Distributed Trust-based Routing Decision Making for WSN

Nor Azimah Khalid

A thesis submitted to Auckland University of Technology
in fulfilment of the requirement for
the degree of Doctor of Philosophy

Supervisors:
Dr Quan Bai
Professor Adnan Al-Anbuky

2019

School of Engineering, Computer and Mathematical Sciences

Abstract

This thesis describes novel approaches to deal with routing in distributed wireless sensor networks (WSNs) decision making and proposes new distributed protocols based on trust. The trust is defined as the level of belief that a sensor node has on another node for specific action, based on certain criterion that is specified according to applications. As WSNs are applications specific, the proposed trust-based solutions are mainly targeting at two types of network structures, namely, the static homogeneous network, and the network with mobile sink.

The first contribution of the thesis is a multi criteria trust model called Hierarchical Trust-based Model (HTM). The model considers several criteria and evaluates the trustworthiness of a node in two levels. HTM is different from most of the existing trust models as it evaluates the trust for multiple nodes rather than a single node evaluation. The model uses the Analytical Hierarchical Process (AHP) in computing the node's trust.

The second contribution is a novel distributed trust-based protocol called Adaptive Trust-based Routing Protocol (ATRP). The proposed ATRP embed the proposed HTM in its process. Four network performance metrics (energy, reliability, coverage and reputation) were considered in the forwarder selection. The reputation, which is the accumulated value provided by indirect nodes about evaluated nodes previous communication behaviours is gained using Q-learning. ATRP takes into consideration the resource constrained factors of the nodes by introducing several control mechanisms (timeliness and number of interactions).

Thirdly, the thesis considers the implementation of the mobile sink and taken into consideration the relocation issue which is the main concern in existing distributed mobile sink routing. A new distributed mobile sink routing protocol called Blockchain-based Routing Protocol (BCRP) is presented where it adapts the blockchain elements in its relocation decision strategy. The decision in BCRP is determined by other mobile sinks in ensuring the relocation position is not redundantly covered. This is because the redundant coverage in some applications are unnecessary and will consume more energy. The participating mobile sinks are able

to make decisions without the central entity's help but based on a set of rules that are pre-agreed by all mobile sinks. The relocation will only happen if it is agreed (verified) by a certain number of mobile sinks. In such situations, the decision making will benefit a larger number of nodes and all nodes are able to get updated information. The performances of BCRP are evaluated and compared under several simulation environments in terms of five performance metrics, i.e., energy consumption, packet delivery ratio, average delay, throughput and coverage level. Based on the simulation results, the proposed approaches outperform the other comparable protocols for all the performance metrics.

Attestation of Authorship

"I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person (except where explicitly defined in the acknowledgements), nor material which to a substantial extent has been submitted for the award of any other degree or diploma of a university or other institution of higher learning."

Auckland, 2019

Nor Azimah Khalid

Acknowledgement

In the name of Allah, the most Gracious, the most Merciful. Alhamdulillah, to Allah for the blessing, wisdom, health, strength and patience that he gave upon me throughout this long, challenging, adventurous, exciting and inspiring journey.

First and foremost, I would like to thank the Ministry of Higher Education Malaysia for providing a scholarship to enable me to pursue this doctoral study, and the Universiti Teknologi Mara for granting me a study leave.

I would like to thank my energetic and dedicated supervisor Dr Quan Bai for his undivided guidance, endless support, understanding, encouragement and patience throughput this study. His continuous supports have been such an inspiration to help me persevere in this PhD journey. Many thanks also go to my co-supervisor, Professor Adnan Al-Anbuky for his generous and thoughtful suggestions through the research period.

I dedicated this thesis to my parents, Khalid Hj Haron and Patimah Sakim, for their endless blessing and encouragement, and for always been there to support me in every possible way. My gratitude also goes to my mother-in-law, Saadiah Abang Jajol, brothers and sisters, for their endless encouragement, continuous support and prayers.

I would like to acknowledge the postgraduate office of AUT School of Engineering, Computer and Mathematical Sciences for their support and necessary assistance during my study. Special thanks to my dear friends in Auckland, MAPSA mount, AUT friends, and my collegues at UiTM, for being part of my support system throughout my PhD journey. I would also like to offer my sincere appreciation to all of those who have helped me in any respect during my PhD journey.

Finally, my deepest gratitude to my dearest husband, Abang Affendy Abang Sepuan for your patience, sacrifices, love and endless support. To my junior supporters, Abang Muhammad Danish and Dayang Nur Alisha, thank you for coping with me throughout the time of this research.

Table of Contents

List of Figures

List of Tables

List of Algorithms

List of Abbreviations

ACQUIRE	Active Query Forwarding in Sensor Network
AHP	Analytical Hierarchical Process
AODV	Ad Hoc On-Demand Distance Vector
ATRP	Adaptive Trust-based Routing Protocol
ATSN	Agent-based Trust Model in Wireless Sensor Network
ATSR	Ambient Trust Sensor Routing
AUT	Auckland University of Technology
BCRP	Blockchain-based Routing Protocol
CRF	Composite Routing Function
DIRL	Distributed Independent Reinforcement Learning
DTLSR	Direct Trust Dependent Link State Routing
EDTM	Efficient Distributed Trust Model
EEMSRA	Energy Efficient Mobile Sink Routing Algorithm
ETARP	Secure and Energy Aware Routing Protocol
GBR	Gradient Based Routing
GMRE	Greedy Maximum Residual Energy
HTM	Hierarchical Trust-based Model
MAL	Multi-agent learning
MAPSA	Malaysia Auckland Postgraduate Student Association
MAS	Multi-agent system
MCDA	Multi Criteria Decision Analysis
NBBTE	Node Behavioural Strategies Banding Belief Theory of the Trust Evaluation Algorithm
PBTrust	Priority-based Trust model
PDR	Packet Delivery Ratio
PLUS	Parameterized and Localized Trust Management Scheme
QBDCS	Query-based Data Collection Scheme
QELAR	Machine Learning-based Adaptive Routing
REDM	Robust and Energy Efficient Dynamic Routing for Mobile Sink
TARF	Trust-Aware dynamic Routing Framework
TERP	Trust and Energy Aware Routing Protocol
UiTM	Universiti Teknologi MARA
WSN	Wireless Sensor Network

Chapter 1
INTRODUCTION

A Wireless Sensor Network (WSN) is formed by randomly or deterministically deploying a large number of battery powered, small and inexpensive sensor nodes without the need of a dedicated infrastructure [Senouci 2014]. These nodes observe the physical and environmental conditions of the region to be monitored. WSNs are notoriously challenging because of their interdependency, resource availability, complexity, scalability, dynamics and physical distribution requirements. Firstly, the random deployment of nodes and decentralised network topology cause several problems due to nonuniform distribution of resource constrained nodes, which are expected to response well to the dynamic behavior and changes in the network. Among others, routing has been identified to be the most dominant contributor to the limited resources in the network. The need to serve such limitations has urged for efficient mechanism to assist the nodes better and more accurate. Among the existing approaches, trust-based has been proved to be an efficient way in assisting the nodes in making autonomous decision when incomplete information is unavailable.

Thus, this thesis proposes distributed decision making protocols using trust-based mechanisms for decentralised and randomly distributed wireless sensor networks (WSNs), aims to improve routing efficiency through effective 1) selection of forwarder and 2) relocation of mobile sinks.

1.1 Background

1.1.1 Wireless Sensor Network

WSNs are dynamic systems that respond to internal changes or variable external forces. In fact, nodes can appear or disappear (by depletion or destruction) over time due. These dynamics can be represented by changes in communication links caused by environmental events and phenomena (such as weather conditions and animal attacks). Therefore, the sensor nodes must adaptively cope with unexpected

changes in topology [Van Dyke Parunak 1997], and in resources such as available energy. These coping mechanisms must combat node depletion and sensor failures, which further changes the network topology [Fuentes-Fernández 2009] or the role assignments in agent organizations [Badica 2011].

To achieve high-level tasks that cannot be achieved by a single sensor, a network must normally collaborate or coordinate the operations of different sensors. Therefore, the dependencies among the sensors must be known during the network operation.

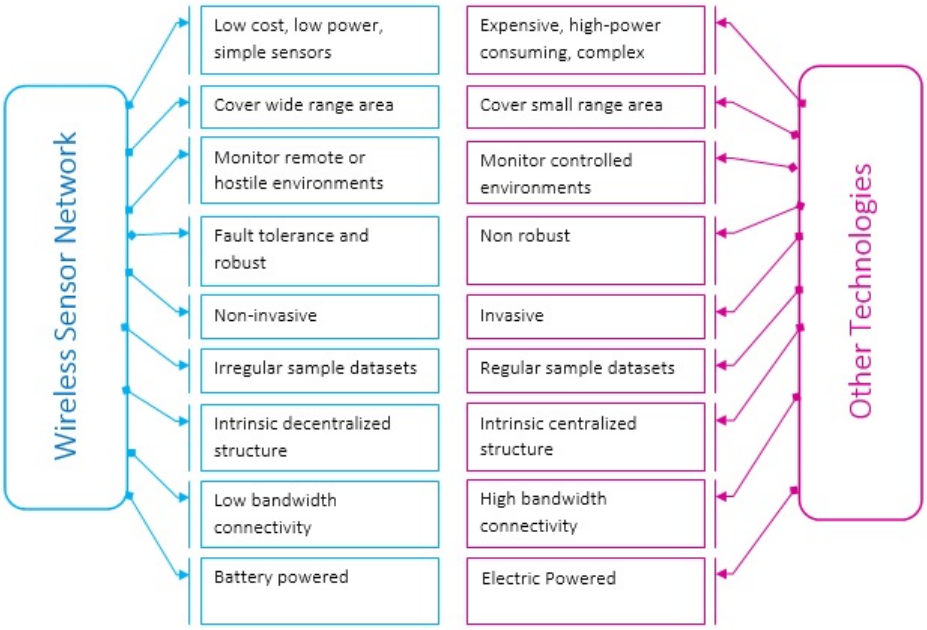

Figure 1.1: Advantages and limitations of WSNs and other monitoring technologies.

Despite the above problems, WSNs offer huge advantages to a wide range of applications. Figure 1.1 shows several advantages and limitations of WSNs and (for comparison) other monitoring technologies. The advantages of WSNs include the ease and low cost of installation, the ability to monitor remote or hostile environments with minimal supervision, fault tolerance (robustness), non-invasiveness and an intrinsic decentralised structure that enables multiple applications.

1.1.1.1 Sensor nodes deployment

The nodes and the sinks in a deployed network may be static or mobile. The node deployment significantly affects the coverage, connectivity, lifetime and robustness of the WSNs (Younis and Akkaya, 2008). Sensor node deployment is broadly classified

as random or manual, depending on the application requirements (see Figure 1.2 for examples). This classification is further discussed in [Sharma 2016].

In manual deployment, the static nodes are placed at predetermined locations of interest over a small region (health care applications), in buildings interiors (smart home applications), or over bridges or similar structures. Manual deployment usually requires expensive nodes and incurs a high initial cost. Therefore, it is unsuitable for large-scale sensor network deployment.

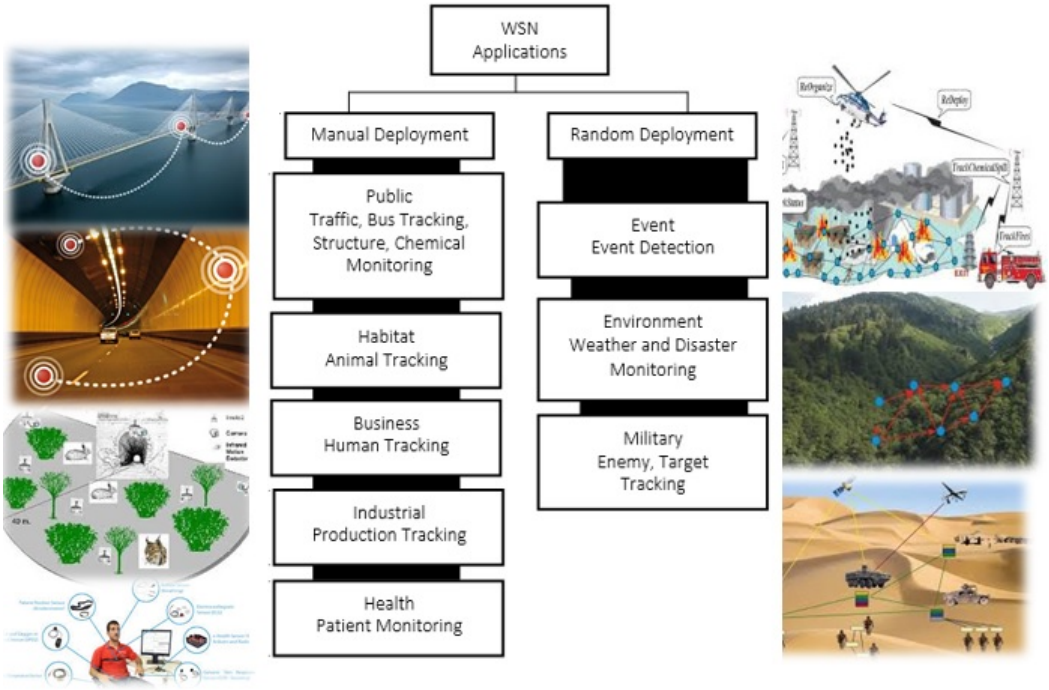

Figure 1.2: Examples of WSN applications using randomly and manually deployed nodes.

Deterministic deployment is also unsuitable in working environments related to battlefield surveillance, military, fire forest detection, harsh environments and toxic regions. In these environments, the nodes are dropped at random locations from a plane and operates without an infrastructure. These working environments always require complete coverage of the target area [Wang 2011] with every location covered by a single sensor node (1-coverage) or multiple sensor nodes (k-coverage). However, this requirement cannot always be fulfilled, especially when the sensor network interrupted by obstacles such as buildings and trees. Wind and tree movements also causes incorrect and inaccurate positioning of the sensors, node failures, frequent relays of packets through the nodes in the sink vicinity and other problems.

In addition, full coverage and network connectivity may be an expensive task. In applications such as environment monitoring, full coverage of a given area is not required, whereas applications such as forest fire monitoring requires full coverage of the forest during the dry season but only partial coverage in the rainy season [Khoufi 2017]. WSNs with mobile sinks are also deployed in other applications such as fire detection systems [Grammalidis 2011] and on robots that collects information from the sensors deployed on different areas of a large field [Yun 2010].

1.1.1.2 Network Topology

The network topology, defining the organisation of the nodes in the network is broadly classifiable into centralised and decentralised (Figure 1.3). In centralised scheme, information is sent, computed, decided and controlled by a central manager. This scheme provides a well-manageable structure (as no computational decision costs incurred at individual nodes), but failure of the central node, causes collapse of the entire network. Moreover, the transmission cost and delay increase in large-scale networks, especially when the central controller is located far away.

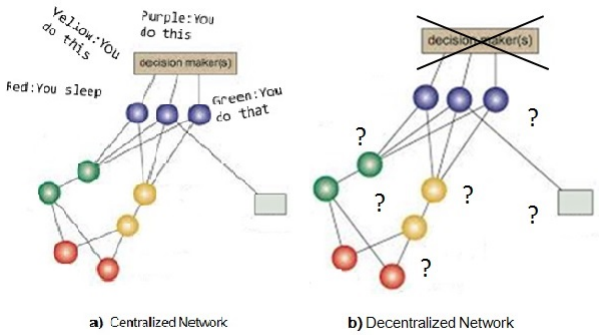

Figure 1.3: Broad classification of WSN network topologies.

In event detection, military and battlefield applications, the sensors are decentralised and inaccessible. The decentralised approach enables individual nodes to make decisions without intervention by a central controller (which is suitable for large scale network) [Ye 2011] [Garcia 2013] [Meng 2013]. Decentralised control architecture is more reliable than centralised control for large networks, and improves the data collection and backup, by avoiding failure of the central node [Gowrishankar 2008] [Bernon 2006]. Nodes deployed in a decentralised manner will

self-organised into their own network topology (Figure 1.3b). Due to computational and communication constraints, the nodes must rely on their neighbours for decision making [Kaler 2010].

WSNs are expose to situation which involves imperfect or unknown information (i.e. uncertainties). The uncertainties in WSNs are classified into communication uncertainty (e.g., the availability, quality and connection patterns of communication links), sensing uncertainty ((e.g., uncertainty in sensor range) and data uncertainty (e.g., imprecision in sensor readings, collected and reported data [Lee 2010]. Such uncertainties require an efficient distributed decision making solutions.

1.1.1.3 Routing task as the main consumer

The main tasks of a sensor node in a field are event detection, local data processing and data transmission. To perform these tasks, a sensor device requires four basic components: a sensing unit, a processing unit, a transceiver unit and a power unit. Among these components, the most important is the transceiver unit, which communicates (routes) the data between two wireless sensor nodes, providing connectivity to the rest of the network. Various experiment results confirm that communication subsystem is a prominent source of energy dissipation [Goyal 2012], [Li 2011a]. The other tasks (collision, overhearing, packet control, idle listening and interference) consumes less energy [Minet 2009].

The routing procedure selects, discovers and maintains the data transfer paths between the source and destination nodes [Nayak 2016]. Owing to the limited power of individual sensors, routing protocol designs for WSNs require special considerations, that are not demanded in normal ad hoc networks such as mobile and cellular networks. The low bandwidth connectivity might also prohibit the direct messaging of distant nodes to the sink. Such a large network requires multi-hop communication whereby the sensor node receives the data sent by its neighbors and forwards them to its neighbours according to the routing decisions.

The routing in decentralised and randomly distributed wireless is more challenging because it must find the optimal route between the source and destination under various uncertainties [Cobo 2015] [Raja 2016]. The complexity introduced by the decentralised and non-uniform node distribution must be handled by different

measures. For example, routing in a dense network must focus on duplication and redundancy, whereas routing in a sparse network is more concerned with covering the hole in the network. In addition, the decisions need to be made by limited-capability nodes with restricted sensing and communication distance, information and resources. These restrictions demand collaboration and assistance among the network nodes. As the routing decision affect the performance of the WSN, routing has become an important research area in the WSN domain.

1.1.1.4 Wireless sensor network as Multi-agent System

A system can be considered as an open dynamic system if its agents are reactive, autonomous, proactive and sociable. The agents can come from any background with heterogeneous abilities, organizational affiliations or credentials, must make independent decisions (i.e., must solve its own design objectives, rather than being instructed at any given moment), and can join or leave the system at will [Yu 2013]. This kind of system is widely used in computer applications such as peer-to-peer computing, the semantic Web, Web services, e-business, m-commerce, autonomic computing, pervasive computing environments and file-sharing systems. Agent-based approaches are used in many distributed system solutions due to their appropriateness for open, highly dynamic, uncertain and complex systems [Alan 1988], [Jennings 1998], [Vinyals 2011].

An open multi-agent system is composed of autonomous agents that must interact with each other in flexible ways through particular mechanisms and protocols to achieve their goals in uncertain and dynamic environments [Simon 1996]. The agents in an MAS normally possess limited local views of the environment and insufficient expertise, resources and information. To compensate these limitations and solve the target problem, they need to cooperate via a sequence of interactions [Durfee 1989], [del Carmen Delgado-Roman 2013]. Thus, interactions have become the core aspect of multi-agent systems, motivating the development of coordination, collaboration and negotiation models by the agent research community [Jennings 2001]. Interaction models are also applied in the task distribution of computations, resource sharing and action coordination [Van Dyke Parunak 1997]. MAS agents can be categorized as fully cooperative or fully competitive (selfish). Agents in the former

group all share the same utility function, whereas those in the latter group are interested only in maximising their own utility functions [Birk 2000].

