbours based on packet forwarding acknowledge. LTBS encourages cooperation between nodes while thwarts misbehaving nodes in capturing the communication and create inconsistency in packet forwarding process. Substantial simulations have been conducted to evaluate the proposed scheme. The results show that the scheme achieves better performance in reducing the attackers in their different magnitudes and severities.

Fortunately, results of the simulation show that the proposed secure routing protocols provide enhancements in network performance and security. It reduces the communication overheads, end-to-end delay while improving the packet delivery to the destination when no attackers are presented in the communication link. Also, it detects the routing attacks such as black hole and Sybil nodes by minimizing their selection in routing processes in contrary to the existing secure routing protocols.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia
sebagai memenuhi keperluan untuk ijazah Doktor Falsafah

PROTOKOL PENGHANTARAN GEOGRAFIK YANG SELAMAT UNTUK RANGKAIAN WAYARLES PENDERIA

Oleh

ALI IDAROUS ADNAN

November 2017

Pengerusi: Zurina Mohd Hanapi, PhD
Fakulti: Sains Komputer dan Teknologi Maklumat

Kemajuan sistem mikro-elektro-mekanikal (MEMS), komunikasi tanpa wayar, dan alat elektronik berkuasa rendah telah memudahcara pembangunan peranti pengesan serba guna kos rendah. Beratus-ratus atau beribu-ribu peranti ini digunakan di kawasan sasaran untuk mencapai objektif iaitu mengumpul dan menghantar maklumat melalui *multi-hop* kepada pengguna/komputer jarak jauh, menggunakan pola komunikasi khas yang dikenal sebagai penghalauan protokol.

Sememangnya prestasi keseluruhan protokol penghalauan WSN sangat dipengaruhi oleh penggunaan langkah keselamatan dalam prosedur penghalauan yang bertujuan untuk mencegah serangan penghalauan. Walaupun terdapat banyak penggunaan WSN dalam pelbagai aplikasi yang sensitif, pembangunan teknik keselamatan yang boleh diyakini untuk melindungi maklumat yang dihantar masih merupakan cabaran yang besar dan tidak dapat disesuaikan dengan kekangan sumber nod pengesan. Ini kerana alat keselamatan yang sedia ada seperti skema kriptografi dan pengurusan utama terlalu mahal dari segi sumber pengiraan untuk disepadukan terus kepada nod pengesan. Tambahan pula, komunikasi 'multi-hop' dan ketiadaan pentadbiran pusat di persekitaran terbuka meningkatkan kelemahan WSN terhadap kegagalan dan kerumitan penghalauan kerana nod perantaraan perlu melakukan beberapa fungsi sebagai penghalau dan beberapa fungsi lagi sebagai unit pemprosesan. Oleh itu, protokol penghalauan selamat yang tidak efisien akan menyebabkan kemerosotan yang tinggi prestasi apabila menghadapi serangan dalam proses komunikasi.

Untuk meningkatkan prestasi rangkaian dan meningkatkan keupayaan protokol penghalauan selamat dalam menangani kewujudan penyerang, kajian ini mencadangkan protokol *Bound collection Geographic Forwarding* (BCGF) yang direka

untuk WSN. BCGF membantu mengurangkan penyertaan seorang penyerang dalam proses komunikasi serta mencegah penghantaran semula paket kawalan apabila tiada penyerang dalam hubungan komunikasi. Selepas itu, eksperimen simulasi yang lebih teliti dijalankan untuk menilai prestasi BCGF yang dicadangkan untuk dibandingkan dengan protokol penghalaan geografi terselindung yang sedia ada. Hasilnya menunjukkan bahawa BCGF meningkatkan prestasi rangkaian apabila protokol tersebut tiada penyerang, dan kecekapan bagi penghantaran paket ke destinasi pula meningkat dalam situasi penyerang tunggal.

Tambahan pula, protokol *Secure Region-based Geographic Routing* (SBRGR) dicadangkan untuk meningkatkan bilangan penggerak balas sah dalam proses komunikasi apabila bilangan serangan Sybil meningkat di kawasan penghantaran yang diperuntukkan, di mana bilangan pilihan penyerang adalah tinggi yang membawa kepada kejatuhan paket. SBRGR mencadangkan perluasan kawasan penghantaran yang lebih luas daripada kawasan yang diperuntukkan bagi tujuan keselamatan. Eksperimen simulasi ekstensif menunjukkan bahawa protokol yang dicadangkan mencapai prestasi yang lebih tinggi dalam mengurangkan pilihan penyerang berbanding protokol keselamatan yang lain.

Selain itu, LTBS dicadangkan untuk membina komunikasi kepercayaan antara nod berjiran semasa proses penghalaan dan untuk menghalang nod jahat menjatuhkan paket. LTBS, membolehkan setiap nod untuk memantau dan menentukan kebolehpercayaan jiran-jirannya berdasarkan pengenalan paket. LTBS menggalakkan kerjasama antara nod di samping menghentikan nod yang melakukan salah laku dalam menangkap komunikasi dan mencipta kecelaruan dalam proses pemajuan paket. Simulasi mendalam telah dijalankan untuk menilai skema yang dicadangkan. Hasil menunjukkan bahawa skema tersebut mencapai prestasi yang lebih baik dalam mengurangkan penyerang dalam skala dan keseriusan yang berbeza.

Hasil simulasi menunjukkan bahawa protokol penghalaan selamat yang dicadangkan membawa peningkatan kepada prestasi dan keselamatan rangkaian. Ia mengurangkan overhead komunikasi dan kelewatan sepenuhnya sambil meningkatkan penghantaran paket ke destinasi apabila tiada penyerang muncul dalam pautan komunikasi. Ia juga mengesan serangan penghalaan seperti *nod Black Hole* dan *Sybil* dengan meminimumkan pemilihan mereka dalam proses penghalaan yang bertentangan dengan protokol penghalaan selamat yang sedia ada.

ACKNOWLEDGEMENTS

All praises belong to Allah, the Most Beneficent, the Most Merciful, Lord of all the World. I am immensely grateful to Allah for guiding me to praise Him. I praise Allah for giving me the strength and intellectual health to overcome fears over success. I would like to take this opportunity to address my enormous gratitude to all individuals who have in all ways contributed to the completion of this thesis.

First and foremost, I would like to express my gratitude to my supervisor Associate Prof. Dr. Zurina Mohd Hanapi for her patience, motivation, constructive comments and constant support during my entire Ph.D. study. I have no appropriate words to equate and express my appreciation to her. Her guidance meant a lot from the start to the final stage of completion of this thesis. I would like to document my deepest thanks to the rest of my thesis committee member: Prof. Dr. Mohamed Othman and Associate Prof. Dr. Zuriati Ahmad Zukarnain, for their thoughtful motivation questions, supportive comments, and encouragement which helped me to continue to work towards success. My special heartfelt appreciation goes to Prof. Mohamed Othman who always guide me to strive for excellence and quality work.

I am also very grateful to The State University of Zanzibar - the place where I belong, and its leaderships for their full supports during the whole period of my studies, their constant support is very much appreciated and was a pillar in finishing this important work of mine. I express my deepest thanks to my mother, my nieces, my brothers, Abubakar, Hussein and Ahmed Idarous who were my guide and support to my young family when I was not around them.

Words fail me to express my appreciation to my lovely wife Mwanaimani Moh'd whose dedication, patience, and love were the foundation of my Ph.D. journey that has now taken me to the finish end. I owe her a lot of love and respect. Special thank goes to my three beautiful sons Idarous, Muhammad, and Taher, you are my joy and my guiding lights. Thanks for giving me your valuable time through all this long process. This time, I promise I will be always around you.

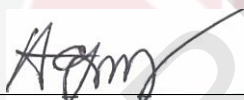
Last but not least, it gives me immense pleasure to express my deepest gratitude to my friends, Salim Mkubwa, Sheikh Mnyero Janja and especially my lab mates Maman, Sadiq, Alaa, Nadeem and Hudhaif for their motivation, encouragement and unlimited moral and material supports throughout my Ph.D. studies. Finally, I would like to thank everybody who was important to the successful realization of this thesis, as well as I express my apology that I could not mention you all personally.

Declaration by graduate student

I hereby confirm that:

- this thesis is my original work;
- quotations, illustrations and citations have been duly referenced;
- this thesis has not been submitted previously or concurrently for any other degree at any other institutions;
- intellectual property from the thesis and copyright of thesis are fully-owned by Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- written permission must be obtained from supervisor and the office of Deputy Vice-Chancellor (Research and Innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated in the Universiti Putra Malaysia (Research) Rules 2012;
- there is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the Universiti Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software.

Signature: _____



Date: _____

Name and Matric No.: _____

Ali Idarous Adnan (GS 33215)

Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of this thesis was under our supervision
- supervision responsibilities as stated in the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) are adhered to.

