TRUST-BASED ENERGY EFFICIENT ROUTING PROTOCOL FOR WIRELESS SENSOR NETWORKS

RAJA WASEEM ANWAR

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Doctor of Philosophy (Computer Science)

School of Computing
Faculty of Engineering
Universiti Teknologi Malaysia

APRIL 2021

DEDICATION

This thesis is dedicated to my (late) mother, to my wife and children.

ACKNOWLEDGEMENT

First and foremost, praises and thanks to the **Allah**, the Almighty, for providing me knowledge, guidance and patience to achieve this goal.

I would like to express my deep and sincere gratitude to my research supervisor, **Assoc. Prof. Dr. Anazida Zainal** for giving me the opportunity to do research and providing invaluable guidance throughout this research. It was a great privilege and honor to work and study under her guidance. It would have been very difficult to complete this research successfully without her suggestions and thoughts. I am also very thankful to **Dr. Majid Bakhtiari** for his generous support guidance and motivation without his continued support and interest, this thesis would not have been the same as presented here. The members of Pervasive Computing Research Group are appreciated for their intellectual discussion and input in this thesis.

I am extremely grateful to my family for their love, prayers, care and sacrifices for educating and preparing me for my future. Especially, I wish to acknowledge my late mother, without her prays I cannot achieve my goal. I owe my deepest gratitude towards my wife for her eternal support and understanding of my goals and aspirations. Her infallible love and support have always been my strength. I am thankful to my children **Hamza, Rafay and Aisha** for their continuous love and encouragement during my studies.

I would like to extend my gratitude to my friends **Dr. Muhammed Abrar Khan and Dr. Saleem Iqbal** for the keen interest shown by them to complete this thesis, successfully. Finally, my thankfulness for all those who have supported me to complete the research work directly or indirectly.

ABSTRACT

Wireless Sensor Networks (WSNs) consist of a number of distributed sensor nodes that are connected within a specified area. Generally, WSN is used for monitoring purposes and can be applied in many fields including health, environmental and habitat monitoring, weather forecasting, home automation, and in the military. Similar, to traditional wired networks, WSNs require security measures to ensure a trustworthy environment for communication. However, due to deployment scenarios nodes are exposed to physical capture and inclusion of malicious node led to internal network attacks hence providing the reliable delivery of data and trustworthy communication environment is a real challenge. Also, malicious nodes intentionally dropping data packets, spreading false reporting, and degrading the network performance. Trust based security solutions are regarded as a significant measure to improve the sensor network security, integrity, and identification of malicious nodes. Another extremely important issue for WSNs is energy conversation and efficiency, as energy sources and battery capacity are often limited, meaning that the implementation of efficient, reliable data delivery is an equally important consideration that is made more challenging due to the unpredictable behaviour of sensor nodes. Thus, this research aims to develop a trust and energy efficient routing protocol that ensures a trustworthy environment for communication and reliable delivery of data. Firstly, a Belief based Trust Evaluation Scheme (BTES) is proposed that identifies malicious nodes and maintains a trustworthy environment among sensor nodes while reducing the impact of false reporting. Secondly, a State based Energy Calculation Scheme (SECS) is proposed which periodically evaluates node energy levels, leading to increased network lifetime. Finally, as an integrated outcome of these two schemes, a Trust and Energy Efficient Path Selection (TEEPS) protocol has been proposed. The proposed protocol is benchmarked with A Trust-based Neighbour selection system using activation function (AF-TNS), and with A Novel Trust of dynamic optimization (Trust-Doe). The experimental results show that the proposed protocol performs better as compared to existing schemes in terms of throughput (by 40.14%), packet delivery ratio (by 28.91%), and end-to-end delay (by 41.86%). In conclusion, the proposed routing protocol able to identify malicious nodes provides a trustworthy environment and improves network energy efficiency and lifetime.

ABSTRAK

Rangkaian Sensor Tanpa Wayar (WSN) terdiri daripada sebilangan nod sensor yang berselerakan yang saling terhubung antara satu sama lain dalam kawasan yang ditentukan. Secara umum, WSN digunakan untuk tujuan pemantauan dan dapat diimplementasikan dalam banyak bidang termasuk kesihatan, pemantauan persekitaran dan habitat, ramalan cuaca, automasi rumah dan ketenteraan. Sama seperti rangkaian berwayar tradisional, WSN memerlukan langkah-langkah keselamatan untuk memastikan persekitaran komunikasi yang boleh dipercayai. Walau bagaimanapun, kerana senario penyebaran, nod terdedah kepada penangkapan fizikal dan kemasukan nod jahat menyebabkan serangan rangkaian dalaman. Oleh itu, menyediakan penyampaian data yang dapat dipercayai dan persekitaran komunikasi yang boleh dipercayai adalah mencabar. Juga, nod jahat sengaja menjatuhkan paket data, menyebarkan pelaporan palsu, dan menurunkan prestasi rangkaian. Penyelesaian keselamatan berdasarkan kepercayaan dianggap sebagai langkah penting untuk meningkatkan keselamatan, integriti rangkaian sensor dan mengenalpasti nod jahat. Masalah lain yang sangat penting bagi WSN adalah penjimatan tenaga dan kecekapan, kerana sumber tenaga dan kapasiti bateri adalah terhad. Oleh itu, pelaksanaan penghantaran data yang cekap dan boleh dipercayai adalah juga pertimbangan yang penting dan mencabar kerana tingkah laku nod sensor yang tidak dapat diramalkan. Oleh itu, tujuan penyelidikan ini adalah untuk membangunkan protokol penghalaan kepercayaan dan cekap tenaga yang dapat memastikan persekitaran yang dipercayai untuk komunikasi dan penghantaran data yang baik. Pertama, Skema Penilaian Kepercayaan berdasarkan Kepercayaan (BTES) dicadangkan yang mengenalpasti nod jahat dan mengekalkan persekitaran yang boleh dipercayai di antara nod sensor sambil mengurangkan kesan pelaporan palsu. Kedua, Skema Pengiraan Tenaga berdasarkan Keadaan (SECS) dicadangkan, yang menilai tahap tenaga pada nod secara berkala, yang membawa kepada peningkatan jangka hayat rangkaian. Akhirnya, sebagai hasil integrasi dari kedua skema ini, sebuah protokol Pemilihan Laluan Dipercayai dan Cekap Tenaga (TEEPS) telah dicadangkan. Protokol cadangan ini dibandingkan dengan sistem pemilihan berdasarkan Kepercayaan Jiran yang menggunakan fungsi pengaktifan (AF-TNS); dan dengan Kepercayaan Ulung pengoptimuman dinamik (Trust-Doe). Hasil eksperimen menunjukkan bahawa protokol yang dicadangkan menunjukkan prestasi yang lebih baik berbanding dengan skema yang ada dari segi *throughput* (bertambah sebanyak 40.14%), nisbah penghantaran paket (bertambah sebanyak 28.91%) dan kelewatan hujung-ke-hujung (berkurang sebanyak 41.86%). Kesimpulannya, protokol yang dicadangkan ini dapat mengenal pasti nod berbahaya, menyediakan persekitaran yang boleh dipercayai dan meningkatkan kecekapan dan jangka hayat tenaga rangkaian.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ADC	-	Analog to Digital Converter
BM	-	Bad-mouthing
BS	-	Base Station
BSI	-	Behaviour Status Index
BTES	-	Belief based Trust Evaluation Scheme
CBR	-	Constant Bit Rate
CEi	-	Cumulative Energy
CH	-	Cluster Head
CIDEi	-	Cumulative Indirect Energy Value
DEi	-	Direct Energy
Dij	-	Total Drop Packets
DoS	-	Denial of Service
DTEM	-	Direct Trust Evaluation Mechanism
Ei	-	Energy Value
IdEi-j	-	Indirect Energy
IdWi	-	Indirect Weight
INi	-	Immediate Neighbours
ITEM	-	Indirect Trust Evaluation Mechanism
MAC	-	Media Access Control
MN	-	Malicious Node
NED	-	Network Description Language
NS2	-	Network Simulator 2
NS3	-	Network Simulator 3
O | E	-	Occurrence | Evidence
OMNet++	-	Objective Modular Network Testbed in C++
OPNET	-	Optimized Network Engineering Tool
P (E)	-	Normalizing Constant
P (J)	-	Prior Probability
PDR	-	Packet Delivery Ratio
PRE	-	Packet Received Evaluation

PREP	-	Route Reply
PREQ	-	Route Request
PSE	-	Packet Sending Evaluation
QoS	-	Quality of Service
RE	-	Residual Energy
Rij	-	Data Packet Received
RIN	-	Reputed Immediate Neighbour
Rx	-	Receiving
SECS	-	State based Energy Calculation Scheme
SNi	-	Current State of Sensor Node as input
TE	-	Trust Estimator
TEEPS	-	Trust and Energy Efficient Path Selection
TEi	-	Total Energy
Th	-	Threshold Value
TI	-	Time Interval
TMM	-	Traffic Monitoring Module
Tp	-	Traffic Profiles
TPE	-	Transit Packet Evaluation
TR	-	Trust Receiver
TV | J	-	Probability of Trust Value
Tx	-	Transmission
UDP	-	User Datagram Protocol
WSN	-	Wireless Sensor Network

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Overview

A ubiquitous part of the modern world, Wireless Sensor Networks (WSNs) have become a key enabling technology that has seen widespread use in a variety of domestic and commercial applications. Each device (sensor or actuator, commonly referred only as a sensor) has computation, communication, and sensing or controlling capabilities (Akyildiz *et al.*, 2002; Duan *et al.*, 2014; Yetgin *et al.*, 2015). A new concept that seems to be the future of the WSNs is the Internet of Things (IoT) where it is expected that each object in human life is equipped with sensors that communicate with each other to constitute a network and thus the usage of WSNs will also grow rapidly in various industrial areas and applications (Atzori *et al.*, 2010; Sharma *et al.*, 2020; Suh and Cho, 2019). The integration of sensors with the Internet of Things enables the incorporation of information and communication technologies into the entire physical infrastructure, enabling sensors to perform a host of monitoring and management roles through the use of base stations Yetgin *et al.* (2017). However, due to dense and unattended deployment WSNs are considered unsafe than other types of networks and more vulnerable to various external and insider attacks where an adversary could inject the false information or even includes the malicious node. Besides, energy efficiency is another challenge in maximizing the lifetime of the network Daia *et al.* (2018). Therefore, effective security measures and efficient energy utilization mechanisms can prolong the lifetime of networks with better throughput and data delivery Desai and Nene (2019).

Sensor networks can be deployed in either a centralised (clustered-architecture) or a distributed (ad-hoc) manner. Although all sensors are equipped with sensing and communicating capabilities, they require unconventional paradigms for protocol design since ad-hoc routing protocols are not suitable for WSNs due to limited energy, processing power, and storage capabilities Mendoza and Kleinschmidt (2018a). The dense and distributed deployment of nodes degrades network performance due to the difficulty of detecting malicious and untrustworthy nodes, which waste network resources and increase energy depletion rates Jhaveri *et al.* (2018). On the other hand, sensors that are deployed centrally with pre-defined settings can increase network performance and can reduce unnecessary maintenance (Dasgupta *et al.*, 2003; Hamzeloei and Dermany, 2016). Importantly, achieving the goal of delivering reliable data delivery and trustworthy communication with improved network lifetime and performance requires the use of data transmission methods between sensor nodes, cluster-head (CH), and base stations that are trustworthy and energy-efficient. These factors mean that designing and deploying sensor networks using clustering approaches offers many advantages, such as better communication, minimised delay, and energy efficiency with better topology management (Alshehri and Hussain, 2018; Tang *et al.*, 2016).

A common problem with WSNs is unpredictable behaviour and frequent loss of data items due to compromised nodes, data faults, and security threats Karthik and Ananthanarayana (2017b). In open deployed areas where human interaction is minimal, attackers can easily capture a node and physically inject false information or even eventually force a malicious node (MN) onto the network. The nodes compromised by an external adversary pose a serious security threat to a network because of false reporting and internal attacks such as Bad-Mouth, On-Off, and Denial of Service (DoS), resulting in inconsistent network performance which leads to incorrect decisions. Therefore, the detection of MNs reduces the risk of network damage and limits security threats, thereby helping to maintain network performance. However, the existing cryptographic security-based defending mechanisms are effective against external attacks but are often unable to detect or withstand the internal attacks caused by malicious nodes and drop the data packets legitimately or even increase energy drain (Kulin *et al.*, 2016; Prabha and Latha, 2017). Besides, sensor networks cannot function effectively if they are vulnerable to attacks, as MNs do not

cooperate with other nodes and can generate incorrect readings or misleading reports, potentially harming the decision-making process and degrading network performance. For this reason, timely detection of the malicious node has the potential to increase collaboration among nodes in the network and ensure trustworthy communication, which in turn improves network performance (Jiang et al., 2015; Lim and Choi, 2013; Rani et al., 2019; Sun et al., 2006).

The concept of WSNs is as a network of low-cost sensor nodes. However, providing physical security to every sensor node requires a significant cost, which is contrary to this concept Grgic et al. (2016). Trust based security is a new and promising alternative to traditional cryptographic security mechanisms for the identification and isolation of malicious nodes in WSNs Sultana et al. (2015). The inclusion of trust to a sensor node can be an effective way to curtail the effect of MNs, based on prediction of the future behaviour of the node. Trust refers to the degree of reliability with which each sensor node monitors the packet forwarding behaviour of its neighbouring node and uses this information to measure the trustworthiness of the nodes around it. Trust-based communication mechanisms can facilitate the identification of MNs, which spread false reporting and harm network performance by causing reliance on incorrect information (Ishmanov *et al.*, 2015; Momani and Challa, 2010). Performance can also be improved by different approaches to monitoring, with the application of periodic evaluation strategies to node energy level assessment being an effective way to identify energy depleted nodes that intentionally drop data packets and to prolong network lifetime. A trust based secure routing mechanism provides trustworthy end-to-end routing paths that improve network throughput, increase packet delivery ratio, and reduce delay. However, while many security and trust-based routing solutions are already in place in many systems, networks are still vulnerable regarding the detection and isolation of MNs. In addition, some proposed solutions do not consider the energy and computational constraint of sensor nodes (Karlof and Wagner, 2003; Liu *et al.*, 2016).

