UNIVERSITI PUTRA MALAYSIA

MITIGATING MALICIOUS NODES USING TRUST AND REPUTATIONBASED MODEL IN WIRELESS SENSOR NETWORKS

MUHAMMAD DANIEL HAFIZ ABDULLAH

FSKTM 2018 20

MITIGATING MALICIOUS NODES USING TRUST AND REPUTATION-BASED MODEL IN WIRELESS SENSOR NETWORKS

By

MUHAMMAD DANIEL HAFIZ ABDULLAH

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

January 2018

COPYRIGHT

DEDICATION

Dedicated to my wife, Normalia Samian;

To my kids, Nur Qystina & Adam Uqayl;

Members of my family, Dominic Chung, Launi Gaulusi, Samian Sawiyo, Masnah Jamin, brothers and sisters

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

MITIGATING MALICIOUS NODES USING TRUST AND REPUTATION-BASED MODEL IN WIRELESS SENSOR NETWORKS

By

MUHAMMAD DANIEL HAFIZ ABDULLAH

January 2018

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

Wireless sensor network (WSN) is one of the promising network infrastructures for many applications such as healthcare monitoring, environmental monitoring, structural health monitoring, homeland security, military and battlefield surveillance. These applications are basically involve in monitoring of sensitive information such as tracking of enemy movement and patient's health information. Therefore, delivering these information becomes one of the challenging issues in WSNs. Generally, in WSNs, data are forwarded via multi-hop manner and because of this, the security of these data faced several challenges due the malicious nodes that could potentially be selected as one of the intermediate nodes. Trust and reputation-based technique has been acknowledged as one of the promising solutions to overcome this problem. However, many of existing trust and reputation models in WSNs are insecure due to inaccurate node's trustworthiness evaluation which cause node to accidentally choose a malicious node during the data forwarding process. This problem occurs due to the limited number of trust information used to compute node's trustworthiness value. In addition, to increase the accuracy of node trustworthiness evaluation, node in the network solicits more information through recommendations from other nodes in the network. However, information collected using recommendations are vulnerable to dishonest recommendation attacks that can potentially mislead the trust computation engine. Most, if not all, existing models in trust and reputation domain are lack in providing sufficient behavioral-based trust information. Many of them focus too much on Quality-of-Service (QoS) types of trust information and less consideration has been put on other sources of trust information such as in Mobile Ad hoc Networks (MANETs) and Online Social Networks (OSNs). This significantly contributes to the scarcity of trust information which leads to poor network and security performances. This research aims to increase the accuracy of node trustworthiness evaluation process in order to helps node to make more informed decision prior to establish secure communications. In order to achieve this, different

sets of trust information including QoS, OSNs and ant colony system (ACS) algorithm are proposed to improve the selection of trustworthy node. In this research, three models have been proposed namely Trust and Reputation Model for Wireless Sensor Networks (TReM-WSN), Recommendation-based Trust Model (RecommTM) and a multidimensional Trust and Reputation Model using Social, Quality of service and Ant colony system (TRM-SQA). The effectiveness of each of these models in evaluating node's trustworthiness and mitigating malicious nodes, as well as their influence on network and security performances will be tested and validated through simulation. The network and security performances such as Packet Delivery Ratio (PDR), packet loss, selection accuracy, path length, node's trust value, recognition proportion (RP), false negative proportion (FNP) and false positive proportion (FPP) will be evaluated during the simulation process. Results gained from the performance evaluation show that the proposed models able to improve PDR, selection accuracy, path length, node's trust value and significantly reduced the packet loss rate. In addition, the problems related to RP, FNP and FPP are also have been successfully addressed.

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

MODEL BERASASKAN KEPERCAYAAN DAN REPUTASI UNTUK MENGURANGKAN NOD HASAD DALAM RANGKAIAN SENSOR WAYARLES

Oleh

MUHAMMAD DANIEL HAFIZ ABDULLAH

Januari 2018

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

Rangkaian sensor wayarles (WSN) adalah salah satu infrastruktur rangkaian yang menjanjikan banyak aplikasi seperti pemantauan kesihatan, pemantauan alam sekitar, pemantauan kesihatan struktur, keselamatan tanah air, pengawasan tentera dan medan peperangan. Aplikasi-aplikasi ini pada dasarnya melibatkan pemantauan maklumat sensitif seperti pengesanan pergerakan musuh dan maklumat kesihatan pesakit. Oleh yang demikian, penghantaran maklumat-maklumat ini menjadi salah satu isu yang mencabar dalam rangkaian sensor wayarles. Umumnya, penghantaran data dalam rangkaian sensor wayarles adalah secara pelbagai hop, disebabkan itu, keselamatan penghantaran data ini menghadapi beberapa cabaran dimana nod hasad berpotensi untuk dipilih sebagai salah satu daripada nod perantaraan. Teknik berasaskan kepercayaan dan reputasi diakui sebagai salah satu daripada penyelesaian yang dapat mengatasi masalah ini. Walau bagaimanapun, kebanyakan model kepercayaan dan reputasi yang sedia ada adalah tidak selamat disebabkan ketidaktepatan pada penilaian kepercayaan nod yang seterusnya mengakibatkan nod secara tidak sengaja memilih nod hasad semasa proses penghantaran data. Masalah ini berlaku disebabkan oleh jumlah maklumat kepercayaan yang terhad digunakan semasa menghitung nilai kepercayaan nod. Di samping itu, untuk meningkatkan ketepatan penilaian kebolehpercayaan nod, nod dalam rangkaian akan mengumpul lebihan maklumat melalui cadangan daripada nod yang lain dalam rangkaian. Walau bagaimanapun, maklumat yang dikumpul menggunakan kaedah cadangan terdedah kepada serangan cadangan tidak jujur yang berpotensi mengelirukan enjin pengiraan kepercayaan. Kebanyakan, jika tidak semua, model-model yang sedia ada di dalam domain kepercayaan dan reputasi kurang menyediakan maklumat kepercayaan tingkah laku yang mencukupi. Kebanyakan model-model ini terlalu memberi tumpuan yang banyak terhadap jenis maklumat kepercayaan berasaskan kualiti perkhidmatan (QoS) dan kurang memberi pertimbangan terhadap sumber maklumat kepercayaan yang lain

seperti rangkain ad hoc bergerak (MANET) dan rangkaian sosial dalam talian (OSN). Situasi ini menyumbang kepada kekurangan maklumat kepercayaan yang membawa kepada proses penilaian kepercayaan yang tidak tepat. Penyelidikan ini bertujuan untuk meningkatkan ketepatan proses penilaian kebolehpercayaan untuk membantu nod dalam membuat keputusan yang lebih tepat sebelum melakukan komunikasi yang selamat. Untuk mencapai matlamat ini, pelbagai maklumat kepercayaan termasuk dari QoS, OSN dan algoritma sistem koloni semut (ACS) dicadangkan untuk memperbaiki pemilihan nod yang boleh dipercayai. Dalam penyelidikan ini, tiga model telah dicadangkan iaitu model kepercayaan dan reputasi untuk rangkaian sensor wayarles (TReM-WSN), model kepercayaan berasaskan cadangan (RecommTM) dan model kepercayaan dan reputasi multidimensi yang menggunakan sosial, kualiti perkhidmatan dan sistem koloni semut (TRM-SQA). Keberkesanan setiap model-model ini dalam menilai kebolehpercayaan nod dan mengurangkan nod hasad, serta pengaruh mereka terhadap prestasi rangkaian dan keselamatan akan diuji dan disahkan melalui simulasi. Prestasi rangkaian dan keselamatan seperti nisbah penghantaran paket (PDR), kehilangan paket, ketepatan pemilihan, kepanjangan laluan, nilai kepercayaan nod, perkadaran pengiktirafan (RP), perkadaran negatif palsu (FNP) dan perkadaran positif palsu (FPP) akan dinilai semasa proses simulasi. Keputusan yang diperolehi daripada penilaian prestasi menunjukkan bahawa model-model yang dicadangkan dapat memperbaiki PDR, ketepatan pemilihan, kepanjangan laluan, nilai kerpercayaan nod dan berjaya mengurangkan kadar kehilangan paket. Disamping itu, masalah berkaitan RP, FNP dan FPP juga telah berjaya diatasi.

ACKNOWLEDGEMENTS

Alhamdulillah… Praise be to Allah S.W.T for giving me the guidance and strength to complete this thesis despite of the ups and downs journey that I went through.

First and foremost, I would like to thank to Almighty God for giving me guidance, strength and courage to complete this thesis. Also, I would like to take this opportunity to convey my greatest gratitude to my dearest supervisor Associate Professor Dr. Zurina Mohd Hanapi, co-supervisor Professor Dr. Zuriati Ahmad Zukarnain and Dr. Mohamad Afendee Mohamed who have been my mentors throughout the research project. Their great ideas, suggestions, advices and guidance are sincerely and highly appreciated.

My special thanks to my family in Sabah especially to my dearest father and mother, Dominic Chung and Launi Gaulusi for the sacrifices, advices, encouragements and wonderful motivations throughout my study. Not forgetting to my lovely wife, Normalia Samian for her love, supports and understanding and my wonderful little daughter and son, Nur Qystina and Adam Uqayl for being my source of inspiration throughout this study.