A MAS improves the network efficiency in resource constrained environments by distributing the computation, bandwidth and power usage among agents. Owing to their inherent features, WSNs can be regarded as open dynamic systems. To operate successfully, they must perform critical tasks such as organisational structuring, coordination, collaboration and real-time resource allocation. To model a WSN as a MAS, each sensor can be inherently distributed as a flexible agent.

1.1.2 Trust as Potential Solutions

Collaboration can work towards similar interests, a gained reward, a consensus strategy, negotiation, or reinforcement learning. Collaboration mechanisms such as cluster formation, task-based allocation, role-based self-organisation, consensus strategy, negotiation-based scheduling, game-theory based, learning-based and trust-based approaches have been incorporated into routing protocols. In WSNs, these collaboration mechanisms minimize the energy consumption, reduce overlapping, homogenise the energy consumption, reduce the number of transmissions, avoid redundancy in task allocations, maximize the WSN lifetime under the specified quality of service, balance the energy distribution of task allocations, and operate partially connected networks with imperfect information. However, most of the existing works assume that all nodes are connected and trusted. In addition, the uncertainties caused by the decentralised and random distribution are not well considered.

When the agents cannot preview the quality of their services or resources, the network decisions are based on trust between the truster agent (agent requiring the resources or services) and the trustee agent (agent providing the resources or services), which incurs a certain level of risk [Yu 2013]. In large-scale open distributed systems, trust is a fundamental concern of all interactions among the entities operating in uncertain and inconstant environments [Ramchurn 2004]. Without complete information, a trust model minimises the uncertainty of the interactions in an open distributed system by deciding on the interaction process, the time and the agent to interact without guaranteeing that the interaction will actually deliver the intented benefits [Ramchurn 2004].

Trust is an important component of many fields, including psychology, sociology, economics, political science, anthropology and (more recently) wireless networks [Hassan 2008] and [Nguyen 2009]. The term *trust* has been differently defined in different literatures and domains [Rani 2014].

In WSNs, trust is specified as the reliability or trustworthiness of the sensor nodes. Trust is important for identifying misbehaving nodes and collaborating among the trustworthy nodes. It also assists the decision-making processes such as data aggregation, routing and reconfiguring the sensor nodes [Rani 2014]. [Buskens 1998] defined trust as a belief level that articulates the reliability degree that a sensor node has on another node for a specific action, based on currently and previously observed behaviours. [Mcknight 1996] claimed that trust is an abstract concept combining many complicated factors, which defines an accurate definition.

[Han 2014] reviewed several decentralised nodes trust models. However, few of the reviewed models consider multiple criteria in their trust decisions and most of them perform only single-hop evaluation. Trust models in WSN are used in attack detection, secure routing, secure data aggregation, secure localisation and secure node selection [Han 2014] but only few have considered the critical aspects of WSNs, which are resource constrained.

In this thesis, the trust concept is used in two different scenarios: 1) in selecting the trusted forwarder to forward the packets and 2) in improving routing through collaboration among trusted sinks in the network. In the first scenario, the trust lies on the belief that a node has on other nodes based on four trust factors: reliability, coverage, energy efficiency and reputation. In the second scenario, the trust lies on the belief among nodes between the regions, in improving routing efficiency through coverage and redundancy as its trust factor.

1.2 Research Motivation, Objectives and Contribution

1.2.1 Research Motivation

As an abstract concept, trust-based has a huge potential to overcome the uncertainties in distributed and decentralised decision making. Due to the challenges in random deployment and decentralised network topology, collaboration among nodes

is crucial. With the lack of the global information, a decision relies on surrounding nodes. The reliability of the information and the source (the nodes that provide information) is a priority. Being the major consumer of communication cost, efficient routing is very critical. The formulated mechanisms should ensure autonomous and resource-aware routing under the challenges highlighted below:

- Multiple criteria considerations for more reliable decision making.

  Due to their limited communication range, nodes cannot view the whole network. Uncertainty in WSNs is also introduced by various sources. In existing research, the next hop in packet routing is decided by single or multiple parameters, such as distance, energy or power consumption. It has been proven that node selection based on multiple criteria improves the network performance. Thus, identifying multiple factors could assist the decision making by nodes in decentralised and distributed network in making more accurate decisions.

- Trust-based mechanism in WSN.

  As the characteristics of WSNs mimic those of an open system, trust-based mechanisms designed for open systems are applicable to WSNs. However, current trust-based mechanisms applied to WSNs focus solely on security measures such as detecting malicious nodes in specific attacks. Trust and reputation in WSNs should be considered from other aspects without compromising the resources.

- Coverage hole problems.

  Resource limitation is recognised as a critical issue in WSN design and must be considered when designing WSN protocols. In randomly deployed networks, hole coverage is another crucial consideration. Previous research has focussed on load balancing. A predetermined scheduled (sleep-wake mechanisms) can benefit some applications. Other researches have balanced the node utilisation by adaptive behaviour that allows other nodes to be chosen before the frequently chosen nodes are depleted. Another potentially helpful approach is shifting a mobile sink. However, in the existing research on mobile sinks, sink movement is either random or based on certain values provided by the nodes nearby the sink. Consequently, the mobile sink may move to a new

location which is undesired by nodes at some parts of the network. Also, most of the existing works assume that mobile sinks are not resource constrained. Although the existing mobile sink mechanisms can fill holes in the network, they are prone to many pitfalls such as hot spots, coverage hole, aging and unreported event. Efficient collaboration mechanisms are needed to coordinate and assist sink mobility in a network.

- The validity of the information provider.

  Single-hop packet routing can lead to incorrect decisions making. For example, the packet in a large network, may require several hops to arrive at their destination. The next hop node might capably deliver the data, but if no further node is available, the data will not reach the destination. Eventually, the packets may be dropped or retransmitted. In the absence of global information, a larger awareness of the network, would assist the nodes in making better and more accurate assessments. Thus, information from the reliable (or validated) neighbours will improve the routing decisions. Unfortunately, most of the existing works evaluate only the single hop nodes in the route. Hence, works involving multi-hop assessment are required.

1.2.2 Research Questions

As mentioned in the previous sections, an efficient distributed and decentralised decision making is needed to assist nodes in the decentralised and randomly distributed network. In this open and unpredictable environment, the provided information and the information provider play important role in decision making. When the available information is incomplete, the decision relies on the information provided by the surrounding nodes. To make wise decisions based on this limited information, the nodes require assistance.

The main question in this research is framed as follows: " How can we assist decision making by resource-constrained nodes in randomly distributed and decentralised networks?". To identify possible solutions, we divide the main research question into four subordinate research questions:

1. How do existing protocols work, what causes inefficiencies in WSNs, and how are these mitigated by existing mechanisms?

To answer this question, we conducted an extensive review guided by a wide range of keywords. The literature search informed us on the state-of-the-art of current mechanisms. The investigation identified the factors causing the inefficiency, and hinted at improvements in current mechanisms.

2. How do existing distributed trust-based mechanisms identify how, when and with whom the agents should trust and work with?

   This investigation identified the purpose of trust in the current research (to reach a common goal), determined the factors to be considered in decision making by the nodes, and seeks mechanisms that ensure the credibility of the information provider. It also identified ways of computing the trust values on which the nodes base their decisions. Based on these findings, we developed the proposed approach.

3. How does the proposed distributed and decentralised decision making perform in WSN?

   The feasibility and effectiveness of the proposed method in a randomly distributed and decentralised network were evaluated in simulations.

1.2.3 Research Objectives

The nodes in the decentralised and randomly distributed network must self-configure and self-organised. Self-configurability and autonomous actions are possible if the nodes are treated as intelligent agents. The main objective of this research is to propose a distributed and decentralised decision making, particularly in routing through 1) adaptive multi criteria forwarder selection and 2) relocation of mobile sinks respectively. To this end, the research considers two types of network: one with static sink, the other with mobile sinks. In network with static sink, the trust and reputations of the nodes for decision making are based on multiple criteria. The networks with mobile sinks collaborate with each other based on the coverage level in deciding the new mobility location. Specifically, the research will achieve the following objectives:

1. To identify the state of the art of existing distributed routing decision making in WSNs.

2. To investigate the existing solutions for distributed decision making and determine the relevancy of the existing solutions for WSNs.

3. To decide the factors, processes, and mechanisms for the design of proposed protocols.

4. To evaluate and compare the performances of proposed protocol with regards to several network performance metrics (energy consumption, throughput, packet delivery ratio, delay, and coverage level).

1.2.4 Research Contribution

The contributions of this thesis are summarised below:

- This thesis proposes a novel trust model, called Hierarchical Trust Model (HTM) which considers multiple factors in routing-decision making in open, randomly distributed and decentralised WSNs.

  WSNs are exposed to many uncertainties and are affected by several factors, such as physical obstacles and nodes depletion. The trust modelling in HTM, considers the agents involved in the interaction, when they should interact and how the interactions occur. Multi criteria considerations may improve the network performance, especially when the network is exposed to many uncertainties, however, limited number of multi-criteria trust-based models for WSNs exist in the literatures. The HTM will expand this limited body of knowledge.

- The thesis develops an efficient trust-based routing protocol through effective forwarder selection decision making, called the Adaptive Trust-based Routing Protocol (ATRP), with multiple criteria, multiple nodes evaluation, and multiple layer decision making for WSNs with static sink.

  Trust models are deployed in secure routing and node selections. However, most of the existing trust models detect and handle security measures. The proposed ATRP uses the developed HTM that consider other network measures to route packets through the network. As HTM is a dynamic model

which builds trust from credibility and reliability, the ATRP provides a different perspective from most of the existing trust models, which base their trust on security. This new approach aims to improve the network performance. The ATRP adopts a novel selection method that evaluates the nodes a few hops away from the source, instead of the single-hop evaluation in most of the existing methods.

- The thesis proposes blockchain-based coordination mechanisms between mobile sinks that overcome the coverage problem and balanced the WSNs.

  Coverage holes are critical complications in decentralised and randomly deployed networks. Most of the existing researches overcome the coverage problem by deploying mobile sinks, but rarely consider the network assistance in the sink mobility. The proposed blockchain-based mechanism (a distributed trust approach) expands the limited number of network-assisted routing protocols for WSNs. The BCRP improves the coverage and balance of the decentralised and randomly deployed network via collaborations among the mobile sinks.

- Finally, the findings in this research will help other researchers to identify their future research directions.

1.2.5 Thesis Organisation

This chapter introduces the background of the research, focussing on the challenges in decentralised and randomly distributed WSNs. Lack of information and limited capability nodes in the network, requires collaboration among them to complete a task. Relying on surrounding nodes information demands close attention in ensuring that the information and the nodes providing the information is reliable. Efficient distributed and decentralised decision making mechanisms are required to assist the nodes. In the following chapters, how multiple criteria considerations are considered, and how to determine the participating nodes in the forwarder selection and relocation decision making are explained respectively. This thesis is structured as follows:

Chapter 2 reviews previous studies related to the research scope. Current state-

of-the-art approaches, were identified from extensive reviews of journal articles and conference proceedings, concentrating on WSNs, collaboration in multi-agent systems, distributed networks, routing protocols for WSNs, trust-based management, mobile assisted mechanisms, coverage holes and blockchain-based mechanisms.

Chapters 3 and 4 work together. In Chapter 3, a novel multi-criteria and adaptive trust-based model for forwarder selection (namely, the Hierarchy Trust Model (HTM)) is proposed. In HTM, multi-criteria decision making is performed by an analytical hierarchy process (AHP), which assist decision makers in selecting the best forwarder. The HTM is modelled in a hierarchical manner, consisting of several criteria, sub-criteria and alternatives.

Chapter 4 proposes our trust-based routing protocol for WSNs (namely, the ATRP), where HTM is applied in the forwarder selection decision. In this chapter, several control mechanisms are embedded considering the resource constrained nodes in the decentralised and randomly distributed network with a static sink. The ATRP performances in terms of four network metrics (energy consumption, delay, packet delivery rate, and number of dead nodes) over two existing protocols (DTLSR and ETARP) were measured.

Chapter 5 proposes a collaborative routing protocol based on blockchain called the Blockchain-based Routing Protocol (BCRP), which assists the mobile sink mobility and relocation in distributed networks. The performances of three existing protocols (random walk, TERP and GMRE) were compared with BCRP.

Chapter 6 concludes the thesis and suggests directions for future research.

1.2.6 Publications

1. Khalid N.A., Bai Q., "Adaptive Forwarder Selection for Distributed Wireless Sensor Networks", in Multi-agent and Complex System in Computational Intelligence, vol 670. Springer, Singapore, 2017, pp 95-107, DOI 10.1007/978-981-10-2564-8-7.

2. Khalid N.A., Bai Q., A. Al-Anbuky, "An Adaptive Agent-Based Partner Selection for Routing Packet in Distributed Wireless Sensor Network", in IEEE International Conference on Agents (ICA), Matsue, Japan, 2016, pp 37-42, DOI 10.1109/ICA.2016.34.

Chapter 2
LITERATURE REVIEW

2.1 Introduction

Many approaches to WSN problems have been proposed in the literature. This chapter provides insight into the work related to the aspects of distributed routing decision making for WSNs. The different protocols designed for WSNs are discussed and the requirements for a new distributed and decentralised routing protocol are highlighted. This chapter identifies the key parameters of the protocol design.

To identify the articles containing the most valuable information, we searched for related researches in title, abstract, and keywords utilizing the Elsevier, Springer, ScienceDirect, and IEEExplore databases which include journal articles and conference proceedings.

2.2 Routing Protocols for Wireless Sensor Network

For this study, a number of related areas of research were thoroughly reviewed, including WSNs, distributed routing protocols, trust-based mechanisms and collaborative approaches. Figure 2.1 visualised and summarised the most recent research and development related to the work, in order to place this study in the right context.

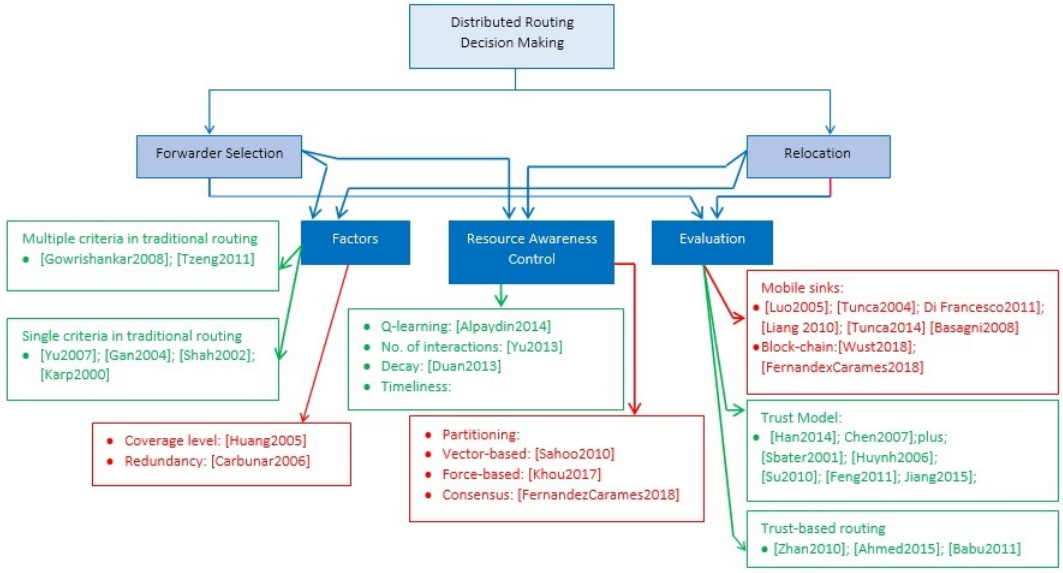

Figure 2.1: Works related to the aspects of distributed routing decision making for WSNs.

The reviews on related works are divided into two aspects of distributed routing decision making: the forwarder selection and relocation. The factors contributed to both aspects are presented. Due to the fact that resources are paramount issue in WSNs, existing resource aware mechanisms are reviewed. The evaluation on how existing distributed decision making was conducted is observes for its state of art.

2.2.1 Single and Multi-attributes Routing Protocols

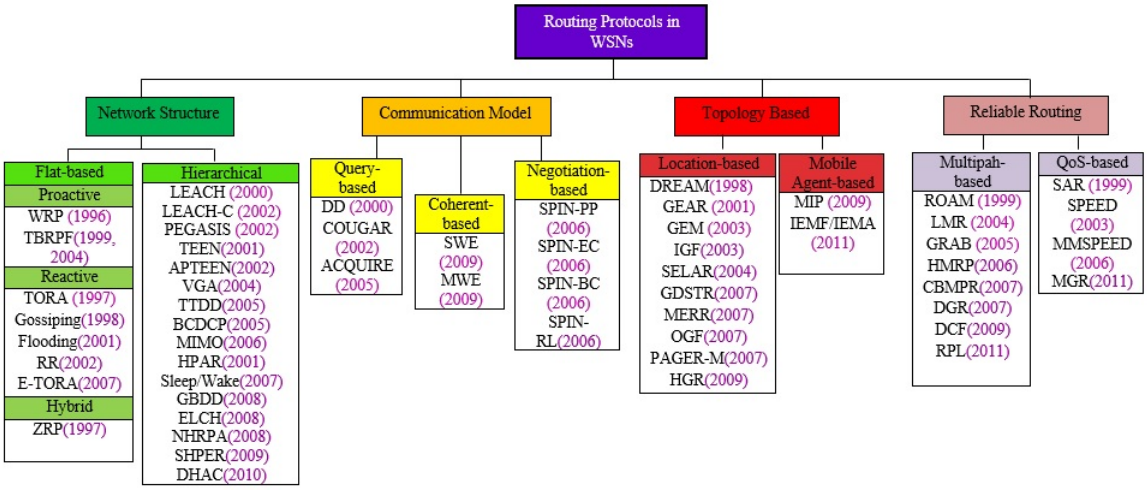

Figure 2.2: Classification of routing protocols for WSN.

Design issues, techniques and challenges in WSNs routing protocols have been comprehensively surveyed in [Akyildiz 2002a], [Al-Karaki 2004], [Pantazis 2013] and

[Akkaya 2005]. Routing protocols have been classified in terms of their network structures, communication models, topologies and reliable routing methods (see Figure 2.2). Some of these protocols may fall into more than one routing category. Each routing protocol under different classification has its own advantages and limitations. For example, the proactive (also called table driven) structure, in which routing information is readily available, provides fast routing decisions (i.e. small delay in the route setup process) but the maintenance of several tables (broadcast link-state updates or topological changes) demands a high overhead (powerful processing nodes and large memory). Therefore, it has restricted scalability and is normally unsuitable for large networks. In contrast, flooding is inexpensive in terms of topology maintenance and complex route discovery, but normally generates an enormous amount of surplus traffic. In query-based routing protocols, the sink sends queries to nodes in the network area and the nodes receiving queries will respond and send their responses to the sink. Query-based routing protocols include the Active Query Forwarding in Sensor Network (ACQUIRE) protocol [Sadagopan 2003], and the directed diffusion protocol [Intanagonwiwat 2000]. Reactive or source-initiated protocols consider certain criteria in their routing decisions. The selection criterion include the location information between source and sink [Park 1997], or the node power in [Yu 2007] (to avoid from selecting the same nodes repeatedly and to evade the use of nodes having low energy), the energy [Gan 2004], [Shah 2002], and distance [Karp 2000]. Naderan et al., considers the sensing ranges of the nodes in task allocations decision [Naderan 2013]. Reducing the sensing range affects the utility function of the nodes. When the utility of a node is reduced, the task is assigned to other nodes with higher utility, which reduces overlap and improves the uniformity of the energy consumption.