1.2 Problem Background

Provision of providing a secure and trustworthy environment for communication and preserving the energy efficiency for wireless sensor networks (WSNs) to prolong network life has been identified as a major challenge, the secure routing protocol should be carefully designed to ensure the security and along with efficient utilization of node energy level. The routing protocol is a method for providing the secure end-to-end path selection between source and destination node while avoiding the malicious and energy depleted nodes. The identified problem is discussed in the order of:

i. Identification and isolation of malicious node (MN), to reduce the impact of false reporting.
ii. State based node energy evaluation using behavioral aspects of nodes such as sleep, and wake states to save the node energy level which affects in improving the network lifetime.
iii. Is about the selection of end-to-end efficient path.

The open distribution of sensor nodes in a hostile and unattended environment makes them an ideal target for adversaries where they can capture the node physically and even able to access to stored information with a potential avenue for the injection of false data or launching malicious attacks (Amutha *et al.*, 2020; Gopal *et al.*, 2013). Moreover, WSNs are extremely susceptible to certain kinds of internal security threats, such as compromised malicious nodes. These kinds of MNs provide a platform for attackers to harm system performance or integrity in a number of ways: providing dishonest recommendations and propagating false information about well-behaved or trustworthy nodes (Bad-Mouth attacks); alternating behaviour between benign and harmful network activity (On-off attacks); and disrupting normal network operation (Denial-of-Service, or DoS, attacks). MN attacks are difficult to detect and can seriously damage network operations, as well as enabling other type of attacks. In addition to the threat from MNs, nodes are also prone to failure due to energy depletion and communication link-error (Feng *et al.*, 2013; Ghugar *et al.*, 2019).

Recent years have seen the design of several trust-based security and routing mechanisms intended to improve the detection of malicious nodes and provide trustworthy communication, while also improving energy efficiency (Farsi *et al.*, 2019; Khalil *et al.*, 2010). Although these trust and secure routing protocols provide a degree of security, numerous critical issues still need to be considered, including malicious node detection with higher reliability, the ability to respond against various attacks, periodic evaluation of node energy level and selection of end-to-end trustworthy path computation (Bhushan and Sahoo, 2020; Desai and Nene, 2019). Most of the established approaches attempt to protect sensor networks from a wide variety of attacks using strategies that include exploiting cryptography (Bhat and Reddy, 2015; Elhoseny and Hassanien, 2019), pairwise shared key (Chakraborty and Chaki, 2012; Iqbal and Shafi, 2019; Ramos, 2015) and authentication (Cui *et al.*, 2020; Nie, 2017) based security mechanisms. However, these approaches are not robust or effective in the detection of MNs and also raise energy overheads, which is problematic in the context of resource constrained WSNs. The majority of the existing approaches (Alshehri and Hussain, 2018; Ghani *et al.*, 2019; Ishmanov *et al.*, 2015; Wang *et al.*, 2017) assume that communicating nodes are trustworthy, because the nodes share keys and mutually authenticate during the initial deployment of network. However, key based security measures are not feasible for the protection of WSNs due to lack of internal attack detection. Instead, trust based, secure end-to-end routing mechanisms are needed to increase throughput and minimum delay, thereby improving network reliability and lifetime Chen *et al.* (2019), as security issues are crucial in determining whether deployed sensor networks function correctly and effectively.

The issue of energy consumption in WSN poses a major design challenge due to the limited capabilities of nodes and the fact that communication between nodes consumes energy. The fact that sensor nodes have limited communication bandwidth, inherent computational complexities and energy constraints can have a significant impact on the ability to prolong the network lifetime. Also, the deployed nodes are equipped with batteries that are either non-replaceable or deployed in inaccessible areas. This means that, saving energy from physical level to routing level to improve reliability of data delivery though the improvement of data acquisition strategies can be especially important in this context (Cheng *et al.*, 2012; Saini *et al.*, 2019; Shah *et al.*, 2018).

Maximising the lifetime of a sensor network is a core design goal, but this depends on the energy available to participating nodes. Therefore, improving network lifetime and increasing the performance may be possible by dividing the sensor network into equal clusters and use of centralised or hierarchical routing protocols in order to reduce energy costs. A number of energy consumption and network routing overhead schemes have been proposed in order to achieve this overarching objective (Batra and Kant, 2016; Heinzelman *et al.*, 2002; Kannan and Raja, 2015; Mahajan *et al.*, 2014; Wang *et al.*, 2019b). However, the amount of energy is consumed during transmission (Tx) and reception (Rx) of data between active and the sleep state can be high (Cardei *et al.*, 2002; Jayarajan *et al.*, 2020; Stine and De Veciana, 2002). Therefore, it is important to formulate a well-designed network informed by reliable, energy aware routing protocols. A key consideration in the design and deployment of WSN is clustering, with well-designed clustered network architecture increasing network lifetime through the efficient utilisation of energy. In a cluster environment sensor node are grouped into various layers, each of which contains a node elected as a Cluster-Head (CH), which periodically collects data from member nodes using Time Division Multiple Access (TDMA) and then communicates this data to Base-Station (BS) for further processing and decision making. The adoption of clustering in sensor networks could improve network reliability and decrease communication overheads by filtering redundant data, thereby minimising size and increasing communication range via data aggregation (Anastasi *et al.*, 2009; Chen *et al.*, 2017a; Thiagarajan, 2020). These considerations make increasing network lifetime extremely challenging task, requiring careful selection of energy-oriented sensor nodes and routing paths between source and destination.

Figure 1.1 outlines the scenario which inspired the problem addressed by this research, detailing the challenges and threats of MN detection with limited resources in WSNs and the limitation of existing solutions.

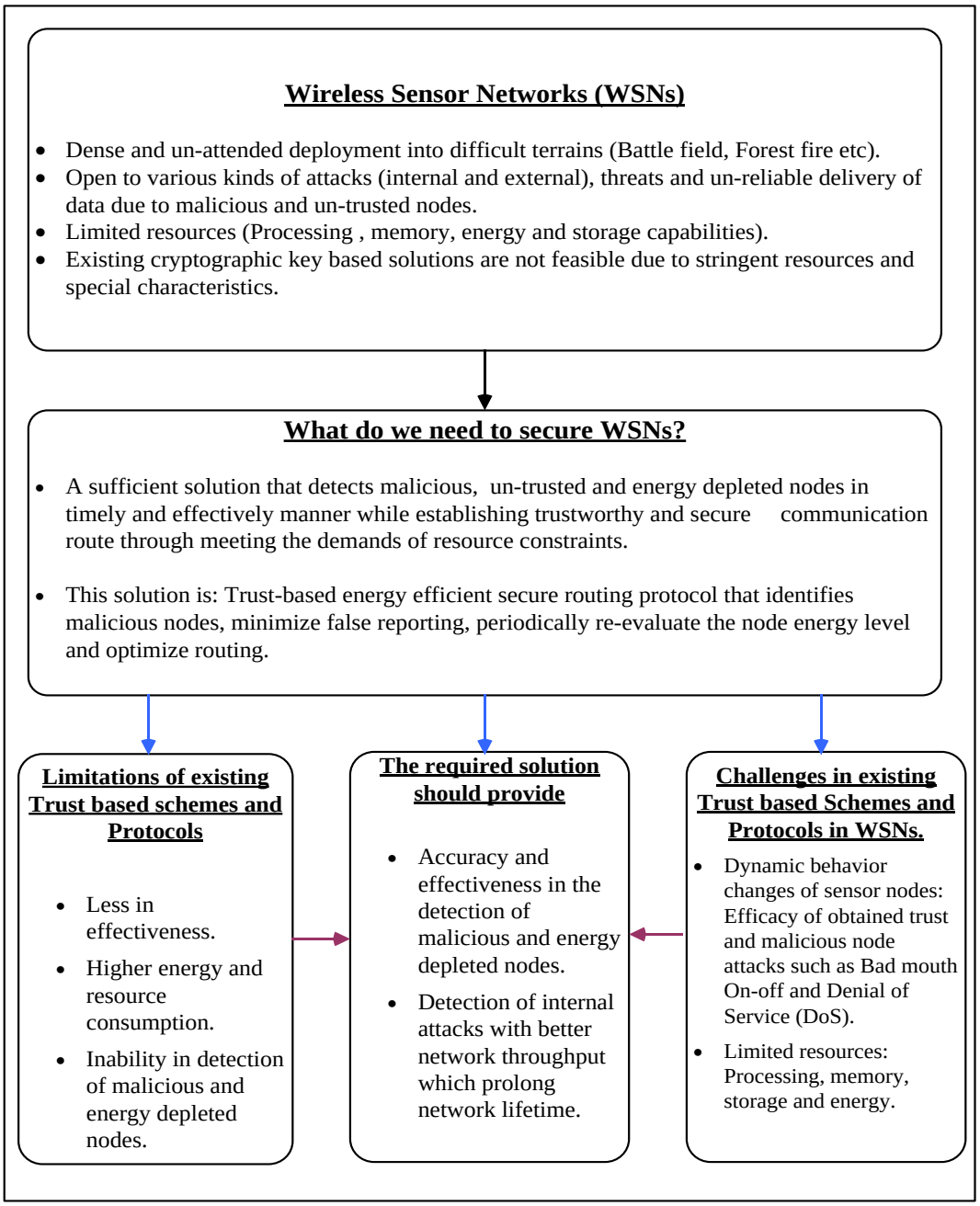

Figure 1.1 Scenario leading to the research problem

The scenario presented in Figure 1.1 highlights the main considerations informing the design of trust and energy evaluation schemes, which need to enable the detection of malicious and untrustworthy energy depleted nodes. The following sections provide a detailed explanation of the previously mentioned trust-based security and routing mechanisms.

1.2.1 Identification and isolation of malicious node (MN)

The open and distributed nature of the communication in WSNs is untrusted and energy constrained, meaning that the behaviour of deployed nodes is constantly changing in response to environmental disturbance, network anomalies and physically capture from attacks. During data collection, sensor nodes operate without human oversight and use unreliable communication channels which it very easy to compromise them and disrupt communication or render it untrustworthy. As MNs are difficult to scrutinise once they are part of the network, it can be challenging to detect and isolate them. This issue can be exacerbated by the false data that MNs can communicate to the centralised authority for decision making, which affects network performance and application where data reliability is an important measure. As a result, increasing the reliability and assurance level of a network through the trustworthy assessment of data not only increases the network lifetime and performance but also improves throughput. In recent years, trust-based security has played a foundational and diverse role in the detection of malicious and non-cooperating (faulty) nodes through the provision of a trustworthy environment and data towards the aim of improving reliability (Akyildiz *et al.*, 2002; He *et al.*, 2019; Jiang *et al.*, 2015; Sultana *et al.*, 2015). However, trust is a subjective matter that involves assessment of reliability and probability, with an evaluating node assessing the behaviour of an evaluated node for a specific action, according to recommendations or previous direct and indirect information from observation of behaviour (Jiang *et al.*, 2015; Nie, 2017; Zawaideh and Salamah, 2019). In the presence of a malicious and faulty node, unreliable and false reporting can occur between nodes, resulting in incorrect decisions being made and potentially actively contributing to Bad-Mouth, On-Off and DoS attacks being made. Similarly, energy depleted nodes can drop legitimate data packets and instead communicate false information to a destination node. However, traditional methods of providing security such as cryptographic solutions incur high overhead of messages which raises usage of energy, memory and computational resources and thereby limits the viability of such solutions, potentially leading to abnormal functioning of the network (Jawad *et al.*, 2017b; Kumar and Mehfuz, 2019; Rajeshkumar and Valluvan, 2017; Teng *et al.*, 2020).

Preventing a node from acting maliciously and disrupting the normal functioning of the trust-based security mechanisms in place on a network can solve the issue of finding and isolating an MN through the assessment of the trustworthiness level. Recently, (Rikli and Alnasser, 2016) proposed a lightweight centralised trust model for the detection of the malicious nodes causing misbehaviour. Their model uses communication between nodes and their neighbouring nodes by sending this data to the CH, which maintains the current and past interaction information about each node. The gathered information is then used in decision making processes, such as calculating trust levels and isolating MNs. In the proposed model, each node evaluates its one-hop neighbour and communicates the received information to the centralised repository. As a consequence, this model is able to detect jamming and selfishness node attacks. Although the proposed model is able to detect and isolate MNs without considering recommendation or indirect trust from neighbouring nodes, its key limitation is the extra overhead involved in running the model.

A Trust-based Neighbour Selection system using activation function (AF-TNS) was proposed by AlFarraj et al. (2018) as a way to use direct trust and additive metrics to evaluate trustworthiness and data retention of trusted neighbouring nodes in WSNs. The proposed scheme isolates MNs by considering only direct trust from the neighbouring nodes but exhibits several flaws and vulnerabilities. The AF-TNS trust calculation incorporates only received data packets, which is a key weakness, because the trust of sensor nodes varies over time and a trusted node may become an MN due to energy depletion. AF-TNS also fails to consider indirect trust and recommendations, making it vulnerable to false reporting (e.g. Bad-Mouth attacks) and associated failures in decision making. Furthermore, the operation of the network depends on the cooperation of participating nodes. This means that when there is no history of past interactions and recommendations, a node needs to evaluate the other node by performing various calculations every time, which increases consumption of energy and computation, causing node energy to drain quickly and leading to increased numbers of MNs in turn, thereby reducing network performance.

Nie (2017) proposed a different trust based model, known as a novel trust model of dynamic optimisation using entropy (Trust-Doe). This approach forms numerous trust features based on the communication behaviour between any two neighbouring nodes, which is then processed using the attenuation function and weighted average to determine the indirect trust values of the sensor nodes at different time intervals. While the Trust-Doe model is able to detect malicious nodes and to defend against attacks but has several limitations such as higher level of energy consumption, limited detection of MNs and inability to defend against internal attacks, such as Bad-Mouth, On-Off and DoS attacks.