Last but not least, my greatest thanks to my family members in Sabah and Johor especially to Samian Sawiyo, Masnah Jamin, big brother Sylvester, brothers and sisters, Tommy, Jimmy, Melanie, Terrence, Atiqah, Haizad and Hariz for preserving and enabling me in completing my study.

This thesis was submitted to the Senate of the Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of Doctor of Philosophy. The members of the Supervisory Committee were as follows

Zurina Mohd Hanapi, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Zuriati Ahmad Zukarnain, PhD
Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

Mohamad Afendee Mohamed, PhD
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

ROBIAH BINTI YUNUS, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

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 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.: Muhammad Daniel Hafiz Abdullah, GS38441

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) were adhered to.

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

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

Signature: _____
Name of Member of Supervisory Committee: Dr. Mohamad Afendee Mohamed

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ABC	Artificial Bee Colony
ACS	Ant Colony System
AL	Agent Launcher
ANN	Artificial Neural Network
API	Application Program Interface
AS	Ant System
ATMP	Adaptive Trust Management Protocol
ATRCM	Authenticated Trust and Reputation Calculation and Management
ATRM	Agent-based Trust and Reputation Management
ATSN	Agent-based Trust model for wireless Sensor Node
ATSR	Ambient Trust Sensor Routing
B-GPSR	Beta-Greedy Perimeter Stateless Routing
BMA	Bad-Mouthing Attack
BNs	Beacon Nodes
BSA	Ballot-Stuffing Attack
BT-GPSR	Beta Trusted-Greedy Perimeter Stateless Routing
BTRM-WSN	Bio-inspired Trust and Reputation Model for Wireless Sensor Network
CBA	Conflict Behavior Attack
CBR	Constant Bit Rate
CC-WSN	Cloud Computing and Wireless Sensor Network
CH-Level	Cluster Head-level
CONFIDANT	Cooperation Of Nodes: Fairness In Dynamic Ad hoc Networks
CORC	Credit-Only Reputation Computation

CORE	COllaborative REputation
CRATER	Cautious RAting for Trust Enable Routing
CSP	Cloud Service Provider
CSU	Cloud Service User
DCRC	Debit-Credit Reputation Computation
DETM-WSN	Distributed Event-triggered Trust Management for Wireless Sensor Networks
DHT	Distributed Hash Table
DoS	Denial of Service
DRBTS	Distributed Reputation-based Beacon Trust System
DTMED-WSN	Data Trust Model for Event Detection in Wireless Sensor Networks
ECC	Elliptic Curve Cryptography
EDTM	Efficient Distributed Trust Model
EMPIRE	Efficient Monitoring Procedure In REputation
FHI	First-Hand Information
FNP	False Negative Proportion
FPP	False Positive Proportion
GA	Genetic Algorithm
GEAR	Geographic and Energy Aware Routing
GETAR	Geographic, Energy and Trust Aware Routing
HSN	Hash Sequence Number
IBA	Intelligent Behavior Attack
ID	Identification
IDS	Intrusion Detection System
IP	Internet Protocol
IRIS	Interactions Relationship Interest Similarity

LBA	Location-Based Attack
MANETs	Mobile Ad hoc Networks
NBP	Natural Behavior Period
NCA	Newcomer Attack
NMA	Nodal Monitoring Activity
NRT	Neighbor-Reputation-Table
O-OA	On-Off Attack
OSNs	Online Social Networks
P2P	Peer to Peer
PDF	Probability Density Function
PDR	Packet Delivery Ratio
P-Grid	Peer-Grid
PLUS	Parameterized and Localized trUst management Scheme
PSO	Particle Swarm Optimization
QoS	Quality of Service
RCA	Reputation Computation Agent
RecommTM	Recommendation Trust Model
REP	Recommendation Exchange Protocol
RESISTOR	REputation System-Independent Scale for Trust On Routing
RFSN	Reputation-based Framework for Sensor Network
RP	Recognition Proportion
SA	Simulated Annealing
SECURE	Secure Environment for Collaboration among Ubiquitous Roaming Entities
SHI	Second-Hand Information
SN-level	Sensor Node Level

SNP	Sensor Network Provider
SNs	Sensor Nodes
STrust	Social Trust model
TACS	Trust Ant Colony System
TAP	Trust Assistant Policy
TCE	Trusted Center Entity
TCM-UWSNs	Trust Cloud Model for Underwater Wireless Sensor Networks
T-GPSR	Trusted-Greedy Perimeter Stateless Routing
THA	Trust-Holding Agent
TinyAFD	Tiny Attack and Fault Detection framework
TMBBT	Trust Model Based on Bayes Theorem
TOMS	Trust cOmputation and Management System
TRA	Trust and Reputation Assessor
TReM-WSN	Trust and Reputation Model for Wireless Sensor Network
TRMSim-WSNs	Trust and Reputation Models Simulator for Wireless Sensor Networks
TRM-SQA	Trust and Reputation Model-Social, QoS and ACS
TS	Travelling Salesman
TT	Total Trust
TTSN	Task-based Trust framework for Sensor Network
VANETs	Vehicular Ad hoc Networks
VCG	Vickrey-Clarke-Grove
WD	Watchdog
WSNs	Wireless Sensor Networks

CHAPTER 1

INTRODUCTION

1.1 Introduction

Advances in wireless communication systems, digital electronics and microelectronics devices have improved the design and the development of cost-effective, energy efficient and adaptable sensor nodes. These sensor nodes are small in size and conceptually consist of four different components which are sensing, processing, communication and power. Recent developments and improvements on these sensor components make it possible to deploy effective and efficient Wireless Sensor Networks (WSNs) over traditional wired sensor networks in terms of power, data acquisition, health monitoring and communication infrastructures (Hsu et al., 2014; Hualin et al., 2016; Velez et al., 2015). WSN is a self-configuring network of a group of sensor nodes communicating among themselves by using radio signal which is usually deployed in a sparse or dense structure to sense, monitor and understand the physical environments. In general, WSNs can be classified into two major architectures which are centralized network and distributed network architectures (Bi, 2013; Cao et al., 2016; Rashid et al., 2014). In centralized network architecture, the network formation is controlled by a central node. This central node is responsible to manages network operations such as event detection, traffic routing, data filtering and node localization. Meanwhile, in distributed network architecture, nodes are autonomous and the communication formation is managed between neighboring nodes. To enable communication in WSNs, sensor nodes will collaborate to each other to form a temporary network called ad hoc network. This ad hoc network is basically performed via a multi-hop manner due to the short radio range and powered by a limited energy sources. WSNs have been used in many promising applications such as environmental monitoring (Bi, 2013), military battlefield (tracking and targeting enemies) (Pawgasame, 2016; Roy & Nene, 2015), ecological monitoring (Yan et al., 2014), health-related monitoring (Jafari et al., 2005; X. Li et al., 2016) natural disaster relief (Khan et al., 2015; Mehmood et al., 2012), structural monitoring (Hsu et al., 2014) and smart cities communication systems (Ferrandis et al., 2012; Ortiz et al., 2013). These applications are basically involve in monitoring of sensitive information and therefore data security becomes paramount important issue. However, due to some limitations and resource constraints such as limited memory, limited energy, low computational power, susceptibility to physical capture attack and insecure wireless communication channels, enforcing security in WSNs becomes difficult and challenging task especially when the sensor networks are operated in a hostile and unattended environments.

Nowadays, many work have been done to strengthen the security of WSNs (Kandah et al., 2017; Kesavan & Radhakrishnan, 2012; Le et al., 2009; Louw et al., 2016; Lu, Lin, Zhang, et al., 2008; Nadir et al., 2016; Shi et al., 2007; Shim, 2017; Zhang, 2012; Zheng et al., 2016). However, almost all of these existing solutions are mainly depend on cryptographic based solutions such as symmetric and asymmetric encryptions. It is

undeniable that cryptographic-based solutions have the capabilities to secure data communication in WSNs. However, cryptographic-based solutions require large memory and high processing power and these indeed cannot be fulfilled by a sensor node that has limited resources and capabilities. In addition, cryptographic-based solutions also require the execution of complex mathematical calculation which in turn generates high computational and communication overheads. These problems can be solved by implementing trust and reputation-based technique as this technique can overcomes the aforementioned problems which cannot be solved effectively by using traditional security and authentication mechanisms. Trust and reputation-based is a technique that discovers, records and utilizes reputation to form trust (Sen, 2010). It also known as a technique that collect process and disseminate feedback about node's history or past behavior (Alzaid et al., 2013; Alzaid et al., 2008b). Unlike traditional security mechanisms, trust and reputation technique does not require large memory and complex solution. Therefore, implementing this technique could save those aforementioned limitations and resource constraints in WSNs. Trust and reputation concept in WSNs can be represented as a personal opinion of one node (evaluating node) towards other node (evaluated node) which are based on node's past behaviour and recommendations given by other nodes (recommender nodes) in the network (Alzaid, 2011).