However, selection based on a single criterion (such as residual energy), may increase the end-to-end delay by lengthening the distance between the selected node and the sink, which increases the path length (i.e. hop count). In contrast, if the selection is based on shortest distance (to minimise the path), the node nearest the sink might have low residual energy. Hence, single criterion selection does not guarantee a single routing decisions.

Both the node interconnections and path selection play a major roles in minimis-

ing the power consumption and maximising the network lifetime. Therefore, multiple criteria selection might provide an ideal solution [Gowrishankar 2008]. Multiple criteria can be managed by multi-criteria decision analysis methods (e.g. [Tzeng 2011]), but such methods have rarely been applied to WSN routing [Das 2015].

Since there is no fixed infrastructure or cooperative control base in wireless sensor networks, the data transmission requires a mutual aid among the nodes. For this purpose, nodes in the distributed and decentralised network collaborate in making decision (examples of existing collaboration mechanisms are shown in Figure 2.3). The collaboration lengthens the network lifetime, minimises the energy consumption, energy-balance of task allocation, and reduces the redundancy.

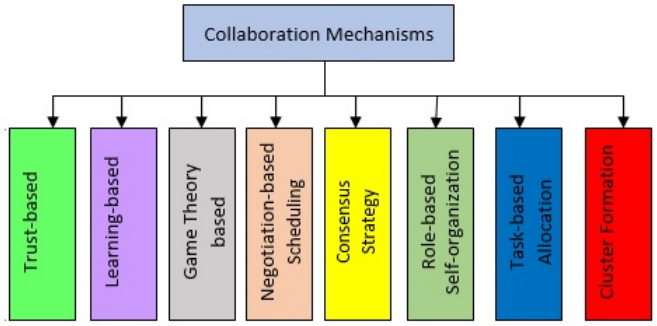

Figure 2.3: Collaboration mechanisms.

The nodes in the WSNs commonly collaborate when determining the group leader [Tyagi 2012] [Jadidoleslamy 2013], which is based on threshold values [Heinzelman 2000], adaptive criteria such as energy consumption [Kamath 2013], [Manjeshwar 2002], [Melese 2010], [Manjeshwar 2002], [Abusaimeh 2009], [Li 2011b] and [Gautam 2009]. The nodes in the network also interact and collaborate for decision making in certain situations, such as when restructuring by link failures. In determining the suitable nodes for certain task, capabilities of the agents in the network are used in the decision of the task allocation [Li 2010b].

A decision can also be performed through consensus under certain conditions (events) [Henningsson 2008], [Lunze 2010], [Dimarogonas 2009] or can be time driven among the nodes in the network. The time driven approach is commonly adopted in the distributed control of multi-agent system, engaged in continuous

communications [Li 2013] or intermittent interaction at discrete sampling instants [Xie 2009], [Chen 1995]. Distributed consensus and average-consensus problems, in which all agents reach agreement under an appropriately designed protocol based on the local relative information among neighbouring agents [Wen 2013], have attracted great interests in recent years [Li 2011b], [Wen 2013], [Li 2013], [Li 2010a] and [Fatima 2002]. In addition, an event-based consensus conserves energy by reducing the data transmission as updates are necessary only during specific events [Henningsson 2008], and [Lunze 2010].

Voulkidis et al. [Voulkidis 2013], exploiting the spatial correlations among the sensed phenomena to formulate a cooperation scheme among nodes. The Lyapunov function is commonly used in distributed systems that base their estimations on average errors. If the gain value exceeds the average error, a condition is set to a certain state indicating abnormal behavior of the system. As the coalition involvement is based on the computed value analysis, this approach reduces the number of transmissions.

Negotiation has been studied in social sciences, management, decision and game theory, team robotics, artificial intelligence agents, and unmanned vehicle applications [Brzostowski 2008]. In negotiation-based methods, the interacting nodes perform their tasks based on roles, interests or rewards [Tyagi 2012]. Negotiation is considered as an effective way of reaching an agreement that is mutually accepted by both the self-interested agents and collaborative agents [Lai 2008a].

The negotiation procedure of Kulik eliminates the transmission of redundant data by ensuring that only the useful data are transmitted when necessary. In [Le 2012], the negotiation mechanism allocates appropriate sensors to appropriate tasks by dynamically rearranging the resource allocation, which avoids unfair advantages to certain nodes [Le 2012]. Wu et al. [Wu 2011] solved a resource allocation problem by multi-issue negotiation.

Multi-attributes negotiation can tackle issue by issues one by one, or as a package. As some issues are related to other issues, the issue-by-issue approach can degrade the utility and increase the risk of conflict deals. After investing the different approaches, Fatima et al. concluded that multi-issue negotiation is optimised when all issues are bundled and negotiated simultaneously (i.e., package

approach). However, the package approach may lead to total rejection or total acceptance of an offer. Although multi-attribute negotiation better reflects the real environment, the computational cost becomes inhibiting when handling many issues [Fatima 2002]. The number of bids and multi-round negotiations are also problematic in negotiation-based approaches. Using a threshold adjustment protocol, Elmakias et al. [Elmakias 2008] proposed a mechanism that limits the number of bids generated by the agents in multi-round negotiations.

Most multi-attribute negotiation studies are based on simplified assumptions (e.g. linear additive utility functions or attributes of the agents, issue-by-issue negotiation, a non-biased mediator, binary-valued attributes complete information and cooperative agents [Lai 2006]). The negotiation protocol also requires that the bidding orders of all rounds are pre-specified and fixed throughout the negotiation. The reservation value that affects the threshold is assumed constant, deterministic (determined by the human) and centralised (as in [Elmakias 2008]).

Game theory provides mathematical solutions to bargaining problems [Abedin 2012]. Usually applied in e-commerce [de Oliveira 1999], online service applications [Fatima 2004] and resource allocation among resource providers (sellers) and consumers (buyers) [An 2008], game theory has recently been introduced to distributed multi-agent coordination [Ren 2011].

Edelat et al. [Edalat 2012] identified the winner as the agent with the highest budget value in a reverse-auction algorithm for distributed task allocation in WSNs. They applied the application deadline (time constraint)) as the negotiation constraint. Klein [Klein 2008] applied a, multiple-issue auction approach, which adjusts the sampled points by their bid expressions via a mediator [Klein 2008].

The simplest scenario in game theory, is cooperative agents sharing complete information. In this situation, all agents know the utility functions of all other agents, and the Pareto frontier of the negotiation is easily computed. However, these approaches imposes strict assumptions that are inapplicable in realistic situations. Lai et al. proposed a decentralised model based on the alternating offer protocol, where the multi-attribute negotiation enables the self-interested agents to reach a win-win agreements [Lai 2008b].

However, the benefits of game theory-based approaches are partially offset by

several limitations. For instance, many models assume that the agents know the information (i.e., the possible values in and probability distributions) of the uncertain parameters, which is impractical in real life. The major challenge of game-theoretic methods is to apply the equilibrium solutions in practice, especially when there is incomplete information in negotiation, the utility functions which is non-linear, or both [Wu 2009]. The agents in game theory construct models of each other's possible moves and pay-off and estimate the best moves. However, a single agent is incapable of building an elaborated model of each of the other agents when the number of participants evolves as more nodes are joining or leaving the system at any time [An 2011].

An alternative learning approach that models an opponent in negotiations with imperfect information has been proposed for decision making involving partially connected networks [Lai 2006] [Klein 2008], [Badica 2011], and [Niemann 2009]. An important component of MASs is multi-agent learning (MAL) [Yu 2012], which is commonly applied in modern partially connected networks [Klein 2008] [Lai 2006] [Niemann 2009]. Many other self-organisation approaches use reinforcement learning (RL), a branch of machine learning that optimises the policy that maps the states of the world to the actions by which an agent can to maximise its payoff [Badica 2011]. RL is especially important for estimating and predicting an event, as it potentially trains a system to self-diagnose its present situations and react to some unknown actions.

A distributed decision making is also feasible using Q-learning, a common model-free reinforcement learning technique, in which agents receive responding rewards from the environment for taking certain action in a given state [Barto 1998]. The action that the Q-learning selects is always the one that maximizes the sum of the immediate reward and the value of the instantaneous successor state.

An independent learning-based technique called Distributed Independent Reinforcement Learning (DIRL) is proposed, in which each agent self-configures itself independently and dynamically in maximizing its own reward [Shah 2007]. In [Shah 2012], Shah et al. proposed a dynamic reward-based approach, in which individual nodes can self-schedule their tasks through learning using their local information [Shah 2011].

Dimarogonas and Johansson [Dimarogonas 2009] proposed a two-phase, combinatorial reverse auction based on reinforcement learning and some cost-effective models of energy optimization in sensor networks. The estimated cost of the route through neighbouring nodes is represented by the Q value, in terms of the hop count (accounting for energy efficiency) and the minimum battery level among the nodes. A reinforcement learning-based routing algorithms for WSNs, considering energy-aware metrics that combines the energy metrics with load-balancing metrics was investigated in [Devillé 2011]. Hu and Fei [Hu 2010] proposed a machine-learning-based routing protocol called QELAR for longer lifetime and energy efficient underwater wireless sensor network. QELAR calculates the Q-value by considering the residual energy of each node and the energy distribution among groups of nodes. The protocol in [Forster 2009] learns the dynamic of network properties such as battery reserves using machine learning, that enables the nodes to make decision independently whether to form a cluster or not, which consumes less energy.

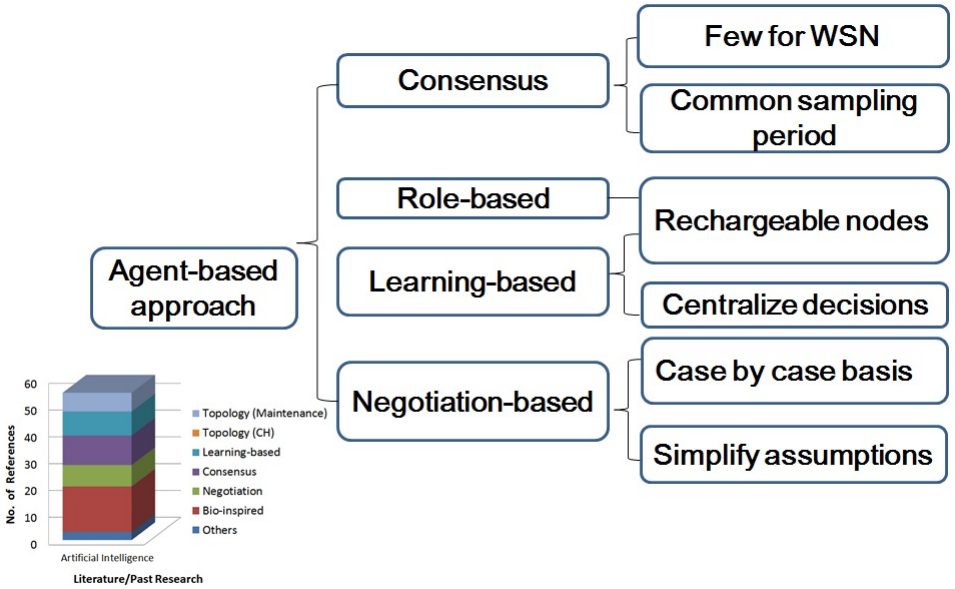

Figure 2.4: Existing researches involving collaboration.

Many collaborative methods above have been proposed for a wide range of applications. Although these mechanisms are designed for distributed systems, they bear some similarities to the mechanisms of centralised systems. For instance, in both types of systems, the energy sources of the nodes are assumed to be easily replaced or recharged and the decision-making is centralised (e.g. controlled by a central controller or sink). However, the central controller incurs a high computa-

tional cost and may be quickly exhausted. In addition, the inherent uncertainty in dynamic network is not considered in existing distributed systems, and the solution is found on a case-by-case basis, which does not always reflects real in distributed environments.

2.2.2 Mobile Sink Implementation

As mentioned in Chapter 1, coverage hole problem may exist in decentralised and randomly distributed networks. New strategies avoid static sink neighbourhoods and coverage holes by deploying mobile sinks that better distribute the energy consumption among the sensors [Luo 2005]. However, maximising coverage area while minimising the energy consumption remains a major challenge in this approach. The benefits of mobile sinks have been well accepted in the recent literature. Tunca et al. compiled a comprehensive review on distributed mobile-sink routing protocols [Tunca 2014] and classified the existing protocols into hierarchical and non-hierarchical types as shown in Figure 2.5. In hierarchical approaches, a virtual hierarchy of nodes is establish with different dynamic roles. The cost of advertising the position of the sink is decreased through established hierarchy. The non-hierarchical mobile sink routing protocols are more flexible than their hierarchical counterparts, because the nodes are guided by a certain value such as the residual energy and coverage hole rather than following a determined path or direction. The overhead for building the virtual structure and the hotspots formation is possibly eliminated in non-hierarchical approach.

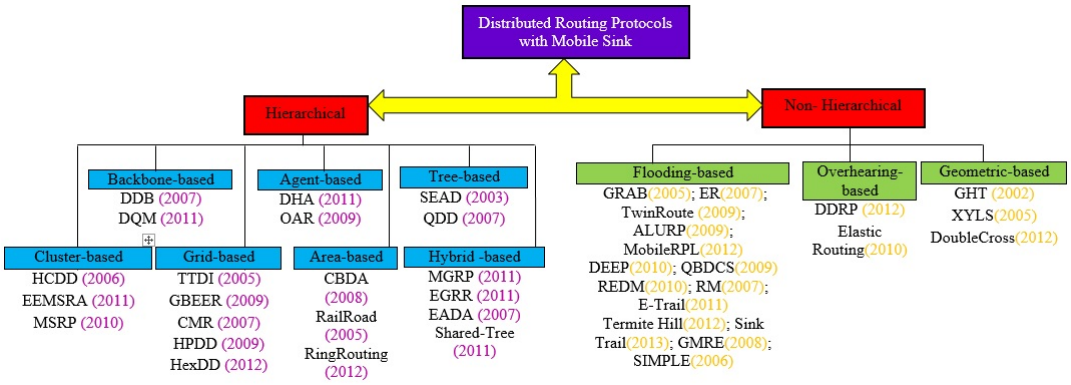

Figure 2.5: Distributed routing protocols for WSNs, with mobile sink assistance.

To improve the lifetime in large-scale networks, many algorithms relocate a mo-

bile sink towards the bottleneck nodes in the network to reduce the formation of holes in the network and extends the dynamic property of the WSNs (node deaths, and the ad-hoc topology) by frequently changing the network topology [Wang 2005]. In relocating the mobile sink, an important consideration is the decision on when and where the sink should be moved. Several existing approaches toward mobile sink relocations are highlighted in this section.

The mobility in WSNs is usually controlled by one of the three methods: the sink is moved between the sensor nodes and gathering the sensor data, the sensor nodes are moved, and mobile relays are deployed to gather and deliver data to the static sink. Sink mobility approaches can be classified into two categories based on their moving strategy: uncontrolled (random) and controlled [Basagni 2007].

Uncontrolled (random) sink mobility is used when the sink must collect data in the network at times and along paths beyond the control of the network. The sink movement is random or adapted to particular needs. The sink exchanges data only with nodes encountered during its movements [Shah 2003], normally according to a schedule that is not defined by the current network conditions (i.e., the data traffic or the the residual energies of the nodes).

Distributed approaches do not rely on a central unit for route management and decision making [Tunca 2014]. In controlled sink mobility, the sink movement depends on the network conditions such as the node energies and the the node density in the regions [Basagni 2008]. Several studies have shown that when the network controls the mobility of the sink, the energy consumption of the network reduces and the network lifetime increases [Gandham 2003], [Luo 2005], [Papadimitriou 2005], [Faheem 2009], [Wang 2005], [Di Francesco 2011], and [Liang 2010]. Recent researches on mobile sinks have improved the trade-offs between the energy consumption and data latency [Basagni 2008]. In [Chakrabarti 2003], the sink plays an observer role and repeated traverses the same path. As the sink passes the nodes, it awakens them and retrieves their data. The mobile sink in [Gandham 2003] selects its new location to minimise the energy expenditure at the nodes. In [Wang 2005], the locations and sojourn times of the sink are selected to maximise the network lifetime, as determined by the linear programming formulation. Papadimitriou and Georgiadis [Papadimitriou 2005] proposed another sink mobility solution to prolong

the network lifetime based on the sink sojourn times and locations. In [Ye 2005], the sink movement is based on a certain degree of predictability. The sink whereabouts is learnt from the statistics and a distributed reinforcement learning technique, by which nodes find routes to the mobile sink. However, these proposed schemes are based on the knowledge of global network parameters, in determining the optimal sink routes and stop times.

In Robust and Energy Efficient Dynamic Routing for Mobile Sink (REDM), the position of the sink is based on the maximum movable distance of the sink, and the average residual energy around the sink (which is the average residual energy of all the neighbour nodes at a distance of a hop from the sink) [Choi 2010]. The sink moves toward the node having the highest energy (among the nodes within maximum move hop count), in order to make energy consumption even among nodes.

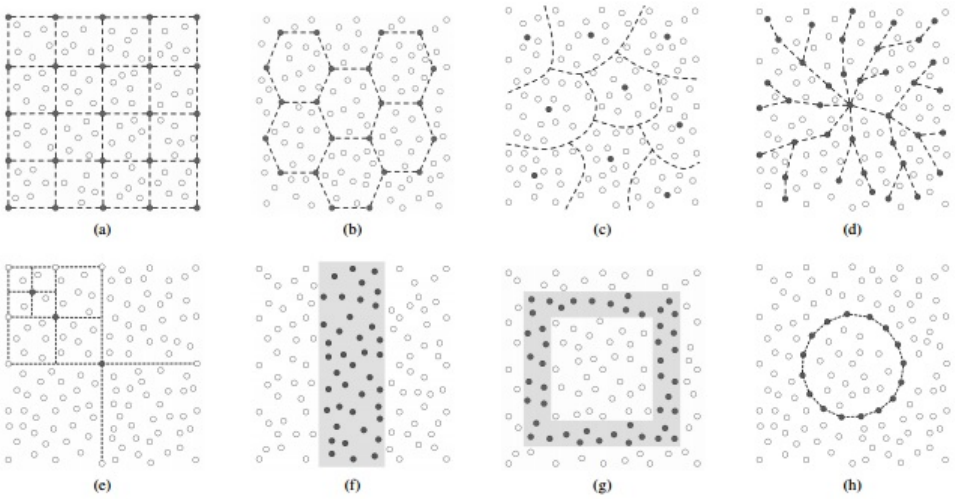

Figure 2.6: Classification of virtual grid structures imposed in hierarchical approaches: (a) Rectangular grid (e.g. TTDD, GBEER, CMR), (b) Hexagonal grid (HPDD), (c) Clusters (e.g. HCDD, EEMSRA, MSRP), (d) Trees (SEAD), (e) Quadtrees (QDD), (f) Lines (LBDD), (g) Rails (Railroad), (h) Rings (Ring Routing) [Tunca 2014].

In grid-based approaches, the nodes are moved on a certain grid pattern, as illustrated in Figure 2.6. The grid can be rectangular, triangular, hexagonal or any other shape. The grid-based hierarchical approach usually requires the geographic coordinates of the sensors, so position-aware sensors are usually preferred. The usefulness of the grid-based approach is limited by the high overhead of constructing the grid and the hotspot problem among the nodes making up the grid, on the border lines, or in the center cell.

In [Yuan 2011], a cluster-based model called the Energy-Efficient Mobile Sink Routing Algorithm (EEMSRA) is proposed where two factors were considered when deciding the next location for mobile sink: each cluster's average energy, and the maximum distance that the mobile sink moves (from current cluster-head to another cluster-head).