A number of studies have proposed the use of a modelling based trust calculation method for WSNs (Bißmeyer, 2014; Hongjun et al., 2008; Zahedi and Parma, 2019). These cases are based on the use of a misbehaviour-frequency module to increase the strength of the trust mechanism, which enabled the creation of a model with better performance than several other trust-based models and with the ability to achieve a higher, more consistent level of attack detection. However, the proposed model suffers from increased network overhead and delay. In a similar study, Naderi *et al.* (2015) created a trust model based on measuring a sinkhole attack area and obtaining an approximate value of the total energy consumed in that network. This was followed by the development of an entropy-based trust mechanism that uses the determinants impacting the calculation of trust, with trust-based routing based on packet trust conditions. Their routing algorithm sought to categorise packets according to security demand and then to transfer the packets associated with each class via the route conforming to the security conditions. However, the complexity of the algorithm and higher energy consumption associated with this model constitute major disadvantages with the mechanism.

Bao *et al.* (2012) devised an extremely scalable cluster-based hierarchical trust management model for WSNs with the aim of efficiently managing selfish, malicious sensor nodes. In contrast with several related researches the authors assessed the complete trustworthiness of the sensor nodes by considering the multidimensional trust characteristics resulting from communication and social networks. A probability model based on stochastic Petri net methods was used to examine the efficiency of the

trust management model. The design was further substantiated by associating the individual trust produced by implementation of the model against neutral trust acquired from the definite node status, after which the hierarchical trust management model was implemented to trust-based geographical routing. They found that trust-based geographic routing under known design situations could be close to the optimal performance level attainable by flooding-based routing in message delivery ratio and message delay without substantially increasing message operating cost. Their model also outpaced the conventional geographic routing models, which have not implemented the trust model for the selection of forwarding nodes in message delivery ratio over a varied choice of design parameter settings. However, the weaknesses of the proposed method are that it incurs a higher overhead, with increased energy consumption resulting in network performance degradation.

As noted above, the unique constraints and features of WSNs make them vulnerable to various malicious attacks, threats and risks that can make certain internal nodes malicious. For this reason, researchers Liu *et al.* (2016) proposed ActiveTrust, a trust based secure routing scheme for sensor networks that counters black hole attacks using multiple route creation and by considering the residual energy of nodes. This model provides reliable and scalable communication, improves system security, and increases network lifetime. In addition, the proposed scheme initiates multiple routes by using residual energy and trust levels of nodes on the route to the destination, although this can create vulnerabilities to other forms of attack such as DoS. Similarly, a secure routing mechanism proposed by Zheng *et al.* (2016) is able to avoid black hole attacks by allowing a communicating node to select nodes with higher trust values. This approach improves reliability, but does not incorporate node energy level, which can harm network performance.

Overall, the majority of the existing trust-based security schemes and mechanisms are able to identify MNs and resist a few types of attacks. However, this increases false positive rates and requires higher energy consumption, memory usage, and computational power. In addition, most of the proposed security mechanisms lack the ability to detect energy depleted nodes with a minimal network overhead and are therefore unable to achieve higher throughput (Kukunuru, 2019; Yang *et al.*, 2020). In

order to overcome the limitations of current security methods in the detection of MNs, further research should be undertaken into trust evaluation mechanisms for WSN capable of accurately identifying and isolating MNs, and reporting findings to a centralised authority for decision making. Such a scheme should consume minimal resources, while being resistant to the most important internal attacks, like Bad-Mouth, On-Off and DoS, ultimately improving the data packet transmission ratio with fewer false positive and higher detection accuracy Abdellatif and Mosbah (2020).

As this review has demonstrated and will be further discussed in the literature review, despite the fact that current trust evaluation schemes and mechanisms sought to enhance the efficiency of WSNs, many of them suffer from a number of key weaknesses, as summarised below:

i. The use of cryptographic security measures imposes exhaustive computational requirements and corresponding overheads on already resource constrained sensor nodes.
ii. Trust estimation that only relies on direct or indirect trust lacks the ability to effectively detect internal attacks caused by malicious nodes.
iii. The complexity of the underlying algorithms can decrease network throughput and performance.

1.2.2 Periodic re-evaluation of node state and energy level to avoid early depletion

One of the most prominent and challenging tasks facing WSNs is the issue of how best to improve energy efficiency and ensure reliable data delivery. In order to fulfil their sensing and communication roles, sensor nodes are spatially distributed in open environments with constrained resources and limited energy, due to reliance on battery operation, which means that nodes can deplete their energy levels quickly volumes of data traffic are high. Sensor nodes utilise battery power to conduct operations such as data collection, evaluation and data communication. After deployment, there is no mechanism to continuously supply power or recharge sensor

node batteries, which means that network lifetime can be profoundly affected by unbalanced energy consumption of nodes, especially in response to malicious acts. Many techniques have been suggested to manage and minimise energy consumption, such as data aggregation, clustering, duty cycling (active state/sleep, or idle, state) and limited control packets (Abdal-Kadhim and Leong, 2020; He *et al.*, 2015; Lee *et al.*, 2016; Qureshi *et al.*, 2020a; Ye *et al.*, 2004). However, suggested approaches have failed to consider conservation and periodic evaluation of residual node energy from a central CH in response to resource limitations of WSN.

Sensor nodes operation varies according to their operation modes: idle, transmit/active, receive and sleep. Moreover, during transmission (Tx) mode energy consumption among the sensor nodes are higher as compared to receiving (Rx) mode. Nodes consume less energy while in sleep mode since data communication stops. Therefore, adopting a sleep/wake schedule can mitigate energy wastage, as the nodes only become active when there is a need for data transmission or reception (Nazir *et al.*, 2011; Wang *et al.*, 2019c). The majority of existing approaches (Molina-Pico *et al.*, 2016; Nazir and Hasbullah, 2011; Rikli and Alnasser, 2016; Shukla and Tripathi, 2020; Van Dam and Langendoen, 2003; Ye, 2018) are concerned with the design of different data forwarding mechanisms for performance improvement. However, these approaches do not focus on determining the energy depleted sensor nodes, or on managing sleep and wake scheduling strategies across the entire network field in consideration of the resource constraints of WSNs. Instead, they emphasise the selection of clusters forming with a higher energy CH in order to improve network lifetime. However, energy consumption cannot be improved effectively due to the presence of energy depleted nodes. Additionally, data transmission will be less effective under such schemes due to lack of node energy revaluation, which increases network overhead and end-to-end transmission delay.

Lin *et al.* (2015) proposed the DeepSleep based energy saving scheme to improve energy-efficiency and reduce the overall outage probability of deployed sensor nodes. The scheme reduces the energy wasted on over-hearing and idle-listening states. The major limitation of the DeepSleep scheme is the synchronisation schedule for sleep and wake times, which increases the communication cost.

Additionally, a radio transceiver is required in the sensor node to continuously monitor the channel for communication. A similar approach was taken by Razaque and Elleithy (2015) who proposed an idle-mode energy consumption duty-cycle based mechanism that switches sensor nodes between on-demand sleeping and listening states in order to save energy and maximise network lifetime. The major limitation of their proposed scheme is the lack of a mechanism to re-evaluate the energy level of sensor nodes after a specific period. Periodic re-evaluation of the energy would also increase node reliability and assist the detection of energy depleted nodes that falsely claims to be higher energy nodes.

Anbuchelian *et al.* (2014) proposed an energy saving scheme for cluster-based sensor networks that improves network performance and lifetime. Their scheme uses CH selection based on energy levels and other cluster member nodes in sleeping mode. During the communication process, the CH computes and distributes the schedule to other nodes, which reduces communication cost and saves energy. However, the proposed scheme does not consider the residual energy level of nodes and also does not conduct periodic re-evaluation, which is a major drawback. Similarly, work by Dong *et al.* (2013) led to the development of a cross-layer, loop free based energy harvesting and duty cycle scheme known as TPGFPlus. This proposed scheme keeps a portion of sensor nodes in sleep mode and provides quality of service for various WSN applications. However, although TPGFPlus conserves energy, the majority of sensor nodes consume significantly more energy during their wakeup schedule, due to excessive message transmission. Another approach was suggested by Almalkawi *et al.* (2012) who devised a cross-layer based energy oriented multipath routing protocol, in which CH selection and network formation is carried out by broadcasting the control packets and signal strength. However, the proposed scheme does not consider the energy level of the node with no path maintenance, with the result that network reliability is not assured.

Recently, the issue of energy saving through wake-up and sleep based scheduling solution was explored in the context of underwater sensor networks Dong *et al.* (2015). They sought to address the peculiarities of underwater communication and to compress the sleep-cycle of the nodes using acoustic wakeup. They found that this approach increases energy efficiency but decreases response time. Another energy aware intelligent routing protocol based study was carried out by Jin *et al.* (2017) who devised a system based on Q-learning technique and cost function to select the energy aware CH, with each node calculating the energy level of their neighbouring node and then selecting the node with highest energy for transmission. Although, the proposed protocol saves some energy and extends the lifetime of the network, but there is no mechanism which re-evaluates node energy level on a periodic basis.

In order to counter malicious power exhaustion in WSN, as in a denial of sleep attack, Naik and Shekokar (2015) propose a secure energy aware scheduling scheme that uses a periodic sleep/wakeup scheduling mechanism to manage behaviour between the sensor nodes. Under this approach nodes wake up periodically and sense whether there is any data they have to receive on the network. A denial of sleep attack is a constant threat to the node sleep state, since it prohibits the node from entering an idle state and instead forces data packets to be processed continuously, which turns the node into an MN and degrades the overall network performance. Although, Naik and Shekokar's scheme prevents denial of sleep attacks and saves a certain amount of network energy, it does not periodically re-evaluate the energy level of nodes. Furthermore, the need for constant communication between sensor nodes reduces network performance and overall power. A different approach was taken by Wang *et al.* (2016), who proposed a trust and energy efficient approach for cluster based WSNs, although it is not suitable for large scale WSN deployment scenarios due to its inherent complexities. For example, while it provides security and improves energy efficiency in the selection of CH, their scheme requires each CH to be equipped with a trusted hardware module (TM), which also increases computational overhead. The most important drawbacks of the existing schemes can be summarised as follows (Mohd *et al.*, 2020; Shagari *et al.*, 2020):

i. Additional communication overheads are incurred due to the inclusion of false information through node capturing attacks, where malicious and energy depleted nodes behave as trustworthy.
ii. Hardware based trust solutions may not be feasible for all kinds of WSN applications due to frequent changes in the applications.
iii. Failure to consider periodic re-evaluation of node energy and trust level levels.

1.2.3 Efficient end-to-end path selection

The provision of reliable, trustworthy routing is a critical issue for WSNs due to their limited power and the energy constraints on their nodes. In addition, on-demand routing protocols use multi-hop-based communication mechanisms for data forwarding towards destination. Their ease of deployment and data dissemination make on-demand distance vector protocols particularly suitable for emergency and disaster situation networks, such as forest fire monitoring. However, multi-hop communication is extremely vulnerable to energy depletion, the actions of malicious and compromised nodes, and certain type of attacks. The existing secure routing schemes and protocols utilise cryptosystems that are demanding in terms of energy and power consumption with inability in the detection of internal attacks, thereby making them less suitable in energy limited WSN contexts. Therefore, the provision of trustworthy, energy efficient options for WSNs is essential to ensure efficient data delivery with minimal end-to-end delay (Anisi *et al.*, 2012; Jin and Ahn, 2016; Srivastava *et al.*, 2020; Wang *et al.*, 2019a). Pathan *et al.* (2018) propose the use of trust based multi-hop routing protocols for WSNs, in which secure, reliable path selection can be achieved through the calculation of node trust, competence level and reliability. In this approach, routing decisions are based on the calculated trust values attached to a node's public key based-certificate. However, the use of a centralised authority for issuing certificates, distribution and revoking list puts an extra and undesirable energy burden on sensor nodes. Cryptographic based security mechanisms is also not effective in managing the physical capture of sensor nodes, where an adversary obtains important information and uses it to launch other types of malicious attacks.

Multi-hop routing schemes for WSNs have been proposed by a number of authors (Hammoudeh and Newman, 2015; Jaiswal and Anand, 2019; Jiang *et al.*, 2016; Yao *et al.*, 2015) as a potential way to improve routing performance with minimum overhead. In such schemes, data packets are transferred to base station using Quality of Service (QoS) and energy based path selection via multi-hop, with each node evaluating its neighbour in terms of reliability and remaining energy. Although these routing schemes significantly improve data delivery performance over conventional routing approaches, the addition of control packets increases overheads. In addition, the need for frequent route requests between communicating nodes lowers network consistency and raises energy consumption, as well as increasing delay and lowering throughput Hassan *et al.* (2019).

Duan *et al.* (2014) proposed a Trust-aware Secure Routing Framework (TSRF) that incorporates direct and indirect trust of the WSN nodes to overcome attacks caused by malicious and compromised nodes. Their routing protocol uses multi-hop communication to avoid unreliable paths during dissemination of data from source to destination. A similar approach was proposed by Rezgui and Eltoweissy (2007), who designed a trust-based routing scheme (TARP) that collects data from sensor nodes and routes to the BS. In their approach, data forwarding relies on cooperation between nodes, with each using the stored history of its interactions with other nodes to determine good reputation and recommendations. Although the scheme constitutes a significant improvement in terms of energy and scalability, it could not respond effectively to identity deception attacks that replay routing information. Subsequent studies (Chen *et al.*, 2014; Jain *et al.*, 2020; Jiang *et al.*, 2015; Zhang *et al.*, 2019) proposed trust-based routing schemes that use information on trust and energy levels that is stored in tables. This information is then used to select secure routes between nodes. Although such schemes improved the use of trust between nodes, the provision of reliable, energy efficient end-to-end paths adversely affected the design of the routing protocol by continually focusing on the scarce resources of sensor nodes, resulting in frequent route failures, more delays and less efficient.