For the past few years, there has been significant number of researches have been done to improve routing security in WSNs by improving the trust and reputation evaluation model (A. Boukerche & Xu, 2005; Gomez & Perez, 2011; Haiguang et al., 2008; Labraoui, 2015; Maarouf et al., 2009; Naseer, 2012; Román et al., 2009; Vamsi et al., 2014; Zhan et al., 2010). However, many of the existing work are inaccurate due to design issues where limited trust information used to evaluate node's trustworthiness. In addition, some of the proposed models also assumed or declared a fully trusted node only based on the returned requested services without thoroughly investigate node's behaviors such as refusing to forward packets, dropping packets and rerouting the packets to the wrong destination. Such mentioned problems and unrealistic assumptions may contribute to inaccuracy of node trustworthiness evaluation which may leads to unsecure or poor selection of trusted node for routing in WSNs. Therefore, rigorous investigation on node's behaviors are needed to ensure the accuracy on node's trustworthiness evaluation can be achieved.

The use of recommendation-based trust approach in WSNs can help node to make better or more informed decision on the selection of trustworthy node (Chen et al., 2012; Guo et al., 2015; J. Hu et al., 2008; Iltaf et al., 2012; Jiang et al., 2015). However, gathering information through recommendations is a challenging and difficult tasks due to the risk of dishonest recommendation attacks such as bad-mouthing, ballot-stuffing and intelligent behavior attacks. Dishonest recommendation attacks are difficult to be detected due to the assumption that trusted nodes are also honest in giving recommendations. This assumption is impractical because trusted nodes with certain trust properties such as good or high forwarding rate could act maliciously by giving bad recommendations. Therefore, an effective and honest recommendation model is needed in order to mitigate and eliminate dishonest recommendation attacks.

Most of the existing trust and reputation models are lack in behavioral-based trust information characteristics and some of them only rely on single trust metric such as packets forwarding rate or node cooperation to evaluate trustworthiness of a node. Besides, many of the existing models also focus too much on trust information which are derived from quality-of-service (QoS) and neglecting the importance of other sources of trust information such as in social networks and mobile ad hoc networks. Neglecting these trust information may cause information scarcity due to the limited trust information available in the network. This scarcity of trust information may leads to inaccuracy of node trustworthiness evaluation which in turn affecting the security of routing in WSNs. Therefore, utilizing and considering other sources of trust information are necessary in order to ensure the availability of more trust information for node trustworthiness evaluation process. Providing more trust information in the network not only can help node to make more informed and effective decision making, but also can help to secure the routing process in WSNs.

1.2 Background and Motivations

In the past few years, many trust and reputation models have been proposed to improve security in WSNs where nodes in the network are allowed to evaluate their neighboring nodes using direct observation (direct experience) or indirect observation (recommendations) (Khalid et al., 2013; Román et al., 2009). Trust and reputation-based approaches have been proven to effectively mitigate and isolate malicious node by monitoring any suspicious or malicious activities such as packet dropping and packet misroute. It is irrefutable that current existing trust and reputation models have significant contributions on improving the security of WSNs. However, many of the existing models are lack in providing accurate mechanism to evaluate node trustworthiness due to the limited trust information used to compute node trust value. In addition, since majority of existing models solicit information through recommendations, dishonest recommendations problems become one of the challenging task need to be addressed. Furthermore, many of the existing models are also focus too much on detection of malicious nodes by using QoS types of trust information and neglecting other sources of trust information. These are among the problems that contribute to the inaccuracy in node trustworthiness evaluation. To the best of our knowledge, current solutions to tackle these problems are still immature and inadequate. We acknowledge that this is the main research gap that need to be fulfilled and therefore rigorous studies and investigation are needed in order to bridge this gap.

In this thesis, a Trust and Reputation Model for WSNs called TReM-WSN has been proposed to evaluate the trustworthiness of nodes before initiating secure communication. Inspired by the Ant colony system (ACS) we develop our model using the combination of ACS trust information with QoS trust information. Specifically, we integrate the ACS trust information with QoS trust information with aim to improve the accuracy on selection of next relay node for data routing in WSNs. Nowadays, ant colony system has been used in many applications including travelling salesman problem, mobile ad hoc networks, peer-to-peer networks and optimization applications. Several work also have been done in WSNs in order to secure the routing

process (Kaur & Kaur, 2017; Song & Yao, 2017; Y. Sun et al., 2017). However, their work are limited to route discovery and optimal path discovery without considering the accuracy on the selection of trustworthy node. In this thesis, we also proposed an honest Recommendation Trust Model called RecommTM in order to mitigate and isolate dishonest recommender nodes by using social trust information. Moreover, we also extend the work done in the TReM-WSN and RecommTM models by integrating trust information from ACS, QoS and Online Social Network (OSN) in the new proposed model called Trust and Reputation Model - Social, QoS and ACS (TRM-SQA).

1.3 Problem Statement

The reliability of delivering data in multi-hop network becomes one of the important security issues in WSNs due to malicious nodes reside along the routing path from source to destination node. Secure routing via trust and reputation technique has been proposed as an effective solution to monitor, detect and isolate malicious nodes while searching for secure route to destination (Alzaid et al., 2008a; Gomez & Perez, 2011). However, existing proposed models for routing in WSNs are insecure due to inaccurate node's trustworthiness evaluation which cause node to accidentally choose a malicious node during routing process which significantly cause poor security and network performances.

Recommendation-based trust approach plays an important role in helping nodes to make more informed decisions on selection of trustworthy recommender nodes. Recommendation-based trust models have been proven to be effective security solution for trust establishment and identifying of malicious nodes (Chen et al., 2012; Iltaf et al., 2012; Luo et al., 2009; Shabut et al., 2015). Is undeniable that recommendation-based model can help node to detect and isolate potential unsecure path and untrusted nodes. However, gathering information by using recommendation can be challenging and difficult task due to dishonest recommendation attacks such as bad-mouthing, ballot-stuffing and collusion attacks (Chen et al., 2012; Shabut et al., 2015; Zouridaki et al., 2009). Most of the existing models assumed that a node with high forwarding rate or high trust value will cooperates and behaves honestly in giving recommendations. This assumption seems unrealistic since such node can acts maliciously by giving bad or dishonest recommendations. In addition, most of the existing recommendation-based trust models utilized majority-based rule to filter out dishonest recommender nodes. This approach seems impractical especially when dishonest recommender nodes are in majority. These aforementioned problems may cause misleading in trust evaluation process which significantly affecting the network performance and security performance as well.

In trust and reputation-based model, node trustworthiness evaluation requires other source of behavioral trust information in order to enhance the accuracy on the selection of trustworthy node. In the current trust evaluation models, many of the existing models are focus too much on QoS types of behavioral trust information and less consideration has been put on other source of trust information such as in OSNs. This

lacks of behavioral-based trust information may leads to poor trustworthiness evaluation that significantly cause substantial amount of packet losses and low packet delivery ratio. This lacking of behavioral trust information also makes the model susceptible to routing and dishonest attacks which leads to poor security performance.

1.4 Research Objectives

The main goal of this research is to develop an accurate trust and reputation-based trustworthiness evaluation model which is able to distinguish between malicious and benevolent nodes, mitigate dishonest recommendation attacks and ultimately securing data routing process in WSNs. In order to achieve this, the following objectives are need to be fulfilled:

1. To propose an accurate trust evaluation model for WSNs by utilizing ant colony system algorithm and quality of service trust information in order to improve the node selection accuracy, packet delivery ratio and path length during the routing process.

2. To propose a recommendation-based trust model that able to detect and eliminate dishonest recommendation attacks in order to improve network performance including packet delivery ration and packet loss. The proposed model also aims to enhance security performance by improving recognition proportion and reducing the effect of false positive and false negative proportions.

3. To propose a multidimensional trust and reputation-based model by combining different sources of behavioral trust information adopted from ant colony system, quality of service and online social networks. The utilization of these trust information are mainly to improve the network performance which include packet delivery ratio, packet loss as well as improving security performance through trust value, recognition proportion, false positive proportion and false negative proportion.

1.5 Research Scopes

This research focuses on the work done in trust and reputation domains. The network considered in this research is WSN where nodes in this network are require to communicate or forward packets by using multi-hop communication fashion. To address the problem related to inaccurate node trustworthiness evaluation process, this research focuses on developing a trust computation model by adopting some features and structure from Bio-inspired Trust and Reputation Model for Wireless Sensor Network (BTRM-WSN) model as this model is considered good platform to fulfill some of the design objectives of our models. This research also focused on blackhole and greyhole attacks at the network layer level while other attacks such as bad-mouthing, ballot-stuffing, collusion and newcomer with self-promoting attack are considered in trust and reputation level. Other attacks are beyond the scope of this

thesis. All the proposed models in this research are built onto the routing system where a node requires to gather trust information from its neighboring nodes before making decision whether to interact with the neighboring nodes or not. The ability of our models to accurately evaluate node's trustworthiness value make them secure, robust, scalable and capable to produce good network performance.

1.6 Research Contributions

This research makes use of trust and reputation techniques together with its unique properties and uses WSNs to model the communication and illustrate how trust can be established among nodes in multi-hop communication in WSNs. This research also investigates the state-of-the-art of trust and reputation techniques in three different distributed networks such as OSNs, Mobile Ad Hoc Networks (MANETs) and WSNs. Results from the investigation including trust properties, concepts, characteristics and techniques are discussed and adopted from these networks to our model. This thesis contributes to the knowledge of trust and reputation models in WSNs in the following areas:

1. The proposal of TReM-WSN using ACS and QoS trust information which can improve the accuracy of node selection process in multi-hop communication of WSNs. The inclusion of ACS and QoS trust information in this model can provide shortest routing path solution and also can increase the security to distinguish between malicious and benevolent nodes. Consequently, this also can contributes to the good network performance outcomes.