Classification		Routing Protocols	Advantages	Limitations
Hierarchical	Grid-based	TTDD;GBEER;CMR; HPDD; HexDD	Can used various shapes to make up grid.	Requires geographic coordinates (requires position-aware sensors).
	Cluster-based	HDD; EEMSRA; MSRP	Can operate without position-awareness sensors. Suitable for delay-tolerant applications.	Construction of cluster is more complicated than grid. No guarantee sink will visit all cluster heads.
	Tree-based	DDB	Redundancy due to establishment of large backbone with branches. Increase energy consumption.	Suitable for delay-tolerant applications.
	Agent-based	DHA; OAR	No formation of infrastructure. Utilize infrequent flooding.	Replacement between agents may cause hotspot and inefficiencies in data transfer.
Non-hierarchical	Flooding-based	GRAB;ER; TwinRoute; ALURP; Mobile RPL;DEEP; QBDCS; REDM;RM; E-TRAIL;GMRE; SIMPLE	Defining local flooding, reduces frequency of global flooding, utilize probabilistic flooding to limit extensive rebroadcasts, employs controlled sink mobility scheme, using route remembering property.	Some nodes outside local flooding range cannot establish routes to sink, validity of remembered route would decay.
	Over-hearing based	DDRP, Elastic Routing;		Cannot be used with duty-cycling low power protocols. Overhearing increase energy consumption significantly;
	Geometric properties Exploitation	GHT ; XYLS; Double blind Data Discovery using Double Cross; RLW;		

Figure 2.7: Classification, advantages and limitations of WSN routing protocols with mobile sinks.

Most of cluster-based approaches are suitable for delay-tolerant applications because the sink will only collects the aggregated data in the cluster heads whenever it approaches the specified distance threshold. However, if the cluster heads are not being visited within a confined time, some portions of the network may be omitted. Hierarchical approaches are advantages for predicting the next location, as the mobile sink knows its possible movements. However, the mobility is impeded by hotspot problems and possible failures of the mobile sink to visit all nodes.

Query-Based Data Collection Scheme (QBDCS) is proposed in [Cheng 2009] to tackle the problem of inefficient data collection in densely and uniformly deployed wireless sensor networks. In QBDCS, the mobile sink will inject a query towards the interested area if it is at the optimal query time. The sensor node closest to the center of the interested area will elect itself as the cluster head. Cluster head will aggregate data and wait for the sink arrival. A response (consists of estimated meeting position) is routed to the mobile sink until it arrives at the sensor node nearest to the estimated meeting position and either wait (if the mobile sink has not passed), be at chasing mode (if the mobile sink has passed) or discarded the packet (if exceed the time limit). The estimated meeting position is calculated based on several parameters (position information, time, packet length, estimated delivery velocity, and velocity of mobile sink).

However, predictive approaches may lose large amounts of data when the sink is obstructed from reaching the predicted position.

2.3 Trust-based approaches

In general, to achieve the desired benefits, trust management decides who to interact with, how to interact, and when should the interaction happens, with no guarantee that the desired benefits will be attained through such interaction [Ramchurn 2004]. Thus, this section reviews existing trust-based approaches in order to identify how they work (particularly the decision on how, when and whom).

2.3.1 Trust models

WSNs trust models are classified into node trust and data trust models (see Figure 2.8. Node trust models are further classified as centralised or distributed. At the individual level, trust models are divided into reputation based, learning based, or socio-cognitive based. Unlike centralised models, the trust values of the sensor nodes is not computed by any particular trusted intermediary or central station to compute the trust values of the sensor nodes. Instead, the trust values are calculated and maintained by the sensor nodes themselves [Han 2014].

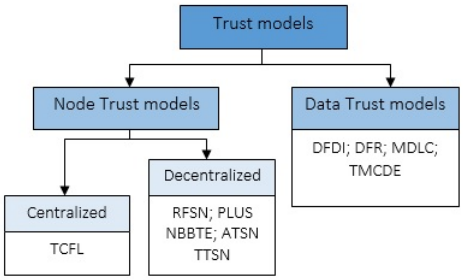

Figure 2.8: Classification of trust models in WSNs.

2.3.1.1 ATSN

Agent-based trust model in wireless sensor networks (ATSN) is a distributed agent-based trust management scheme that detects malicious nodes in WSNs by a watchdog mechanism. The watchdog observes the behavior (i.e. the packet-dropping and Hello Flood Attacks) of the sensor nodes and computes the trust ratings [Chen 2007]. Every node in ATSN has a watchdog and must maintain the trust of other nodes. The watchdog consists of a data collection phase, a data check phase and the status count. The check phase implements two modules: DFRouting and DFProcess. The DFRouting monitors the nodes forwarding behavior, whereas the DFProcess module monitors the raw sensing data, the data aggregates, the data delay, and other data-related phenomena. In the status-count phase, the agent node classifies the nodes behaviors into good or bad depending on the previous result, and counts the number of good behaviors.

2.3.1.2 PLUS

Developed for the sensor network security, the Parameterized and Localised trUst management Scheme (PLUS) [Yao 2006] consider various factors in the trust evaluation. The participants in PLUS include the judge, the suspect or evaluated node within the radio range of the judge, and the jury that maintains the trust value of the suspect being judged, and provides an opinion either periodically or intentionally. The trustworthiness in PLUS is obtained by a weighted summation of the direct trusts (personal references) and recommendations. The personal reference is derived from direct interactions with the suspect, whereas the recommendations(i.e. personal references of individual jury members towards the suspect) are obtained by

combining the recommendation provided by each jury. However, although designed for sensor networks, PLUS model is not suitable for WSNs, which requires special considerations that are not required in other sensor networks.

2.3.1.3 ReGreT model

ReGreT [Sabater 2001] claims to be among the most complete models, in which trust, reputation and credibility levels are calculated from direct experiences, third party information and the social structure of the agents for an actual online marketplace (electronic commerce). The truthfulness calculated in ReGreT take into account three dimensions, i.e., individual dimension (the direct interaction between two agents), social dimension (considering the characteristics of group relation) and ontological dimension (a combined reputations on different aspects).

2.3.1.4 FIRE

FIRE [Huynh 2006] incorporates similar elements to ReGreT. The model integrates four types of trust and reputation: interaction trust (based on the past experiences of direct interactions), role-based trust, witness reputation and certified reputation. The agents likely performance is comprehensively measured based on these trust values in selecting appropriate interaction partners. The certified reputation(CR), rated the agent that rates its partners in past interactions. Figure 2.9 demonstrates the referral process in the FIRE model. Certified Reputation (CR) is a trust model that allows agents to provide third-party references about their previous performances to gain the trust of their potential interaction partners. CR is useful when direct information of the potential partners is not available, or when a selfish witness is unwilling to share the experience of a particular partner. The relevance of each certified rating is calculated by a rating-weight function. The relevancy of a given rating is measured based on the recency of the ratings (using exponential decay). All trust and reputation values in FIRE are combined into a single composite trust value, using the weighted mean method.

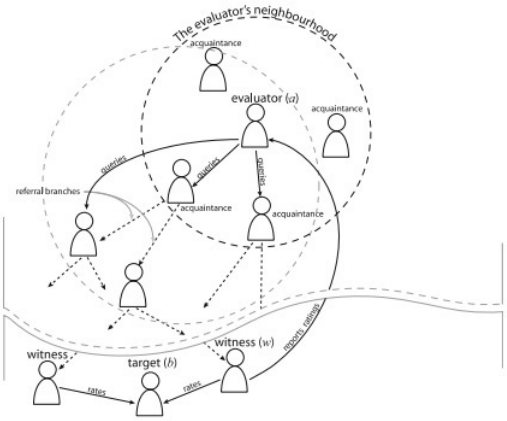

Figure 2.9: Referral process in the FIRE model.

2.3.1.5 PBTrust

The Priority-Based Trust (PBTrust) model [Su 2010] selects the service providers in general service-oriented environments. In PBTrust, the third party evaluation is done for overall performance and the requested service suitability. Instead of representing a single-item service with a single-valued evaluation, PBTrust represents each service by a number of attributes and their corresponding priorities. When the customer evaluates the service under the requested priorities of the service attributes, the accuracy of the service provider's performance is improved.

2.3.1.6 NBBTE

Figure 2.10 shows the Node Behavioural Strategies Banding Belief Theory of the Trust Evaluation Algorithm (NBBTE) [Feng 2011]. As shown in the figure, NBBTE trust evaluation involves three nodes - subject nodes, evaluated nodes and recommendation nodes. Subject node i obtains the trust value of evaluated node j by assessing object j directly and by evaluating the object j through three recommendation nodes k. Trust evaluation in NBBTE is based on various trust factors, including the received packet rate of the evaluated nodes, the rate of successfully sent packets, the packet forwarding rate, the data consistency, time frequency, node availability and security grade. The various trust factors gained by directly assessing the evaluated packets are collected into the direct trust value while the trust values obtained from other nodes' opinions of the evaluated object are called indirect trust values. Rather than simply weight-averaging the trust values, NBBTE obtains an integrated trust value using Dempster-Shafer evidence theory.

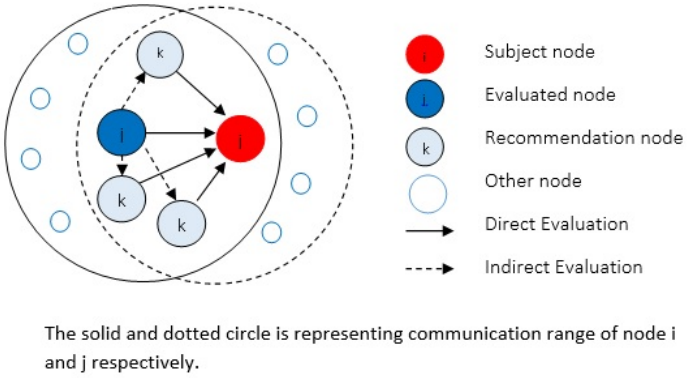

Figure 2.10: Recommendation-based trust relationships among the nodes in NBBTE.

2.3.1.7 EDTM

Efficient Distributed Trust Model (EDTM) is a distributed-node trust model developed for WSNs [Jiang 2015] that considers both direct trust and recommendation trust in its trustworthiness calculation. In EDTM, the trust values of the sensor nodes are based on various factors and are composites of direct trust, recommendation trust and indirect trust. As shown in Figure 2.11, the trust calculation involves three nodes: the subject node, a recommender, and an object node. In EDTM, the communication trust, energy trust and data trust between two neighbouring nodes are used in computing the direct trust value. The trust reliability and familiarity are considered in recommendation trust to improve the accuracy of this trust. The indirect trust is gained through the recommendation nodes when the subject node cannot directly observe the communication behaviours of the object node. EDTM has been demonstrated as an efficient and attack-resistant trust model. In EDTAM, the weight values for the direct trust components are selected within 0 to 1 interval and total weights assigned are summed to 1.

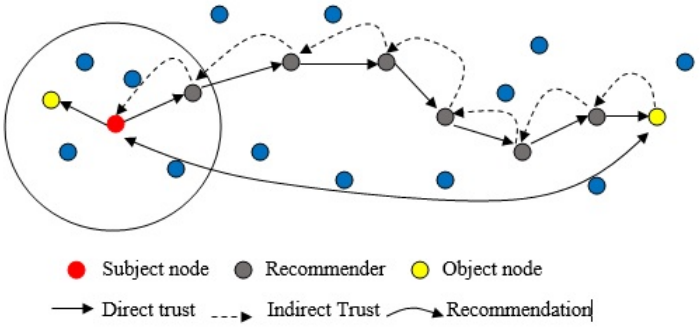

Figure 2.11: Different types of trusts and their evaluators in EDTM.

Figure 2.12 shows the structure of the EDTM model. The weight assigned to assigned to each value in the direct trust calculation are based on the communication, residual energy and data content. If the value of the communication packet is below the set threshold value, the recommendations of the recommenders are integrated to calculate the direct trust value. The recommenders in EDTM are selected by the source (evaluating) node, which identifies and determines the appropriate recommender nodes for the given target (evaluated) node. If the target node needs to be reached via other nodes, the trust calculation is a multi-hop process that incorporates the trust values of the nodes along the source target route (note that this is an indirect trust calculation). The trustworthiness is calculated only by the source node.

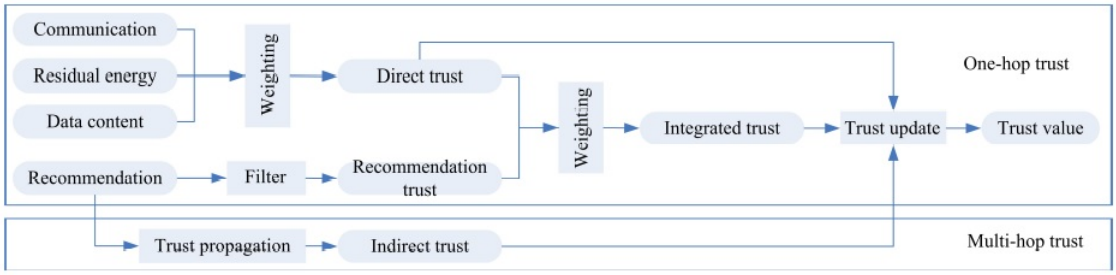

Figure 2.12: Structure of EDTM.

2.3.2 Trust-based Routing Protocols

As seen earlier, most of the trust mechanisms in WSNs are applied in security measures. The applicability of trust models in WSNs has been observed by embedding the models in existing routing protocols. The reason for such applicability is obvious, as trust-based methods can counteract security attacks. For example, cryptography and authentication primitive assume that nodes are cooperative and trustworthy, which cannot protect against insider or node misbehavior attacks. Therefore, in the absence of trust-based protocols, security management requires a central administration at the cost of high computation, large memory and much energy consumption [Ahmed 2015].

Applications of trust models in WSNs can be classified into five categories: in detecting malicious attack, securing routing, data aggregation, localisation and node selection [Han 2014] but only few have considered the critical aspects of WSNs, which are resource constrained. This section focusses on routing applications. It reviews existing trust-based routing protocols with multi factors decisions making, namely, the Trust-Aware dynamic Routing Framework (TARF), the Trust and Energy Aware Routing Protocol for WSNs and the Direct Trust Dependent Link State Routing Protocol (DTLSRP) using route trusts for WSNs.

2.3.2.1 Ambient Trust Sensor Routing (ATSR)

Ambient Trust Sensor Routing (ATSR) [Zahariadis 2013] is proposed to defend against misbehaving nodes in charge for routing attacks. The messages consisting of node ID, remaining energy, and location coordinates are broadcast periodically by each node. Indirect trust information is gained by multicasting the reputation request messages periodically. Each node will monitor its one hop neighboring nodes' packet forwarding behavior. The exchange of these messages at periodic basis cause high volume of network traffic. ATSR also requires a huge memory to store the indirect trust values.

2.3.2.2 Trust-Aware dynamic Routing Framework (TARF)

The Trust-Aware dynamic Routing Framework (TARF) [Zhan 2010] is a trust-aware routing framework for WSNs, that incorporates the trustworthiness of nodes into

routing decisions. TARF secures multi-hop routing through a WSN against the replay of routing information intruders. In this protocol, the nodes only need to decide the neighbouring node that will receive the packet. Once the packet is forwarded to the chosen neighbour, the decision of the next selection is fully delegated to the chosen node. The next-hop node selection in TARF is based on trustworthiness and the energy efficiency of the forwarding node's neighbours, which are maintain by the trust manager and energy watcher, respectively, in a neighbourhood table (Figure 2.13). Suppose that node N wants to send a data packet to the base station. The energy watcher records the energy cost of passing to each known node neighbour observed by N, and the energy costs reported by N's neighbours. The trust levels of the neighbours is tracked by the trust manager based on network loop discovery, and the base station will broadcasted messages regarding the undelivered data packets. The messages broadcasted from the base station inform about the undelivered data packets and the energy cost reported by each node. However, the exchange of broadcast messages and energy control packets increases the routing load and allows the sending of false energy-cost information from compromised nodes. The TARF [Zhan 2010] extends the data-centric routing protocol, Gradient Based Routing (GBR)and characterizes the possible misbehaviour of the attackers in dynamic WSN environments. However, the important design parameters for WSN in terms of energy consumption and network lifetime are not evaluated in TARF to measure the effectiveness of proposed solution.

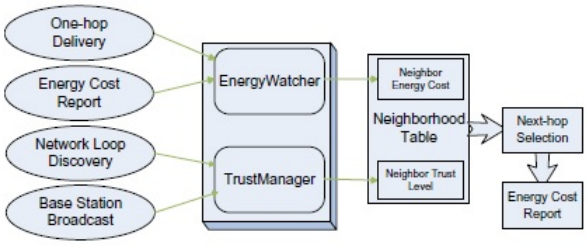

Figure 2.13: Construct of a next-hop neighborhood table in TARF.

2.3.2.3 Trust and Energy Aware Routing Protocol for WSNs (TERP)

Trust and Energy Aware Routing Protocol (TERP) for WSNs in [Ahmed 2015] incorporates a Composite Routing Function (CRF) comprising the trust, residual energy and hop count of the neighbour nodes. In TERP, each node monitors the packet-forwarding behaviour of each of its 1-hop neighbours through promiscuous learning. The total trust is the weighted sum of three components: direct trust, indirect trust and probability of the expected positive behaviours. Direct trust is gained through the node's own experience with it's neighbours. It measures the number of correctly forwarded packets from each neighbour to the total number of packets received (i.e., the packet-forwarding ratio of each neighbour). Indirect trust constitutes the recommendations provided by other nodes. The expected probability of the positive behaviours refers to the expected future of the node based on its forwarding behaviour (the packet forwarding ratio). A Beta probability density function is used to measure the node's expected future behavior. If the neighboring nodes have successfully forwarded the packets that they received, the value of a well-behaved node is incremented by 1. Otherwise, the malicious behaviour value of the node is incremented.

TERP extends the routing mechanism of the AODV protocol by modifying the route discovery packets RREQ and RREP to incorporate the trust and energy information. Figure 2.14 illustrates the route-discovery process of TERP. Initially, the source node (S) checks whether the destination node (D) exists in it's local entry route. Source node will deliver the packet along the route to the destination if there is entry route for destination node. However, if the destination node does not exists in the local route of the source node, or is present but with less energy or trust value than the threshold value, the source node initiates route recovery by broadcasting RREQ packets(see initial phase in Figure 2.14).

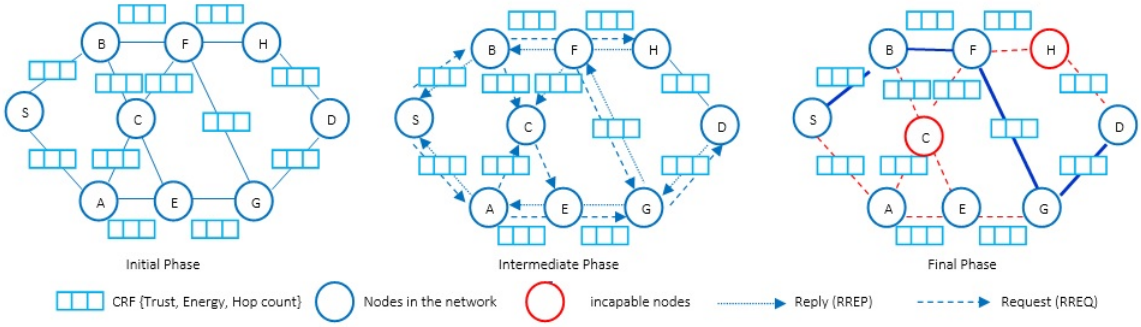

Figure 2.14: Route Discovery process in TERP

.