Signature: _____
Name of
Chairman of
Supervisory
Committee: Associate Prof. Dr. Zurina Mohd Hanapi

Signature: _____
Name of
Member of
Supervisory
Committee: Prof. Dr. Mohamed Othman

Signature: _____
Name of
Member of
Supervisory
Committee: Associate Prof. Dr. Zuriati Ahmad Zukarnain

TABLE OF CONTENTS

	Page
ABSTRACT	i
ABSTRAK	iii
ACKNOWLEDGEMENTS	v
APPROVAL	vi
DECLARATION	viii
LIST OF TABLES	xiii
LIST OF FIGURES	xiv
LIST OF ABBREVIATIONS	xvi
CHAPTER	
1 INTRODUCTION	1
1.1 Background	1
1.1.1 WSNs Overview	1
1.1.2 Security and Routing Protocol Design Challenges	2
1.2 Problem Statement	4
1.3 Motivation	5
1.4 Research Objectives	5
1.5 Research Scope	6
1.6 Thesis Organization	7
2 LITERATURE REVIEW	8
2.1 Introduction	8
2.2 Overview of Wireless Sensor Networks	8
2.3 Routing Protocol in Wireless Sensor Networks	9
2.3.1 General Discussion on Routing Protocol	10
2.3.2 Factors Effecting Efficient and Secure Routing Design	12
2.3.3 Geographic Routing Protocols	14
2.4 Security and Attacks in Wireless Sensor Networks	19
2.4.1 Network Layer Attacks for Wireless Sensor Networks	22
2.4.2 Routing Attacks and Existing Countermeasures	25
2.4.3 Summary of Routing attacks	27
2.5 Secure Routing Protocols in Wireless Sensor Networks	27
2.5.1 Resilient and Secure Routing Protocols	28
2.5.2 Secure Communicating Nodes Using Trust Scheme	33
2.6 Summary	40
3 RESEARCH METHODOLOGY	43
3.1 Introduction	43
3.2 Notations and Definitions	43
3.2.1 Notations	44
3.2.2 Definitions and Conventions	44
3.3 The Research Framework	44
3.3.1 Problem Formulation	45
3.3.2 Previous Algorithms Implementation	46

3.3.3	The Proposed Algorithms	46
3.3.4	Conducting Simulation Experiments	50
3.3.5	Performance Metrics Evaluation	51
3.4	Experiments Environment	51
3.4.1	Software and Hardware Tools	51
3.4.2	Network Topologies	51
3.4.3	Experiments Setup	54
3.5	Performance Metrics	56
3.6	Performance Validation	57
3.7	Summary	58
4	A BOUND COLLECTION WINDOW GEOGRAPHIC FORWARD- ING PROTOCOL FOR WSNs	61
4.1	Introduction	61
4.2	Secure Routing Protocol (BCGF)	61
4.2.1	Dynamic collection Window	62
4.2.2	The Proposed BCGF Protocol	62
4.2.3	Selection Cost	64
4.2.4	BCGF Operation Algorithm	65
4.3	Performance Evaluation	66
4.3.1	Experiment Result Free Attacker Environment	67
4.3.2	Experiment Result with attacker Environment (Black hole)	69
4.3.3	Experiment Result on Sybil attack	76
4.4	Summary	81
5	A SECURE REGION-BASED GEOGRAPHIC ROUTING PROTO- COL (SRBGR) FOR WSNs	83
5.1	Introduction	83
5.2	Restricted, Allocated Sextant for DWSIGF	84
5.3	System, Network, and Attack Model	84
5.4	Proposed: Extended Secure Region-Based Routing Protocol-SRBGR	86
5.4.1	Modified CTS Response Contention Time	87
5.4.2	Verification Cost	88
5.4.3	SRBGR Operation Algorithm	89
5.5	Performance Evaluation	90
5.5.1	The Experiments Setup	90
5.5.2	Attack-Free Communication	90
5.5.3	Attack-based Communication -Black hole	93
5.5.4	Attack-Based Communication-Sybil Attacks	100
5.6	Summary	102
6	A LIGHT-WEIGHT TRUST-BASED ROUTING SCHEME (LTBS) FOR WSNs	105
6.1	Introduction	105
6.2	The Proposed LTBS Scheme	106
6.2.1	Security Limitations in CLT protocol	106
6.2.2	Trust Evaluation for LTBS	107
6.2.3	Trust representation	112

6.3	Theoretical Analysis	113
6.4	Performance Evaluation	115
6.4.1	The Experimental Setup	116
6.4.2	Forwarding Selection Option	116
6.4.3	No attack in the communication link	116
6.4.4	Attacks in the Communication channel	119
6.4.5	Experiment Result on Sybil attack	127
6.5	Summary	131
7	CONCLUSION AND FUTURE WORKS	133
7.1	Conclusion	133
7.2	Future Research	134
	REFERENCES	136
	BIODATA OF STUDENT	149
	LIST OF PUBLICATIONS	150

LIST OF TABLES

Table	Page
2.1 GP Protocols, their Routing techniques and Pro and Cons	20
2.2 Security Overview of Secure Routing Protocol in WSNs	34
2.3 Overview of Trust based Routing Protocols for WSNs	41
3.1 Notations in Equations and Formulas	44
3.2 System parameters for simulation Hanapi and Ismail (2014).	55
6.1 Memory Usage Comparison	113
6.2 Storage Capacity of LTBS (Trust table)	113
6.3 Trust memory computation usage	114

LIST OF FIGURES

Figure	Page
2.1 Typical Wireless Sensor Network	9
3.1 Research Framework	45
3.2 Handshaking Mechanism of DWSIGF (Son et al., 2003)	47
3.3 Forwarding area for Sender S (He et al., 2007).	47
3.4 Extended Forwarding Area in SRBGR	50
3.5 Deployment of sensor nodes with sources S and destinations D	53
3.6 Deployment of sensor nodes with S, D and Attackers(A1&A2&A2&A4)	54
3.7 Increase Attackers in the Forwarding Area	55
3.8 Packet Delivery Ratio	58
3.9 End-to-End Delay	59
3.10 Impact of Sybil nodes on Packet Delivery Ratio	59
4.1 BCGF Forwaring Process	64
4.2 Flowchart of BCGF Algorithm	66
4.3 Packet Delivery Ratio	68
4.4 Communication Overhead	69
4.5 End-to-End Delay (ms)	70
4.6 Black Hole Attackers with CTS Rushing	71
4.7 Possibility of Attacker Selection	72
4.8 Black Hole Attackers with CTS Rushing	74
4.9 Possibility of Attacker Selection	75
4.10 The of Sybil nodes Create by A1 Under Increase Traffic Loads	78
4.11 The Impact of Sybil nodes Create by A2 Under Increases Traffic loads	79
4.12 Performance Under Increase Virtual Nodes created by A1	80
4.13 Performance Under Increase Virtual Nodes created by A2	81
4.14 Transmission Range (m) of Sybil node	81
5.1 Increase Attackers in the Forwarding Area	85
5.2 Packet Delivery Ratio (PDR)	92
5.3 Communication Overheads (packets)	93
5.4 End-to-End Delay (ms)	94
5.5 Packet Delivery Ratio: The impack of Blackhole Attackers	95
5.6 Possibility of Attacker Selection (PAS)	96
5.7 Packet Delivery Ratio: The Impact of Black hole Attackers	98
5.8 Possibility of Attacker Selection (PAS)	99
5.9 Impact on PDR of A1 under increasing Traffic loads	101
5.10 Impact on PDR of A2 under increasing Traffic loads	102
5.11 Sybil attack by A1 with increasing number of virtual nodes	103
5.12 Sybil attack by A2 with increasing number of virtual nodes	103
6.1 Network Topology of the Trust Estimation	107
6.2 Main Flowchart of the Proposed Trust (LTBS) Algorithm	108
6.3 Flowchart For Neighbour Monitoring	109
6.4 Trust Value Representations	113

6.5	Memory Consumption for Trust Computation	115
6.6	Packet Delivery Ratio (PDR)	117
6.7	Communication Overhead (pkts)	118
6.8	End-to-End Delay (ms)	119
6.9	The Impact of Black hole on Packet Delivery Ratio	121
6.10	The Impact Security Scheme on Possibility of Attacker Selection (PAS)	122
6.11	The Impact of Black hole on Packet Delivery Ratio	125
6.12	The Impact of Security Schemes on Possibility of Attacker Selection (PAS)	126
6.13	Performance under Sybil virtual nodes created by A1	129
6.14	Performance under Sybil virtual nodes created by A2	130
6.15	Sybil attack by A1 with increasing number of virtual nodes	131
6.16	Sybil attack by A2 with increasing number of virtual nodes	132