2. The proposal of an honest recommendation-based trust model called RecommTM. The proposed model uses direct and indirect observations in order to filter out bad and unfair ratings caused by dishonest recommendation attacks such as bad-mouthing, ballot-stuffing and collusion attacks. The proposed model adopted and utilized OSNs trust information including conversation trust, similarity trust and popularity trust to increase the ability of the model to mitigate and isolate dishonest recommender nodes.

3. The proposal of a trust and reputation-based model which uses multiple source of behavioral trust information adopted from ACS, QoS and OSNs in order to improve the node's trustworthiness evaluation process. The proposed trust model utilized QoS and OSNs trust information for peer-to-peer trust evaluation and uses ACS trust information for path trust evaluation. These evaluation processes will be conducted by an evaluating node towards its neighboring nodes during the routing process.

1.7 Thesis Organization

Chapter 1 introduces the work and explains the motivation, research problems, research objectives, research scopes and research contributions.

Chapter 2 reviews the notion of trust, reputation and surveys a number of existing trust models in different domains including OSNs, MANETs and WSNs. Several important attacks that related to trust and reputation model are also reviewed and investigated.

Chapter 3 presents the methodology use to conduct the research. It discusses the research operational framework and presents how the work done phase by phase in detail. It also covers other aspects such as simulator, simulation parameters, simulation environments, performance metrics and several assumptions that have been made in this thesis.

Chapter 4 introduces a trust and reputation model that is used to monitor the behaviors of nodes in WSNs. The model utilized ACS and QoS trust information in order to solve the problem related to inaccurate node trustworthiness evaluation using pheromone trace, distance factor, forwarding trust and consistency trust. These trust information are then will be integrated in the simulator and validated through simulation in order to investigate its impact on security and network performances.

Chapter 5 introduces the proposed recommendation-based trust model that utilized OSNs trust information in order to address the problem related to dishonest recommendation attacks such as bad-mouthing, ballot-stuffing and collusion attacks. This chapter also introduces several algorithms that are useful to detect and minimize the impact of dishonest recommendation attacks.

Chapter 6 introduces a hybrid trust and reputation model for WSNs. The model utilized the OSNs, QoS and ACS trust information including pheromone trace, distance factor, interaction trust, popularity trust, familiarity trust, forwarding trust and consistency trust. The combination of these trust information will be measured through appropriate trust metrics based on the behaviors and characteristics of the nodes in WSNs.

Chapter 7 summarizes the contributions and concluding remarks of this thesis and makes some recommendations for future work.

REFERENCES

Abdul-Rahman, A., & Hailes, S. (2000). Supporting Trust in Virtual Communities. In *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences*, Maui, Hawaii, USA.

Abdullah, M. D. H., Hanapi, Z. M., Zukarnain, Z. A., & Mohamed, M. A. (2015). Attacks, Vulnerabilities and Security Requirements in Smart Metering Networks. *KSII Transactions on Internet and Information Systems (TIIS), 9*(4), 1493-1515.

Aberer, K., & Despotovic, Z. (2001). Managing trust in a peer-2-peer information system. In *Proceedings of the Proceedings of the tenth international conference on Information and knowledge management*.

Abkenar, G. S., Shokouhifar, M., & SajediAbkenar, A. (2011). Intelligent Ant Based Routing Algorithm (IARA) in Mobile Ad hoc Networks. In *Proceedings of the IEEE 5th International Conference on Advanced Networks and Telecommunication Systems (ANTS)*, Bangalore, India.

Abu-Ghazaleh, N., Kang, K.-D., & Liu, K. (2005). Towards resilient geographic routing in WSNs. In *Proceedings of the Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks*, Montreal, Quebec, Canada.

Adali, S., Escriva, R., Goldberg, M. K., Hayvanovych, M., Magdon-Ismail, M., Szymanski, B. K., . . . Williams, G. (2010). Measuring behavioral trust in social networks. In *Proceedings of the 2010 IEEE International Conference on Intelligence and Security Informatics*.

Alzaid, H. (2011). *Secure Data Aggregation in Wireless Sensor Networks.* (Ph.D Thesis), Queensland University of Technology.

Alzaid, H., Alfaraj, M., Ries, S., Jøsang, A., Albabtain, M., & Abuhaimed, A. (2013). Reputation-Based Trust Systems for Wireless Sensor Networks: A Comprehensive Review. In *Proceedings of the 7th International Conference Trust Management*, Berlin, Heidelberg.

Alzaid, H., Foo, E., & Nieto, J. G. (2008a). RSDA: Reputation-based Secure Data Aggregation in Wireless Sensor Networks. In *Proceedings of the Ninth International Conference on Parallel and Distributed Computing, Applications and Technologies, PDCAT 2008*, Dunedin, New Zealand.

Alzaid, H., Foo, E., & Nieto, J. G. (2008b). Secure Data Aggregation in Wireless Sensor Network: A Survey. In *Proceedings of the Sixth Australasian Conference on Information Security (AISC '08)*, Darlinghurst, Australia.

Anbuchelian, S., Lokesh, S., & Baskaran, M. (2016). Improving security in Wireless Sensor Network using trust and metaheuristic algorithms. In *Proceedings of the 2016 3rd International Conference on Computer and Information Sciences (ICCOINS).*

Anderegg, L., & Eidenbenz, S. (2003). Ad hoc-VCG: a truthful and cost-efficient routing protocol for mobile ad hoc networks with selfish agents. In *Proceedings of the 9th annual international conference on Mobile computing and networking*.

Arivazhagu, U. V., & Srinivasan, S. (2012). Ant Colony Optimization of Semantic Query Routing in Peer to Peer Networks. In *Proceedings of the Fourth International Conference on Advanced Computing (ICoAC)*, Chennai, India.

Azzedin, F., & Maheswaran, M. (2002). Evolving and Managing Trust in Grid Computing Systems. In *Proceedings of the IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, Winnipeg, Manitoba, Canada.

Bao, F., Chen, I. R., Chang, M., & Cho, J. H. (2012). Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection. *IEEE Transactions on Network and Service Management, 9*(2), 169-183. doi: 10.1109/TCOMM.2012.031912.110179

Bi, Z. (2013). An integrated environment for visualization of distributed wireless sensor networks. In *Proceedings of the 2013 10th IEEE International Conference on Control and Automation (ICCA)*.

Biswas, S., Dey, P., & Neogy, S. (2012). Trusted Checkpointing Based on Ant Colony Optimization in MANET. In *Proceedings of the Third International Conference on Emerging Applications of Information Technology (EAIT)*, Kolkata, India.

Boukerche, Xu, L., & El-Khatib, K. (2007). Trust-based Security for Wireless Ad Hoc and Sensor Networks. *Computer Communications, 30*(11), 2413-2427.

Boukerche, A., & Ren, Y. (2008). A Trust-based Security System for Ubiquitous and Pervasive Computing Environments. *Computer Communications, 31*(18), 4343-4351.

Boukerche, A., & Xu, L. (2005). An Agent-based Trust and Reputation Management Scheme for Wireless Sensor Networks. In *Proceedings of the IEEE Global Telecommunications Conference, 2005. GLOBECOM '05*, St. Louis, MO, USA.

Bradai, A., Bradai. (2014). *Secured trust and reputation system : analysis of malicious behaviors and optimization.* Institut National des Télécommunications. Retrieved from https://tel.archives-ouvertes.fr/tel-01127164 StarCnrsInstitut-telecomTelecom-sudparis database. (2014TELE0019)

Buchegger, S., & Boudec, J.-Y. (2003). A Robust Reputation System for Mobile Ad-hoc Networks.

Buchegger, S., & Boudec, J.-Y. L. (2002). Performance Analysis of the CONFIDANT Protocol. In *Proceedings of the 3rd ACM International Symposium on Mobile ad hoc Networking and Computing*, Lausanne, Switzerland.

C'Ceres, E. N., Fingler, H., Mongelli, H., & Song, S. W. (2012). Ant Colony System Based Solutions to the Quadratic Assignment Problem on GPGPU. In *Proceedings of the 2012 41st International Conference on Parallel Processing Workshops (ICPPW)*, Pittsburgh, PA, USA.

Cahill, V., Gray, E., Seigneur, J.-M., Jensen, C. D., Chen, Y., Shand, B., . . . English, C. (2003). Using trust for secure collaboration in uncertain environments. *IEEE Pervasive Computing, 2*(3), 52-61.

Cao, X., Wang, X., & Lin, X. (2016). Design and implementation of a centralized routing protocol for wireless sensor network. In *Proceedings of the 2016 10th International Conference on Sensing Technology (ICST)*.

Caverlee, J., Liu, L., & Webb, S. (2008). Socialtrust: tamper-resilient trust establishment in online communities. In *Proceedings of the Proceedings of the 8th ACM/IEEE-CS joint conference on Digital libraries*, Pittsburgh PA, PA, USA.