The dynamic nature of wireless links, computational, memory and energy constraints on sensor nodes make trustworthy routing much challenging for WSN. Energy consumption is a key designing criterion for the routing protocols and efficient use of energy prolongs the network lifetime. Sridhar *et al.* (2013) presented secure routing protocol (EN-AODV), which conserves energy consumption and provides effective routing through reduce number of control packets and balance the network load. EN-AODV, calculates the node energy level before transmitting the data packets and then send this information to other neighboring nodes through hello packets. However, overlooking multi-hop route construction may result in higher energy consumption hence not suitable for large scale networks deployment. Moreover, frequent use of hello packets generates unnecessary network traffic which consume nodes energy hence cause unnecessary delay. Secure and Energy Efficient Trust-aware routing (ETARP) protocol was proposed by Gong *et al.* (2015) for energy efficiency and security which is based on the existing on- demand distance vector routing protocol (AODV). Route request (PREQs) and route replies (PREQs) fields are modified for energy field incorporation. The proposed protocol establishes a trustworthy route using current and previous interactions between the nodes and isolates the malicious node. Although the protocol selects trustworthy and energy efficient route but none of the attacks are considered which ultimately affects the network performance and deployment.

Most recently, a multi-layer security (MLS) protocol was proposed for wireless sensor networks Vidhya and Sasilatha (2018). This protocol is founded on top of the existing AODV protocol using an energy-power consumption (EPC-AODV) mechanism that implements security through the advanced encryption standard (AES). In addition to using encryption mechanisms, the proposed protocol evaluates the energy of neighbouring nodes before transmitting data. Although this approach improves data integrity through the selection of higher energy nodes, the use of encryption at each layer incurs a higher overhead, which adversely affects network throughout and performance.

Given the aforementioned work conducted in this field, it is a well proven fact that sensor nodes are prone to failure from their operation constraints and the impact of internal attacks. In addition, most trust aware routing schemes focus exclusively on the selection of trusted nodes and ignore the energy level of nodes in trusted path selection. It is apparent that trust and energy related security schemes have received less attention in the literature and that lightweight trust and energy efficient aware security mechanisms are therefore still required. The majority of existing trust-aware methods do not consider the periodic re-validation of node trustworthiness or energy levels, resulting in the early depletion of trustworthy nodes and increased presence of MNs in the network. The goal of maximising network lifetime, trustworthiness and energy efficiency requires the network environment to detect and isolate MNs, resist internal attacks and preserve node energy levels. Consequently, the selection of appropriate trustworthy, energy efficient node during data routing improves network lifetime and performance, as well as creating a secure end-to-end path. However, the following limitations are observed in the existing solutions (Khan *et al.*, 2019; Qabulio *et al.*, 2020):

i. Selection of end-to-end path is based exclusively on trust level, meaning that node energy levels are ignored.
ii. Computational complexity and additional overhead can reduce network lifetime, especially given the special characteristics of WSNs.
iii. Avoiding and less attention is given to internal attacks that can occur due to the inclusion of malicious and untrustworthy nodes in a system.

The current research addresses the problem of identifying and isolating the MNs that are responsible for causing internal attacks and decreasing network performance and throughput. In particular, this research focuses on addressing the highlighted problems through the identification and isolation of MNs using trust as a security measure, as well as the evaluation of node energy level, and trust and energy efficient route discovery.

1.3 Problem Statement

The operation of WSNs is highly dependent on the cooperation of participating nodes. Therefore, the inclusion of MNs will not only disrupt communication, but may also harm the decision-making process, eventually resulting in degradation of network throughput and lifetime. MNs can also affect network performance by launching Bad-Mouth, On-Off and DoS attacks. For these reasons, it is important to design an efficient trust evaluation scheme.

In WSNs, an energy depleted node may reduce data delivery performance. Therefore, avoiding such nodes while establishing a trustworthy communication environment can play an important role in prolonging network lifetime. The main function of sensor nodes is to sense the physical environment and communicate any relevant information back to the base station (BS). However, the dynamic nature of communication between the deployed sensor nodes can quickly exhaust the limited energy resources of WSNs. Network throughput and performance can also be compromised by increases in network size, transmission power and the malicious behaviour of energy depleted nodes. As sensor nodes are prone to failure due to untrusted energy depleted nodes, communication range and limited transmission power, the selection of an optimised end-to-end route for reliable data delivery is another important challenge in terms of maximising WSN effectiveness and lifespan.

The proposed approaches address the above challenges through the detection and isolation of MNs using trust, energy and optimised route selection, in order to significantly improve overall network throughput and lifetime.

1.4 Research Questions

In order to address the above problem, this research will investigate the following research questions:

i. What is the best way to detect the unpredictable behaviour of sensor nodes in order to improve communication and network trustworthiness levels, while identifying and isolating the malicious node (MN) responsible for misbehaviour and false reporting?
ii. How should cluster-based sensor networks periodically monitor and improve node trust and energy levels to prolong network lifetime?
iii. How can reliability and routing trustworthiness be developed by optimising routing paths and improving packet delivery ratio, while reducing the delay and prolonging network lifetime?

1.5 Research Aim

This research aims to design and develop a trust-based, energy efficient secure routing protocol for WSNs that is capable of identifying and isolating malicious nodes and protecting against internal network attacks with periodic re-evaluation of node energy and trust level, while maintaining lower communication overhead and reducing end-to-end delay.

1.6 Research Objectives

In support of this overarching aim, the objectives of this research are:

i. To develop belief based trust evaluation scheme that identifies and isolates malicious nodes, while improving node trustworthiness and communication levels.
ii. To develop a state based energy evaluation scheme that improves network lifetime by monitoring node state level.
iii. To develop a trust and energy efficient path selection protocol for data forwarding using optimum routes, while avoiding untrusted and energy depleted nodes, thereby improving packet delivery ratio and throughput with minimal network delay.

1.7 Research Scope and Assumptions

The scope of this research includes the following limitations and assumptions:

i. The participating sensor nodes in a network have similar resources in terms of energy, power processing, interface and memory (AlFarraj *et al.*, 2018; Baradaran and Navi, 2017; Juliana and Maheswari, 2016).
ii. The malicious sensor nodes intentionally drop the packets. Malicious node attacks manifest as Bad-Mouth, On-off and Denial of Service (DoS) (Caminha *et al.*, 2018; Desai and Nene, 2019; Liu *et al.*, 2016; Teng *et al.*, 2020).
iii. The malicious nodes do not collude themselves (Choudhury *et al.*, 2002; Iqbal *et al.*, 2016; Shamshirband *et al.*, 2014).
iv. Source and destination nodes are not malicious (Ahmed *et al.*, 2015; Zahariadis *et al.*, 2013).
v. After initial deployment, no new nodes added to the network Baradaran and Navi (2017).
vi. OMNeT++ (version 3.3), simulator is used to conduct the experiments Vargas (2011).

1.8 Significance of Research

The emerging WSN field has the potential to affect almost every aspect of modern life. Given this potential and widespread presence, it is important to secure WSNs against the actions of MNs. The fulfilment of the research objectives will contribute to the development of a reliable trust and energy based routing mechanism capable of repelling internal attacks that occur due to compromised nodes. This mechanism will therefore enable WSN users to route data in a relatively safe manner, while also optimising the use of limited energy resources. Moreover, the proposed BTES offers a realistic solution that could be viable in real world applications, such as wildfire based disaster scenarios where the adverse impact of an MN attack would degrade performance and threaten the credibility of sensed information. The proposed trust and energy aware routing mechanism will also make a meaningful contribution to the broader research domain in the following contexts:

i. Unsupervised and challenging environments such as wildfire monitoring where human interaction is difficult and deployed sensor nodes are therefore more exposed to malicious attacks, where compromised nodes significantly and randomly drop critical data packets. By isolating the MN quickly, the proposed BTES offers reliable data delivery and improves network trustworthiness levels.

ii. In areas where sensor nodes are deployed heavily, periodic re-evaluation of energy levels between communicating nodes improves reliability, trust detection rates and network performance. The SECS presented in this research improves node energy levels through state monitoring and the consideration of residual energy levels to ensure trustworthiness.

iii. The proposed TEEPS protocol is suitable for a wide range of sensor-based applications that are energy limited and require reliable data delivery. Such applications can benefit from improved packet delivery ratio while minimising routing overheads and delay.

1.9 Thesis Organization

The thesis is structured into seven chapters, which provide an overview of the steps taken in the current research. Chapter 1 provides an introduction and background to this study. Chapter 2 provides an in-depth literature review into the extant research conducted in this field. Chapter 3 presents the details of the chosen methodology adopted for this research, including the operational framework used for the design and development of the proposed trust and energy efficient routing protocol for WSNs. Chapter 4 discusses the specifics of the design and development of the Belief based Trust Evaluation Scheme (BTES), after which chapter 5 presents the State based Energy Calculation Scheme (SECS) used to periodically evaluate the energy level based on the node state. Chapter 6 then discusses the trust and energy efficient path selection (TEEPS) protocol utilised in this study to provide reliable data delivery. This three phase protocol is tested in a simulation that uses a range of performance based performance evaluation metrics against a sample of contemporary trust and energy aware algorithms. Finally, Chapter 7 provides a conclusion to this study, describing the contribution of this research and suggesting possible avenues for future investigations in this area.

REFERENCES

Abdal-Kadhim, A. M., and Leong, K. S. (2020). Event Priority Driven Dissemination EPDD management algorithm for low power WSN nodes powered by a dual source energy harvester. *AEU-International Journal of Electronics and Communications, 113*, 152988.

Abdalzaher, M. S., Seddik, K., Elsabrouty, M., Muta, O., Furukawa, H., and Abdel-Rahman, A. (2016). Game theory meets wireless sensor networks security requirements and threats mitigation: A survey. *Sensors, 16*(7), 1003.

Abdellatif, T., and Mosbah, M. (2020). Efficient monitoring for intrusion detection in wireless sensor networks. *Concurrency and Computation: Practice and Experience, 32*(15), e4907.

Ahmed, A., Bakar, K. A., Channa, M. I., Haseeb, K., and Khan, A. W. (2015). TERP: A trust and energy aware routing protocol for wireless sensor network. *IEEE Sensors Journal, 15*(12), 6962-6972.

Airehrour, D., Gutierrez, J., and Ray, S. K. (2016). Secure routing for internet of things: A survey. *Journal of Network and Computer Applications, 66*, 198-213.

Aivaloglou, E., and Gritzalis, S. (2010). Hybrid trust and reputation management for sensor networks. *Wireless Networks, 16*(5), 1493-1510.

Aivaloglou, E., Gritzalis, S., and Skianis, C. (2008). Trust establishment in sensor networks: behaviour-based, certificate-based and a combinational approach. *International Journal of System of Systems Engineering, 1*(1-2), 128-148.

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. (2002). Wireless sensor networks: a survey. *Computer networks, 38*(4), 393-422.

Al-Riyami, A., Zhang, N., and Keane, J. (2016). An adaptive early node compromise detection scheme for hierarchical WSNs. *IEEE Access, 4*, 4183-4206.

AlFarraj, O., AlZubi, A., and Tolba, A. (2018). Trust-based neighbor selection using activation function for secure routing in wireless sensor networks. *Journal of Ambient Intelligence and Humanized Computing*, 1-11.

Ali, A., Ming, Y., Chakraborty, S., and Iram, S. (2017). A comprehensive survey on real-time applications of WSN. *Future Internet, 9*(4), 77.

Ali, H. (2020). Multiprocessor System-on-Chips based Wireless Sensor Network Energy Optimization.

Alkhatib, A. A. (2013). Smart and low cost technique for forest fire detection using wireless sensor network. *International Journal of Computer Applications, 81*(11).

Almalkawi, I. T., Guerrero Zapata, M., and Al-Karaki, J. N. (2012). A cross-layer-based clustered multipath routing with QoS-aware scheduling for wireless multimedia sensor networks. *International Journal of Distributed Sensor Networks, 8*(5), 392515.

Almomani, I., Al-Kasasbeh, B., and Al-Akhras, M. (2016). WSN-DS: a dataset for intrusion detection systems in wireless sensor networks. *Journal of Sensors, 2016*.

Alshehri, M. D., and Hussain, F. K. (2018). A fuzzy security protocol for trust management in the internet of things (Fuzzy-IoT). *Computing*, 1-28.

Alwan, H., and Agarwal, A. (2013). *Multi-objective QoS routing for wireless sensor networks*. Paper presented at the International Conference on Computing, Networking and Communications (ICNC).

Amutha, J., Sharma, S., and Nagar, J. (2020). WSN strategies based on sensors, deployment, sensing models, coverage and energy efficiency: Review, approaches and open issues. *Wireless Personal Communications, 111*(2), 1089-1115.

Anastasi, G., Conti, M., Di Francesco, M., and Passarella, A. (2009). Energy conservation in wireless sensor networks: A survey. *Ad hoc networks, 7*(3), 537-568.

Anbuchelian, S., Selvamani, K., and Chandarasekar, A. (2014). *An energy efficient multipath routing scheme by preventing threats in Wireless Sensor Networks*. Paper presented at the 27th Canadian Conference on Electrical and Computer Engineering (CCECE), 2014 IEEE

Anisi, M. H., Abdullah, A. H., Razak, S. A., and Ngadi, M. A. (2012). Overview of data routing approaches for wireless sensor networks. *Sensors, 12*(4), 3964-3996.

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.

Anita, X., Martin Leo Manickam, J., and Bhagyaveni, M. A. (2013). Two-way acknowledgment-based trust framework for wireless sensor networks. *International Journal of Distributed Sensor Networks, 9*(5), 952905.

Arampatzis, T., Lygeros, J., and Manesis, S. (2005). *A survey of applications of wireless sensors and wireless sensor networks*. Paper presented at the Intelligent Control, 2005. Proceedings of the 2005 IEEE International Symposium on, Mediterrean Conference on Control and Automation.

Aranzazu-Suescun, C., and Cardei, M. (2017). *Reactive Routing Protocol for Event Reporting in Mobile-Sink Wireless Sensor Networks*. Paper presented at the 13th ACM Symposium on QoS and Security for Wireless and Mobile Networks.

Atzori, L., Iera, A., and Morabito, G. (2010). The internet of things: A survey. *Computer networks, 54*(15), 2787-2805.