LIST OF ABBREVIATIONS

ARQ	Automatic Repeat-Request
ARAN	Authenticated Routing for Ad hoc Networks
ATM	Asynchronous Transmission Mode
ATSR	Ambient Trust Secure Routing
ASF	Avoidance Simultaneous Forwarding
ADC	Analogy-to-Digital Converter
AFR	Adaptive Face Routing
ACK	Aknowledgment
BCGF	Bound Collection Geographic Forward
BRG	Beacon-less Routing Geographic
BS	Base Station
BCW	Bound Collection Window
CBR	Constant Bit Rate
CPS	Cyber Physical System
CLT	Collaborative Lightweight Trust Management Scheme
CENTERA	CENTralized Trust based Efficient Routing
CASER	Cost-aware SEcure Routing Protocol
DCW	Dynamic Collection Window
DARPA	Defence Research Project Agency
DWSIGF	Dynamic Secure Implicit Geographic Forward
DHGR	Dynamics (adjustable) Hybrid Geographic Routing
DIFS	Distributed Coordination Function Interframe Spacing
DoS	Denial-of-Service
EARP	Energy-aware geographic routing protocol
FR	Face Routing
GPS	Global Positioning System
GPSR	Greedy Perimeter Stateless Routing
GEAR	Geographic and Energy Aware Routing
GeRaf	Geographic Random Forwarding
GAF	Geographic Adaptive Fidelity
GOAFR	Geometric Ad-hoc Forwarding Routing
GOR	Geographic Opportunistic Routing
GPSR	Greedy Perimeter Stateless Routing
GTMS	Group-based Trust Management Scheme
GPI	Geographic Priority Index
GMR	Multicast Geographic Routing
HGR	Hybrid Geographic Routing
HBGR	Hybrid Beaconless Geographic Routing
HSecGR	Highly Secure Geographic Routing
IGF	Implicit Geographic Forward
IoT	Internet of Things
ID	Identification
LTBS	Light-weight Trust-Based Scheme
LDTs	Light-weight Dependable Trust Scheme
LEAP	Localized Encryption Authentication Protocols
MAC DCF	Media Access Distributed Coordination Function
MACRO	An Integrated MAC/Routing protocol

MDT	Multi-Dataflow Topologies
MEMS	Micro-Electronic-Mechanical Systems
NMS	Neighbourhood Monitoring System
NAV	Network Allocation Vector
MAC	Message Authentication Codes
OFR	Other Face Routing
ORTS	Open Request-To-Send
PRR	Packet Reception Rate
PTP	Pre-loaded Token Protocol
PDR	Packet Delivery Ratio
PDA	Personal Digital Assistance
PDA	Personal Digital Assistant
PHACK	Per-Hop Acknowledgement
PAS	Possibility Of Attacker Selection
PFACK	Packet Forwarding Acknowledgments
QoS	Quality of Services
QPI	Queue Priority Index
RAM	Random Access Memory
RTS/CTS	Request-To-Send/Clear-To-Send
RSS	Radio Signal Strength
RFID	Radio-frequency identification
SRBGR	Secure Region-Based Geographic Routing
SeMuRa	secure multipath routing algorithm
SRD	Secure Routing on the Diameter
SPIN	Security Protocol for Sensor network
SIGF	Secure Implicit Geographic Forward
SIFS	Short Inter Frame Spacing
SPIN	Sensor Protocol for Information via Negotiation
SBGR	Simple self-protected Beaconless Geographic
SeRWA	Secure Routing protocol against Wormhole
SEC-LEACH	Secure Low Energy Adaptive Clustering Hierarchy
SEC-TEEN	Secure Threshold sensitive Energy Efficient sensor Network
SEEM	Secure Energy-Efficient Multipath
SEIF	Secure and Efficient Intrusion-Fault tolerant routing protocol
TLR	Terminode Local Routing
TRECON	Trust-based economic framework for efficient internet routing
TS	Ticket Server
TRR	Terminode Remote Routing
TESRP	Trust Energy aware Secure Routing Protocol
TRANS	Trust-Aware Routing
TARF	Trust-Aware Routing Framework
WSN	Wireless Sensor Networks

CHAPTER 1

INTRODUCTION

1.1 Background

Wireless Sensor Networks (WSNs) have gained substantial and critical attention over the past few years, due to the advancement of Micro-Electronic-Mechanical Systems (MEMS) technology, which has largely contributed to the development of the low-cost, low-power, self-organized, multifunction sensor nodes. These nodes are inexpensive and normally deployed randomly, inaccessible, in a target region to sense and gather physical information about that region before making a local decision to transmit the sensed information to the end users/computers. Their ease deployments as well as being inexpensive devices are among the benefits that influence their wide acceptability in many real-world applications. These applications range from military, health and ecological related areas to domestic appliances and to applications in emergency response services (Akyildiz et al., 2002a). Nowadays, the potential of WSN gradually increases as it has been recognized as an underlying technology that is propelling the Internet of Things (IoT) (Stankovic, 2014; Atzori et al., 2010; Wu et al., 2011) paradigm.

WSNs consist of hundreds, or even thousands of sensor nodes with limited communication resources. Using routing protocols, WSN manages to coordinate the communication between each node for the global purpose of gathering information, for example from a reconnaissance mission in the battlefield and forwards the collected information to the required end. In such situation, routing operations are expected to be resilient and equipped with defence characteristics to prevent any misbehaving activities to its transmitted data as well as routing operations. Thus, security for routing protocols in WSNs is important for successful data transmission. In addition, sensor nodes are powered by a battery which implies a clear finite computational resource. Therefore, factors such as constrained in computational power and storage capacity have made efficient routing operations as well as security development and implementation as one of the challenging issues for sensor networks.

1.1.1 WSNs Overview

Rapid technological advancement of wireless communication devices and a microprocessor have made wireless sensor networks (WSNs) technically and economically possible to be widely used in many real-time applications related to both, military and civilian (Tang et al., 2015). WSNs could be used to gather physical information on enemy movements in the battlefields or collect sensitive information about the condition of patients in the medical fields. A unique feature of WSN which consists of hundred or thousand nodes is their ability to be

deployed in a large number, in unattended fashion for a defined long period of time and sometimes in an unprotected environment. In order to communicate with each other, sensor node has to work under the influence of special communication pattern known as routing protocol. Routing protocols are responsible for ensuring that sensed information is transmitted securely without being dropped or compromised from the target area through multiple hops to the end users/computers. Hence, it's imperative important to secure routing protocols against various attacks, especially when WSNs are intended to be deployed in a very sensitive area. In the next section, an overview of security characteristics for routing protocols in WSNs is presented in details.

1.1.2 Security and Routing Protocol Design Challenges

WSN exhibits a unique characteristic, which calls for efficient security methods to protect routing procedures as well as transmitted information from various malicious activities during monitoring and or data transmission operations. The operations here could be critical mission applications which demand the utmost care otherwise a severe tragedy could occur that may cost the loss of human life and creates damage on civil infrastructures. On the hand, WSNs constitute unique challenges in a way that direct implementation of traditional wireless' security techniques found to be undesirable and or difficult choices. This is due to the following reasons; first, WSNs consist of a number of sensor nodes with little or no infrastructure and depend mainly on the insecure wireless communication channel to communicate with each other which exposes them to different kinds of external or internal attacks either passively or actively. The attacker may take advantages of broadcast nature of the wireless link to capture the communication between nodes, splits the network and hindering information transmission operations.

Then, sensor nodes are inherently resource constrained devices. They have limited processing and computation capability, as well as storage and communication bandwidth. This is largely because, they have been made to be tiny in physical size, and powered by a battery. The resource limitation issues of sensor nodes call for bound security solutions that not only thwart routing attacks in inflicting damages in the routing operations but also take care of the resource constraint issues.

Final, sensor nodes are normally deployed in unprotected environments which made them vulnerable to different kinds malicious nodes. When a network topology is changed due to the attacker or one and/or more nodes running out of energy it is expected that a new sensor node may join the network to maintain network functionalities. With a large scale of nodes deployed in the unprotected and unattended environment the malicious nodes may try to take control of the sensor network by compromising some nodes and extract all sensitive nodes' information or insert bogus information causing chaos in routing operations. For

these reasons, different security techniques for WSNs have been developed to protect WSN functionality. These include authentication schemes that make use of public cryptographic keys or asymmetric cryptographic keys, access control which include trust-based schemes, and secure aggregation.

In addition to these techniques, secure routing protocols have been considered with different security features to secure data transmission and ensure data packets are securely received at the target nodes in accurate form and timely manner.

However, sensor nodes in WSN have to operate as both processing device for collecting and manipulating collected data as well as act as a router to forward data packets to the target end. Thus, routing design for WSN becomes more challenging, especially when dealing with the sensor nodes that are known to possess limited capabilities in communication resources and sensing region. Moreover, when sensor nodes are engaged in the forwarding of data packets to the far end target node through multiple hops there is a possibility that one unfortunate situations may occur which may prevent network layer to perform its routing tasks. The situations include the presence of different malicious activities executed by one or more intermediate nodes (i.e. attackers) during the routing initiation or data transmission. In the presence of such activities, the routing layer becomes more critical due to the high chance that the layer may drop or misdirect the data packets to the unwanted end before reaching the target end. Also, the attacker may eavesdrop, inject and reply bogus packets to the network layer, compromise the confidentiality and integrity of the data transmitted. It may also collude with other malicious nodes or more powerful devices (i.e. laptop class attacker) which energize the attacker to become more powerful than normal nodes. Therefore, it is important to have better secure routing techniques as well as efficient routing procedures.