Chen. (2009). Task-based trust management for wireless sensor networks. *International Journal of Security and its applications, 3*(2), 21-26.

Chen, Wu, H., Zhou, X., & Gao, C. (2007). Agent-Based Trust Model in Wireless Sensor Networks. In *Proceedings of the Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing-Volume 03*.

Chen, Zhang, Y., Liu, Q., & Feng, J. (2012). Dealing with dishonest recommendation: The trials in reputation management court. *Ad Hoc Networks, 10*(8), 1603-1618. doi: http://dx.doi.org/10.1016/j.adhoc.2011.07.014

Chen, J., & Wu, J. (2010). A survey on cryptography applied to secure mobile ad hoc networks and wireless sensor networks. *Handbook of Research on Developments and Trends in Wireless Sensor Networks: From Principle to Practice*, 262-289.

Cho, J. H., Alsmadi, I., & Xu, D. (2016). Privacy and Social Capital in Online Social Networks. In *Proceedings of the 2016 IEEE Global Communications Conference (GLOBECOM)*.

Correia, S. L. O. B., Celestino, J., & Cherkaoui, O. (2011). Mobility-aware Ant Colony Optimization Routing for Vehicular Ad hoc Networks. In *Proceedings of the 2011 IEEE Wireless Communications and Networking Conference (WCNC)*, Cancun, Quintana Roo.

Crosby, G. V., Hester, L., & Pissinou, N. (2011). Location-aware, Trust-based Detection and Isolation of Compromised Nodes in Wireless Sensor Networks. *IJ Network Security, 12*(2), 107-117.

Cui, H., Li, J., Li, Z., Pan, D., & He, Y. (2016). Distributed Interference-Aware Cooperative Random Access in Multi-Hop Wireless Networks. *IEEE Access, 4*, 4823-4828. doi: 10.1109/ACCESS.2016.2594767

Daly, E. M., & Haahr, M. (2009). Social Network Analysis for Information Flow in Disconnected Delay-Tolerant MANETs. *IEEE Transactions on Mobile Computing, 8*(5), 606-621. doi: 10.1109/TMC.2008.161

Dasgupta, P. (2000). Trust as a Commodity. *Journal of Trust: Making and Breaking Cooperative Relations, 4*, 49-72.

Deneubourg, J.-L., & Goss, S. (1989). Collective Patterns and Decision-Making. *Ethology Ecology & Evolution, 1*(4), 295-311.

Dorigo, M., Birattari, M., & Stutzle, T. (2006). Ant Colony Optimization. *IEEE Computational Intelligence Magazine, 1*(4), 28-39.

Dorigo, M., Bonabeau, E., & Theraulaz, G. (2000). Ant Algorithms and Stigmergy. *Future Generation Computer Systems, 16*(8), 851-871.

Dorigo, M., & Gambardella, L. M. (1997). Ant Colony System: A Cooperative Learning Approach to the Traveling Salesman Problem. *IEEE Transactions on Evolutionary Computation, 1*(1), 53-66.

Dorigo, M., Maniezzo, V., & Colorni, A. (1996). Ant System: Optimization by A Colony of Cooperating Agents. *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics, 26*(1), 29-41.

Dorigo, M., & Stützle, T. (2003). The Ant Colony Optimization Metaheuristic: Algorithms, Applications and Advances *Handbook of Metaheuristics* (pp. 250-285): Springer.

Douceur, J. R. (2002). The sybil attack. In *Proceedings of the International Workshop on Peer-to-Peer Systems*.

Du, W., Lin, H., Sun, J., Yu, B., & Yang, H. (2016). A new trust model for online social networks. In *Proceedings of the 2016 First IEEE International Conference on Computer Communication and the Internet (ICCCI)*.

Eirinaki, M., Louta, M. D., & Varlamis, I. (2014). A Trust-Aware System for Personalized User Recommendations in Social Networks. *IEEE Transactions on Systems, Man, and Cybernetics: Systems, 44*(4), 409-421. doi: 10.1109/TSMC.2013.2263128

Falcão, E. d. L., Brasileiro, F., Brito, A., & Vivas, J. L. (2016). Enhancing P2P Cooperation through Transitive Indirect Reciprocity. In *Proceedings of the 2016 IEEE 36th International Conference on Distributed Computing Systems Workshops (ICDCSW)*.

Fejzagic, E., & Oputic, A. (2013). Performance Comparison of Sequential and Parallel Execution of the Ant Colony Optimization Algorithm for Solving the Traveling Salesman Problem. In *Proceedings of the 2013 36th International Convention on Information & Communication Technology Electronics & Microelectronics (MIPRO)*, Opatija, Croatia.

Ferrandis, D. T., Climent, S. S., & Payá, V. M. S. (2012). Enabling quick deployment wireless sensor networks for smart cities. In *Proceedings of the 2012 9th IEEE International Workshop on Factory Communication Systems*.

Gambetta, D. (2000). Can We Trust Trust? *Trust: Making and breaking cooperative relations*, 213-237.

Ganeriwal, S., Balzano, L. K., & Srivastava, M. B. (2008). Reputation-based framework for high integrity sensor networks. *ACM Transactions on Sensor Networks (TOSN), 4*(3), 15.

Ganeriwal, S., & Srivastava, M. B. (2004). Reputation-based framework for high integrity sensor networks. In *Proceedings of the Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks*, Washington DC, USA.

Gaware, A., & Dhonde, S. B. (2016). A survey on security attacks in wireless sensor networks. In *Proceedings of the 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*.

Gerrigagoitia, K., Uribeetxeberria, R., Zurutuza, U., & Arenaza, I. (2012). Reputation-based Intrusion Detection System for wireless sensor networks. In *Proceedings of the 2012 Complexity in Engineering (COMPENG). Proceedings*.

Gheorghe, L., Rughiniş, R., & Tătăroiu, R. (2013). Adaptive Trust Management Protocol based on intrusion detection for Wireless Sensor Networks. In *Proceedings of the 2013 RoEduNet International Conference 12th Edition: Networking in Education and Research*.

Golbeck, J., & Hendler, J. (2004). Accuracy of metrics for inferring trust and reputation in semantic web-based social networks. In *Proceedings of the International Conference on Knowledge Engineering and Knowledge Management*.

Golbeck, J., & Hendler, J. (2006). Inferring binary trust relationships in Web-based social networks. *ACM Trans. Internet Technol., 6*(4), 497-529. doi: 10.1145/1183463.1183470

Golbeck, J., & Hendler, J. A. (2004). Reputation Network Analysis for Email Filtering. In *Proceedings of the CEAS*.

Golbeck, J. A. (2005). *Computing and applying trust in web-based social networks.* University of Maryland at College Park.

Gómez-Vilardebó, J. (2017). Routing in Accumulative Multi-Hop Networks. *IEEE/ACM Transactions on Networking, PP*(99), 1-14. doi: 10.1109/TNET.2017.2703909

Gómez, Martínez Pérez, G., & Gómez Skarmeta, A. F. (2009). TACS, a Trust Model for P2P Networks. *Wireless Personal Communications, 51*(1), 153-164. doi: 10.1007/s11277-008-9596-9

Gomez, F. M., & Perez, G. M. (2011). Providing Trust in Wireless Sensor Networks Using a Bio-Inspired Technique. *Telecommunication Systems, 46*(2), 163-180.

Goss, S., Aron, S., Deneubourg, J.-L., & Pasteels, J. M. (1989). Self-organized Shortcuts in The Argentine Ant. *Naturwissenschaften, 76*(12), 579-581.

Granovetter, M. S. (1973). The strength of weak ties. *American journal of sociology, 78*(6), 1360-1380.

Grassé, P.-P. (1959). La reconstruction du nid et les coordinations interindividuelles chezBellicositermes natalensis etCubitermes sp. la théorie de la stigmergie: Essai d'interprétation du comportement des termites constructeurs. *Insectes Sociaux, 6*(1), 41-80. doi: 10.1007/BF02223791

Guo, L., Zhang, C., & Fang, Y. (2015). A Trust-Based Privacy-Preserving Friend Recommendation Scheme for Online Social Networks. *IEEE Transactions on Dependable and Secure Computing, 12*(4), 413-427. doi: 10.1109/TDSC.2014.2355824

Gupta, M., Judge, P., & Ammar, M. (2003). A reputation system for peer-to-peer networks. In *Proceedings of the Proceedings of the 13th international workshop on Network and operating systems support for digital audio and video*, Monterey, CA, USA.

Haiguang, C., Huafeng, W., Jinchu, H., & Chuanshan, G. (2008). Agent-Based Trust Management Model for Wireless Sensor Networks. In *Proceedings of the International Conference on Multimedia and Ubiquitous Engineering, 2008. MUE 2008*, Busan, South Korea.

Hamdi, S., Gancarski, A. L., Bouzeghoub, A., & Yahia, S. B. (2012). IRIS: A Novel Method of Direct Trust Computation for Generating Trusted Social Networks. In *Proceedings of the 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*.