Baker, S. B., Xiang, W., and Atkinson, I. (2017). Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities. *IEEE Access, 5*, 26521-26544.

Balamurugan, M., and Poongodi, R. (2014). Effective Lightweight Trust Decision Making Scheme for Wireless Sensor Networks. *Journal of Theoretical & Applied Information Technology, 67*(3).

Bao, F. (2013). *Dynamic Trust Management for Mobile Networks and Its Applications.* Virginia Tech.

Bao, F., Chen, R., Chang, M., and Cho, J.-H. (2011). *Trust-based intrusion detection in wireless sensor networks*. Paper presented at the IEEE International Conference on Communications (ICC).

Bao, F., Chen, R., Chang, M., and 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.

Baradaran, A. A., and Navi, K. (2017). CAST-WSN: The presentation of new clustering algorithm based on Steiner tree and C-means algorithm

improvement in wireless sensor networks. *Wireless Personal Communications, 97*(1), 1323-1344.

Batra, P. K., and Kant, K. (2016). LEACH-MAC: a new cluster head selection algorithm for Wireless Sensor Networks. *Wireless Networks, 22*(1), 49-60.

Bhat, P., and Reddy, K. S. (2015). *Energy efficient detection of malicious nodes using secure clustering with load balance and reliable node disjoint multipath routing in wireless sensor networks*. Paper presented at the International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2015.

Bhushan, B., and Sahoo, G. (2020). *Requirements, Protocols, and Security Challenges in Wireless Sensor Networks: An Industrial Perspective*: Springer.

Bißmeyer, N. (2014). *Misbehavior detection and attacker identification in vehicular ad-hoc networks.* Technische Universität.

Boukerch, A., Xu, L., and El-Khatib, K. (2007). Trust-based security for wireless ad hoc and sensor networks. *Computer Communications, 30*(11-12), 2413-2427.

Bravo, I., Palomar, E., Gardel, A., and Lázaro, J. L. (2017). Trusted and Secure Wireless Sensor Network Designs and Deployments: Multidisciplinary Digital Publishing Institute.

Byers, J., and Nasser, G. (2000). *Utility-based decision-making in wireless sensor networks*. Paper presented at the 1st ACM International Symposium on Mobile ad hoc networking & computing.

Caminha, J., Perkusich, A., and Perkusich, M. (2018). A Smart Trust Management Method to Detect On-Off Attacks in the Internet of Things. *Security and Communication Networks, 2018*.

Can, O., and Sahingoz, O. K. (2015). *A survey of intrusion detection systems in wireless sensor networks*. Paper presented at the 6th International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO), 2015

Cardei, M., MacCallum, D., Cheng, M. X., Min, M., Jia, X., Li, D., et al. (2002). Wireless sensor networks with energy efficient organization. *Journal of Interconnection Networks, 3*(03n04), 213-229.

Carneiro, G. (2010). *NS-3: Network simulator 3*.

Chakrabarti, A., Parekh, V., and Ruia, A. (2012). *A trust based routing scheme for wireless sensor networks*. Paper presented at the International Conference on Computer Science and Information Technology, 159-169.

Chakraborty, M., and Chaki, N. (2012). ETSeM: a energy-aware, trust-based, selective multi-path routing protocol. *Computer Information Systems and Industrial Management*, 351-360.

Chen, D.-R., Chen, L.-C., Chen, M.-Y., and Hsu, M.-Y. (2019). A coverage-aware and energy-efficient protocol for the distributed wireless sensor networks. *Computer Communications, 137*, 15-31.

Chen, D., Chang, G., Sun, D., Li, J., Jia, J., and Wang, X. (2011). TRM-IoT: A trust management model based on fuzzy reputation for internet of things. *Computer Science and Information Systems, 8*(4), 1207-1228.

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

Chen, M., Gonzalez, S., and Leung, V. C. (2007). Applications and design issues for mobile agents in wireless sensor networks. *IEEE Wireless Communications, 14*(6), 20-26.

Chen, R., Bao, F., Chang, M., and Cho, J.-H. (2014). Dynamic trust management for delay tolerant networks and its application to secure routing. *IEEE Transactions on Parallel and Distributed Systems, 25*(5), 1200-1210.

Chen, R., and Guo, J. (2014). *Dynamic hierarchical trust management of mobile groups and its application to misbehaving node detection*. Paper presented at the 28th International Conference on Advanced Information Networking and Applications (AINA), IEEE

Chen, Z., Liu, A., Li, Z., Choi, Y.-J., Sekiya, H., and Li, J. (2017a). Energy-efficient broadcasting scheme for smart industrial wireless sensor networks. *Mobile Information Systems, 2017*.

Chen, Z., Tian, L., and Lin, C. (2017b). Trust model of wireless sensor networks and its application in data fusion. *Sensors, 17*(4), 703.

Cheng, H., Xiong, N., Vasilakos, A. V., Yang, L. T., Chen, G., and Zhuang, X. (2012). Nodes organization for channel assignment with topology preservation in multi-radio wireless mesh networks. *Ad Hoc Networks, 10*(5), 760-773.

Cho, K., and Cho, Y. (2020). HyperLedger Fabric-Based Proactive Defense against Inside Attackers in the WSN With Trust Mechanism. *Electronics, 9*(10), 1659.

Choudhury, R. R., Yang, X., Ramanathan, R., and Vaidya, N. H. (2002). *Using directional antennas for medium access control in ad hoc networks*. Paper

presented at the 8th annual international conference on Mobile computing and networking.

Chuang, P.-J., and Jiang, Y.-J. (2014). Effective neural network-based node localisation scheme for wireless sensor networks. *IET Wireless Sensor Systems, 4*(2), 97-103.

Conti, M., Di Pietro, R., Mancini, L. V., and Mei, A. (2007). *A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks*. Paper presented at the 8th ACM international symposium on Mobile ad hoc networking and computing.

Crosby, G. V., Hester, L., and 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, Z., Fei, X., Zhang, S., Cai, X., Cao, Y., Zhang, W., et al. (2020). A hybrid BlockChain-based identity authentication scheme for multi-WSN. *IEEE Transactions on Services Computing, 13*(2), 241-251.

Daia, A. S. A., Ramadan, R. A., Fayek, M. B., and AETiC, A. (2018). Sensor networks attacks classifications and mitigation. *Annals of Emerging Technologies in Computing (AETiC), Print ISSN*, 2516-0281.

Darwish, A., and Hassanien, A. E. (2011). Wearable and implantable wireless sensor network solutions for healthcare monitoring. *Sensors, 11*(6), 5561-5595.

Dasgupta, K., Kalpakis, K., and Namjoshi, P. (2003). *An efficient clustering-based heuristic for data gathering and aggregation in sensor networks*. Paper presented at the WCNC.

Desai, S. S., and Nene, M. J. (2019). Node-Level Trust Evaluation in Wireless Sensor Networks. *IEEE Transactions on Information Forensics and Security*.

Developer, O. OMNET++ Network Simulation Frame-work.

Dong, L., Tao, H., Doherty, W., and Young, M. (2015). A sleep scheduling mechanism with PSO collaborative evolution for wireless sensor networks. *International Journal of Distributed Sensor Networks, 11*(3), 517250.

Dong, Y., Han, G., Shu, L., Guo, H., and Zhu, C. (2013). *Two-hop geographic multipath routing in duty-cycled wireless sensor networks*. Paper presented at the International Wireless Internet Conference.

Douceur, J. R. (2002). *The sybil attack.* Paper presented at the International workshop on peer-to-peer systems, 251-260.

Duan, J., Gao, D., Yang, D., Foh, C. H., and Chen, H.-H. (2014b). An energy-aware trust derivation scheme with game theoretic approach in wireless sensor networks for IoT applications. *IEEE Internet of Things Journal, 1*(1), 58-69.

Duan, J., Yang, D., Zhu, H., Zhang, S., and Zhao, J. (2014). TSRF: A trust-aware secure routing framework in wireless sensor networks. *International Journal of Distributed Sensor Networks, 10*(1), 209436.

Durrani, N. M., Kafi, N., Shamsi, J., Haider, W., and Abbsi, A. M. (2013). *Secure multi-hop routing protocols in Wireless Sensor Networks: Requirements, challenges and solutions*. Paper presented at the Eighth International Conference on Digital Information Management (ICDIM 2013).

Eissa, T., Razak, S. A., Khokhar, R. H., and Samian, N. (2013). Trust-based routing mechanism in MANET: Design and implementation. *Mobile Networks and Applications, 18*(5), 666-677.

Elhoseny, M., and Hassanien, A. E. (2019). Secure data transmission in WSN: an overview. In *Dynamic Wireless Sensor Networks* (pp. 115-143): Springer.

Fang, W., Zhang, W., Chen, W., Liu, Y., and Tang, C. (2019). TMSRS: trust management-based secure routing scheme in industrial wireless sensor network with fog computing. *Wireless Networks*, 1-14.

Farooq, H., and Tang Jung, L. (2013a). Energy, traffic load, and link quality aware Ad Hoc routing protocol for wireless sensor network based smart metering infrastructure. *International Journal of Distributed Sensor Networks, 2013*.

Farooq, H., and Tang Jung, L. (2013b). Energy, traffic load, and link quality aware Ad Hoc routing protocol for wireless sensor network based smart metering infrastructure. *International Journal of Distributed Sensor Networks, 9*(8), 597582.

Farsi, M., Elhosseini, M. A., Badawy, M., Ali, H. A., and Eldin, H. Z. (2019). Deployment techniques in wireless sensor networks, coverage and connectivity: A survey. *IEEE Access, 7*, 28940-28954.

Feng, R., Che, S., Wang, X., and Yu, N. (2013). Trust management scheme based on DS evidence theory for wireless sensor networks. *International Journal of Distributed Sensor Networks, 9*(6), 948641.

Galmés, S., and Escolar, S. (2018). Analytical Model for the Duty Cycle in Solar-Based EH-WSN for Environmental Monitoring. *Sensors, 18*(8), 2499.

Ganeriwal, 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.

Geetha, V., and Chandrasekaran, K. (2014). A distributed trust based secure communication framework for wireless sensor network. *Wireless Sensor Network, 6*(09), 173.

Ghani, A., Mansoor, K., Mehmood, S., Chaudhry, S. A., Rahman, A. U., and Najmus Saqib, M. (2019). Security and key management in IoT-based wireless sensor networks: An authentication protocol using symmetric key. *International Journal of Communication Systems, 32*(16), e4139.

Ghugar, U., Pradhan, J., Bhoi, S. K., and Sahoo, R. R. (2019). LB-IDS: Securing wireless sensor network using protocol layer trust-based intrusion detection system. *Journal of Computer Networks and Communications, 2019*.

Giruka, V. C., Singhal, M., Royalty, J., and Varanasi, S. (2008). Security in wireless sensor networks. *Wireless communications and mobile computing, 8*(1), 1-24.

Gomathi, S., and Gopala Krishnan, C. (2020). Malicious Node Detection in Wireless Sensor Networks Using an Efficient Secure Data Aggregation Protocol. *Wireless Personal Communications*, 1-16.

Gong, P., Chen, T. M., and Xu, Q. (2015). ETARP: An energy efficient trust-aware routing protocol for wireless sensor networks. *Journal of Sensors, 2015*.

Gopal, R., Parthasarathy, V., and Mani, A. (2013). *Techniques to identify and eliminate malicious nodes in cooperative wireless networks*. Paper presented at the International Conference on Computer Communication and Informatics (ICCCI).

Govindan, K., and Mohapatra, P. (2012). Trust computations and trust dynamics in mobile adhoc networks: A survey. *IEEE Communications Surveys & Tutorials, 14*(2), 279-298.

Grgic, K., Zagar, D., and Krizanovic Cik, V. (2016). System for malicious node detection in IPv6-based wireless sensor networks. *Journal of Sensors, 2016*.

Gupta, A., Pandey, O. J., Shukla, M., Dadhich, A., Ingle, A., and Gawande, P. (2014). *Towards context-aware smart mechatronics networks: Integrating swarm intelligence and ambient intelligence*. Paper presented at the International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT).

Hammoudeh, M., and Newman, R. (2015). Adaptive routing in wireless sensor networks: QoS optimisation for enhanced application performance. *Information Fusion, 22*, 3-15.

Hamzeloei, F., and Dermany, M. K. (2016). A TOPSIS based cluster head selection for wireless sensor network. *Procedia Computer Science, 98*, 8-15.

Han, G., Jiang, J., Shu, L., Niu, J., and 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.

Haseeb, K., Almogren, A., Islam, N., Ud Din, I., and Jan, Z. (2019). An Energy-Efficient and Secure Routing Protocol for Intrusion Avoidance in IoT-Based WSN. *Energies, 12*(21), 4174.

Hassan, M. U., Shahzaib, M., Shaukat, K., Hussain, S. N., Mubashir, M., Karim, S., et al. (2019). *DEAR-2: An Energy-Aware Routing Protocol with Guaranteed Delivery in Wireless Ad-hoc Networks*: Springer.

He, J., Duan, L., Hou, F., Cheng, P., and Chen, J. (2015). Multiperiod scheduling for wireless sensor networks: A distributed consensus approach. *IEEE Transactions on Signal Processing, 63*(7), 1651-1663.

He, Y., Han, G., Wang, H., Ansere, J. A., and Zhang, W. (2019). A sector-based random routing scheme for protecting the source location privacy in WSNs for the Internet of Things. *Future Generation Computer Systems, 96*, 438-448.

Heinzelman, W. B., Chandrakasan, A. P., and Balakrishnan, H. (2002). An application-specific protocol architecture for wireless microsensor networks. *IEEE Transactions on wireless communications, 1*(4), 660-670.

Henderson, T. R., Roy, S., Floyd, S., and Riley, G. F. (2006). *ns-3 project goals*. Paper presented at the Workshop on ns-2: the IP network simulator.

Hong, Z., Shao, Q., Liao, X., and Beyah, R. (2018). A secure routing protocol with regional partitioned clustering and Beta trust management in smart home. *Wireless Networks*, 1-19.