Nodes with low energy, and those suspected as malicious, are eliminated during the route recovery. The route recovery process continues until the RREQ packets have reached the destination. When it receives the RREQ packets, the destination node sends a reply message (RREP) through the discovered route back to the source node. As shown in the intermediate phase of Figure 2.14, the source node receives multiple RREP packets and chooses the optimal route, that minimises the routing cost (i.e. the most reliable route with the most remaining energy and the lowest hop count).

In the route maintenance phase of TERP, a new route must be discovered whenever an intermediate node finds some energy deficiency and packet-forwarding misbehaviour by malicious nodes along the route.

2.3.2.4 Direct Trust Dependent Link State Routing Protocol Using Route Trusts for WSNs (DTLSRP)

The Direct Trust Dependent Link State Routing Protocol (DTLSRP) using route trusts for WSNs [Babu 2011] protects against routing attacks in WSNs by eliminating the non-trusted nodes and finding the best trustworthy route among the remaining nodes. The parameters of the direct trust are calculated using the geometric mean. DTLSRP considers the basic features of link-state routing protocols and calculates the multiple hops along a route, but the trustworthiness calculation includes only the direct trust.

2.3.3 Blockchain-based Technology

Blockchain is a well-known technology applied in domains such as e-commerce, online business and banking. Blockchain is renowned for being trustworthy, self-executable and self enforceable, in the absence of third-party management [OâDwyer 2015]. Accordingly, blockchain applications have extended beyond financial transactions, into distributed cloud storage, smart properties, Internet of Things, supply chain management, healthcare, ownership and royalty distribution, and decentralized autonomous organizations [Wüst 2017], and [Nakamoto 2008]. Wust, regarded blockchain as a technological innovation that can revolutionise how society trades and interacts [Wüst 2017].

Blockchain as a distributed solution: Blockchain is an algorithmic tool that can track, coordinate, carry out transactions, and store information from many devices [Fernández-Caramés 2018] and fosters trust in distributed environments without requiring centralised authorities which is potentially changing in many industries.

The way it governs information: The distributed ledger for data storage, and a smart contract that governs the mechanism of the blcokchain network. Unlike traditional models, in which the data are controlled by a single authority, the distributed ledger, controls the data through a set of pre-agreed rules. The distributed ledger (also called the blockchain rules, network rules, or rules of the ledger), decides the validity of new information, determines how the new information is handled, and specifies the proper reaction of participants to the new information.

Verifying information in a distributed manner: Blockchain allows the verification of transactions by a group of unreliable actors and the materialisation of smart contracts [Reyna 2018]. Although blockchain was conceptualised as a cryptocurrency tool, a cryptocurrency is not required for using a blockchain and building decentralized applications [Raval 2016].

Methodologies that identify whether a blockchain is suitable for solving certain problems, and that determine the appropriate type of blockchain for a specific problem, have been proposed by several authors [Wüst 2018], [Fernández-Caramés 2018]. A blockchain-based approach is suitable if updated copies of the information need to be distributed, when the entity managing the distributed computing system is not trusted, or when there is no trust in the third party [Fernández-Caramés 2018].

Blockchains can be public or private, or permissioned and permissionless, depending on the managed data, the availability of such data, and the actions available to users. Some authors use the terms public(and permissionless) or private (and permissioned) as synonyms [Fernández-Caramés 2018].

Dynamic participation in an open and decentralised network: Any peer can join and leave the network either as a reader or writer at any time. Bitcoin and Ethereum [Wood 2014] are examples of permissionless blockchains, that are open and decentralised. The membership is not managed by a central entity, and the set of writers is unfixed and known to all participants. Permissionless blockchain is completely open, implying that its written content is readable by any peer. On the other hand, permissioned blockchains authorize a limited set of readers and writers. Whether individual peers can participate in the read-write operations of the blockchain are decided by a central entity [Wüst 2017].

Despite its acceptance in many domains, the blockchain concept has rarely been applied to WSNs. Motivated by the above mentioned issues; this chapter proposes an efficient network-assisted (or controlled) mobility mechanism for the mobile sink, that avoids flooding and hotspots. Considering the resource availability alone is insufficient in unpredictable environments, where the nodes normally (require verification for security purposes). In existing trust-based approaches, the trust values are computed by neighboring nodes, which are open to misleading decisions. In addition, they are made by a single node, rather than by parts of the network.

2.4 Conclusion

In this chapter, an extensive review has been conducted involving routing protocols in WSNs, trust-based approaches, and collaborative mechanisms. It introduced the state of the art and existing works related to distributed and decentralised routing decision making. The existing routing challenges and solutions were highlighted, specifically considering multiple criteria in selecting forwarder to route the packets and relocation aspects in determining the sink movement. This chapter has reviewed the existing trust-based approaches to observe its applicability for distributed and decentralised routing decision in WSNs. While there are many existing works on routing protocols in WSNs, there are still limitations in terms of several aspects

highlighted below:

- In choosing the nodes to relay the packets, the factors considered in the traditional WSNs routing protocols are restricted to either energy perspective or distance. On the other hand, most of the existing trust-based approaches were focussing on the security aspects in their decision making. Even though there are works that consider both aspects (resource and security) in their decision making, the number of such work is very limited. Other important factors should also be considered in the decision making. The total trust is obtained by weighted summation of several types of trust values. Other potential composite trust value should be explored.

- Most of the evaluation conducted in existing works only considers trustworthiness of the target node. Very few that measures the trustworthiness of the nodes that evaluate the target nodes. Comprehensive evaluation on target node, might not be necessary for network with resource-constrained nodes. Instead, information about more nodes (few hops away) may represent a better picture of the network.

- While the challenges above is concerned static sink, the implementation of mobile sink with controlled mobility is still limited. In deciding the solution for distributed network, a resource-aware and trustable approach is needed.

This chapter provides appropriate input for development of the proposed approaches.

CHAPTER 3

Hierarchical Trust-based Model (HTM)

3.1 Introduction

In this chapter, a distributed Hierarchical Trust-based Model (HTM) is proposed. The reviews conducted in Chapter 2 reveal that efficient mechanism is needed to improve the efficiency of existing distributed routing decision making, in terms of the criteria considered and the information provider in selecting the reliable forwarder to relay the packets. This chapter will respond to the forwarder selection problems highlighted in previous chapters. Due to the limited number of multi-criteria trust-based models for WSNs in the literature, HTM is proposed to improve the efficiency in forwarder selection by comprehensively considering various trust factors in its decision and ensuring that the evaluation done is made by the credible nodes. The trust in HTM is defines as the belief that a node has on other nodes based on the four network performances: reliability, energy efficiency, coverage and reputation. These four trust factors will determine the trustworthiness level of the nodes, where the nodes having the highest trustworthiness values will be chosen as the next forwarder.

HTM utilises the multi-criteria analysis technique called Analytical Hierarchy Process (AHP) that is well accepted in other domains but rarely in WSNs to select the best candidate as the forwarder.

In this chapter, the structure of HTM is introduced and the components that constitute the trustworthiness of the selected node is explained. The developed HTM will be used in Chapter 4 in order to measure its effectiveness when applied to the distributed routing decision making.

In order to explain the Hierarchical Trust-based Model (HTM) better, this chapter is divided into several subsections. In Section 3.3, the structure and components in HTM are explained. The analytical hierarchical process (AHP), which is the mechanism used for selection decision in HTM is highlighted in Section 3.4. In Sec-

tion 3.6, example of HTM implementation is demonstrated. Finally, the conclusion of this chapter is presented in Section 3.7.

3.2 Motivation

In Chapter 2, we have highlighted several existing trust models from open MASs such as service-oriented applications and also trust models meant for resource constrained systems such as WSNs.

As we can see, all these models consider multiple trust values that include direct trust, recommendation trust, witness trust and also indirect trust. However, there are several limitations and unrealistic common consumptions made by these models, as outlined below.

- In a decentralized network, especially consisting of resource constrained nodes (or agents), each node highly depends on information provided by its surrounding neighbours. Thus, the reliability of the information and the credibility of the information provider are crucial. Works involving multiple-criteria consideration exists, but very few. The considered factors in existing works include residual energy, receive and forwarding packet rate etc. While some of the involved factors contribute to the same performance metrics, we construct our HTM in a hierarchical form, where at the top hierarchy is the performance metrics (as the main factors) and at the lower level is the related attributes of the main factors (the performance metrics). By doing so, we can determine which factors to be considered in the selection decision.

- Most of the existing work focuses on evaluating a specific target (or known node), which is normally one hop away node. To gather information, process and transmit packets for every single transmission, especially when the source and target are far apart, is troublesome and costly, as more hops may involve. On the other hand, evaluating a few hops in advance is expected to cause less communication consumption.

- In addition to the situation in the previous point, relying only on direct experience between evaluator and evaluated nodes may result in inaccurate decision. In such situations, information from the third party is required. However,

the information provided could be from reliable and also may be from unreliable providers. Thus, mechanism is required to verify the credibility of these information providers.

- Nodes in a decentralized network normally lack information about the whole network. They are restricted to limited knowledge provided by neighbours within their communication range. However, some existing works assume that the source (evaluating) nodes have the ability to identify and choose recommenders or witness for evaluated nodes, which is an impractical assumption for WSNs.

- In ensuring the evaluators are reliable, the trustworthiness of nodes that evaluates evaluated nodes is obtained. There is existing work that considers this mechanism but very limited and not meant for WSN.

- Many distributed networks are homogenous, where all the nodes in the network may have the same initial capabilities and resources. In such a situation, it is burdensome to let the source node to do all the calculations and trust evaluations. Unfortunately, most of the trustworthiness in existing works is computed by the source node. Thus, mechanism is required to reduce the burden on the source nodes.

Based on the highlighted points above, HTM aims to overcome these issues by proposing a distributed trust-based model which is based on Analytical Hierarchy Process (AHP) methods. It is one of the well-known multi criterion decision making (MCDM) used in many research domains. AHP is adapting in HTM to give insight into the best options among several potential providers. The details on AHP is given in Section 3.4.

The mechanism used in HTM could also reduce the burden of source nodes by providing filtering mechanisms, where only selected and good reputation providers will be short listed and forwarded to the source for decision making.

The following sections will detail on how selection decision is made in HTM. In order to do that, we introduce HTM in Section 3.3, and its overall structure and components in Subsection 3.3.

3.3 Hierarchical Trust-based Model (HTM)

As mentioned earlier, the trust in HTM is defines as the belief level or degree of reliability that a sensor node has on other nodes for a specific action, based on multiple trust factors that relates to the network performance measurements explained in Section 3.3.2. The trust values are provided by three types of nodes (called source node, direct node and witness node). A higher gained value indicates a higher belief level, which regards the node as the more trusted node to be selected as the forwarder. The proposed model, called Hierarchical Trust-based Model (HTM) is an integrated trust and reputation model that comprises three main components: direct trust, indirect trust and witness reputation. Subsections 3.3.1 to 3.3.1.3 will explain about these components.

According to [Pinyol 2013], existing trust models can be classified as centralized and decentralized, depending on how the trust information is stored. The centralized trust model has least computational overhead and least memory usage but involves most communication overhead, is least reliable and lacks scalability. HTM, on the other hand, is a distributed model, where the trust values are of is calculated and maintained locally by each node which involves most computational overhead. However, it is more reliable and scalable [Rani 2014].

Figure 3.1 shows the process and the three types of nodes involved in HTM: source node, direct nodes and witness nodes:

- Source nodes (denoted as S) is node that has data to be sent and requires relay service.
- Direct nodes are nodes within direct communication range with source nodes. n_1 and n_2 are direct nodes of S, which normally 1-hop away from the S.
- Witness nodes are nodes within direct node's communication range. Witness node for direct node n_1 is n_8 and witness nodes for direct node n_2 are nodes n_3 and n_4. Witness nodes are the 1-hop away nodes from the S's direct nodes and 2-hop away from the S.

Due to the distance between source and the destination, more hops may be involved. The nodes will be identified as the same, i.e., the selected witness will

then be the source, and nodes within its direct communication will be direct nodes and so on.

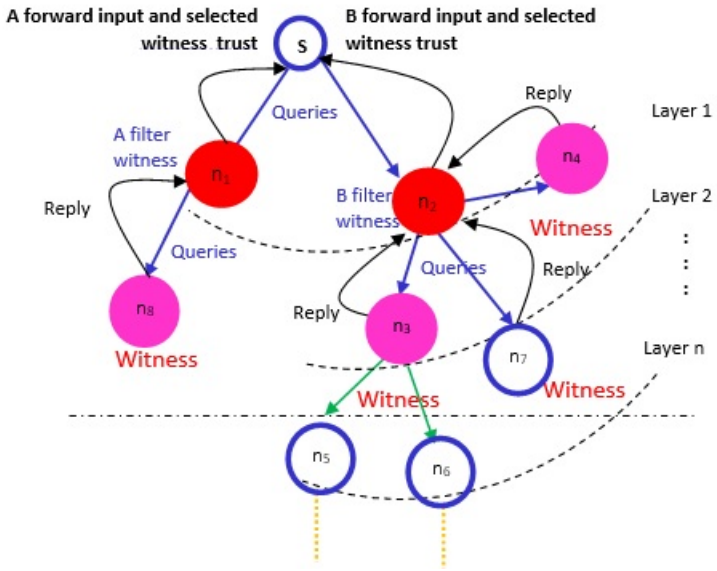

Figure 3.1: The process and types of nodes in proposed HTM.

Asymmetry, composability and transitivity are the three main properties of trust that are commonly defined in many literatures. Asymmetry indicates that node B will not necessarily trusts node A although node A trusts node B. Composability is the integrated value consists of trust values gained from multiple available paths. Transitivity implies when node A trust node C and node B at a certain level, node B will also trusts node C. HTM adopts transitivity properties where in Figure 3.1 for example, source node S will trust n_1's witness (n_8) if n_1 trusts it's witness (n_8) and also S will trust n_2's witness (n_3 and n_4) if n_2 trusts it's witness (n_3 and n_4).

3.3.1 Structure of HTM

In this section, the overall structure of HTM will be described, based on Figure 3.2. As shown in Figure 3.2, HTM consists of three main components of trust: direct trust, witness trust and indirect trust. The trust value of each component is evaluated by source node, direct node and witness node, respectively. In each trust evaluation, several inputs are involved. These inputs are the criteria or metrics that are required in computing each trust value. There are two types of evaluators (decision makers) in HTM, named source node and direct node, located at different hops (layers). Thus, there are two phases of decisions involve in HTM.

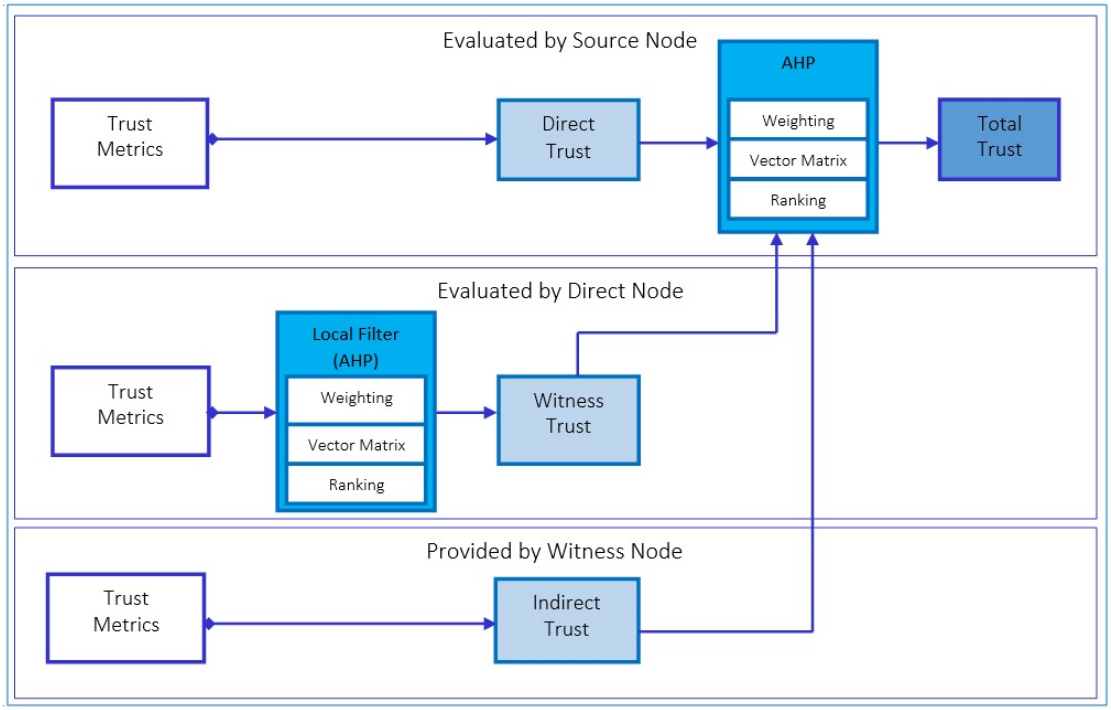

Figure 3.2: The overall structure of HTM.

The first phase involves direct nodes as evaluator and its direct neighbours as evaluated nodes (witnesses). Several criteria and sub-criteria may be used as evaluation metrics. The values collected will be used by direct nodes to calculate the witness trust (WT). The high ranked witness information will be sent to source nodes for evaluation in the second phase (final trust or trustworthiness).

There may have existed communication or interaction in the past between direct nodes and their witnesses. This may consist of previous communication behaviour or experiences (success or failure transmissions). This information will also be sent together by the direct nodes, to the source nodes. This value will be used by the source nodes and is identified as Indirect Trust (value of direct nodes given by other parties, i.e., the witness).

In the second phase, source nodes will evaluate their direct nodes (i.e., the decision maker in Phase 1). As explained in Subsection 3.5.1, direct trust in Phase 2 is calculated based on direct communication between the source (evaluator) and its direct (immediate) neighbours. In this phase, the source node can consider the same criteria evaluation as direct nodes in Phase 1 or it can use other criteria evaluations. The value gained from direct interaction between the source node and it's direct neighbours is known as Direct Trust of direct nodes. The value gained

from direct interaction between the direct node and it's direct neighbours is known as Witness Trust of witness nodes. The value provided by witness nodes about the direct nodes that evaluate them is known as Indirect Trust. Upon gaining all the trust values, source nodes will do a final computation of trustworthiness and rank in decreasing order. Based on the rank, the source nodes will choose its next forwarder and witness.

3.3.1.1 Direct Trust (DT)

Direct trust is gained through direct interaction between two nodes. Figure 3.3 shows an example of direct interaction between source node S and three direct nodes, n_1, n_2 and n_3. Direct nodes of S in this example are nodes within the source radius (R_{Source}). Direct interaction may also exist between direct nodes n_1, n_2 and n_3 and its direct neighbours that are within the direct nodes' radius, (R_{Direct}). Direct trust in HTM is calculated by two types of evaluators: source node and direct node. The source of direct trust information is thus gained from: 1) the source node's interaction with the direct node and 2) the direct nodes interaction with the direct node's neighbours (called witness, when direct node evaluating witness).

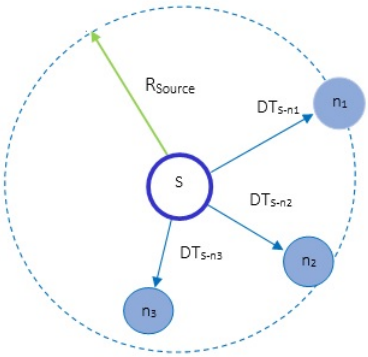

Figure 3.3: Direct Trust on direct nodes of source nodes, evaluated by S.S is the source node, n_1 is the direct neighbours of S, i.e., nodes within the source node's radius (R_{source}) and DT_{s-n_1} is direct trust between n_1 and the evaluating node (i.e., source node).