The design and implementation of secure routing protocols in WSN also have to address multiples research challenges. First, wireless communication in the sensor node is vulnerable to many attacks including eavesdropping, unauthorized access, spoofing, replay sinkhole and wormhole attacks, selective forwarding, black hole and denial-of-services (DoS) (Wood et al., 2006; Karlof and Wagner, 2003; Kur, 2008). Then, sensor nodes are highly resource constrained devices in terms memory, communication bandwidth as well as processing power. These limitations limit the degree of implementation of security mechanisms such as encryption, decryption and authentication methods on individual sensor nodes and raise the question of reliability, and sustainability of these mechanisms for such a resource constrained sensor nodes (Wood et al., 2006; Wood and Stankovic, 2002; Abu-Ghazaleh et al., 2005; Bala and Verma, 2009).

Final, secure routing protocols for ad hoc networks have been developed (Lan et al., 2009; Guerhazi and Abid, 2011; Lacuesta et al., 2013; Zhao et al., 2013; Kaliappan and Paramasivan, 2015; Sarkar and Datta, 2016; Sawant et al., 2015;

Taherian et al., 2015) to provide security for communicating mobiles or stationary nodes. However, the preventing mechanisms used in these networks cannot be directly deployed in sensor networks due to their differences in communication resources and characteristics. These mechanisms are too expensive in terms routing computation and node state which demand more memory and generates more communication overheads and high delay.

1.2 Problem Statement

Routing protocols for WSNs have to constantly provide communication regardless of adversarial activities. Numerous studies on secure routing protocols (Perig et al., 2002; Karlof and Wagner, 2003; Wood et al., 2006; Shi and Gong, 2013; Zhang et al., 2008; Saleem et al., 2016) have been conducted to provide defense against routing attacks and guarantee continuous and safe transmission of data between each node in the network. These protocols use different security techniques include cryptographic and authentication tools which are essential to protect data transmitted as well as communicating sensor nodes. However, due to limited communication resources, such techniques may found difficult to be directly used in sensor networks. Hence, there is a call to build security methods that provide a sufficient defense against attacks and lend well with the instinct of sensor networks' communication resources.

Although, the work by Hanapi and Ismail (2014) promises security of routing operations and data packets by protecting routing operations during the selection of a forwarding node in the presence of attackers in the communication link. The deployment of dynamic collection window in (Hanapi and Ismail, 2014), resulting in poor network performance in terms of communication overhead, end-to-end delay as well as a high number of packet drop in the presence of an attacker.

The existing secure routing protocols find difficult to provide an acceptable number of legitimate nodes when multiples attackers (i.e. Sybil nodes increase in the communication link) due to the insufficient allocated sextant which reduces packet delivery ratio due to the high number of attackers selection.

Existing security scheme for multi-hop communication presents performance degradation due to the existence of unauthorized nodes in the network that capture the communication processes and drop packets. The lack of consideration of resource-constrained nature of sensor node during security design led to a poor network performance and more resource consumption.

1.3 Motivation

The future of wireless sensor networks (WSNs) is bright and promising. WSNs have contributed a lot in many real-world applications within many contexts, including recent Internet of Things (IoT). Despite the wide deployment of sensor networks, they still have some critical issues related to the way security techniques are designed, developed and integrated into the routing procedures that are critical in ensuring data packets are securely propagated from one node to another towards destination without modification. The routing procedures themselves may require an improvement for efficient data packet operations. The state-of-the-art shows that the existing secure routing protocols are insufficient in three ways; first, they may use conventional security techniques that have been used by another wireless network. With limited communication resources of sensor nodes, such techniques seem to be impractical. Second, they may use inefficient security measures to try to tackle a different type of attackers based on their locations, magnitude and scenario. Last, as operations to forward information towards destination demand the full cooperation of all nodes in the network, the majority of the secure routing protocols ignore the importance of using the instinct cooperation features of sensor nodes in defining their trustworthiness and/or hostility towards the data packets forwarding operations.

1.4 Research Objectives

The main goal of this thesis is to design secure routing protocol for WSNs that provides defense against routing attacks over the network layer using resource security bound approach. The proposed protocol is aiming at minimizing the selection of attackers presented in the communication link while improving network performance in during the routing process. The general objective aforementioned can be divided into the following specific objectives:

To propose and design a new bound collection (BCW) window for routing protocol that accepted sufficient forwarding nodes with mainly aims to improve network performance by minimizing the end-to-end delay as well as network communication overhead when the protocol is subjected to attacker in the communication link.

To design a novel secure region that extends forwarding area beyond the allocated sextant within a coverage area in order to encourage more responses from legitimate nodes to participate in communication process in the presence of multiple attackers, such as Sybil nodes located in the communication link and prevent the failure of selecting an appropriate forwarding node.

To propose a novel routing protocol that extended forwarding area beyond the allocated sextant to encourage more responses from legitimate nodes to partici-

pate in data and improves packet delivery to the destination when the number of attackers increase in the communication link

To design a light-weight security scheme for communicating nodes to engage in communication process and thwart the threats posed by unauthorized nodes so as to improve network performance.

1.5 Research Scope

This thesis concentrates on studying secure routing protocols in WSNs based on Implicit Geographic Forwarding protocol (i.e. DWSIGF, and SIGF). These protocols has been selected since it has a tendency of minimizing the utilization of communication resources. This is because they work with no routing table which eliminates the cost of maintaining the neighbourhood tables. Also, the protocol has been proven to reduce network congestion, communication overhead, end-to-end delay, energy consumption and message loss due to the absence of routing discovery and beacon messages in maintaining routing tables (Hanapi et al., 2009; Son et al., 2003). Nevertheless, the work in this thesis has excluded power consumption analysis since the inherited protocols have been proven to execute the routing activities with minimum energy consumption (Son et al., 2003; Hanapi et al., 2009). Also, the effort of the work in this thesis is to enhance the routing operations between communication nodes and realize the better performance according to the objectives. In addition, it focuses on improving the security of proposed routing protocol at both MAC and network layer.

In this thesis the analyses of two types of attacks, black hole and Sybil are considered. The selection of the former attacker is due to its simplicity in its development but has devastating results when executed. While Sybil selection is interesting for studying the defence capability of the protocols since it has heterogeneity character, in which much of the real-world applications have often relied upon by deploying an authority to implement a workable system (Douceur, 2002; Mathur et al., 2016). Other attackers related to routing table information manipulation are not considered since the baseline protocols operate independently of routing tables while the routing processes occur dynamically and without routing information exchanges (Hanapi et al., 2009; Wood et al., 2006).

All routing protocol algorithms in this thesis are implemented and tested using simulation programming in MATLAB and focus on WSN densely deployment. The simulation follows 802.11 MAC handshaking mechanisms since the baseline routing protocols used a hybrid of network/MAC layer protocol. All protocols are evaluated in terms of free attacks and attacks environments for black hole and Sybil attacks and the intuitions behind their method of operations. It then presents simulation results, demonstrates the effect of the proposed solution and improvement of communication performance exhibits by the routing protocols

under different attacker scenarios and deployment topologies.

1.6 Thesis Organization

The rest of this thesis is organized as follows: Chapter 2 presents the overview of Wireless Sensor Network including its components, architecture, model, communications, applications and technical challenges. It is followed by security issue in WSNs with emphasis is put on the security challenges and attacks. The chapter continued with the main discussion related to research work which include geographic routing in WSN, routing attacks and its countermeasure in WSN, secure routing protocol based on different security techniques including trust based-routing.

Chapter 3 presents a general description of the research methodology used in this thesis including the research framework, experimental set-up, network topologies, proposed methods, performance metrics and performance validation .

Chapter 4 explores the design of the proposed bound collection window with verification process in WSN and presents its algorithm (BCGF). The chapter also presents the evaluation of the proposed BCGF protocol in two based scenario: the protocol without attacks. In this scenario, the performance of the proposed protocol is measured in terms of the packet delivery ratio, message communication overheads, and end-to-end delay. In the second scenario, the protocol is subjected to attackers threats located in the communication link. In this case, the protocol is measured in terms of packet delivery ratio as well as the probability of selecting attacker (PAS).

Chapter 5 presents the proposed secure region-based geographic routing (SR-BGR) protocol for WSN. The chapter also presents the performance evaluation of the proposed protocol and compares it with other existing secure routing protocols.