Hongjun, D., Zhiping, J., and Xiaona, D. (2008). *An entropy-based trust modeling and evaluation for wireless sensor networks.* Paper presented at the Embedded Software and Systems, 2008. ICESS'08. International Conference on, 27-34.

Hu, Y.-C., Perrig, A., and Johnson, D. B. (2006). Wormhole attacks in wireless networks. *IEEE journal on selected areas in communications, 24*(2), 370-380.

Hu, Z., Bie, Y., and Zhao, H. (2015). Trusted tree-based trust management scheme for secure routing in wireless sensor networks. *International Journal of Distributed Sensor Networks, 11*(12), 385849.

Hwang, P., and Burgers, W. P. (1997). Properties of trust: An analytical view. *Organizational behavior and human decision processes, 69*(1), 67-73.

Iqbal, S., Abdullah, A. H., Mohamad, M. M., Qureshi, K. N., and Hussain, K. (2016). Adaptive Interface Reconfiguration in Low-Rate Mesh WPANs. *Journal of Computational and Theoretical Nanoscience, 13*(7), 4703-4710.

Iqbal, U., and Shafi, S. (2019). *A provable and secure key exchange protocol based on the elliptical curve diffe–hellman for wsn*: Springer.

Ishmanov, F., and Bin Zikria, Y. (2017). Trust mechanisms to secure routing in wireless sensor networks: current state of the research and open research issues. *Journal of Sensors, 2017*.

Ishmanov, F., Kim, S. W., and Nam, S. Y. (2014). A secure trust establishment scheme for wireless sensor networks. *Sensors, 14*(1), 1877-1897.

Ishmanov, F., Malik, A. S., Kim, S. W., and Begalov, B. (2015). Trust management system in wireless sensor networks: design considerations and research challenges. *Transactions on Emerging Telecommunications Technologies, 26*(2), 107-130.

Issariyakul, T., and Hossain, E. (2009). *Introduction to network simulator 2 (NS2)*: Springer.

Issariyakul, T., and Hossain, E. (2012). *Introduction to Network Simulator 2 (NS2)*: Springer.

Jadidoleslamy, H., Aref, M. R., and Bahramgiri, H. (2016). A fuzzy fully distributed trust management system in wireless sensor networks. *AEU-International Journal of Electronics and Communications, 70*(1), 40-49.

Jain, A., Khari, M., Verdu, E., Omatsu, S., and Crespo, R. G. (2020). A route selection approach for variable data transmission in wireless sensor networks. *Cluster Computing - The Journal of Networks Software Tools and Applications*.

Jain, A. K., Khare, A., and Pandey, K. K. (2012). *Developing an efficient framework for real time monitoring of forest fire using wireless sensor network*. Paper presented at the 2012 2nd IEEE International Conference on Parallel Distributed and Grid Computing (PDGC).

Jaiswal, K., and Anand, V. (2019). EOMR: An energy-efficient optimal multi-path routing protocol to improve QoS in wireless sensor network for IoT applications. *Wireless Personal Communications*, 1-23.

Jawad, H., Nordin, R., Gharghan, S., Jawad, A., and Ismail, M. (2017a). Energy-efficient wireless sensor networks for precision agriculture: A review. *Sensors, 17*(8), 1781.

Jawad, H. M., Nordin, R., Gharghan, S. K., Jawad, A. M., and Ismail, M. (2017b). Energy-Efficient wireless sensor networks for precision agriculture: A review. *Sensors, 17*(8), 1781.

Jayarajan, P., Kanagachidambaresan, G., Sundararajan, T., Sakthipandi, K., Maheswar, R., and Karthikeyan, A. (2020). An energy-aware buffer management (EABM) routing protocol for WSN. *The Journal of Supercomputing, 76*(6), 4543-4555.

Jhaveri, R. H., Patel, N. M., Zhong, Y., and Sangaiah, A. K. (2018). Sensitivity analysis of an attack-pattern discovery based trusted routing scheme for mobile ad-hoc networks in industrial IoT. *IEEE Access, 6*, 20085-20103.

Jiang, D., Ying, X., Han, Y., and Lv, Z. (2016). Collaborative multi-hop routing in cognitive wireless networks. *Wireless personal communications, 86*(2), 901-923.

Jiang, J., Han, G., Wang, F., Shu, L., and Guizani, M. (2015). An efficient distributed trust model for wireless sensor networks. *IEEE Transactions on Parallel & Distributed Systems*(1), 1-1.

Jin, J., and Ahn, S. (2016). A Multipath Routing Protocol Based on Bloom Filter for Multihop Wireless Networks. *Mobile Information Systems, 2016*.

Jin, Z., Ma, Y., Su, Y., Li, S., and Fu, X. (2017). A Q-learning-based delay-aware routing algorithm to extend the lifetime of underwater sensor networks. *Sensors, 17*(7), 1660.

Jøsang, A. (2001). A logic for uncertain probabilities. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 9*(03), 279-311.

Juliana, R., and Maheswari, P. U. (2016). An energy efficient cluster head selection technique using network trust and swarm intelligence. *Wireless Personal Communications, 89*(2), 351-364.

Kannan, G., and Raja, T. S. R. (2015). Energy efficient distributed cluster head scheduling scheme for two tiered wireless sensor network. *Egyptian Informatics Journal, 16*(2), 167-174.

Karim, L., Nasser, N., and Sheltami, T. (2014). A fault-tolerant energy-efficient clustering protocol of a wireless sensor network. *Wireless Communications and Mobile Computing, 14*(2), 175-185.

Karlof, C., and Wagner, D. (2003). *Secure routing in wireless sensor networks: Attacks and countermeasures*. Paper presented at the International Workshop on Sensor Network Protocols and Applications.

Karthik, N., and Ananthanarayana, V. (2017a). *Data trust model for event detection in wireless sensor networks using data correlation techniques*. Paper presented at the Fourth International Conference on Signal Processing, Communication and Networking (ICSCN).

Karthik, N., and Ananthanarayana, V. (2017b). A Hybrid Trust Management Scheme for Wireless Sensor Networks. *Wireless Personal Communications, 97*(4), 5137-5170.

Khalid, O., Khan, S. U., Madani, S. A., Hayat, K., Khan, M. I., Min-Allah, N., et al. (2013). Comparative study of trust and reputation systems for wireless sensor networks. *Security and Communication Networks, 6*(6), 669-688.

Khalil, I., Bagchi, S., Rotaru, C. N., and Shroff, N. B. (2010). UnMask: Utilizing neighbor monitoring for attack mitigation in multihop wireless sensor networks. *Ad Hoc Networks, 8*(2), 148-164.

Khan, M. S., Midi, D., Khan, M. I., and Bertino, E. (2015). *Adaptive trust threshold strategy for misbehaving node detection and isolation*. Paper presented at the Trustcom/BigDataSE/ISPA, 2015 IEEE.

Khan, T., Singh, K., Abdel-Basset, M., Long, H. V., Singh, S. P., and Manjul, M. (2019). A novel and comprehensive trust estimation clustering based approach for large scale wireless sensor networks. *IEEE Access, 7*, 58221-58240.

Kim, T. K., and Seo, H. S. (2008). A trust model using fuzzy logic in wireless sensor network. *World academy of science, engineering and technology, 42*(6), 63-66.

Kukunuru, N. (2019). Secure and Energy Aware Shortest Path Routing Framework for WSN. In *Data Management, Analytics and Innovation* (pp. 379-390): Springer.

Kulin, M., Fortuna, C., De Poorter, E., Deschrijver, D., and Moerman, I. (2016). Data-driven design of intelligent wireless networks: An overview and tutorial. *Sensors, 16*(6), 790.

Kumar, A., Kaushik, S. K., Sharma, R., and Raj, P. (2012). *Simulators for wireless networks: A comparative study*. Paper presented at the International Conference on Computing Sciences (ICCS), 2012.

Kumar, S., and Mehfuz, S. (2019). *A PSO based malicious node detection and energy efficient clustering in wireless sensor network.* Paper presented at the 2019 6th International Conference on Signal Processing and Integrated Networks (SPIN), 859-863.

Labraoui, N., Gueroui, M., and Sekhri, L. (2016). A risk-aware reputation-based trust management in wireless sensor networks. *Wireless Personal Communications, 87*(3), 1037-1055.

Lee, S. H., Kim, H., and Choi, L. (2016). Sleep Control Game for Wireless Sensor Networks. *Mobile Information Systems, 2016*.

Leligou, H.-C., Trakadas, P., Maniatis, S., Karkazis, P., and Zahariadis, T. (2012). Combining trust with location information for routing in wireless sensor networks. *Wireless Communications and Mobile Computing, 12*(12), 1091-1103.

Li, J., Li, R., and Kato, J. (2008). Future trust management framework for mobile ad hoc networks. *IEEE Communications Magazine, 46*(4).

Li, M., Li, Z., and Vasilakos, A. V. (2013). A survey on topology control in wireless sensor networks: Taxonomy, comparative study, and open issues. *Proceedings of the IEEE, 101*(12), 2538-2557.

Li, X., Jia, Z., Zhang, P., Zhang, R., and Wang, H. (2010). Trust-based on-demand multipath routing in mobile ad hoc networks. *IET information security, 4*(4), 212-232.

Li, Y., Xu, H., Cao, Q., Li, Z., and Shen, S. (2015). Evolutionary game-based trust strategy adjustment among nodes in wireless sensor networks. *International Journal of Distributed Sensor Networks, 11*(2), 818903.

Liangzhou, C., Wenkang, S., and Feng, D. (2005). New weighting factors assignment of evidence theory based one vidence distance. *Journal of Systems Engineering and Electronics, 16*(2), 273-278.

Lien, C.-h., Wu, J.-J., Chen, Y.-H., and Wang, C.-J. (2014). Trust transfer and the effect of service quality on trust in the healthcare industry. *Managing Service Quality, 24*(4), 399-416.

Lim, S. Y., and Choi, Y.-H. (2013). Malicious node detection using a dual threshold in wireless sensor networks. *Journal of Sensor and Actuator Networks, 2*(1), 70-84.

Lin, H.-H., Shih, M.-J., Wei, H.-Y., and Vannithamby, R. (2015). DeepSleep: IEEE 802.11 enhancement for energy-harvesting machine-to-machine communications. *Wireless Networks, 21*(2), 357-370.

Liu, A., and Zhao, S. (2018). High-performance target tracking scheme with low prediction precision requirement in WSNs. *International Journal of Ad Hoc and Ubiquitous Computing, 29*(4), 270-289.

Liu, X., Dong, M., Ota, K., Yang, L. T., and Liu, A. (2018a). Trace malicious source to guarantee cyber security for mass monitor critical infrastructure. *Journal of Computer and System Sciences, 98*, 1-26.

Liu, X., Xiong, N., Zhang, N., Liu, A., Shen, H., and Huang, C. (2018b). A trust with abstract information verified routing scheme for cyber-physical network. *IEEE Access, 6*, 3882-3898.

Liu, Y., Dong, M., Ota, K., and Liu, A. (2016). ActiveTrust: secure and trustable routing in wireless sensor networks. *IEEE Transactions on Information Forensics and Security, 11*(9), 2013-2027.

Ma, X., Liu, Q., and Zhan, J. (2017). A survey of decision making methods based on certain hybrid soft set models. *Artificial Intelligence Review, 47*(4), 507-530.

Mahajan, S., Malhotra, J., and Sharma, S. (2014). An energy balanced QoS based cluster head selection strategy for WSN. *Egyptian Informatics Journal, 15*(3), 189-199.

Mahalle, P. N., Thakre, P. A., Prasad, N. R., and Prasad, R. (2013). *A fuzzy approach to trust based access control in internet of things*. Paper presented at the Wireless VITAE 2013.

Marchang, N., and Datta, R. (2012). Light-weight trust-based routing protocol for mobile ad hoc networks. *IET Information security, 6*(2), 77-83.

Mármol, F. G., and Pérez, G. M. (2011). Providing trust in wireless sensor networks using a bio-inspired technique. *Telecommunication systems, 46*(2), 163-180.

Marsh, S. P. (1994). Formalising trust as a computational concept.

Marzi, H., and Marzi, A. (2014). *A security model for wireless sensor networks.* Paper presented at the Computational Intelligence and Virtual Environments for Measurement Systems and Applications (CIVEMSA), 2014 IEEE International Conference on, 64-69.

Mejia, M., Peña, N., Muñoz, J. L., Esparza, O., and Alzate, M. A. (2011). A game theoretic trust model for on-line distributed evolution of cooperation inMANETs. *Journal of Network and Computer Applications, 34*(1), 39-51.

Mendoza, C. V., and Kleinschmidt, J. H. (2015). Mitigating On-Off attacks in the Internet of Things using a distributed trust management scheme. *International Journal of Distributed Sensor Networks, 11*(11), 859731.

Mendoza, C. V. L., and Kleinschmidt, J. H. (2018a). A distributed trust management mechanism for the Internet of things using a multi-service approach. *Wireless Personal Communications, 103*(3), 2501-2513.

Mendoza, C. V. L., and Kleinschmidt, J. H. (2018b). A Distributed Trust Management Mechanism for the Internet of Things Using a Multi-Service Approach. *Wireless Personal Communications*, 1-13.

Merrett, G. V., White, N. M., Harris, N. R., and Al-Hashimi, B. M. (2009). *Energy-aware simulation for wireless sensor networks*. Paper presented at the 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks.

Miglani, A., Bhatia, T., and Goel, S. (2015). *TRUST based energy efficient routing in LEACH for wireless sensor network*. Paper presented at the Global Conference on Communication Technologies (GCCT).

Minakov, I., Passerone, R., Rizzardi, A., and Sicari, S. (2016). A comparative study of recent wireless sensor network simulators. *ACM Transactions on Sensor Networks (TOSN), 12*(3), 20.

Mohd, N., Singh, A., and Bhadauria, H. (2020). A novel SVM based IDS for distributed denial of sleep strike in wireless sensor networks. *Wireless Personal Communications, 111*(3), 1999-2022.