3.3.1.2 Indirect Trust (IT)

In [Huynh 2006], witness reputation and certified reputation (CR) are used in collecting information from third-parties about evaluated nodes. HTM exploits the certified reputation component in CR in gaining references about evaluated nodes.

Witness reputation helps in situations where direct information is not available. However there are some situations that are not feasible in most witness-based reputation model, such as:

- New nodes joining the environment may not have any interaction history with the other nodes in that environment. If the node only depends on direct experience, it may need to interact with other agents to explore and learn about the other node's performance. These explorations consume time and effort.

- Assuming the willingness of an agent in sharing its experiences such as in a witness-based model cannot be guaranteed in the real world. This is due to the selfishness of the agents (unlikely to be willing to sacrifice their resources in providing witness reports) or the difficulty locating a witness for any given agent in the distributed and open environments [Huynh 2006].

Some form of centralized mechanism is commonly used to collect witness reports in the presence of self-interested agents. However, centralized mechanisms may raise issues of trustworthiness of a central authority. In addition, locating witnesses in the distributed and open environments may involve high cost in terms of time and resources.

As shown in Figure 3.4, Indirect Trust (IT) in HTM is obtained from the direct node's neighbours and stored by the direct node itself, then being forwarded to the source node (evaluator) for further evaluations. The agents giving references (i.e., the direct node's neighbours) are called witnesses in HTM. The references are about direct node's communication behaviours in the past interactions between the direct nodes and its neighbours (of success or fail transmission).

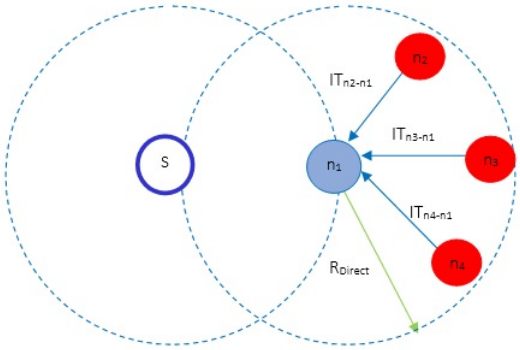

Figure 3.4: Indirect Trust of direct nodes, evaluated by witness nodes. Witness nodes are nodes within direct nodes n_1 radius R_{n_1}) and $IT_{n_2-n_1}$ is the indirect trust of n_1 given by the witness node n_2, $IT_{n_3-n_1}$ is the indirect trust of n_1 given by the witness node n_3 and $IT_{n_4-n_1}$ is the indirect trust of n_1 given by the witness node n_4 respectively.

In gaining the trust of the potential partners, the references provided by witness nodes enable the direct node to prove its capabilities to its potential partners, based on its previous interaction partners. In CR, the evaluated node is allowed to choose which references to put forward [Huynh 2006]. In HTM, only references from the selected witness are forwarded to the source node. This is feasible as selected witnesses (those having a good ranking given by direct nodes), are assumed to provide trusted information about their partners (the direct nodes). This can be illustrated by the scenario of applying for a job, where the applicant will forward referrals that have a good reputation and that they believe can give good feedback about the applicant's previous performance.

Storing references at the evaluated nodes provides high availability, since the information can directly provided to evaluator, and also involves very low communication and processing compared to sources like witness reputation. In HTM, allowing the direct node (evaluated node) to filter references, could move the burden of obtaining and maintaining trust information from the trust evaluator to the evaluated agent.

3.3.1.3 Witness Trust (WT)

Most existing trust models are concern on one hop (layer) evaluation [Yao 2006], [Sabater 2001], [Su 2010], [Feng 2011], and [Jiang 2015]. For example, consumer may select the best provider, based on direct experience with the provider and also

reputations given by other parties that have past interactions with the provider. In some cases, it is important to have knowledge of the reputations and performance of the parties involved in the evaluation too. This is because the performance of the selected provider is a result of the performance of the parties involved in providing the service. By having such knowledge, consumers can have a better idea of future expectations if the consumer knows in advance that they are dealing with a provider who has links to good reputation parties.

In resource constrained environments, such as WSN, the single layer (1-hop) evaluation is normally conducted on single node. Mechanisms such as certified reputation and witness reputation are used to gain information about the 1-hop nodes [Huynh 2006]. A similar need is applicable to WSNs, where in large networks consisting of resource constrained nodes, evaluating more than 1-hop nodes at a time may provide several benefits. The challenges in evaluating 1-hop nodes are listed below:

- Sensor nodes works within a limited range. In a large network, the packets need to travel via several hop (multi-hop) to reach their destination. In the case of a transmitting packet that is far from its destination, evaluating 1-hop nodes will requires a number of evaluations.

- Energy is consumed when a packet is transferred or received. High energy consumption may be involved per transmission of request and reply messages in every hop.

- Distributed and open environments such as WSNs are exposed to many uncertainties. It is not guaranteed that the best selected 1-hop nodes may have capable neighbours to continue delivering the packets to the end destination. In addition, packets delivered via an optimal 1-hop node (single node evaluation) may not necessarily successful.

- In a homogenous network, where all the nodes have the same capabilities, allowing source nodes to compute and decide may burden and shorten the source node's life.

To overcome such issues, Witness Trust is proposed where the evaluation is done at several hops (layers). By doing this, the number of evaluations may be reduced

and less energy is consumed. By allowing direct nodes to evaluate their own peers (its neighbouring nodes that are within the direct node's radius), the load on the source could be distributed to direct nodes. Evaluation done by direct nodes in terms of ranking, acts as a filtering process, where only good ranked nodes are forwarded to source nodes. This will as well reduce the number of tasks at the source node, as the number of evaluations is less.

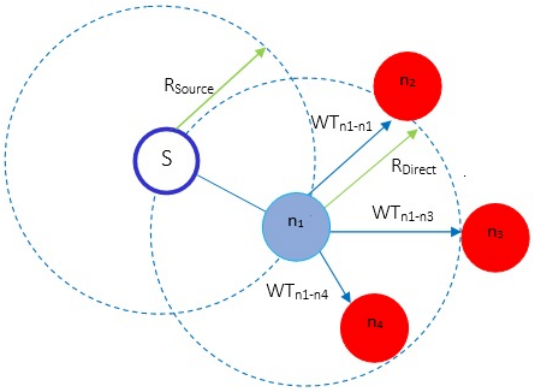

Figure 3.5: Witness Trust evaluated by direct nodes n_1. S is the source node, n_1 is the direct neighbours of the source node, i.e., nodes within the source node's radius (R_{source}) and $WT_{n_1n_2}$, $WT_{n_1n_3}$ and $WT_{n_1n_4}$ is the trust given by direct node n_1 on witness nodes n_2, n_3 and n_4.

In Figure 3.5, when direct node n_1 receives a request from S, it will send a request to it's neighbours within it's R_{direct}, i.e., n_2, n_3 and n_4.

The direct node neighbours (n_2, n_3 and n_4) will reply to direct nodes n_1, with their own information and their past experience with the direct node's (IT). n_1 will then compute, rank (using pairwise comparison), select witnesses and forward message to S .

3.3.1.4 Integrating Trust

To gain the total trust of evaluated nodes, all components of trusts (Direct Trust, Indirect Trust and Witness Trust) are integrated into a single value, to depict an overall performance of the agent. Figure 3.6 shows integrated trust values computed at S. The final selection will be based on the ranking in decreasing order. S will select the direct node and the direct node's witness pair that is in top of the ranking. The weight considered in our decision is gained via pairwise comparison between evaluated factors (which will be explained in Section 3.4.1), thus it differs from

the commonly used weight consideration in most existing literatures, i.e., weighted mean.

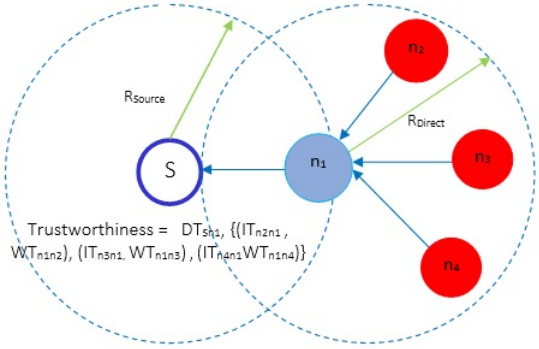

Figure 3.6: Integrated Trust consists of Direct Trust, Indirect Trust and Witness Trust computed by source node *S*.

3.3.2 Assumption and Network Model

HTM is developed based on the assumptions below:

1. To ensure cooperation from interaction partners, it is necessary for agents to provide information. This is feasible by making it a standard part of any task allocation agreement, i.e., by forcing them to give information.

2. Trust assessment will be solely on direct trust between the source and the evaluated nodes whenever there is no witness or reputation from indirect nodes available.

3.3.2.1 Trust Metrics Determination

The factors considered in HTM are organised according to the performance measurements. A metric is defined as a measure for quantitatively assessing a process, event, or institution, using different procedures to carry out measurements and the procedures for the interpretation of the assessment, leveraging previous assessments [Khan 2012], [Akyildiz 2002b]. Pereira et. al had classified the metrics into individual metrics and composed metrics [Pereira 2016]. Individual parameters are related to a single node, while the composition of parameters of a group of nodes constitutes collective parameters.

In WSNs, the performance measurements include designing efficient routing protocols in terms of coverage, energy efficiency, network lifetime etc. Several metrics were used in order to achieve such routing efficiency. Routing metrics have a great influence on the operation of routing protocols, hence an appropriate routing metric is significant to avoid routing loops and suboptimal paths [Khan 2012]. Below are some related metrics used in WSNs for measuring performance efficiencies.

A study conducted in [Pereira 2016] proposed seven requirements of performance measurements: delay tolerance, loss tolerance, capacity, reliability, energy efficiency, criticality and fault tolerance. Under each of these requirements, the author identified related metrics, such as node delivery delay, delay per hop etc., for delay tolerance and number of packet losses for loss delay. In [Khan 2012], performance metrics highlighted by the author include throughput, average end-to-end delay of data packets, packets delivery ratio etc. The metrics highlighted by the author in [Anadozie] include energy efficiency, latency, accuracy, fault tolerance, scalability and throughput.

In measuring performance based on energy efficiency, metrics used are energy per packet, network lifetime, average packet delay, packet delivery ratio, packet size and distance [Pantazis 2013].

Several metrics related to coverage evaluation were highlighted in [Zhu 2012] and [Singh 2015], which include quality of service (QoS) of coverage, number of active nodes, energy efficiency, communication overhead and network scalability. In [Akl 2011], the author highlights the factors that have influence over the network density, i.e., mobility, transmission range, throughput and deployment scheme.

Studies above shown that different metrics were used in measuring different aspects of network performances. In HTM, the performance measurements (i.e., in terms of coverage, energy, reliability and reputation) are represented as main criteria and exist in the Layer 1 of Figure 3.7. Related metrics are determined for each of these performance aspects. For example, in terms of coverage, number of nodes is used to measure coverage efficiency etc. In HTM, these metrics represent sub-criteria of the main criteria and exist in the Layer 2 of Figure 3.7. The criteria and sub-criteria are the trust metrics used in HTM decision making.

3.4 Analytical Hierarchy Process (AHP)

In this section, a detail explanation about Analytic Hierarchy Process (AHP), i.e., the processes and steps involve in generating the weight and the trustworthiness is presented. AHP, introduced by Thomas Saaty (1980), is the most frequently used Multi Criteria Decision Analysis (MCDA) and are used in variety of research fields [Tscheikner-Gratl 2017]. Its extensive use in an incredible number of applications is due to several benefits, as listed below:

1. It allows the possibility to use qualitative and quantitative criteria.
2. It provides quality assurance through the use of consistency indices.
3. The ordered fashion of the decision making allows good traceability of the decision.

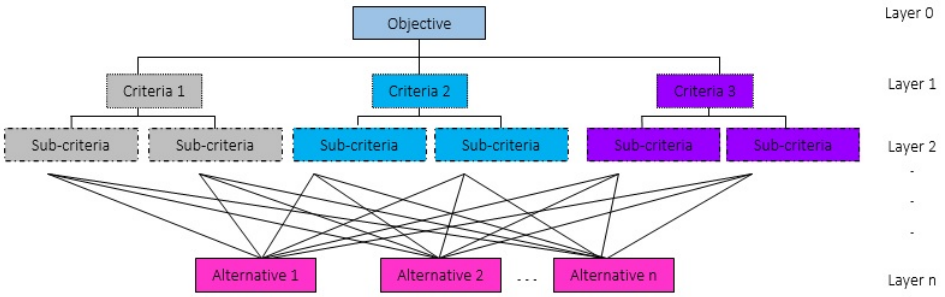

Figure 3.7: Structure of hierarchy in Analytic Hierarchical Process (AHP).

Figure 3.7 demonstrates a general structure of AHP, where the goal is at the highest level (Layer 0), followed by selection criteria at the second level (Layer 1). In Figure 3.7, sub-criterion exist in Layer 2 of the hierarchy. In some applications, there could exist sub-criterion for each of the sub-criterion, thus more levels may involve. The base of the hierarchy comprises the alternatives. Example in Figure 3.7 demonstrates the existence of three alternatives, i.e. Alternatives 1, 2 and 3.

The implementation of AHP follows three simple consecutive steps: (1) Computation of the criteria weights vector (2) Computation of the option scores matrix and (3) Ranking the available options. In addition to this, another important step is (4) Checking inconsistency. The details of each step is explain below:

3.4.1 Computation of criteria weights vector w

The weight of each criteria is computed by first, creating the pairwise comparison matrix A. The matrix A is a $m \times m$ matrix, where the number of considered criteria for evaluation is represented by m.

The pairwise comparison matrix A of a decision maker has the following form (Equation 3.1):

$$A = [aij] = \begin{bmatrix} a_{11} & a_{12} & a_{13} & ... & a_{1n} \\ a_{21} & a_{22} & a_{23} & ... & a_{2n} \\ : & : & a_{3n} & ... & : \\ a_{n1} & a_{n2} & a_{n3} & ... & a_{nn} \end{bmatrix} \tag{3.1}$$

The importance of the i^{th} criterion relative to the j^{th} criterion is represented by each entry a_{ij} of the matrix A.

The relative importance between i^{th} and j^{th} criteria is measured using the numerical scale proposed by [Saaty 1991], in a scale from 1 to 9, where 1 is representing equal importance, 3, 5, 7, and 9 represent moderate, strong, very strong and extreme strong importance respectively, of one over another factor. If the criterion in the column is preferred to the criterion in the row, the inverse of the rating is given.

The normalized pairwise comparison matrix for the matrix A is built by dividing each element in the matrix by the column total in Equation 3.2

$$x_{ij} = \frac{a_{ij}}{\sum_{i=1}^{n} a_{ij}} \tag{3.2}$$

Finally, the criteria weight vector w is built by dividing the sum of the normalized row of matrix by the number of criteria used (n), as in Equation 3.3.

$$w_{ij} = \frac{\sum_{j=1}^{n} x_{ij}}{m} \tag{3.3}$$

, where m represents the number of criteria used.

3.4.2 Computing the option scores matrix

The option scores matrix (S) is a $n \times m$ matrix, where each of its entry (s_{jj}) denotes the score of the i^{th} option with respect to the j^{th} criterion.

A pairwise comparison matrix ($B^{(j)}$) for each criteria is built, where for each criteria, the evaluation of i^{th} option compared to the h^{th} option for criteria j^{th} is represented by each ($b_{ih}^{(j)}$) entry in the ($B^{(j)}$) matrix.

3.4.3 Checking the consistency

The consistency ratio (CR) in Equation 3.4 of a matrix is the ratio of the confidence index (CI) of that matrix to the random consistency index (RI) for the same matrix order. If the consistency ratio is 0.10 or less, the decision maker is not too inconsistent and the result obtained by the AHP is acceptable. However, if the CR. is larger than 0.10, more serious inconsistency exists and the priority vector might not provide an accurate solution to the decision making process. Thus, the preference given should be re-evaluate.

$$CR = \frac{CI}{RI} \tag{3.4}$$

CI can be derived from Equation 3.5:

$$CI = \frac{(\lambda_{max} - n)}{(n-1)} \tag{3.5}$$

, where n is number of criteria considered and λ_{max} is the largest eigenvalue that can be gained using Equation 3.6 and the value for RI can be retrieved using random consistency index (RI) proposed in [Saaty 1980].

$$\lambda_{max} = \sum_{j=1}^{n} a_{ij} \frac{w_j}{n_i W_i} \tag{3.6}$$

The evaluated options scores for j^{th} criterion are then represented in the score vectors $s^{(j)}$, where j=1,...,m , which is obtained using the pairwise comparison matrix steps used in computing matrix A. The score matrix S is obtained as:

$$S = [s(1).....s(m)] \tag{3.7}$$

3.4.4 Ranking the options

The vector v of global scores is then obtained a by multiplying w and S, i.e.

$$\nu = S \cdot w \tag{3.8}$$

The i^{th} entry v_i of v is the global score assigned to the i^{th} option. Finally, the global scores are organised in decreasing order to accomplish the option.

Figure 3.8 demonstrates the overall steps involve in determining and calculating weights and the final score in the node's selection in HTM.

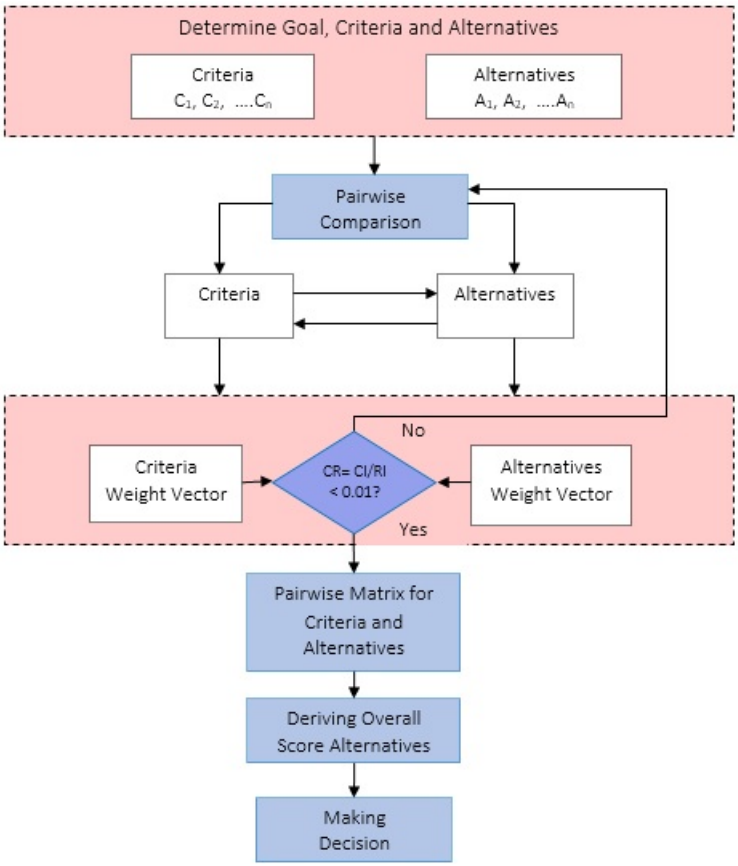

Figure 3.8: Steps in the AHP model of the Forwarder Selection.

3.5 Trust Calculation

In Subsection 3.3, the components of trust have been explained. The following section will demonstrate how Direct Trust, Indirect Trust and Witness Trust are calculated. At the end, these trust values will be integrated to get the total trustworthiness of the evaluated agents.