Chapter 6 presents the design of lightweight trust-based routing scheme (LTBS) for WSN as well as the introduction of techniques to minimizes the memory consumption and communication overhead during the trust computation. Also, it presents the performance evaluation of the protocol and compares it with other existing trust-based secure routing protocols.

Chapter 7 concludes the work and recommends some promising directions for further research.

REFERENCES

- Abu-Ghazaleh, N., Kang, K.-D., and Liu, K. (2005). Towards resilient geographic routing in wsns. In *Proceedings of the 1st ACM International Workshop on Quality of Service & Security in Wireless and Mobile Networks*, pp. 71–78. ACM.
- Ahmed, A., Bakar, K. A., Channa, M. I., and Khan, A. W. (2016). A secure routing protocol with trust and energy awareness for wireless sensor network. *Mobile Networks and Applications*, 21(2):272–285.
- Akkaya, K. and Younis, M. (2005). A survey on routing protocols for wireless sensor networks. *Ad hoc Networks*, 3(3):325–349.
- Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., and Cayirci, E. (2002a). A survey on sensor networks. *IEEE Communications Magazine*, 40(8):102–114.
- Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., and Cayirci, E. (2002b). Wireless sensor networks: a survey. *Computer Networks*, 38(4):393–422.
- Al-Karaki, J. N. and Kamal, A. E. (2004). Routing techniques in wireless sensor networks: a survey. *IEEE Wireless Communications*, 11(6):6–28.
- Alcaraz, C. and Lopez, J. (2010). A security analysis for wireless sensor mesh networks in highly critical systems. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, 40(4):419–428.
- Anandkumar, C., Prasad, A., and Suma, V. (2017). Multipath load balancing and secure adaptive routing protocol for service oriented wsns. In *Proceedings of the 5th International Conference on Frontiers in Intelligent Computing: Theory and Applications*, pp. 595–601. Springer.
- Anita, X., Bhagyaveni, M. A., and Manickam, J. M. L. (2015). Collaborative lightweight trust management scheme for wireless sensor networks. *Wireless Personal Communications*, 80(1):117–140.
- Atzori, L., Iera, A., and Morabito, G. (2010). The internet of things: A survey. *Computer Networks*, 54(15):2787–2805.
- Azharuddin, M. and Jana, P. K. (2015). A distributed algorithm for energy efficient and fault tolerant routing in wireless sensor networks. *Wireless Networks*, 21(1):251–267.
- Azharuddin, M., Kuila, P., and Jana, P. K. (2015). Energy efficient fault tolerant clustering and routing algorithms for wireless sensor networks. *Computers & Electrical Engineering*, 41:177–190.
- Bairaktaris, K., Chatzigiannakis, I., Liagkou, V., and Spirakis, P. G. (2008). Adaptive probabilistic secure routing in mobile wireless sensor networks. In *Software, Telecommunications and Computer Networks, 2008. SoftCOM 2008. 16th International Conference on*, pp. 208–212. IEEE.
- Bala, S. and Verma, A. (2009). *Secure routing in wireless sensor networks*. PhD thesis, Thapar Institute of Engineering and Technology, Punjab, India.

- Baskar, R., Raja, P. K., Joseph, C., and Reji, M. (2017). Sinkhole attack in wireless sensor networks-performance analysis and detection methods. *Indian Journal of Science and Technology*, 10(12).
- Boukerche, A., Turgut, B., Aydin, N., Ahmad, M. Z., Bölöni, L., and Turgut, D. (2011). Routing protocols in ad hoc networks: A survey. *Computer Networks*, 55(13):3032–3080.
- Breslau, L., Estrin, D., Fall, K., Floyd, S., Heidemann, J., Helmy, A., Huang, P., McCanne, S., Varadhan, K., Xu, Y., et al. (2000). Advances in network simulation. *Computer*, 33(5):59–67.
- Buchegger, S. and Le Boudec, J.-Y. (2002). Performance analysis of the confidant protocol. In *Proceedings of the 3rd ACM International Symposium on Mobile Ad hoc Networking & Computing*, pp. 226–236. ACM.
- Buchegger, S. and Le Boudec, J.-Y. (2003). A robust reputation system for mobile ad-hoc networks. Technical report.
- Carson, I., Nicol, D. M., Nelson, B. L., Banks, J., et al. (2005). Discrete-event system simulation.
- Champ, J. and Saad, C. (2008). An energy-efficient geographic routing with location errors in wireless sensor networks. In *Parallel Architectures, Algorithms, and Networks, 2008. I-SPAN 2008. International Symposium on*, pp. 105–110. IEEE.
- Chanak, P., Banerjee, I., and Sherratt, R. S. (2017). Energy-aware distributed routing algorithm to tolerate network failure in wireless sensor networks. *Ad Hoc Networks*, 56:158–172.
- Chen, D.-R. (2016). An energy-efficient qos routing for wireless sensor networks using self-stabilizing algorithm. *Ad Hoc Networks*, 37:240–255.
- Chen, M., Leung, V. C., Mao, S., Xiao, Y., and Chlamtac, I. (2009a). Hybrid geographic routing for flexible energy—delay tradeoff. *IEEE Transactions on Vehicular Technology*, 58(9):4976–4988.
- Chen, Q. J., Kanhere, S. S., Hassan, M., and Lan, K.-C. (2006). Adaptive position update in geographic routing. In *Communications, 2006. ICC'06. IEEE International Conference on*, volume 9, pp. 4046–4051. IEEE.
- Chen, X., Makki, K., Yen, K., and Pissinou, N. (2009b). Sensor network security: a survey. *IEEE Communications Surveys & Tutorials*, 11(2).
- Cheng, L., Niu, J., Cao, J., Das, S. K., and Gu, Y. (2014). Qos aware geographic opportunistic routing in wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems*, 25(7):1864–1875.
- Chiu, H. S. and Lui, K.-S. (2006). Delphi: wormhole detection mechanism for ad hoc wireless networks. In *Wireless Pervasive Computing, 2006 1st International Symposium on*, pp. 6–pp. IEEE.
- Choi, B. G., Cho, E. J., Kim, J. H., Hong, C. S., and Kim, J. H. (2009). A sinkhole attack detection mechanism for lqi based mesh routing in wsn. In *Information Networking, 2009. ICOIN 2009. International Conference on*, pp. 1–5. IEEE.

- de Morais Cordeiro, C. and Agrawal, D. P. (2011). *Ad hoc and sensor networks: theory and applications*. World Scientific.
- Demirbas, M. and Song, Y. (2006). An rssi-based scheme for sybil attack detection in wireless sensor networks. In *Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks*, pp. 564–570. IEEE Computer Society.
- Denardin, G. W., Barriquello, C. H., Campos, A., and do Prado, R. N. (2011). A geographic routing hybrid approach for void resolution in wireless sensor networks. *Journal of Systems and Software*, 84(10):1577–1590.
- Deng, J., Han, R., and Mishra, S. (2006). Insens: Intrusion-tolerant routing for wireless sensor networks. *Computer Communications*, 29(2):216–230.
- Douceur, J. R. (2002). The sybil attack. In *International Workshop on Peer-to-Peer Systems*, pp. 251–260. Springer.
- Duan, J., Yang, D., Zhu, H., Zhang, S., and Zhao, J. (2014). Tsrfs: A trust-aware secure routing framework in wireless sensor networks. *International Journal of Distributed Sensor Networks*, 2014.
- El-Semary, A. M. and Azim, M. (2012). A dual-sink secure routing protocol for wireless sensor networks. *Journal of Information Assurance & Security*, 7(6).
- Elrahim, A. G. A., Elsayed, H. A., Ramly, S. E., and Ibrahim, M. M. (2010). An energy aware wsn geographic routing protocol. *Universal Journal of Computer Science and Engineering Technology*, 1(2):105–111.
- Erdene-Ochir, O., Minier, M., Valois, F., and Kountouris, A. (2010). Toward resilient routing in wireless sensor networks: Gradient-based routing in focus. In *Sensor Technologies and Applications (SENSORCOMM), 2010 Fourth International Conference on*, pp. 478–483. IEEE.
- Erdene-Ochir, O., Minier, M., Valois, F., and Kountouris, A. (2011). Enhancing resiliency against routing layer attacks in wireless sensor networks: Gradient-based routing in focus. *International journal on advances in networks and services*.
- Fasolo, E., Rossi, M., Widmer, J., and Zorzi, M. (2007). In-network aggregation techniques for wireless sensor networks: a survey. *IEEE Wireless Communications*, 14(2).
- Frey, H., Rührup, S., and Stojmenović, I. (2009). Routing in wireless sensor networks. In *Guide to Wireless Sensor Networks*, pp. 81–111. Springer.
- Ganeriwala, S., Balzano, L. K., and Srivastava, M. B. (2008). Reputation-based framework for high integrity sensor networks. *ACM Transactions on Sensor Networks (TOSN)*, 4(3):15.
- Ganesan, D., Govindan, R., Shenker, S., and Estrin, D. (2001). Highly-resilient, energy-efficient multipath routing in wireless sensor networks. *ACM SIGMOBILE Mobile Computing and Communications Review*, 5(4):11–25.