Molina-Pico, A., Cuesta-Frau, D., Araujo, A., Alejandre, J., and Rozas, A. (2016). Forest monitoring and wildland early fire detection by a hierarchical wireless sensor network. *Journal of Sensors, 2016*.

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

Momani, M., Challa, S., and Alhmouz, R. (2008). *Can we trust trusted nodes in wireless sensor networks?* Paper presented at the International Conference on Computer and Communication Engineering ICCCE 2008.

Momani, M. C., and GTRSSN, S. (2008). Gaussian Trust and Reputation System for Sensor Networks Book Title: Advances in Computer and Information Sciences and Engineering: Springer Netherlands.

Naderi, O., Shahedi, M., and Mazinani, S. M. (2015). A trust based routing protocol for mitigation of sinkhole attacks in wireless sensor networks. *International Journal of Information and Education Technology, 5*(7), 520-526.

Naik, S., and Shekokar, N. (2015). Conservation of energy in wireless sensor network by preventing denial of sleep attack. *Procedia Computer Science, 45*, 370-379.

Nazir, B., and Hasbullah, H. (2011). *Dynamic sleep scheduling for minimizing delay in wireless sensor network*. Paper presented at the Saudi International Electronics, Communications and Photonics Conference (SIECPC)

Nazir, B., Hasbullah, H., and Madani, S. A. (2011). Sleep/wake scheduling scheme for minimizing end-to-end delay in multi-hop wireless sensor networks. *EURASIP Journal on Wireless Communications and Networking, 2011*(1), 92.

Nie, S. (2017). A novel trust model of dynamic optimization based on entropy method in wireless sensor networks. *Cluster Computing*, 1-10.

Oh, S. H., Hong, C. O., and Choi, Y. H. (2012). A malicious and malfunctioning node detection scheme for wireless sensor networks. *Wireless sensor network, 4*(03), 84.

Oracevic, A., Akbaş, S., Ozdemir, S., and Kos, M. (2014). *Secure target detection and tracking in mission critical wireless sensor networks.* Paper presented at the Anti-counterfeiting, Security, and Identification (ASID), 2014 International Conference on, 1-5.

Pathan, M. S., Zhu, N., He, J., Zardari, Z. A., Memon, M. Q., and Hussain, M. I. (2018). An Efficient Trust-Based Scheme for Secure and Quality of Service Routing in MANETs. *Future Internet, 10*(2), 16.

Perkins, C., Belding-Royer, E., and Das, S. (2003). *Ad hoc on-demand distance vector (AODV) routing* (No. 2070-1721)o. Document Number)

Pirbhulal, S., Zhang, H., E Alahi, M. E., Ghayvat, H., Mukhopadhyay, S. C., Zhang, Y.-T., et al. (2016). A novel secure IoT-based smart home automation system using a wireless sensor network. *Sensors, 17*(1), 69.

Piro, G., Baldo, N., and Miozzo, M. (2011). *An LTE module for the ns-3 network simulator*. Paper presented at the 4th International ICST Conference on Simulation Tools and Techniques.

Prabha, V. R., and Latha, P. (2017). Fuzzy trust protocol for malicious node detection in wireless sensor networks. *Wireless Personal Communications, 94*(4), 2549-2559.

Priayoheswari, B., Kulothungan, K., and Kannan, A. (2016). *Beta reputation and direct trust model for secure communication in wireless sensor networks*. Paper presented at the International Conference on Informatics and Analytics.

Probst, M. J., and Kasera, S. K. (2007). *Statistical trust establishment in wireless sensor networks*. Paper presented at the International Conference on Parallel and Distributed Systems.

Pu, L., Chen, X., Xu, J., and Fu, X. (2016). D2D fogging: An energy-efficient and incentive-aware task offloading framework via network-assisted D2D collaboration. *IEEE Journal on Selected Areas in Communications, 34*(12), 3887-3901.

Qabulio, M., Malkani, Y. A., Memon, M. S., and Keerio, A. (2020). Security of Wireless Sensor Networks: The Current Trends and Issues. In *Industrial Internet of Things and Cyber-Physical Systems: Transforming the Conventional to Digital* (pp. 239-264): IGI Global.

Quan, Z., Wu, D., Xiao, D., Zhang, Y., and Tang, C. (2013). *An Energy Efficiency Trusted Dynamic Routing Protocol for Wireless Sensor Networks.* Paper presented at the Fourth International Conference on Emerging Intelligent Data and Web Technologies (EIDWT), 329-334.

Qureshi, K. N., Bashir, M. U., Lloret, J., and Leon, A. (2020a). Optimized Cluster-Based Dynamic Energy-Aware Routing Protocol for Wireless Sensor Networks in Agriculture Precision. *Journal of Sensors, 2020*.

Qureshi, K. N., Iftikhar, A., Bhatti, S. N., Piccialli, F., Giampaolo, F., and Jeon, G. (2020b). Trust management and evaluation for edge intelligence in the Internet of Things. *Engineering Applications of Artificial Intelligence, 94*, 103756.

Rajeshkumar, G., and Valluvan, K. (2017). An energy aware trust based Intrusion Detection System with adaptive acknowledgement for Wireless Sensor Network. *Wireless Personal Communications, 94*(4), 1993-2007.

Ramos, A. (2015). Sensor data security level estimation scheme for wireless sensor networks. *Sensors, 15*(1), 2104-2136.

Rani, R., Kumar, S., and Dohare, U. (2019). Trust Evaluation for Light Weight Security in Sensor Enabled Internet of Things: Game Theory Oriented Approach. *IEEE Internet of Things Journal*.

Rault, T., Bouabdallah, A., and Challal, Y. (2014). Energy efficiency in wireless sensor networks: A top-down survey. *Computer Networks, 67*, 104-122.

Raymond, D. R., and Midkiff, S. F. (2008). Denial-of-service in wireless sensor networks: Attacks and defenses. *IEEE Pervasive Computing*(1), 74-81.

Razaque, A., and Elleithy, K. M. (2015). Low duty cycle, energy-efficient and mobility-based boarder node—MAC hybrid protocol for wireless sensor networks. *Journal of Signal Processing Systems, 81*(2), 265-284.

Reddy, V. B., Negi, A., and Venkataraman, S. (2018). *Trust computation model using hysteresis curve for wireless sensor networks.* Paper presented at the 2018 IEEE SENSORS, 1-4.

Rehman, E., Sher, M., Naqvi, S. H. A., Badar Khan, K., and Ullah, K. (2017). Energy Efficient Secure Trust Based Clustering Algorithm for Mobile Wireless Sensor Network. *Journal of Computer Networks and Communications, 2017*.

Ren, Y., Zadorozhny, V. I., Oleshchuk, V. A., and Li, F. Y. (2014). A novel approach to trust management in unattended wireless sensor networks. *IEEE Transactions on Mobile Computing, 13*(7), 1409-1423.

Rezgui, A., and Eltoweissy, M. (2007). Tarp: A trust-aware routing protocol for sensor-actuator networks.

Richert, V., Issac, B., and Israr, N. (2017). Implementation of a modified wireless sensor network MAC protocol for critical environments. *Wireless Communications and Mobile Computing, 2017*.

Rikli, N.-E., and Alnasser, A. (2016). Lightweight trust model for the detection of concealed malicious nodes in sparse wireless ad hoc networks. *International Journal of Distributed Sensor Networks, 12*(7), 1550147716657246.

Rodrigues, L., Montez, C., Budke, G., Vasques, F., and Portugal, P. (2017). Estimating the lifetime of wireless sensor network nodes through the use of embedded analytical battery models. *Journal of Sensor and Actuator Networks, 6*(2), 8.

Roseline, R., and Sumathi, P. (2012). *Local clustering and threshold sensitive routing algorithm for Wireless Sensor Networks*. Paper presented at the International Conference on Devices, Circuits and Systems (ICDCS).

Saini, A., Kansal, A., and Randhawa, N. S. (2019). Minimization of energy consumption in WSN using hybrid WECRA approach. *Procedia Computer Science, 155*, 803-808.

Savas, O., Jin, G., and Deng, J. (2013). *Trust management in cloud-integrated wireless sensor networks*. Paper presented at the International Conference on Collaboration Technologies and Systems (CTS).

Schandy, J., Steinfeld, L., and Silveira, F. (2015). *Average power consumption breakdown of Wireless Sensor Network nodes using IPv6 over LLNs*. Paper presented at the International Conference on Distributed Computing in Sensor Systems.

Selvakumar, K., Sairamesh, L., and Kannan, A. (2017). An intelligent energy aware secured algorithm for routing in wireless sensor networks. *Wireless Personal Communications, 96*(3), 4781-4798.

Selvi, M., Thangaramya, K., Ganapathy, S., Kulothungan, K., Nehemiah, H. K., and Kannan, A. (2019). An energy aware trust based secure routing algorithm for effective communication in wireless sensor networks. *Wireless Personal Communications, 105*(4), 1475-1490.

Senthil, T., and Kannapiran, B. (2017). ECTMRA: Energy conserving trustworthy multipath routing algorithm based on cuckoo search algorithm. *Wireless Personal Communications, 94*(4), 2239-2258.

Shagari, N. M., Idris, M. Y. I., Salleh, R. B., Ahmedy, I., Murtaza, G., and Shehadeh, H. A. (2020). Heterogeneous Energy and Traffic Aware Sleep-Awake Cluster-Based Routing Protocol for Wireless Sensor Network. *IEEE Access, 8*, 12232-12252.

Shah, S. B., Chen, Z., Yin, F., Khan, I. U., and Ahmad, N. (2018). Energy and interoperable aware routing for throughput optimization in clustered IoT-wireless sensor networks. *Future Generation Computer Systems, 81*, 372-381.

Shahabi, S., Ghazvini, M., and Bakhtiarian, M. (2016). A modified algorithm to improve security and performance of AODV protocol against black hole attack. *Wireless Networks, 22*(5), 1505-1511.

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.

Shamshirb, S., Kalantari, S., sam Daliri, Z., and Ng, L. S. (2010). Expert security system in wireless sensor networks based on fuzzy discussion multi-agent systems. *Scientific Research and Essays, 5*(24), 3840-3849.

Shamshirband, S., Anuar, N. B., Kiah, M. L. M., Rohani, V. A., Petković, D., Misra, S., et al. (2014). Co-FAIS: cooperative fuzzy artificial immune system for detecting intrusion in wireless sensor networks. *Journal of Network and Computer Applications, 42*, 102-117.

Sharma, A., Pilli, E. S., Mazumdar, A. P., and Gera, P. (2020). Towards trustworthy Internet of Things: A survey on Trust Management applications and schemes. *Computer Communications*.

Sharma, V., Patel, R., Bhadauria, H., and Prasad, D. (2016). Deployment schemes in wireless sensor network to achieve blanket coverage in large-scale open area: A review. *Egyptian Informatics Journal, 17*(1), 45-56.

She, W., Liu, Q., Tian, Z., Chen, J.-S., Wang, B., and Liu, W. (2019). Blockchain trust model for malicious node detection in wireless sensor networks. *IEEE Access, 7*, 38947-38956.

Shen, S., Huang, L., Fan, E., Hu, K., Liu, J., and Cao, Q. (2016). Trust dynamics in WSNs: An evolutionary game-theoretic approach. *Journal of Sensors, 2016*.

Shukla, A., and Tripathi, S. (2020). An Effective Relay Node Selection Technique for Energy Efficient WSN-Assisted IoT. *Wireless Personal Communications*, 1-31.

Sicari, S., Rizzardi, A., Grieco, L. A., and Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer networks, 76*, 146-164.

Sobeih, A., Hou, J. C., Kung, L.-C., Li, N., Zhang, H., Chen, W.-P., et al. (2006). J-Sim: a simulation and emulation environment for wireless sensor networks. *IEEE Wireless Communications, 13*(4), 104-119.

Sridhar, S., Baskaran, R., and Chandrasekar, P. (2013). Energy supported AODV (EN-AODV) for QoS routing in MANET. *Procedia-Social and Behavioral Sciences, 73*, 294-301.

Srinivasan, A., Teitelbaum, J., and Wu, J. (2006). *DRBTS: distributed reputation-based beacon trust system*. Paper presented at the 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing.

Srivastava, V., Tripathi, S., and Singh, K. (2020). Energy efficient optimized rate based congestion control routing in wireless sensor network. *Journal of Ambient Intelligence and Humanized Computing, 11*(3), 1325-1338.

Stine, J. A., and De Veciana, G. (2002). Improving energy efficiency of centrally controlled wireless data networks. *Wireless Networks, 8*(6), 681-700.

Sugiarto, B., and Sustika, R. (2016). *Data classification for air quality on wireless sensor network monitoring system using decision tree algorithm*. Paper presented at the 2nd International Conference on Science and Technology-Computer (ICST).

Suh, T., and Cho, Y. (2019). An Enhanced Trust Mechanism with Consensus-Based False Information Filtering Algorithm against Bad-Mouthing Attacks and False-Praise Attacks in WSNs. *Electronics, 8*(11), 1359.

Sultana, S., Ghinita, G., Bertino, E., and Shehab, M. (2015). A lightweight secure scheme for detecting provenance forgery and packet dropattacks in wireless sensor networks. *IEEE transactions on dependable and secure computing, 12*(3), 256-269.

Sun, B., and Li, D. (2018). A Comprehensive Trust-Aware Routing Protocol With Multi-Attributes for WSNs. *IEEE Access, 6*, 4725-4741.

Sun, Y., Han, Z., and Liu, K. R. (2008). Defense of trust management vulnerabilities in distributed networks. *IEEE Communications Magazine, 46*(2), 112-119.

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.

Suryaprabha, E., and Kumar, N. S. (2019). Enhancement of security using optimized DoS (denial-of-service) detection algorithm for wireless sensor network. *Soft Computing*, 1-11.

Tague, P., and Poovendran, R. (2008). *Modeling node capture attacks in wireless sensor networks*. Paper presented at the 46th Annual Allerton Conference on Communication, Control, and Computing.

Tajeddine, A., Kayssi, A., Chehab, A., Elhajj, I., and Itani, W. (2015). CENTERA: a centralized trust-based efficient routing protocol with authentication for wireless sensor networks. *Sensors, 15*(2), 3299-3333.