3.5.1 Direct Trust

Direct Trust: As explained in Section 3.3.1, Direct Trust is a trust value calculated based on direct communication between the source (evaluator) and its direct (immediate) neighbours and also between direct nodes and its direct neighbours (witness nodes).

$$\begin{aligned} n_1(DT) &= (s(1) \cdot w(1) + s(2) \cdot w(2) + s(3) \cdot w(3)) \\ n_2(DT) &= (s(1) \cdot w(1) + s(2) \cdot w(2) + s(3) \cdot w(3)) \\ &\vdots \\ n_n(DT) &= (s(1) \cdot w(1) + s(2) \cdot w(2) + s(3) \cdot w(3)) \end{aligned} \tag{3.9}$$

Direct Trust calculated by the source nodes, i.e., $n_1(DT), (n_2(DT), ...(n_n(DT)$ can be represented as:

$$n_i(DT) = \sum_{i=1}^{m} s_{ij} \cdot w_{ij} \tag{3.10}$$

, where s_{ij} is an entry in the matrix of option scores, i and j = 1, 2,....m and m represents the number of evaluated criteria.

3.5.2 Indirect Trust

Indirect Trust: As explained in Section 3.3.1.1, Indirect Trust is a trust value of the evaluated node, calculated or gained from indirect neighbours of the evaluator. The indirect neighbours of the evaluator are direct neighbours of the evaluated node. Some information may not be available through direct communication. For example, the previous performance of the evaluator in any interaction in the past can be assessed through other nodes indirectly. This also applies in the case of the source node having no previous experience with the direct node. In HTM the indirect trust value is about communication behavior between nodes, i.e., whether evaluated nodes have successful or failure communication (in transmitting any data etc.). The Indirect Trust value is forwarded by the direct node to the source node for computation of total trust.

3.5.3 Witness Trust

Witness Trust: Witness Trust is trust of indirect neighbours (direct neighbours of the evaluated node) given by the evaluated node.

$$\begin{aligned} n_1(WT) &= (s(1) \cdot w(1) + s(2) \cdot w(2) + s(3) \cdot w(3)) \\ n_2(WT) &= (s(1) \cdot w(1) + s(2) \cdot w(2) + s(3) \cdot w(3)) \\ &\vdots \\ n_n(WT) &= (s(1) \cdot w(1) + s(2) \cdot w(2) + s(3) \cdot w(3)) \end{aligned} \tag{3.11}$$

Witness trust calculated by direct nodes, i.e., $n_1(WT), n_2(WT), ...n_n(WT)$ can then be represented as:

$$n_i(WT) = \sum_{i=1}^{m} s_{ij} \cdot w_{ij} \tag{3.12}$$

, where i and j = 1, 2,....m and m represents the number of evaluated criteria.

Above, we have defined the three trust values that contribute to total trust in our forwarder selection. Thus, to find the best forwarder, the source node will consider direct trust, indirect trust and witness trust in its total trust calculation. After the total scores of all alternatives have been calculated, the decision maker (source node) should choose the alternatives that have high scores.

$$TotalTrust = DT + WT + IT \tag{3.13}$$

3.6 HTM Application Scenarios

In this section we will demonstrate how provider is selected in HTM. The overall structure of HTM is shown in Figure 3.9.

The starting point for selecting the evaluation criteria is the project goal. The goal of our hierarchy is to select an optimal forwarder so that the packet can be route from the source to the sink efficiently. The optimal forwarder refers to selected nodes that have a good ranking based on their total trust value, i.e. the trustworthiness. The specified goal exists at the top of HTM hierarchy, i.e. at Level 0.

Once the goal is determined, related criteria in achieving the goal are identified. As explained in Section 3.3.2, the performance can be measured in terms of coverage, energy, reliability and reputation. These performance aspects are used as main criteria in trust evaluation in HTM and exist at Level 1 in Figure 3.9. The trust metrics for each performance exist at Level 2 in HTM hierarchy. Depending on applications, more layers may involve if there are sub-criteria of the sub-criteria need to be considered. Further explanation on trust metrics is discussed in Section 3.6.1.

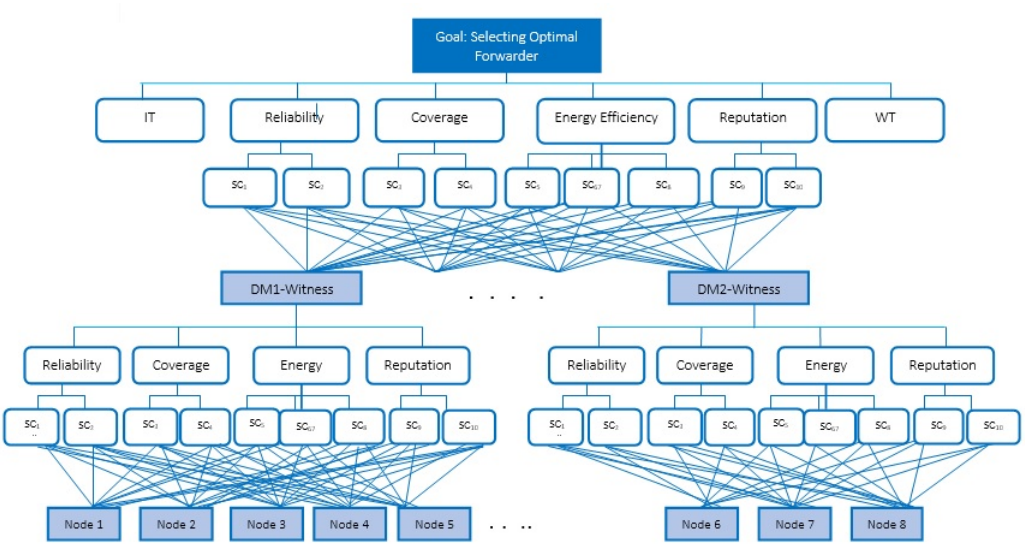

Figure 3.9: Hierarchy involving decision makers at different level of HTM. *SC* denotes the sub-criteria and *DM* denotes the decision maker.

In Figure 3.9, a scenario of one source node with two direct nodes is illustrated. Each direct node (labeled DM1-Witness and DM2-Witness) is responsible for evaluating its direct nodes (called witness). In Figure 3.9, DM1-Witness has five witness nodes labeled $Node_1$, $Node_2$, $Node_3$, $Node_4$ and $Node_5$ while DM2-Witness has three witness labeled $Node_6$, $Node_7$ and $Node_8$. These witness nodes are alternatives that will be considered by direct nodes DM1-Witness and DM2-Witness respectively. The number of alternatives varies depending on applications and environments. Alternatives lies at the bottom of the hierarchy. In this example, it exists at Layer 3 of HTM hierarchy.

3.6.1 Criteria Consideration in HTM

As mentioned previously, there are several metrics considered in the literatures depending on goals or specific application requirements. Thus, the metrics (criteria) considered in HTM, are concerned with performance measurements which are commonly used in many studies when evaluating performances. Also, based on Section 3.3.2, metrics selected in HTM are composed type of metrics as the composition of parameters constitute from a group of nodes.

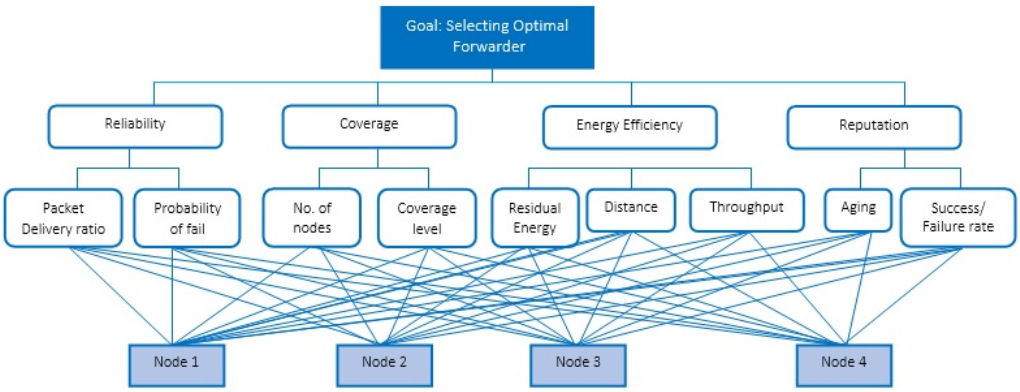

Figure 3.10: Hierarchy involving one decision maker in HTM.

Figure 3.10 illustrates an example of one decision maker (a direct node, represented as DM1-Witness in Figure 3.9). In Figure 3.10, the four main criteria are reliability, coverage, energy and reputation. There are two trust metrics under reliability: delivery packet rate and probability of failure. Under coverage, the trust metrics related to it are the number of nodes and the coverage detection level. For energy efficiency, the trust metrics that define it are remaining energy, distance between the source and the node itself and distance between the node and the sink. Throughput is also another trust metrics considered under energy efficiency. For reputation, there are two trust metrics considered: success rate and aging. There are several ways to gain these trust metric. Below are some common examples used in existing works.

- Packet Delivery Ratio (PDR): Link failures and CSMA/CA channel access mechanisms were among common causes of packet loss. PDR can be used to represent congested network. PDR can be calculated as below [Khan 2012]:

$$\text{Packet Delivery Ratio} = \frac{\text{number of received packets}}{\text{number of transmitted packets}} \times 100 \qquad (3.14)$$

- Probability of failure: The probability of not having failure within certain time interval can be captured using Poisson distribution, to model reliability $R_k(t)$ of a sensor node [Al-Obaisat 2007]. The equation that represents such probability is given as:

$$R_k(t) = e^{-\lambda_k t} \tag{3.15}$$

, where λ_k is the failure rate of sensor node k and t is the time period.

- Number of nodes: Number of nodes within the node's radius.

- Coverage Detection Level: Depending on the coverage problems, i.e. point coverage or area coverage, some studies use the density as indication of coverage problem. In the case of area coverage, an area is densely covered when a large number of nodes is deployed in that area. The more densely nodes deployed in certain area, the more overlapped and redundancy exist. Coverage importance (CovI) metric in Equation 3.16, can be used to indicate level of coverage of an area, where the smaller the CovI value, shows that the overall coverage performance of network is just slightly effected (as there are more nodes that could repair the coverage hole, if exist) [Fredrick 2015].

$$CovI(s_i) = \frac{1}{\text{number of received packets}} \tag{3.16}$$

- Remaining energy: Energy is consumes when transmits packets, receives packets and listens to the channel. In general, remaining energy can be measured as:

$$\text{Remaining energy} = \text{Initial Energy} - \text{Consumed Energy} \tag{3.17}$$

- Distance between two nodes (the source and the direct nodes or the witness node and the sink) using equation below:

$$\text{Distance } (d) = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2} \tag{3.18}$$

, where x_1 and x_2 are x-coordinates for the first and the second node, respectively while y_1 and y_2 y-coordinates for the first and the second node, respectively.

- Throughput reflects the effective network capacity. It is defined as the total number of bits which are delivered at the destination in a given period of time

successfully [Khan 2012]. The higher the throughput the better will be the protocol performance [Gupta 2010].

$$\text{Throughput} = \frac{\text{Packet Size}}{\text{Total Time to transfer/receive packets}} \tag{3.19}$$

The other criteria considered in HTM, i.e. reputation, is refers to communication behaviour or history of transmission between the evaluator and evaluated nodes in the past where it could be successful or fail transmissions.

For each of this metric, there are certain requirements needed to be fulfilled in order for the nodes to be eligible for the selection. Table 3.4 illustrates the requirements needed for each of the criteria.

3.6.2 Scenario for HTM Evaluation

Upon identifying the metrics for HTM, the preference for each criterion is set by a decision maker (i.e. source nodes and direct nodes). Preferences of the decision maker can be set based on application requirements. Below are some possible scenarios that requires different settings of preferences:

- Scenario 1: A dense network is considered. For example, if the decision maker observes that there are many available nodes to choose from (based on the number of interactions or coverage detection levels), then the density preference could be less than the energy etc.

- Scenario 2: A situation where the decision maker has no experience or past interaction with its direct nodes. In such a situation, the decision maker may need to gain information from other surrounding neighbours who have knowledge about the decision maker's performance. Thus, the preference for reputation given by a witness on evaluated nodes is high.

- Scenario 3: In some situations, for example when the decision maker need to gain information about larger part of the network, it may prefer nodes that leads to larger coverage. Thus, the coverage become the most important metrics in such situations where the preference for coverage would be set higher than other metrics.

3.6.3 Scenario 1

In Table 4.2, we illustrates the preference set for Scenario 1. The values in each cell are given based on [Saaty 1980]. Here, as the network is dense, coverage was given less preference compared to reliability, energy efficiency and reputation.

3.6.3.1 Computation of criteria weights vector w for Scenario 1

Table 3.1: Comparison matrix for Scenario 1: When the decision maker sensed dense network.

	Energy	Reputation	Reliability	Coverage
Energy	1	3	5	7
Reputation	0.33	1	5	6
Reliability	0.2	0.2	1	3
Coverage	0.143	0.167	0.33	1

Once a preference table has been generated, weights w for each criterion is calculated by dividing each value in columns with the sum of each column, then summing the values for each row. The calculated value is identified as the local weight for each criterion. The result is presented in Table 3.2:

Table 3.2: Normalized Matrix and Weight Values.

	Energy	Reputation	Reliability	Coverage	RowSum	Weight (w)
Energy	0.597	0.687	0.442	0.411	2.137	0.534
Reputation	0.199	0.229	0.441	0.353	1.222	0.305
Reliability	0.119	0.046	0.088	0.176	0.430	0.107
Coverage	0.085	0.038	0.029	0.059	0.212	0.053

Normalized matrix and weight for each sub-criteria is computed following the same processes. The local value for each criteria for Scenario 1 is computed as shown in the fourth column of Table 3.3. The global weight is gained by multiplying the local weight of each sub-criterion with the local weight for criteria. For example, to get global weight for reliability and packet delivery rate (PDR), the local weight of sub-criteria PDR (i.e.,0.833) is multiplied by the reliability criteria weight (i.e., 0.108) to get its global weight (i.e., 0.090).

Table 3.3: Local and Global Weight of Features.

Factors	Local weight (%)	Sub-criteria	Local weights (%)	Global weights (%)
Reliability	0.107	PDR	0.833	0.090
		% Not fail	0.167	0.018
Coverage	0.053	No.of nodes	0.875	0.046
		CDL	0.125	0.007
Energy Efficiency	0.534	E_{Res}	0.572	0.305
		$Dist_{W-DM}$	0.270	0.144
		$Dist_{W-Sink}$	0.106	0.057
		Throughput	0.052	0.028
Reputation	0.305	S/F Rate	0.75	0.229
		Aging	0.25	0.076

Table 3.4 is indicating the requirements needed in each sub-criteria evaluation. For example, in determining the reliability of a node, the packet delivery rate can be measured by dividing the number of received packets by the number of sent packets [Patil 2012]. Table 3.4 shows some examples on how scores for each sub-criteria is calculated.

Table 3.4, indicates the desirability of each criterion. For some criteria, a higher value is preferred while less value is more preferred for others. HB represents higher values while LB represents lower values. For example, in terms of residual energy, nodes with higher residual energy are more preferred than nodes with lower residual energy, as higher residual energy nodes may sustain longer in the network. On the other hand, in terms of distance, nodes with shorter distance are more preferred due to higher energy being consumed if selecting nodes that are further away.

Table 3.4: Requirements considered in evaluating nodes in HTM.

Criteria	Sub-Criteria	Requirements	Desirability
Reliability	% Packet Delivery Rate(PDR)	$\frac{PktReceive}{PktSent}] \times 100$	HB
	Probability of Not Fail	$R_k(t) = e^{-\lambda_k t}$	HB
Coverage	No. of Nodes	No.of Nodes	HB
	Coverage Detection Level(CDL)	$\frac{\sum_{x'=0}^{x} \sum_{y'=0}^{y} g(x', y')}{xy}$	HB
EnergyEfficiency	Residual Energy (E_{res})	(E_{res})	HB
	Distance between DM-Witness	Distance	LB
	Distance between Witness-Sink	Distance	LB
	Throughput	Throughput	HB
Reputation	Success/Failure Rate	No. Success/Failure Rate	HB/LB
	Aging	Response Time	HB

Note: HB- Higher is better, LB-Lower is better.

Table 3.5 shows the global weight for each sub-criterion previously calculated. The sub-criteria are labeled as *SC1* to SC_{10}, which represents the packet delivery rate, percentage of success, number of nodes, coverage detection level, residual energy, distance between direct nodes and its witness, distance between witness nodes and the sink, throughput, success or failure rate and aging, respectively. As represented in Figure 3.9, *DM1-Witness* has five witness nodes connected to it. Table 3.5 demonstrates the values that each witness has with regards to each sub-criterion. For example, the reliability value for witness nodes $Node_1$, $Node_2$, $Node_3$, $Node_4$ and $Node_5$ with regards to packet delivery rates are 30, 30, 70, 55, 45, respectively. These values can be gained using requirement measurements in Table 3.4 and will be used in calculating the option score in Table 3.7.

Table 3.5: Local and global weight for criteria (the trust metrics) and direct nodes $n_1(D)$'s witnesses values for each metrics.

Criteria	Sub-Criteria	Global Weights	Node 1	Node 2	Node 3	Node 4	Node 5
Reliability	SC-1	0.090	30	30	70	55	45
	SC-2	0.0179	60	75	95	60	35
Coverage	SC-3	0.046	1	3	10	5	4
	SC-4	0.007	20	45	80	50	40
Energy Efficiency	SC-5	0.263	50	30	70	70	50
	SC-6	0.144	3	4	5	4	5
	SC-7	0.057	1	4	5	6	7
	SC-8	0.028	0.2	0.1	0.5	0.6	0.5
Reputation	SC-9	0.229	30	30	70	50	40
	SC-10	0.076	5	4	1	3	3

SC is Sub-criteria for each criterion, following the sequence in Table 3.4. $Node_1$ to $Node_5$ are witness nodes for direct node $DM1-Witness$.

Table 3.6 demonstrates the values for each trust metrics of direct node *DM2-Witness* witnesses.

Table 3.6: Local and global weight for criteria (the trust metrics) and direct nodes $DM2-Witness$'s witnesses values for each metrics.

Criteria	Sub-Criteria	Global Weights	Node 6	Node 7	Node 8
Reliability	SC-1	0.090	5	7	6
	SC-2	0.018	10	95	40
Coverage	SC-3	0.046	2	10	7
	SC-4	0.007	35	80	75
Energy Efficiency	SC-5	0.263	25	80	80
	SC-6	0.144	7	2	10
	SC-7	0.057	8	3	10
	SC-8	0.028	0.1	0.8	0.8
Reputation	SC-9	0.229	10	70	80
	SC-10	0.076	5	1	2

SC is Sub-criteria for each criterion, following the sequence in Table 3.4. $Node_6$, $Node_7$ and $Node_8$ are witness nodes for direct node $DM2-Witness$.

3.6.3.2 Computing the matrix of option scores for Scenario 1

Table 3.7 shows the result of evaluation for five witness nodes $Node_1$, $Node_2$, $Node_3$, $Node_4$ and $Node_5$, evaluated by direct node $DM1-Witness$. Table 3.7 (i.e. Norm(Score)) shows the normalization values of each witness with regards to each sub-criterion and the score that the witness gain for each of the sub-criterion.

The normalization and score value will depends on desirability of each trust metrics in Table 3.4. For higher is better (HB) requirement, the nodes having the highest value will be set to 1. For the remaining nodes, the normalization value for each trust metric is gain by diving the node's value with the highest node's value for that particular trust metric. On the other hand, for trust metric that desire less is better (LB), the node having lowest value for that particular trust metric will be set to 1. The remaining nodes normalization value can then be calculated by diving the lowest value with its value. The score for each trust metric can then be derived be multiplying each normalization value with the global weight.