- García-Otero, M., Zahariadis, T., Álvarez, F., Leligou, H. C., Población-Hernández, A., Karkazis, P., and Casajús-Quirós, F. J. (2010). Secure geographic routing in ad hoc and wireless sensor networks. *Eurasip Journal on Wireless Communications and Networking*, 2010(1):975607.
- Ghazizadeh, S., Ilghami, O., Sirin, E., and Yaman, F. (2002). Security-aware adaptive dynamic source routing protocol. In *Local Computer Networks, 2002. Proceedings. LCN 2002. 27th Annual IEEE Conference on*, pp. 751–760. IEEE.
- Ghosh, T., Pissinou, N., and Makki, K. (2005). Towards designing a trusted routing solution in mobile ad hoc networks. *Mobile Networks and Applications*, 10(6):985–995.
- Goyal, D. and Tripathy, M. R. (2012). Routing protocols in wireless sensor networks: A survey. In *Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on*, pp. 474–480. IEEE.
- Granjal, J., Monteiro, E., and Silva, J. S. (2015). Security for the internet of things: a survey of existing protocols and open research issues. *IEEE Communications Surveys & Tutorials*, 17(3):1294–1312.
- Guermazi, A. and Abid, M. (2011). An efficient key distribution scheme to secure data-centric routing protocols in hierarchical wireless sensor networks. *Procedia Computer Science*, 5:208–215.
- Gui, T., Ma, C., Wang, F., and Wilkins, D. E. (2016). Survey on swarm intelligence based routing protocols for wireless sensor networks: An extensive study. In *Industrial Technology (ICIT), 2016 IEEE International Conference on*, pp. 1944–1949. IEEE.
- Hai, T. H. and Huh, E.-N. (2008). Detecting selective forwarding attacks in wireless sensor networks using two-hops neighbor knowledge. In *Network Computing and Applications, 2008. NCA'08. Seventh IEEE International Symposium on*, pp. 325–331. IEEE.
- Han, Y. and Lin, Z. (2012). A geographically opportunistic routing protocol used in mobile wireless sensor networks. In *Networking, Sensing and Control (IC-NSC), 2012 9th IEEE International Conference on*, pp. 216–221. IEEE.
- Hanapi, Z., Ismail, M., Jumari, K., and Mahdavi, M. (2009). Dynamic window secured implicit geographic forwarding routing for wireless sensor network. In *World Academy of Science, Engineering and Technology. Int. Conf. Wireless Commun. Sensor Network*. Citeseer.
- Hanapi, Z. M. and Ismail, M. (2014). Impact of blackhole and sybil attacks on dynamic windows secured implicit geographic forwarding routing protocol. *IET Information Security*, 8(2):80–87.
- Haseeb, K., Bakar, K. A., Abdullah, A. H., Ahmed, A., Darwish, T., and Ullah, F. (2016). A dynamic energy-aware fault tolerant routing protocol for wireless sensor networks. *Computers & Electrical Engineering*, 56:557–575.

- He, T., Blum, B. M., Cao, Q., Stankovic, J. A., Son, S. H., and Abdelzaher, T. F. (2007). Robust and timely communication over highly dynamic sensor networks. *Real-Time Systems*, 37(3):261–289.
- Heurtefeux, K., Erdene-Ochir, O., Mohsin, N., and Menouar, H. (2015). Enhancing rpl resilience against routing layer insider attacks. In *Advanced Information Networking and Applications (AINA), 2015 IEEE 29th International Conference on*, pp. 802–807. IEEE.
- Hong, C., Xiong, Z., and Zhang, Y. (2016). A hybrid beaconless geographic routing for different packets in wsn. *Wireless Networks*, 22(4):1107–1120.
- Hu, L. and Evans, D. (2004). Using directional antennas to prevent wormhole attacks. In *NDSS*, pp. 241–245.
- Hu, Y.-C., Perrig, A., and Johnson, D. B. (2003a). Packet leashes: a defense against wormhole attacks in wireless networks. In *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, volume 3, pp. 1976–1986. IEEE.
- Hu, Y.-C., Perrig, A., and Johnson, D. B. (2003b). Rushing attacks and defense in wireless ad hoc network routing protocols. In *Proceedings of the 2nd ACM Workshop on Wireless Security*, pp. 30–40. ACM.
- Hu, Y.-C., Perrig, A., and Johnson, D. B. (2005). Ariadne: A secure on-demand routing protocol for ad hoc networks. *Wireless Networks*, 11(1-2):21–38.
- Huang, H., Hu, G., and Yu, F. (2013). Energy-aware geographic routing in wireless sensor networks with anchor nodes. *International Journal of Communication Systems*, 26(1):100–113.
- Hung, K.-S., Lui, K.-S., and Kwok, Y.-K. (2007). A trust-based geographical routing scheme in sensor networks. In *Wireless Communications and Networking Conference, 2007. WCNC 2007. IEEE*, pp. 3123–3127. IEEE.
- Intanagonwiwat, C., Govindan, R., Estrin, D., Heidemann, J., and Silva, F. (2003). Directed diffusion for wireless sensor networking. *IEEE/ACM Transactions on Networking (ToN)*, 11(1):2–16.
- Jahandoust, G. and Ghassemi, F. (2017). An adaptive sinkhole aware algorithm in wireless sensor networks. *Ad Hoc Networks*.
- Jameel, H., Hung, L. X., Kalim, U., Sajjad, A., Lee, S., and Lee, Y.-K. (2005). A trust model for ubiquitous systems based on vectors of trust values. In *Multimedia, Seventh IEEE International Symposium on*, pp. 6–pp. IEEE.
- Jan, M., Nanda, P., Usman, M., and He, X. (2016). Pawn: a payload-based mutual authentication scheme for wireless sensor networks. *Concurrency and Computation: Practice and Experience*.
- Kaliappan, M. and Paramasivan, B. (2015). Enhancing secure routing in mobile ad hoc networks using a dynamic bayesian signalling game model. *Computers & Electrical Engineering*, 41:301–313.

- Kalita, H. K. and Kar, A. (2009). Wireless sensor network security analysis. *International Journal of Next-Generation Networks (IJNGN)*, 1(1):1–10.
- Kang, K.-D., Liu, K., and Abu-Ghazaleh, N. (2006). Securing geographic routing in wireless sensor networks. In *Proc. 2006 Cyber Security Conf. Inf. Assurance*.
- Karlof, C. and Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. *Ad Hoc Networks*, 1(2):293–315.
- Karp, B. and Kung, H.-T. (2000). Gpsr: Greedy perimeter stateless routing for wireless networks. In *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking*, pp. 243–254. ACM.
- Kaur, M. and Kumar, S. (2015). Improved routing protocol for coverage and connectivity (rpcc) in heterogeneous wireless sensor network (hwsn). *International Journal of Computer Applications*, 110(15).
- Khan, K., Waris, A., and Safi, H. (2016). A qualitative comparison of various routing protocols in wsn. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 1(7-13).
- Kim, S., Lee, M., and Yeom, I. (2008). Simulating ieee 802.16 uplink scheduler using ns-2. In *Proceedings of the 1st International Conference on Simulation Tools and Techniques for Communications, Networks and Systems & Workshops, March*.
- Krishnamachari, B., Estrin, D., and Wicker, S. (2002). Modelling data-centric routing in wireless sensor networks. In *IEEE Infocom*, volume 2, pp. 39–44.
- Krontiris, I., Dimitriou, T., Giannetsos, T., and Mpasoukos, M. (2007). Intrusion detection of sinkhole attacks in wireless sensor networks. In *International Symposium on Algorithms and Experiments for Sensor Systems, Wireless Networks and Distributed Robotics*, pp. 150–161. Springer.
- Krontiris, I., Giannetsos, T., and Dimitriou, T. (2008). Launching a sinkhole attack in wireless sensor networks; the intruder side. In *Networking and Communications, 2008. WIMOB'08. IEEE International Conference on Wireless and Mobile Computing*, pp. 526–531. IEEE.
- Kumar, P. and Lee, H.-J. (2011). Security issues in healthcare applications using wireless medical sensor networks: A survey. *Sensors*, 12(1):55–91.
- Kur, B. J. (2008). Secure routing protocols for wireless sensor networks. *Yüksek Lisans Tezi, Masaryk University Faculty of Informatics*.
- Lacuesta, R., Lloret, J., Garcia, M., and Penalver, L. (2013). A secure protocol for spontaneous wireless ad hoc networks creation. *IEEE Transactions on Parallel and Distributed Systems*, 24(4):629–641.
- Lan, Y., Lei, L., and Fuxiang, G. (2009). A multipath secure routing protocol based on malicious node detection. In *Control and Decision Conference, 2009. CCDC'09. Chinese*, pp. 4323–4328. IEEE.
- Langendoen, K. and Reijers, N. (2003). Distributed localization in wireless sensor networks: a quantitative comparison. *Computer Networks*, 43(4):499–518.