Han, G., Jiang, J., Shu, L., Niu, J., & Chao, H.-C. (2014). Management and applications of trust in Wireless Sensor Networks: A survey. *Journal of Computer and System Sciences, 80*(3), 602-617. doi: http://dx.doi.org/10.1016/j.jcss.2013.06.014

Hernandez-Orallo, E., Serrat, M. D., Cano, J. C., Calafate, C. T., & Manzoni, P. (2012). Improving Selfish Node Detection in MANETs Using a Collaborative Watchdog. *IEEE Communications Letters, 16*(5), 642-645. doi: 10.1109/LCOMM.2012.030912.112482

Hoffman, K., Zage, D., & Nita-Rotaru, C. (2007). A Survey of attacks on Reputation Systems.

Hsu, C. H., Lin, C. T., Tserng, H. P., & Han, J. Y. (2014). An implementation of light-weight compression algorithm for wireless sensor network technology in structure health monitoring. In *Proceedings of the 2014 IEEE World Forum on Internet of Things (WF-IoT).*

Hu, H., Lu, R., Zhang, Z., & Shao, J. (2017). REPLACE: A Reliable Trust-Based Platoon Service Recommendation Scheme in VANET. *IEEE Transactions on Vehicular Technology, 66*(2), 1786-1797. doi: 10.1109/TVT.2016.2565001

Hu, J., Wu, Q., & Zhou, B. (2008). RBTrust: A Recommendation Belief Based Distributed Trust Management Model for P2P Networks. In *Proceedings of the High Performance Computing and Communications, 2008. HPCC '08. 10th IEEE International Conference on*.

Hualin, Z., Mengxia, W., Baoyu, W., Jibu, H., & Zhiqiang, X. (2016). Research and development of general data acquisition system based on wireless sensor network dynamic network technology. In *Proceedings of the 2016 IEEE International Conference of Online Analysis and Computing Science (ICOACS).*

Hung, K.-S., Lui, K.-S., & Kwok, Y.-K. (2007). A trust-based geographical routing scheme in sensor networks. In *Proceedings of the Wireless Communications and Networking Conference, 2007. WCNC 2007. IEEE*.

Iltaf, N., Ghafoor, A., & Zia, U. (2012). An attack resistant method for detecting dishonest recommendations in pervasive computing environment. In *Proceedings of the 2012 18th IEEE International Conference on Networks (ICON).*

Islam, N., & Shaikh, Z. A. (2013). Security Issues in Mobile Ad Hoc Network. In S. Khan & A.-S. Khan Pathan (Eds.), *Wireless Networks and Security: Issues, Challenges and Research Trends* (pp. 49-80). Berlin, Heidelberg: Springer Berlin Heidelberg.

Jafari, R., Encarnacao, A., Zahoory, A., Dabiri, F., Noshadi, H., & Sarrafzadeh, M. (2005). Wireless sensor networks for health monitoring. In *Proceedings of the The Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services*.

Janzadeh, H., Fayazbakhsh, K., Dehghan, M., & Fallah, M. S. (2009). A secure credit-based cooperation stimulating mechanism for MANETs using hash chains. *Future Generation Computer Systems, 25*(8), 926-934. doi: http://dx.doi.org/10.1016/j.future.2008.12.002

Jiang, Han, G., Wang, F., Shu, L., & Guizani, M. (2015). An Efficient Distributed Trust Model for Wireless Sensor Networks. *IEEE Transactions on Parallel and Distributed Systems, 26*(5), 1228-1237. doi: 10.1109/TPDS.2014.2320505

Jiang, J., Han, G., Zhu, C., Chan, S., & Rodrigues, J. J. P. C. (2017). A Trust Cloud Model for Underwater Wireless Sensor Networks. *IEEE Communications Magazine, 55*(3), 110-116. doi: 10.1109/MCOM.2017.1600502CM

Jiang, W., & Wu, J. (2014). Trust Models in Wireless Sensor Networks and Online Social Networks: A Comparative Study. In *Proceedings of the 2014 IEEE 11th International Conference on Mobile Ad Hoc and Sensor Systems*.

Jøsang, A. (1999). An Algebra for Assessing Trust in Certification Chains. In *Proceedings of the NDSS*.

Jøsang, A., Ismail, R., & Boyd, C. (2007). A Survey of Trust and Reputation Systems for Online Service Provision. *Journal of Decision Support Systems, 43*(2), 618-644.

Kamvar, Schlosser, M. T., & Garcia-Molina, H. (2003). The Eigentrust algorithm for reputation management in P2P networks. In *Proceedings of the Proceedings of the 12th international conference on World Wide Web*, Budapest, Hungary. http://dl.acm.org/citation.cfm?doid=775152.775242

Kandah, F. I., Nichols, O., & Li, Y. (2017). Efficient key management for Big Data gathering in dynamic sensor networks. In *Proceedings of the 2017 International Conference on Computing, Networking and Communications (ICNC)*.

Kannhavong, B., Nakayama, H., Nemoto, Y., Kato, N., & Jamalipour, A. (2007). A survey of routing attacks in mobile ad hoc networks. *IEEE Wireless Communications, 14*(5), 85-91. doi: 10.1109/MWC.2007.4396947

Karia, D. C., & Godbole, V. V. (2013). New Approach for Routing in Mobile Ad-hoc Networks Based on Ant Colony Optimisation with Global Positioning System. *IET Networks, 2*(3), 171-180. doi: 10.1049/iet-net.2012.0087

Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: attacks and countermeasures. *Ad Hoc Networks, 1*(2–3), 293-315. doi: http://dx.doi.org/10.1016/S1570-8705(03)00008-8

Kazemi, B., Ahmadi, M., & Talebi, S. (2013). Optimum and Reliable Routing in VANETs: An Opposition Based Ant Colony Algorithm Scheme. In *Proceedings of the 2013 International Conference on Connected Vehicles and Expo (ICCVE)*, Las Vegas, NV.

Kesavan, V. T., & Radhakrishnan, S. (2012). Secret Key Cryptography based Security Approach for Wireless Sensor Networks. In *Proceedings of the 2012 International Conference on Recent Advances in Computing and Software Systems*.

Khalid, O., Khan, S. U., Madani, S. A., Hayat, K., Khan, M. I., Min-Allah, N., . . . Chen, D. (2013). Comparative Study of Trust and Reputation Systems for Wireless Sensor Networks. *Security and Communication Networks, 6*(6), 669-688. doi: 10.1002/sec.597

Khalil, I., & Bagchi, S. (2011). Stealthy Attacks in Wireless Ad Hoc Networks: Detection and Countermeasure. *IEEE Transactions on Mobile Computing, 10*(8), 1096-1112. doi: 10.1109/TMC.2010.249

Khan, F., Memon, S., Jokhio, I. A., & Jokhio, S. H. (2015). Wireless sensor network based flood/drought forecasting system. In *Proceedings of the 2015 IEEE SENSORS*.

Kinateder, M., Baschny, E., & Rothermel, K. (2005). Towards a Generic Trust Model–Comparison of Various Trust Update Algorithms *Trust Management* (pp. 177-192): Springer.

Kuen-Han, L., Jenq-Shiou, L., & Hoek, J. (2013). Ant-Based On-Demand Clustering Routing Protocol for Mobile Ad-Hoc Networks. In *Proceedings of the 2013 Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS)*, Taichung, China.

Kuter, U., & Golbeck, J. (2007). SUNNY: a new algorithm for trust inference in social networks using probabilistic confidence models. In *Proceedings of the Proceedings of the 22nd national conference on Artificial intelligence - Volume 2*, Vancouver, British Columbia, Canada.

Labraoui, N. (2015). A Reliable Trust Management Scheme in Wireless Sensor Networks. In *Proceedings of the 12th International Symposium on Programming and Systems (ISPS), 2015*, Algiers.

Laizhong, C., Peng, O., Nan, L., & Guanjing, Z. (2016). A comprehensive trust-based item evaluation model for recommendation in social network. In *Proceedings of the 2016 IEEE Symposium on Computers and Communication (ISCC)*.

Le, X. H., Lee, S., Butun, I., Khalid, M., Sankar, R., Kim, M., . . . Lee, H. (2009). An energy-efficient access control scheme for wireless sensor networks based on elliptic curve cryptography. *Journal of Communications and Networks, 11*(6), 599-606. doi: 10.1109/JCN.2009.6388413

Lei, Y., Zhiguang, Q., Can, W., Yao, L., & ChaoSheng, F. (2010). A P2P Reputation Model Based on Ant Colony Algorithm. In *Proceedings of the 2010 International Conference on Communications, Circuits and Systems (ICCCAS)* Chengdu, China.

Li, & Lui, J. C. S. (2014). Friends or Foes: Distributed and Randomized Algorithms to Determine Dishonest Recommenders in Online Social Networks. *IEEE Transactions on Information Forensics and Security, 9*(10), 1695-1707. doi: 10.1109/TIFS.2014.2346020

Li, R., Li, J., Liu, P., & Kato, J. (2009). A Novel Hybrid Trust Management Framework for MANETs. In *Proceedings of the 2009 29th IEEE International Conference on Distributed Computing Systems Workshops*.

Li, X., Huang, H., & Sun, Y. (2016). DriTri: An in-vehicle wireless sensor network platform for daily health monitoring. In *Proceedings of the 2016 IEEE SENSORS*.