Tang, C., Shokla, S. K., Modhawar, G., and Wang, Q. (2016). An effective collaborative mobile weighted clustering schemes for energy balancing in wireless sensor networks. *Sensors, 16*(2), 261.

Teng, Z., Pang, B., Du, C., and Li, Z. (2020). Malicious Node Identification Strategy with Environmental Parameters. *IEEE Access*.

Thiagarajan, R. (2020). Energy consumption and network connectivity based on Novel-LEACH-POS protocol networks. *Computer Communications, 149*, 90-98.

Tripathi, M., Gaur, M., and Laxmi, V. *Simulation of Snooze attack in LEACH*. Paper presented at the 3rd International Conference of Computer Science, Engineering and Applicaions (ICCSEA'13).

Tripathi, M., Gaur, M., Laxmi, V., and Sharma, P. (2013). Detection and countermeasure of node misbehaviour in clustered wireless sensor network. *ISRN Sensor Networks, 2013*.

Tuna, G., Kogias, D. G., Gungor, V. C., Gezer, C., Taşkın, E., and Ayday, E. (2017). A survey on information security threats and solutions for Machine to Machine (M2M) communications. *Journal of Parallel and Distributed Computing, 109*, 142-154.

Vamsi, P. R., and Kant, K. (2014). *Adaptive trust model for secure geographic routing in wireless sensor networks*. Paper presented at the Seventh International Conference on Contemporary Computing (IC3).

Van Dam, T., and Langendoen, K. (2003). *An adaptive energy-efficient MAC protocol for wireless sensor networks.* Paper presented at the Proceedings of the 1st international conference on Embedded networked sensor systems, 171-180.

Varga, A. (2001). The OMNeT++ Discrete Event Simulation System (http://www. omnetpp. org). European Simulation Multiconference (ESM2001), Prague. *Czech Republic*.

Varga, A. (2010). OMNeT++. In *Modeling and tools for network simulation* (pp. 35-59): Springer.

Varga, A., and Hornig, R. (2008). *An overview of the OMNeT++ simulation environment.* Paper presented at the Proceedings of the 1st international

conference on Simulation tools and techniques for communications, networks and systems & workshops, 60.

Vargas, A. (2011). Objective modular network testbed in c++(omnet++). version 4.2. *Disponıvel em:< www. omnetpp. org>. Acesso em, 17*.

Velloso, P. B., Laufer, R. P., Cunha, D. D. O., Duarte, O. C. M., and 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.

Vidhya, S., and Sasilatha, T. (2018). Secure Data Transfer Using Multi Layer Security Protocol with Energy Power Consumption AODV in Wireless Sensor Networks. *Wireless Personal Communications*, 1-23.

Vinitha, A., and Rukmini, M. (2019). Secure and energy aware multi-hop routing protocol in WSN using Taylor-based hybrid optimization algorithm. *Journal of King Saud University-Computer and Information Sciences*.

Wang, A., Shen, J., Vijayakumar, P., Zhu, Y., and Tian, L. (2019a). Secure big data communication for energy efficient intra-cluster in WSNs. *Information Sciences, 505*, 586-599.

Wang, F., Liu, W., Wang, T., Zhao, M., Xie, M., Song, H., et al. (2019b). To reduce delay, energy consumption and collision through optimization duty-cycle and size of forwarding node set in WSNs. *IEEE Access, 7*, 55983-56015.

Wang, J., Jiang, S., and Fapojuwo, A. O. (2017). A protocol layer trust-based intrusion detection scheme for wireless sensor networks. *Sensors, 17*(6), 1227.

Wang, J. P., Bin, S., Yu, Y., and Niu, X. X. (2013a). *Distributed trust management mechanism for the internet of things*. Paper presented at the International Conference on Applied Mechanics and Materials.

Wang, N., and Chen, Y. (2015). A Comprehensive Trust Model Based on Multi-factors for WSNs. *International Journal of Computers Communications & Control, 10*(2), 248-262.

Wang, Q., Lin, D., Yang, P., and Zhang, Z. (2019c). An energy-efficient compressive sensing-based clustering routing protocol for WSNs. *IEEE Sensors Journal, 19*(10), 3950-3960.

Wang, T., Zhang, G., Yang, X., and Vajdi, A. (2016). A trusted and energy efficient approach for cluster-based wireless sensor networks. *International Journal of Distributed Sensor Networks, 12*(4), 3815834.

Wang, W., Zhang, S., Duan, G., and Song, H. (2013b). Security in wireless sensor networks. In *Wireless Network Security* (pp. 129-177): Springer.

Wu, X., Huang, J., Ling, J., and Shu, L. J. I. A. (2019). BLTM: beta and LQI based trust model for wireless sensor networks. *7*, 43679-43690.

Xia, H., Jia, Z., Li, X., Ju, L., and Sha, E. H.-M. (2013). Trust prediction and trust-based source routing in mobile ad hoc networks. *Ad Hoc Networks, 11*(7), 2096-2114.

Xian, X., Shi, W., and Huang, H. (2008). *Comparison of OMNET++ and other simulator for WSN simulation*. Paper presented at the 3rd IEEE Conference on Industrial Electronics and Applications.

Xu, X., Gao, Z., and Han, L. (2018). An Efficient Compromised Nodes Detection System in Wireless Sensor Networks. *IJ Network Security, 20*(5), 960-970.

Yadav, S., and Yadav, R. S. (2016). A review on energy efficient protocols in wireless sensor networks. *Wireless Networks, 22*(1), 335-350.

Yan, Z., Zhang, P., and Vasilakos, A. V. (2014). A survey on trust management for Internet of Things. *Journal of network and computer applications, 42*, 120-134.

Yang, H., Zhang, X., and Cheng, F. (2020). A Novel Algorithm for Improving Malicious Node Detection Effect in Wireless Sensor Networks. *Mobile Networks and Applications*, 1-10.

Yang, K., Liu, S., and Li, X. (2015). *A Novel Detection Scheme Based on DS Evidence Theory in Wireless Sensor Networks*. Paper presented at the International Conference on Intelligent Networking and Collaborative Systems (INCOS).

Yang, T., Xiangyang, X., Peng, L., Tonghui, L., and Leina, P. (2018). A secure routing of wireless sensor networks based on trust evaluation model. *Procedia computer science, 131*, 1156-1163.

Yao, Y., Cao, Q., and Vasilakos, A. V. (2015). EDAL: An energy-efficient, delay-aware, and lifetime-balancing data collection protocol for heterogeneous wireless sensor networks. *IEEE/ACM Transactions on Networking (TON), 23*(3), 810-823.

Ye, D. (2018). A self-adaptive sleep/wake-up scheduling approach for wireless sensor networks. *IEEE transactions on cybernetics, 48*(3), 979-992.

Ye, W., Heidemann, J., and Estrin, D. (2004). Medium access control with coordinated adaptive sleeping for wireless sensor networks. *IEEE/ACM Transactions on Networking (ToN), 12*(3), 493-506.

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*.

Yetgin, H., Cheung, K. T. K., El-Hajjar, M., and Hanzo, L. (2015). Network-lifetime maximization of wireless sensor networks. *IEEE Access, 3*, 2191-2226.

Yetgin, H., Cheung, K. T. K., El-Hajjar, M., and Hanzo, L. H. (2017). A survey of network lifetime maximization techniques in wireless sensor networks. *IEEE Communications Surveys & Tutorials, 19*(2), 828-854.

Yu, S., Liu, X., Liu, A., Xiong, N., Cai, Z., and Wang, T. (2018). An adaption broadcast radius-based code dissemination scheme for low energy wireless sensor networks. *Sensors, 18*(5), 1509.

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.

Zahariadis, T., Trakadas, P., Leligou, H., Karkazis, P., and Voliotis, S. (2010). *Implementing a trust-aware routing protocol in wireless sensor nodes.* Paper presented at the Developments in E-systems Engineering (DESE), 2010, 47-52.

Zahariadis, T., Trakadas, P., Leligou, H. C., Maniatis, S., and Karkazis, P. (2013). A novel trust-aware geographical routing scheme for wireless sensor networks. *Wireless personal communications, 69*(2), 805-826.

Zahedi, A., and Parma, F. (2019). An energy-aware trust-based routing algorithm using gravitational search approach in wireless sensor networks. *Peer-to-Peer Networking and Applications, 12*(1), 167-176.

Zawaideh, F., and Salamah, M. (2019). An efficient weighted trust-based malicious node detection scheme for wireless sensor networks. *International Journal of Communication Systems, 32*(3), e3878.

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, T., Yan, L., and Yang, Y. (2018a). Trust evaluation method for clustered wireless sensor networks based on cloud model. *Wireless Networks*, *24*(3), 777-797.

Zhang, W.-A., Yu, L., and He, D. (2019). Sequential fusion estimation for sensor networks with deceptive attacks. *IEEE Transactions on Aerospace and Electronic Systems*.

Zhang, W., Zhu, S., Tang, J., and Xiong, N. J. T. J. o. S. (2018b). A novel trust management scheme based on Dempster–Shafer evidence theory for malicious nodes detection in wireless sensor networks. *74*(4), 1779-1801.

Zhao, J., Huang, J., and Xiong, N. J. I. A. (2019). An effective exponential-based trust and reputation evaluation system in wireless sensor networks. *7*, 33859-33869.

Zheng, G.-p., and Zhou, Y. (2007). *An energy-aware cluster protocol for wireless sensor networks*. Paper presented at the Second International Conference on Innovative Computing, Information and Control ICICIC'07.

Zheng, Z., Liu, A., Cai, L. X., Chen, Z., and Shen, X. S. (2016). Energy and memory efficient clone detection in wireless sensor networks. *IEEE Transactions on Mobile Computing*, *15*(5), 1130-1143.

Zhou, C., Gu, Y., Fan, X., Shi, Z., Mao, G., and Zhang, Y. D. (2018). Direction-of-arrival estimation for coprime array via virtual array interpolation. *IEEE Transactions on Signal Processing*, *66*(22), 5956-5971.

Zhu, C., Nicanfar, H., Leung, V. C., and 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.

LIST OF PUBLICATIONS

Journal Publications

Anwar, R. W., Zainal, A., Outay, F., Yasar, A., & Iqbal, S. (2019). BTEM: Belief based trust evaluation mechanism for Wireless Sensor Networks. ELSEVIER Future Generation Computer Systems, 96, 605-616 **(Impact Factor = 5.768).**

Anwar, R. W., Zainal, A., & Iqbal, S. (2019). Systematic literature review on designing trust-based security for WSNs. Indonesian Journal of Electrical Engineering and Computer Science, 14(3), 1395-1404

Anwar, R. W., Zainal, A., Iqbal, S., & Bashir, M. (2018). Key Security Challenges and Threats to Cyber Physical Systems and Their Applications. QUEST Research Journal, 16(01), 31 – 35.

Anwar, R. W., Bakhtiari, M., Zainal, A., & Qureshi, K. N. (2016). Wireless sensor network performance analysis and effect of blackhole and sinkhole attacks. Jurnal Teknologi Malaysia, 78(4-3). **(Impact Factor = 0.410).**

Anwar, R. W., Zainal, A., Bakhtiari, M., & Qureshi, K. N. (2015). Security Issues in Wireless Sensor Network: Approaches and Issues. TELKMONIKA, Indonesian Journal of Electrical Engineering, p-ISSN: 2302-4046, e-ISSN 2460-7673. Vol 15, No 3.

Anwar, R. W., Zainal, A., Bakhtiari, M., & Qureshi, K. N. (2015). Malicious node detection through trust aware routing in wireless sensor networks. Journal of Theoretical and Applied Information Technology, 74(1).

Anwar, R. W., Bakhtiari, M., Zainal, A., & Qureshi, K. N. (2015). A survey of wireless sensor network security and routing techniques. Research Journal of Applied Sciences, Engineering and Technology, 9(11), 1016-1026.

Anwar, R. W., Bakhtiari, M., Zainal, A., Abdullah, A. H., & Qureshi, K. N. (2014). Security issues and attacks in wireless sensor network. World Applied Sciences Journal, 30(10), 1224-1227.

Conference Publications

Anwar, R. W., Zainal, A., Abdullah, T., & Saleem Iqbal. (2020, April). Security Challenges and Threats to IoT: A Review. IoTNAT2020 – The Sixth International Workshop on Internet of Things: Network Applications and Technologies (IoTNAT2020) April 20 - 23, 2020 – Paris – France

Anwar, R. W., Zainal, A., Bakhtiari, M., & Saleem Iqbal. (2018, December). The Role of Trust, Security and Privacy in Developing Secure Wireless Sensor Networks. AIMC – 2018 Asia International Multidisciplinary conference May 11 - 12, 2018 – UTM – Johor Bahru – Malaysia.

Anwar, R. W., Zainal, A., Bakhtiari, M., & Qureshi, K. N. (2017, December). An intelligent hybrid approach to encounter coverage holes for wireless sensor nodes deployment in the field. 13th International Conference on Emerging Technologies (ICET) (pp. 1-4) IEEE, held in Islamabad – Pakistan.

Anwar, R. W., Zainal, A., Bakhtiari, M., & Qureshi, K. N. (2015, August). Performance Analysis of Wireless Sensor Network in the Presence of Sinkhole and Blackhole Attacks. The 1st International Conference on Computational and Social Sciences – ICCSS2015 – Aug 25- 27, UTM – JB Malaysia.

Anwar, R. W., Bakhtiari, M., Zainal, A., Abdullah, A. H., & Qureshi, K. N. (2015, May). Enhanced trust aware routing against wormhole attacks in wireless sensor networks. In 2015 International Conference on Smart Sensors and Application (ICSSA) (pp. 56-59). IEEE.

Anwar, R. W., Bakhtiari, M., Zainal, A., & Qureshi, K. N. (2014). A Roadmap to Wireless Sensor Security Protocols Implementation in Health Care System. The 2nd International Conference on Applied Information and Communications Technology" - ICAICT 2014, held at Muscat, Sultanate of OMAN.