- Law, A. M. (2008). How to build valid and credible simulation models. In *Proceedings of the 40th Conference on Winter Simulation*, pp. 39–47. Winter Simulation Conference.
- Lee, J., Park, H., Kang, S., and Kim, K.-I. (2015). Region-based collision avoidance beaconless geographic routing protocol in wireless sensor networks. *Sensors*, 15(6):13222–13241.
- Lee, S., Bhattacharjee, B., Banerjee, S., and Han, B. (2010). A general framework for efficient geographic routing in wireless networks. *Computer Networks*, 54(5):844–861.
- Li, X., Zhou, F., and Du, J. (2013). Ldts: A lightweight and dependable trust system for clustered wireless sensor networks. *IEEE Transactions on Information Forensics and Security*, 8(6):924–935.
- Liu, A., Dong, M., Ota, K., and Long, J. (2015). Phack: An efficient scheme for selective forwarding attack detection in wireless sensor networks. *Sensors*, 15(12):30942–30963.
- Madria, S. and Yin, J. (2009). Serwa: A secure routing protocol against wormhole attacks in sensor networks. *Ad Hoc Networks*, 7(6):1051–1063.
- Magotra, S. and Kumar, K. (2014). Detection of hello flood attack on leach protocol. In *Advance Computing Conference (IACC), 2014 IEEE International*, pp. 193–198. IEEE.
- Malik, S. K., Dave, M., Dhurandher, S. K., Woungang, I., and Barolli, L. (2016). An ant-based qos-aware routing protocol for heterogeneous wireless sensor networks. *Soft Computing*, pp. 1–12.
- Mansouri, D., Mokdad, L., Ben-othman, J., and Ioualalen, M. (2017). Dynamic and adaptive detection method for flooding in wireless sensor networks. *International Journal of Communication Systems*.
- Mao, G., Fidan, B., and Anderson, B. D. (2007). Wireless sensor network localization techniques. *Computer Networks*, 51(10):2529–2553.
- Marin-Perez, R. and Ruiz, P. M. (2011). Sbgr: A simple self-protected beaconless geographic routing for wireless sensor networks. In *Mobile Adhoc and Sensor Systems (MASS), 2011 IEEE 8th International Conference on*, pp. 610–619. IEEE.
- Marti, S., Giuli, T. J., Lai, K., and Baker, M. (2000). Mitigating routing misbehavior in mobile ad hoc networks. In *Proceedings of the 6th Annual International conference on Mobile Computing and Networking*, pp. 255–265. ACM.
- Mathur, A., Newe, T., and Rao, M. (2016). Defence against black hole and selective forwarding attacks for medical wsns in the iot. *Sensors*, 16(1):118.
- Nasser, N. and Chen, Y. (2007). Seem: Secure and energy-efficient multipath routing protocol for wireless sensor networks. *Computer Communications*, 30(11):2401–2412.

- Newsome, J., Shi, E., Song, D., and Perrig, A. (2004). The sybil attack in sensor networks: analysis & defenses. In *Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks*, pp. 259–268. ACM.
- Omar, M., Yahiaoui, S., and Bouabdallah, A. (2016). Reliable and energy aware query-driven routing protocol for wireless sensor networks. *Annals of Telecommunications*, 71(1-2):73–85.
- Pan, M.-S. and Yang, S.-W. (2017). A lightweight and distributed geographic multicast routing protocol for iot applications. *Computer Networks*, 112:95–107.
- Papadimitratos, P. and Haas, Z. J. (2002). Secure routing for mobile ad hoc networks. In *the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), San Antonio, TX, January 27-31, 2002*, pp. 193–204.
- Perrig, A., Stankovic, J., and Wagner, D. (2004). Security in wireless sensor networks. *Communications of the ACM*, 47(6):53–57.
- Perrig, A., Szewczyk, R., Tygar, J. D., Wen, V., and Culler, D. E. (2002). Spins: Security protocols for sensor networks. *Wireless Networks*, 8(5):521–534.
- Pires, W., de Paula Figueiredo, T. H., Wong, H. C., and Loureiro, A. A. F. (2004). Malicious node detection in wireless sensor networks. In *Parallel and Distributed Processing Symposium, 2004. Proceedings. 18th International*, p. 24. IEEE.
- Pirzada, A. A. and McDonald, C. (2006). Trust establishment in pure ad-hoc networks. *Wireless Personal Communications*, 37(1):139–168.
- Popescu, A. M., Tudorache, I. G., Peng, B., and Kemp, A. H. (2012). Surveying position based routing protocols for wireless sensor and ad-hoc networks. *International Journal of Communication Networks and Information Security*, 4(1):41.
- Qabajeh, L. K., Kiah, M. M., and Qabajeh, M. (2009). A qualitative comparison of position-based routing protocols for ad-hoc networks. *International Journal of Computer Science and Network*, 9(2):131–140.
- Rajeshkumar, G. and Valluvan, K. (2017). An energy aware trust based intrusion detection system with adaptive acknowledgement for wireless sensor network. *Wireless Personal Communications*, pp. 1–15.
- Rawat, P., Singh, K. D., Chaouchi, H., and Bonnin, J. M. (2014). Wireless sensor networks: a survey on recent developments and potential synergies. *The Journal of Supercomputing*, 68(1):1–48.
- Renold, A. P. and Chandrakala, S. (2016). Survey on state scheduling-based topology control in unattended wireless sensor networks. *Computers & Electrical Engineering*, 56:334–349.
- Rodrigues, J. J. and Neves, P. A. (2010). A survey on ip-based wireless sensor network solutions. *International Journal of Communication Systems*, 23(8):963–981.

- Saleem, K., Derhab, A., Orgun, M. A., Al-Muhtadi, J., Rodrigues, J. J., Khalil, M. S., and Ali Ahmed, A. (2016). Cost-effective encryption-based autonomous routing protocol for efficient and secure wireless sensor networks. *Sensors*, 16(4):460.
- Salehi, S. A., Razzaque, M., Naraei, P., and Farrokhtala, A. (2013). Detection of sinkhole attack in wireless sensor networks. In *Space Science and Communication (IconSpace), 2013 IEEE International Conference on*, pp. 361–365. IEEE.
- Sanchez, J. A., Ruiz, P. M., Liu, J., and Stojmenovic, I. (2007). Bandwidth-efficient geographic multicast routing protocol for wireless sensor networks. *IEEE Sensors Journal*, 7(5):627–636.
- Sanzgiri, K., Dahill, B., Levine, B. N., Shields, C., and Belding-Royer, E. M. (2002). A secure routing protocol for ad hoc networks. In *Network Protocols, 2002. Proceedings. 10th IEEE International Conference on*, pp. 78–87. IEEE.
- Sarangapani, J. (2007). *Wireless Ad Hoc and Sensor Networks: Protocols, Performance, and Control*, volume 25. CRC Press.
- Sarkar, A. and Murugan, T. S. (2016). Routing protocols for wireless sensor networks: What the literature says? *Alexandria Engineering Journal*.
- Sarkar, S. and Datta, R. (2016). A secure and energy-efficient stochastic multipath routing for self-organized mobile ad hoc networks. *Ad Hoc Networks*, 37:209–227.
- Sarma, A. H. K. D., Kar, B. A., and Mall, C. R. (2011). Secure routing protocol for mobile wireless sensor network. In *Sensors Applications Symposium (SAS), 2011 IEEE*, pp. 93–99. IEEE.
- Sarma, H. K. D., Kar, A., and Mall, R. (2016). A hierarchical and role based secure routing protocol for mobile wireless sensor networks. *Wireless Personal Communications*, 90(3):1067–1103.
- Sawant, K., Rawat, M. K., and Jain, A. (2015). Implementation of energy aware secure routing protocol over flooding environment in manet. In *Computer, Communication and Control (IC4), 2015 International Conference on*, pp. 1–5. IEEE.
- Seada, K., Zuniga, M., Helmy, A., and Krishnamachari, B. (2004). Energy-efficient forwarding strategies for geographic routing in lossy wireless sensor networks. In *Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems*, pp. 108–121. ACM.
- Selvam, R. and Senthilkumar, A. (2014). Cryptography based secure multipath routing protocols in wireless sensor network: a survey. In *Electronics and Communication Systems (ICECS), 2014 International Conference on*, pp. 1–5. IEEE.
- Shafiei, H., Khonsari, A., Derakhshi, H., and Mousavi, P. (2014). Detection and mitigation of sinkhole attacks in wireless sensor networks. *Journal of Computer and System Sciences*, 80(3):644–653.