Lin, Y., Zhang, J., Chung, H.-H., Ip, W. H., Li, Y., & Shi, Y.-H. (2012). An Ant Colony Optimization Approach for Maximizing the Lifetime of Heterogeneous Wireless Sensor Networks. *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, 42*(3), 408-420.

Liu, Pang, L., Pei, Q., Ma, H., & Peng, Q. (2009). Distributed Event-Triggered Trust Management for Wireless Sensor Networks. In *Proceedings of the 2009 Fifth International Conference on Information Assurance and Security*.

Liu, Zhang, Z., Liu, S., Ke, Y., & Chen, J. (2011). A Trust Model Based on Bayes Theorem in WSNs. In *Proceedings of the 2011 7th International Conference on Wireless Communications, Networking and Mobile Computing*.

Liu, J., & Issarny, V. (2006). An incentive compatible reputation mechanism for ubiquitous computing environments. In *Proceedings of the Proceedings of the 2006 International Conference on Privacy, Security and Trust: Bridge the Gap Between PST Technologies and Business Services*, Markham, Ontario, Canada.

Liu, W., & Zhou, Y. (2010). An Effective Hybrid Ant Colony Algorithm for Solving the Traveling Salesman Problem. In *Proceedings of the 2010 International Conference on Intelligent Computation Technology and Automation (ICICTA)*, Changsha, China.

Louw, J., Niezen, G., Ramotsoela, T. D., & Abu-Mahfouz, A. M. (2016). A key distribution scheme using elliptic curve cryptography in wireless sensor networks. In *Proceedings of the 2016 IEEE 14th International Conference on Industrial Informatics (INDIN)*.

Lu, R., Lin, X., Zhang, C., Zhu, H., Ho, P. H., & Shen, X. (2008). AICN: An Efficient Algorithm to Identify Compromised Nodes in Wireless Sensor Network. In *Proceedings of the 2008 IEEE International Conference on Communications*.

Lu, R., Lin, X., Zhu, H., Zhang, C., Ho, P. H., & Shen, X. (2008). A Novel Fair Incentive Protocol for Mobile Ad Hoc Networks. In *Proceedings of the 2008 IEEE Wireless Communications and Networking Conference*.

Luo, J., Liu, X., & Fan, M. (2009). A trust model based on fuzzy recommendation for mobile ad-hoc networks. *Computer Networks, 53*(14), 2396-2407. doi: http://dx.doi.org/10.1016/j.comnet.2009.04.008

Maarouf, I., Baroudi, U., & Naseer, A. R. (2009). Efficient Monitoring Approach for Reputation System-based Trust-aware Routing in Wireless Sensor Networks. *Communications, IET, 3*(5), 846-858.

Maarouf, I., Baroudi, U., & Naseer, A. R. (2010). Cautious Rating for Trust-enabled Routing in Wireless Sensor Networks. *EURASIP Journal on Wireless Communications and Networking, 1*, 1-16.

Maheswaran, M., Tang, H. C., & Ghunaim, A. (2007). Towards a Gravity-Based Trust Model for Social Networking Systems. In *Proceedings of the Distributed Computing Systems Workshops, 2007. ICDCSW '07. 27th International Conference on*.

Mármol, F. G., & Pérez, G. M. (2009). TRMSim-WSN, Trust and Reputation Models Simulator for Wireless Sensor Networks. In *Proceedings of the IEEE International Conference on Communications, ICC'09*.

Marsden, P. V., & Campbell, K. E. (1984). Measuring tie strength. *Soc. F., 63*, 482.

Marti, S., Giuli, T. J., Lai, K., & Baker, M. (2000). Mitigating routing misbehavior in mobile ad hoc networks. In *Proceedings of the Proceedings of the 6th annual international conference on Mobile computing and networking*, Boston, Massachusetts, USA.

Mathur, A., Newe, T., & Rao, M. (2016). Defence against Black Hole and Selective Forwarding Attacks for Medical WSNs in the IoT. *Sensors, 16*(1), 118.

McKnight, D. H., & Chervany, N. L. (1996). The meanings of trust.

Mehmood, U., Mansoor, U., Dong Yeop, H., Ki-Hyung, K., Taekkyeun, L., & Seung Wha, Y. (2012). Wireless Sensor Networks for integrated search and rescue efforts for disaster hit areas. In *Proceedings of the 2012 Fourth International Conference on Ubiquitous and Future Networks (ICUFN)*.

Meng, W., Xia, H., & Song, H. (2009). A Dynamic Trust Model Based on Recommendation Credibility in Grid Domain. In *Proceedings of the Computational Intelligence and Software Engineering, 2009. CiSE 2009*.

Michiardi, P., & Molva, R. (2002). Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks *Advanced communications and multimedia security* (pp. 107-121): Springer.

Momani, M., & Challa, S. (2010). Survey of trust models in different network domains. *arXiv preprint arXiv:1010.0168*.

Mouhoub, M., & Zhijie, W. (2008). Improving the Ant Colony Optimization Algorithm for the Quadratic Assignment Problem. In *Proceedings of the IEEE Congress on Evolutionary Computation, 2008. CEC 2008. (IEEE World Congress on Computational Intelligence)*, Hong Kong.

Nadir, I., Zegeye, W. K., Moazzami, F., & Astatke, Y. (2016). Establishing symmetric pairwise-keys using public-key cryptography in Wireless Sensor Networks (WSN). In *Proceedings of the 2016 IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*.

Naseer, A. (2012). *Reputation System Based Trust-Enabled Routing for Wireless Sensor Networks*: INTECH, Open Access Publisher.

Nepal, S., Sherchan, W., & Paris, C. (2011). STrust: A Trust Model for Social Networks. In *Proceedings of the 2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications*.

Ortiz, A. M., Royo, F., Olivares, T., Timmons, N., Morrison, J., & Orozco-Barbosa, L. (2013). Intelligent routing strategies in wireless sensor networks for smart cities applications. In *Proceedings of the 2013 10th IEEE International Conference on Networking, Sensing and Control (ICNSC)*.

Padmavathi, D. G., & Shanmugapriya, M. (2009). A survey of attacks, security mechanisms and challenges in wireless sensor networks. *arXiv preprint arXiv:0909.0576*.

Pawgasame, W. (2016). A survey in adaptive hybrid wireless Sensor Network for military operations. In *Proceedings of the 2016 Second Asian Conference on Defence Technology (ACDT)*.

Pirzada, A. A., & McDonald, C. (2004). Establishing trust in pure ad-hoc networks. In *Proceedings of the Proceedings of the 27th Australasian conference on Computer science - Volume 26*, Dunedin, New Zealand.

Poovendran, R., & Lazos, L. (2007). A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks. *Wireless Networks, 13*(1), 27-59.

Prabhakar, M., Singh, J. N., & Mahadevan, G. (2013). Defensive Mechanism for VANET Security in Game Theoretic Approach Using Heuristic Based Ant Colony Optimization. In *Proceedings of the 2013 International Conference on Computer Communication and Informatics (ICCCI)*, Coimbatore, India.

Qin, D., Yang, S., Jia, S., Zhang, Y., Ma, J., & Ding, Q. (2017). Research on Trust Sensing based Secure Routing Mechanism for Wireless Sensor Network. *IEEE Access, PP*(99), 1-1. doi: 10.1109/ACCESS.2017.2706973

Quercia, D., Hailes, S., & Capra, L. (2006). B-trust: Bayesian Trust Framework for Pervasive Computing *Trust Management* (pp. 298-312): Springer.

Rashid, S., Akram, U., Qaisar, S., Khan, S. A., & Felemban, E. (2014). Wireless Sensor Network for Distributed Event Detection Based on Machine Learning. In *Proceedings of the 2014 IEEE International Conference on Internet of Things (iThings), and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom)*.

Reddy, V. B., Venkataraman, S., & Negi, A. (2017). Communication and Data Trust for Wireless Sensor Networks Using D-S Theory. *IEEE Sensors Journal, 17*(12), 3921-3929. doi: 10.1109/JSEN.2017.2699561

Ren, Y., & Boukerche, A. (2008). Modeling and Managing the Trust for Wireless and Mobile Ad Hoc Networks. In *Proceedings of the IEEE International Conference on Communications, 2008. ICC'08.* , Beijing, China.

Román, R., Fernandez-Gago, C., López, J., & Chen, H. H. (2009). Trust and Reputation Systems for Wireless Sensor Networks. *Security and Privacy in Mobile and Wireless Networking*, 105-128.

Roy, S., & Nene, M. J. (2015). A security framework for military application on infrastructure based wireless sensor network. In *Proceedings of the 2015 IEEE International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN)*.

Ruohomaa, S., Kutvonen, L., & Koutrouli, E. (2007). Reputation Management Survey. In *Proceedings of the Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on*.

Saqib, N., & Iqbal, U. (2016). Security in wireless sensor networks using ECC. In *Proceedings of the 2016 IEEE International Conference on Advances in Computer Applications (ICACA)*.

Sen, J. (2010). *Reputation-and trust-based systems for wireless self-organizing networks*: Aurbach Publications, CRC Press, USA.

Shabut, A. M., Dahal, K. P., Bista, S. K., & Awan, I. U. (2015). Recommendation Based Trust Model with an Effective Defence Scheme for MANETs. *IEEE Transactions on Mobile Computing, 14*(10), 2101-2115.