- Shaikh, R. A., Jameel, H., d'Auriol, B. J., Lee, H., Lee, S., and Song, Y.-J. (2009). Group-based trust management scheme for clustered wireless sensor networks. *IEEE transactions on parallel and distributed systems*, 20(11):1698–1712.
- Shi, E. and Perrig, A. (2004). Designing secure sensor networks. *IEEE Wireless Communications*, 11(6):38–43.
- Shi, W. and Gong, P. (2013). A new user authentication protocol for wireless sensor networks using elliptic curves cryptography. *International Journal of Distributed Sensor Networks*.
- Singh, R., Singh, J., and Singh, R. (2016). Wrht: A hybrid technique for detection of wormhole attack in wireless sensor networks. *Mobile Information Systems*, 2016.
- Singh, V. P., Ukey, A. S. A., and Jain, S. (2013). Signal strength based hello flood attack detection and prevention in wireless sensor networks. *International Journal of Computer Applications*, 62(15).
- Snigdha, I. and Gosain, D. (2016). Analysis of scalability for routing protocols in wireless sensor networks. *Optik-International Journal for Light and Electron Optics*, 127(5):2535–2538.
- Son, S., Blum, B., He, T., and Stankovic, J. (2003). Igf: A state-free robust communication protocol for wireless sensor networks. *Tec. Report Depart. Comput. Sci. Univ. Virginia*.
- Sookhak, M., Akhundzada, A., Sookhak, A., Eslaminejad, M., Gani, A., Khan, M. K., Li, X., and Wang, X. (2015). Geographic wormhole detection in wireless sensor networks. *PloS One*, 10(1):e0115324.
- Ssu, K.-F., Wang, W.-T., and Chang, W.-C. (2009). Detecting sybil attacks in wireless sensor networks using neighboring information. *Computer Networks*, 53(18):3042–3056.
- Stankovic, J. A. (2014). Research directions for the internet of things. *IEEE Internet of Things Journal*, 1(1):3–9.
- Sun, H.-M., Chen, C.-M., and Hsiao, Y.-C. (2007). An efficient countermeasure to the selective forwarding attack in wireless sensor networks. In *TENCON 2007-2007 IEEE Region 10 Conference*, pp. 1–4. IEEE.
- Sun, Y. L., Yu, W., Han, Z., and Liu, K. R. (2006). Information theoretic framework of trust modeling and evaluation for ad hoc networks. *IEEE Journal on Selected Areas in Communications*, 24(2):305–317.
- Taherian, M., Karimi, H., Kashkooli, A. M., Esfahanimehr, A., Jafta, T., and Jafarabad, M. (2015). The design of an optimal and secure routing model in wireless sensor networks by using pso algorithm. *Procedia Computer Science*, 73:468–473.
- Tanachaiwiwat, S., Dave, P., Bhindwale, R., and Helmy, A. (2004). Location-centric isolation of misbehavior and trust routing in energy-constrained sensor networks. In *Performance, Computing, and Communications, 2004 IEEE International Conference on*, pp. 463–469. IEEE.

- Tang, D., Li, T., Ren, J., and Wu, J. (2015). Cost-aware secure routing CASER protocol design for wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems*, 26(4):960–973.
- Theodorakopoulos, G. and Baras, J. S. (2006). On trust models and trust evaluation metrics for ad hoc networks. *IEEE Journal on Selected Areas in Communications*, 24(2):318–328.
- Triki, B., Rekhis, S., and Boudriga, N. (2010). A novel secure and multipath routing algorithm in wireless sensor networks. In *Data Communication Networking (DCNET), Proceedings of the 2010 International Conference on*, pp. 1–10. IEEE.
- Villalpando, R., Vargas, C., and Munoz, D. (2008). Network coding for detection and defense of sink holes in wireless reconfigurable networks. In *Systems and Networks Communications, 2008. ICSNC'08. 3rd International Conference on*, pp. 286–291. IEEE.
- Wehrle, K., Günes, M., and Gross, J. (2010). *Modeling and Tools for Network Simulation*. Springer Science & Business Media.
- Willig, A. (2008). Recent and emerging topics in wireless industrial communications: A selection. *IEEE Transactions on Industrial Informatics*, 4(2):102–124.
- Witt, M. and Turau, V. (2005). Bgr: Blind geographic routing for sensor networks. In *Intelligent Solutions in Embedded Systems, 2005. Third International Workshop on*, pp. 51–61. IEEE.
- Wood, A. D., Fang, L., Stankovic, J. A., and He, T. (2006). SIGF: A family of configurable, secure routing protocols for wireless sensor networks. In *Proceedings of the fourth ACM Workshop on Security of Ad hoc and Sensor Networks*, pp. 35–48. ACM.
- Wood, A. D. and Stankovic, J. A. (2002). Denial of service in sensor networks. *Computer*, 35(10):54–62.
- Wu, B., Chen, J., Wu, J., and Cardei, M. (2007). A survey of attacks and countermeasures in mobile ad hoc networks. In *Wireless network security*, pp. 103–135. Springer.
- Wu, F.-J., Kao, Y.-F., and Tseng, Y.-C. (2011). From wireless sensor networks towards cyber physical systems. *Pervasive and Mobile Computing*, 7(4):397–413.
- Wu, S. and Candan, K. S. (2004). Gper: Geographic power efficient routing in sensor networks. In *Network Protocols, 2004. ICNP 2004. Proceedings of the 12th IEEE International Conference on*, pp. 161–172. IEEE.
- Xiao, Y. (2007). *Security in distributed, grid, mobile, and pervasive computing*. CRC Press.
- Xiao, Y., Rayi, V. K., Sun, B., Du, X., Hu, F., and Galloway, M. (2007). A survey of key management schemes in wireless sensor networks. *Computer Communications*, 30(11):2314–2341.

- Xing, K., Srinivasan, S. S. R., Jose, M., Li, J., Cheng, X., et al. (2010). Attacks and countermeasures in sensor networks: a survey. In *Network security*, pp. 251–272. Springer.
- Yang, R., Lin, C., Jiang, Y., and Chu, X. (2011). Trust based access control in infrastructure-centric environment. In *Communications (ICC), 2011 IEEE International Conference on*, pp. 1–5. IEEE.
- Ye, Z., Wen, T., Liu, Z., Song, X., and Fu, C. (2017). An efficient dynamic trust evaluation model for wireless sensor networks. *Journal of Sensors*, 2017.
- Yick, J., Mukherjee, B., and Ghosal, D. (2008). Wireless sensor network survey. *Computer Networks*, 52(12):2292–2330.
- Yih-Chun, H. and Perrig, A. (2004). A survey of secure wireless ad hoc routing. *IEEE Security & Privacy*, 2(3):28–39.
- Yin, C., Huang, S., Su, P., and Gao, C. (2003). Secure routing for large-scale wireless sensor networks. In *Communication Technology Proceedings, 2003. ICCT 2003. International Conference on*, volume 2, pp. 1282–1286. IEEE.
- Yu, S., Zhang, B., Li, C., and Mouftah, H. (2014). Routing protocols for wireless sensor networks with mobile sinks: A survey. *IEEE Communications Magazine*, 52(7):150–157.
- Yu, Y., Li, K., Zhou, W., and Li, P. (2012). Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures. *Journal of Network and Computer Applications*, 35(3):867–880.
- Zabin, F., Misra, S., Woungang, I., Rashvand, H. F., Ma, N.-W., and Ali, M. A. (2008). Reep: data-centric, energy-efficient and reliable routing protocol for wireless sensor networks. *IET Communications*, 2(8):995–1008.
- Zhan, G., Shi, W., and Deng, J. (2012). Design and implementation of tarf: A trust-aware routing framework for wsns. *IEEE Transactions on Dependable and Secure Computing*, 9(2):184–197.
- Zhang, G., Zhang, Y., and Chen, Z. (2013). Using trust to secure geographic and energy aware routing against multiple attacks. *PLoS One*, 8(10):e77488.
- Zhang, K., Wang, C., and Wang, C. (2008). A secure routing protocol for cluster-based wireless sensor networks using group key management. In *Wireless Communications, Networking and Mobile Computing, 2008. WiCOM'08. 4th International Conference on*, pp. 1–5. IEEE.
- Zhang, Y., Liu, W., Lou, W., and Fang, Y. (2006). Location-based compromise-tolerant security mechanisms for wireless sensor networks. *IEEE Journal on Selected Areas in Communications*, 24(2):247–260.
- Zhao, S., Kent, R., and Aggarwal, A. (2013). A key management and secure routing integrated framework for mobile ad-hoc networks. *Ad Hoc Networks*, 11(3):1046–1061.

Zhou, G.-D. and Yi, T.-H. (2013). Recent developments on wireless sensor networks technology for bridge health monitoring. *Mathematical Problems in Engineering*, 2013.

Zin, S. M., Anuar, N. B., Kiah, M. L. M., and Pathan, A.-S. K. (2014). Routing protocol design for secure wsn: Review and open research issues. *Journal of Network and Computer Applications*, 41:517–530.