Shang-Fu, G., & Jian-Lei, Z. (2012). A Survey of Reputation and Trust Mechanism in Peer-to-Peer Network. In *Proceedings of the Industrial Control and Electronics Engineering (ICICEE), 2012 International Conference on*.

Shi, M., Shen, X., Jiang, Y., & Lin, C. (2007). Self-healing group-wise key distribution schemes with time-limited node revocation for wireless sensor networks. *IEEE Wireless Communications, 14*(5), 38-46. doi: 10.1109/MWC.2007.4396941

Shigang, C., & Shaolong, H. (2013). Ant Colony Algorithm and Its Application in Solving the Traveling Salesman Problem. In *Proceedings of the 2013 Third International Conference on Instrumentation, Measurement, Computer, Communication and Control (IMCCC)*, Shenyang, China.

Shim, K. A. (2016). A Survey of Public-Key Cryptographic Primitives in Wireless Sensor Networks. *IEEE Communications Surveys & Tutorials, 18*(1), 577-601. doi: 10.1109/COMST.2015.2459691

Shim, K. A. (2017). BASIS: A Practical Multi-User Broadcast Authentication Scheme in Wireless Sensor Networks. *IEEE Transactions on Information Forensics and Security, 12*(7), 1545-1554. doi: 10.1109/TIFS.2017.2668062

Singh, A., & Liu, L. (2003). TrustMe: anonymous management of trust relationships in decentralized P2P systems. In *Proceedings of the Third International Conference on Peer-to-Peer Computing, 2003.(P2P 2003)*.

Soltanali, S., Pirahesh, S., Niksefat, S., & Sabaei, M. (2007). An Efficient Scheme to Motivate Cooperation in Mobile Ad hoc Networks. In *Proceedings of the Networking and Services, 2007. ICNS. Third International Conference on*.

Srinivasan, A., Teitelbaum, J., & Wu, J. (2006). DRBTS: Distributed Reputation-based Beacon Trust System. In *Proceedings of the 2006 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing*.

Sun, Y. L., Yu, W., Han, Z., & Liu, K. J. R. (2006). Information theoretic framework of trust modeling and evaluation for ad hoc networks. *IEEE J.Sel. A. Commun., 24*(2), 305-317. doi: 10.1109/jsac.2005.861389

Talbi, S., Koudil, M., Bouabdallah, A., & Benatchba, K. (2015). Adaptive Data-Communication Trust Mechanism for Clustered Wireless Sensor Networks. In *Proceedings of the 2015 IEEE Global Communications Conference (GLOBECOM)*.

Theodorakopoulos, G., & Baras, J. S. (2004). Trust evaluation in ad-hoc networks. In *Proceedings of the 3rd ACM workshop on Wireless security*.

Vamsi, P. R., Batra, P. K., & Kant, K. (2014). BT-GPSR: An Integrated Trust Model for Secure Geographic Routing in Wireless Sensor Networks. In *Proceedings of the 2014 Students Conference on Engineering and Systems (SCES)*, Allahabad, India.

Velez, F. J., Nadziejko, A., Christensen, A. L., Oliveira, S., Rodrigues, T., Costa, V., . . . Gomes, J. (2015). Wireless Sensor and Networking Technologies for Swarms of Aquatic Surface Drones. In *Proceedings of the 2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall)*.

Velloso, P. B., Laufer, R. P., Cunha, D. D. O. O., Duarte, O. C. M. B., & Pujolle, G. (2010). Trust management in mobile ad hoc networks using a scalable maturity-based model. *IEEE Transactions on Network and Service Management, 7*(3), 172-185. doi: 10.1109/TNSM.2010.1009.I9P0339

Walter, F. E., Battiston, S., & Schweitzer, F. (2009). Personalised and dynamic trust in social networks. In *Proceedings of the Proceedings of the third ACM conference on Recommender systems*, New York, New York, USA.

Wang, Y.-F., Hori, Y., & Sakurai, K. (2008). Characterizing Economic and Social Properties of Trust and Reputation Systems in P2P Environment. *Journal of Computer Science and Technology, 23*(1), 129-140. doi: 10.1007/s11390-008-9118-y

Weeks, S. (2001). Understanding trust management systems. In *Proceedings of the 2001 IEEE Symposium on Security and Privacy, 2001. S&P 2001.*

Wikipedia. (2016). Normalizing Constant. Retrieved 02 May 2017, from https://en.wikipedia.org/wiki/Normalizing_constant

Wu, B., Chen, J., Wu, J., & Cardei, M. (2007). A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks. In Y. Xiao, X. S. Shen & D.-Z. Du (Eds.), *Wireless Network Security* (pp. 103-135). Boston, MA: Springer US.

Xiong, L., & Liu, L. (2004). Peertrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities. *IEEE Transactions on Knowledge and Data Engineering, 16*(7), 843-857.

Xu, H., Sharma, D., Aseeri, M., & Almorqi, S. (2011). Secure Wireless Sensor Networks with Dynamic Window for Elliptic Curve Cryptography. In *Proceedings of the 2011 Saudi International Electronics, Communications and Photonics Conference (SIECPC)*, Riyadh, Saudi Arabia.

Yan, Z. R., Fang, C. Y., Qi, S. H., Yang, T., Gao, D., Chen, Z. P., & Wang, Y. Q. (2014). Ecological Monitoring Scheme Based on Wireless Sensor Network in Baisha Lake of the Nanji Wetland Nation Reserve. In *Proceedings of the 2014 International Conference on Wireless Communication and Sensor Network*.

Yavuz, F., Jun, Z., Yagan, O., & Gligor, V. (2015). Designing Secure and Reliable Wireless Sensor Networks Under a Pairwise Key Predistribution Scheme. In *Proceedings of the 2015 IEEE International Conference on Communications (ICC)*, London, UK.

Youcai, Z., TingLei, H., & Wei, W. (2009). A Trust Establishment Scheme for Cluster-Based Sensor Networks. In *Proceedings of the 5th International Conference on Wireless Communications, Networking and Mobile Computing, 2009. WiCom '09*, Beijing, China.

Yu, H., Shen, Z., Miao, C., Leung, C., & Niyato, D. (2010). A Survey of Trust and Reputation Management Systems in Wireless Communications. *Proceedings of the IEEE, 98*(10), 1755-1772.

Yu, L., Qian, C., Liu, Z., Wang, K., & Dai, B. (2010). Ad-hoc multi-dimensional trust evaluation model based on classification of service. In *Proceedings of the 2010 5th International ICST Conference on Communications and Networking in China*.

Yu, Y., Govindan, R., & Estrin, D. (2001). Geographical and Energy Aware Routing: A Recursive Data Dissemination Protocol for Wireless Sensor Networks: Technical report ucla/csd-tr-01-0023, UCLA Computer Science Department.

Yu, Y., Li, K., Zhou, W., & Li, P. (2012). Trust Mechanisms in Wireless Sensor Networks: Attack Analysis and Countermeasures. *Network and Computer Applications, 35*(3), 867-880. doi: http://dx.doi.org/10.1016/j.jnca.2011.03.005

Zahariadis, T., Leligou, H., Karkazis, P., Trakadas, P., Papaefstathiou, I., Vangelatos, C., & Besson, L. (2010). Design and implementation of a trust-aware routing protocol for large WSNs. *International Journal of Network Security & Its Applications (IJNSA), 2*(3), 52-68.

Zhan, G., Shi, W., & Deng, J. (2010). TARF: A Trust-aware Routing Framework for Wireless Sensor Networks *Wireless Sensor Networks* (pp. 65-80): Springer.

Zhang, Y. (2012). The scheme of public key infrastructure for improving wireless sensor networks security. In *Proceedings of the 2012 IEEE International Conference on Computer Science and Automation Engineering*.

Zheng, Z., Liu, A., Cai, L. X., Chen, Z., & X. (2016). Energy and Memory Efficient Clone Detection in Wireless Sensor Networks. *IEEE Transactions on Mobile Computing, 15*(5), 1130-1143. doi: 10.1109/TMC.2015.2449847

Zhiying, Y., Daeyoung, K., & Yoonmee, D. (2006). PLUS: Parameterized and Localized Trust Management Scheme for Sensor Networks Security. In *Proceedings of the 2006 IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS)*, Vancouver, BC.

Zhu, C., Nicanfar, H., Leung, V. C. M., & Yang, L. T. (2015). An Authenticated Trust and Reputation Calculation and Management System for Cloud and Sensor Networks Integration. *IEEE Transactions on Information Forensics and Security, 10*(1), 118-131. doi: 10.1109/TIFS.2014.2364679

Zouridaki, C., Mark, B. L., Hejmo, M., & Thomas, R. K. (2007). Hermes: A quantitative trust establishment framework for reliable data packet delivery in MANETs. *J. Comput. Secur., 15*(1), 3-38.

Zouridaki, C., Mark, B. L., Hejmo, M., & Thomas, R. K. (2009). E-Hermes: A robust cooperative trust establishment scheme for mobile ad hoc networks. *Ad Hoc Networks, 7*(6), 1156-1168. doi: http://dx.doi.org/10.1016/j.adhoc.2008.10.003