Table 3.7: Normalization value and score for each element, evaluated by direct node DM1-Witness on its witnesses for Scenario 1.

Criteria	Sub-Criteria	Node 1 Norm(Score)	Node 2 Norm(Score)	Node 3 Norm(Score)	Node 4 Norm(Score)	Node 5 Norm(Score)
Rel	SC-1	0.429(0.038)	0.429(0.038)	1(0.090)	0.786(0.070)	0.643(0.058)
	SC-2	0.632(0.011)	0.789(0.014)	1(0.018)	0.632(0.011)	0.368(0.007)
C	SC-3	0.1(0.005)	0.3(0.014)	1(0.046)	0.5(0.023)	0.4(0.019)
	SC-4	0.25(0.002)	0.563(0.004)	1(0.007)	0.625(0.004)	0.5(0.003)
EE	SC-5	0.714(.218)	0.429(.131)	1(0.305)	1(0.305)	0.714(0.218)
	SC-6	1(0.144))	0.75(0.108)	0.6(0.866)	0.8(0.115)	1(0.144)
	SC-7	1(0.057)	0.25(0.014)	0.2(0.011)	0.833(0.047)	1(0.714)
	SC-8	0.4(0.011)	0.2(0.006)	1(0.028)	0.833(0.023)	1(0.028)
Rep	SC-9	0.429(0.098)	0.429(0.098)	1(0.229)	0.714(0.164)	0.511(0.131)
	SC-10	0.2(0.015)	0.25(0.019)	1(0.076)	0.333(0.025)	0.333(0.025)
	TotalScore	0.600	0.446	0.897	0.789	0.673

SC is Sub-criteria for each criterion, following the sequence in Table 3.4. Rel, C, EE and Rep represent reliability, coverage, energy efficiency and reputation respectively.

Table 3.8 shows the score of direct node *DM2-Witness*'s witnesses where the normalization and score for each trust metric is calculated in a similar way as for Table 3.7.

Table 3.8: Normalization value and score for trust metrics, evaluated by direct nodes DM2-Witness for Scenario 1.

Criteria	Sub-Criteria	Node 6 Norm(Score)	Node 7 Norm(Score)	Node 8 Norm(Score)
Rel	SC-1	0.714(0.064)	1(0.090)	0.857(0.077)
	SC-2	0.105(0.002)	1(0.018)	0.421(0.008)
C	SC-3	0.2(0.009)	1(0.046)	0.7(0.032)
	SC-4	0.438(0.003)	1(0.007)	0.938(0.006)
EE	SC-5	0.313(0.082)	1(0.263)	1(0.263)
	SC-6	0.286(0.041))	1(0.144)	0.2(0.029)
	SC-7	0.375(0.021)	1(0.057)	0.3(0.017)
	SC-8	0.125(0.003)	1(0.028)	1(0.028)
Rep	SC-9	0.143(.033)	0.875(0.200)	1(0.229)
	SC-10	0.2(.015)	1(0.076)	0.5(0.038)
	TotalScore	0.274	0.929	0.727

SC is Sub-criteria (i.e. trust metrics) for each criterion, following the sequence in Table 3.4. Rel, C, EE and Rep represent reliability, coverage, energy efficiency and reputation respectively.

3.6.3.3 Ranking the options in Scenario 1

Upon completion of the computation, each decision maker will have a rank of its witness. Based on Table 3.5, the final score for witness nodes $Node_1$, $Node_2$, $Node_3$, $Node_4$ and $Node_5$ are 0.600, 0.446, 0.897, 0.789 and 0.673 respectively. The direct node *DM1-Witness* will then make a rank in decreasing order, i.e., witness nodes $Node_3$, $Node_4$, $Node_5$, $Node_1$ and $Node_2$.

The direct node *DM1-Witness* will either forward all the witnesses to the source nodes or only select one. Let say, the direct node *DM1-Witness* will only forward those with the rank above 0.6 or the top three. The value of these top three will be forwarded to the source. Thus, at the source, the alternatives from the direct node *DM1-Witness* are $Node_1$, $Node_4$ and $Node_5$ which are labeled as DM_{13}, DM_{14} and DM_{15} respectively in Table 3.9.

The source nodes will then calculate the total trust values for final selection using pairwise comparison for all main criteria. Table 3.9 is the pairwise comparison matrix for the main criteria used by source node. The pairwise comparison matrix for trust metrics is assumes to be the same as the one used by direct nodes. As seen in Table 3.9, the criteria evaluated by the source node consists of Direct Trust (on criteria reliability, coverage, energy efficiency, reputation given of each direct

node and sub-criterion (SC-1 to SC-10)), Witness Trust (of Nodes 3,4,5,7 and 8) and Indirect Trust (the reputation given by the witness about their direct node).

Table 3.9: Final Score of Source Evaluation (on its direct nodes).

Main Criteria	Criteria	Sub-Criteria	DM_{13} Score	DM_{14} Score	DM_{15} Score	DM_{27} Score	DM_{28} Score
(DT) (0.676)	Reliability (0.107)	SC-1	0.043	0.043	0.043	0.060	0.060
		SC-2	0.001	0.001	0.001	0.012	0.012
	Coverage (0.053)	SC-3	0.006	0.006	0.006	0.031	0.031
		SC-4	0.002	0.002	0.002	0.005	0.005
	Energy Efficiency (0.534)	SC-5	0.064	0.064	0.064	0.178	0.178
		SC-6	0.097	0.097	0.097	0.040	0.040
		SC-7	0.038	0.038	0.038	0.024	0.024
		SC-8	0.004	0.004	0.004	0.018	0.018
	RepDS (0.305)	SC-9	0.022	0.022	0.022	0.155	0.155
		SC-10	0.010	0.010	0.010	0.051	0.051
WT (0.238)			0.203	0.188	0.160	0.221	0.173
RepDW (0.086)			0.065	0.036	0.014	0.043	0.035
			0.022	0.005	0.005	0.0043	0.014
		TotalScore	0.578	0.517	0.385	0.843	0.798

SC is Sub-criteria for each criterion, following the sequence in Table 3.4. Rel, C, EE and Rep represent reliability, coverage, energy efficiency and reputation respectively.

The values for direct trust for DM_{13} to DM_{15} are the same, as these values are direct observations from the same source node on its direct nodes. The other two trust values WT and IT are gained from different witnesses. Thus, the values for each node differs. The value for WT for DM1 witnesses are gained by multiplying the total score of Nodes 3, 4 and 5 from Table 3.7. The value for WT for DM2 witnesses are gained by multiplying the total score of Nodes 7 and 8 from Table 3.8 respectively with local weight of WT, (i.e., 0.238) in Table 3.9. In Table 3.9, the reputation for Node 3 is the highest among all other nodes. This may represent that Node 3 has a very good reputation in delivering packets sent from direct node (the DM1).

3.6.4 Scenario 2

In this scenario, we illustrate a situation where the decision maker has no experience or past interaction with its direct nodes. In such a situation, the decision maker may need to gain information from surrounding neighbours who have knowledge about

decision maker performance. This reflects the situation of asking for reputation from previous employers before considering a candidate for a job. Thus, the preference for reputation given by witnesses on evaluated nodes is high. The preferences for Scenario 2 are shown in Table 4.3:

Table 3.10: Comparison matrix for Scenario 1: When Decision Maker (DM) sensed dense network.

	Energy	Reputation	Reliability	Coverage
Energy	1	0.33	3	5
Reputation	3	1	5	3
Reliability	0.33	0.2	1	3
Coverage	0.33	0.33	0.33	1

Following the same procedures as in Scenario 1, we then observe the results for Scenario 2. Table 3.11 shows the final score for Scenario 2.

Table 3.11: Final Score of Source Evaluation (on its direct nodes) for Scenario 2, when sensor nodes have previous communication about direct nodes, thus it relies more on witness and reputation.

Main Criteria	Criteria	Sub-Criteria	DM_{13} Score	DM_{14} Score	DM_{15} Score	DM_{27} Score	DM_{28} Score
(DT) (0.312)	Reliability (0.134)	SC-1	0.025	0.025	0.025	0.034	0.034
		SC-2	0.001	0.001	0.001	0.007	0.007
	Coverage (0.092)	SC-3	0.005	0.005	0.005	0.025	0.025
		SC-4	0.002	0.002	0.002	0.004	0.004
	Energy Efficiency (0.284)	SC-5	0.016	0.016	0.016	0.044	0.044
		SC-6	0.24	0.24	0.24	0.010	0.010
		SC-7	0.009	0.009	0.009	0.006	0.006
		SC-8	0.001	0.001	0.001	0.005	0.005
	RepDS (0.494)	SC-9	0.017	0.017	0.017	0.016	0.016
		SC-10	0.008	0.008	0.008	0.039	0.039
WT (0.198)			0.182	0.159	0.137	0.198	0.155
RepDW (0.490)			0.368	0.205	0.082	0.246	0.205
			0.123	0.031	0.027	0.025	0.082
		TotalScore	0.816	0.533	0.380	0.796	0.761

SC is Sub-criteria for each criterion, following the sequence in Table 3.4. Rel, C, EE and Rep represents reliability, coverage, energy efficiency and reputation respectively.

3.6.5 Scenario 3

Scenario 3 presents a situation when the decision maker needs to gain information on its surroundings, i.e. it needs to send information to larger areas, so it may prefer

coverage as its important metrics. Thus, the preference for coverage would be set higher than for other metrics, as in Table 4.4:

Table 3.12: Comparison matrix for Scenario 1: When Decision Maker (DM) sensed dense network.

	Energy	Reputation	Reliability	Coverage
Energy	1	5	3	0.25
Reputation	0.2	1	0.33	0.167
Reliability	0.33	3	1	0.25
Coverage	4	6	4	1

Table 3.13 below shows the final scores for Scenario 3.

Table 3.13: Final Score of Source Evaluation (on its direct nodes) for Scenario 3, when sensor nodes need to observe certain areas, i.e., the larger the area covered the better, thus coverage has the main preference in this decision.

Main Criteria	Criteria	Sub-Criteria	DM_{13} Score	DM_{14} Score	DM_{15} Score	DM_{27} Score	DM_{28} Score
(DT) (0.612)	Reliability (0.132)	SC-1	0.049	0.049	0.049	0.067	0.067
		SC-2	0.105	0.105	0.105	0.013	0.013
	Coverage (0.551)	SC-3	0.590	0.590	0.590	0.295	0.295
		SC-4	0.018	0.018	0.018	0.042	0.042
	Energy Efficiency (0.256)	SC-5	0.028	0.028	0.028	0.077	0.077
		SC-6	0.042	0.42	0.42	0.017	0.017
		SC-7	0.017	0.017	0.017	0.010	0.010
		SC-8	0.002	0.002	0.002	0.008	0.008
	RepDS (0.061)	SC-9	0.004	0.004	0.004	0.028	0.028
		SC-10	0.002	0.002	0.002	0.009	0.009
WT (0.298)			0.274	0.240	0.206	0.298	0.233
RepDW (0.091)			0.068	0.038	0.222	0.667	0.556
			0.023	0.006	0.222	0.005	0.015
		TotalScore	0.586	0.504	0.447	0.916	0.854

SC is Sub-criteria for each criterion, following the sequence in Table 3.4. Rel, C, EE and Rep represents reliability, coverage, energy efficiency and reputation, respectively.

3.7 Conclusion

The need for an efficient mechanism to improve the existing distributed routing decision making, in terms of the criteria considered and the information provider in selecting the reliable forwarder to relay the packets has motivated the development of Hierarchical Trust Model (HTM).

In this chapter, HTM is proposed for resource constrained distributed and decentralized wireless sensor networks. HTM utilises the concept of trust in achieving its aims. It defines trust as the level of believe that a node has on the other node based on four trust factors: reliability, energy efficiency, coverage and reputation. In order to determine a trusted forwarder, this chapter has answered important questions such as what, who, when and how to establish the trust among nodes in the network. HTM is a multi criteria decision making model that involves two types of decision makers at different hops (layers) of the network.

The features introduced in HTM have several benefits in handling uncertainties in open and dynamic environments. In an open and dynamic system, agents normally have a partial view of their surroundings. Relying only on direct observations may provide inaccurate information, especially when there is no previous interaction with the communicating nodes. Thus, knowledge or experience from others on evaluated nodes would help the decision maker in its decision making. In HTM these capabilities are provided by witness nodes, which is the neighbour of evaluated nodes.

Reputations are needed from the third party especially when evaluator has no prior experience or knowledge about evaluated nodes. In most existing trust models, evaluation is done only on single hop nodes. Apart from the evaluation on evaluated nodes, it is believed that it is important to evaluate the trust of the third party that evaluates evaluated nodes. In an open system involving large number of nodes, especially when more than one node needs to participate in a communication, such as routing packets through multiple hops when the source is located far away from the source, evaluating a single hop per evaluation is cost consuming. Rather, HTM provides mechanism for evaluating nodes at multiple hops, which helps in making better decisions. Knowing in advance the trustworthiness of more layers' nodes could give a larger view of the network, especially in the open networks where the global information is normally not available. In order to provide such mechanism, a new component called Witness Trust (WT) is introduced.

The benefits provide by HTM structure is in terms of less computations through local decision making. By having two types of evaluators at different layers, potential candidates are first filtered and checked for their eligibility. Only selected one will

be forwarded to a higher evaluator, i.e., the source node. Thus, the number of potential forwarders needing to be processed by source nodes is less, allowing it to select among good rank forwarders.

Another issue considered in HTM is the weight in determining the importance of factors being considered. In fact, this is mentioned as a challenge in many existing works. Most existing works used weighted sum and determine the weight in the range between 0 and 1, which may not be appropriate. In HTM, pairwise comparison in the analytic process hierarchy is utilized in determining appropriate weight to indicate preferences of factors being evaluated. Using this technique, preference is set based on a standard scale. Also, the confidence index acts as a checking mechanism to ensure that the weight assigned is within an acceptable range. The mechanism based on preferences allows the decision maker to tune its preferences to suit its needs (as illustrated by the three scenarios in Section 3.6.2). In an open system, where the nodes deployment is unknown due to the absence of a global view, nodes may need to have different preferences whenever their surroundings change or differ.

Most of existing trust models are not meant for WSNs. Thus, no comparison is made between HTM and other existing trust models. Instead, this chapter focusses on how to gain the trustworthiness by determining the types of nodes involved, the criteria that contribute to the trust values and how they are computed. The application of HTM will be implemented in Chapter 4, in deciding the suitable forwarder to route the packets in the network. The simulation conducted in Chapter 4 aims to observe the performance of HTM compared to the other existing trust-based routing protocols.

In summary, in this chapter, a novel trust based model for a distributed and decentralized network called Hierarchical Trust Model (HTM) has been proposed. The selection processes were demonstrated in detail, describing how node is selected and how the trustworthiness is computed. The proposed HTM have several features including considering multiple factors as trust metrics, evaluates nodes at multiple hops, provides local decision making and delegates the decision making loads among evaluators. In the next chapter, a trust based routing protocol, called Adaptive Trust-based Routing Protocol (ATRP) is proposed, where ATRP will embed the Hierarchical Trust Model (HTM) proposed in this chapter in selecting nodes to route

packet. The performance measures in the next chapter will indicate the effectiveness of HTM in routing application.

CHAPTER 4

Adaptive Trust-based Routing Protocol (ATRP)

4.1 Introduction

Chapter 3, introduced our proposed trust-based model called the Hierarchical Trust Model (HTM). This model aims to improve the efficiency in forwarder selection by comprehensively considering various trust factors in its decision and ensuring that the evaluation done is made by the credible nodes. Chapter 3 also explained the processes and computations of the trustworthiness in the node selection decision. Although Chapter 3 provides the decision making solutions, it did not assess the effectiveness of the proposed trust model. In this chapter, HTM is applied into the routing application in order to measure its performances. A novel distributed routing protocol for WSNs called the Adaptive Trust-based Routing Protocol (ATRP) is proposed to select the most reliable forwarder to ensure an efficient routing. ATRP exploits a distributed trust model and employs a multi-criteria selection strategy that considers the energy consumption, coverage level, reliability and reputation of neighbouring nodes in its trustworthiness value when making routing decision. As HTM implementation is inherent in ATRP, the forwarder selection relies on the belief that a node has on the other node's capabilities in forwarding the packets based on several trust values. There are several additional features introduced in ATRP. Several control mechanisms such as timeliness, and the number of interactions are embed in ATRP to improve its efficiencies. This chapter explains the features and components of ATRP and compares its performance with those of existing multi-criterion trust-based routing protocols in WSNs. The strategy proposed in ATRP ensures that the data is disseminated via trusted nodes and energy consumption among nodes in the network is balanced. As discussed in Chapter 1, data transmission/reception (when routing packets) is the most energy-demanding of the four processes in sensor device. Despite extensive efforts to improve the routing effi-

ciencies of WSNs, several remaining limitations must be overcome. This chapter is divided into several subsections. In Section 4.2, the motivations of ATRP development is highlighted. Section 4.3 explains the structure and components in ATRP. The mechanism used in determining the node's reputation in ATRP is elaborate in Section 4.4. In Section 4.6, the control mechanisms embed in ATRP is explain. Section 4.7 demonstrates the results of ATRP implementation. Finally, the conclusion of this chapter is presented in Section 4.8.

4.2 Motivation

The work in this chapter was motivated by the following objectives:

- In distributed networks, the criteria (factors) considered in the decision-making must be carefully chosen. Considering multiple criteria improves the decision making [Gowrishankar 2008]. However, most of existing trust based routing approaches only concentrate on selecting most trusted neighbours regardless the inadequate energy resources of sensor node in protocol design [Wang 2014], [Duan 2013a], and [Qu 2013]. Little work that combines energy awareness with the concept of trust exists [Ahmed 2016].

- Most studies on trust management have targeted general ad hoc networks and peer-to-peer networks with powerful hardware platforms (storage, battery and processing capability) [Chen 2012], [Gong 2010], and [Cho 2011]. The exchange of trust information between large number of nodes and on periodic basis in existing approaches involve high routing and computational overhead [Duan 2013a], [Zahariadis 2013], [Leligou 2012], and [Sun 2012]. Therefore most of the existing trust based solutions need to be adjusted to suit sensor network due to resource constraint.

- An WSN normally covers a large network area, whereas the area coverage of individual nodes is small. Accordingly, the route from the source to the sink involves multiple hops. However, most of the existing routing protocols base their routing decisions on single hop evaluation, which may not represent the larger part of the network [Zahariadis 2013].

To resolve these deficiencies, ATRP is proposed as an efficient trust-based routing protocol for selecting the relay nodes in distributed and decentralized WSNs. ATRP aims to achieve following desirable goals:

1. Multi-criteria decision making: The trust metrics are selective and depend on the network performance. By involving the uncertainty aspects such as dynamic changes in the network caused by nodes depletion in the selection decision, we can potentially improve the decision making.

2. Resource aware mechanism: The ATRP provides several resource-aware mechanisms such as energy, which might reduce the need for retransmission. The ATRP controls the number of interactions, which limits the flooding effect in the network. The decision provided by the lower-layer evaluator reduces the workload of the higher-layer evaluator, increasing its lifetime in the network. The routing decision that incorporates multiple criteria may balance the load among trusted nodes.

3. Multi-hop evaluations assist the decision making by enlarging the network view of the evaluator, i.e., by providing information about more nodes in the network.

4.3 Adaptive Trust-based Routing Protocol (ATRP)

The Adaptive Trust-based Routing Protocol (ATRP), is a new trust and resource aware routing protocol for distributed and decentralized WSNs that integrates several network performances criteria with the concept of trust to provide efficient delivery of data and prolonged the network lifetime through an effective selection of forwarder.

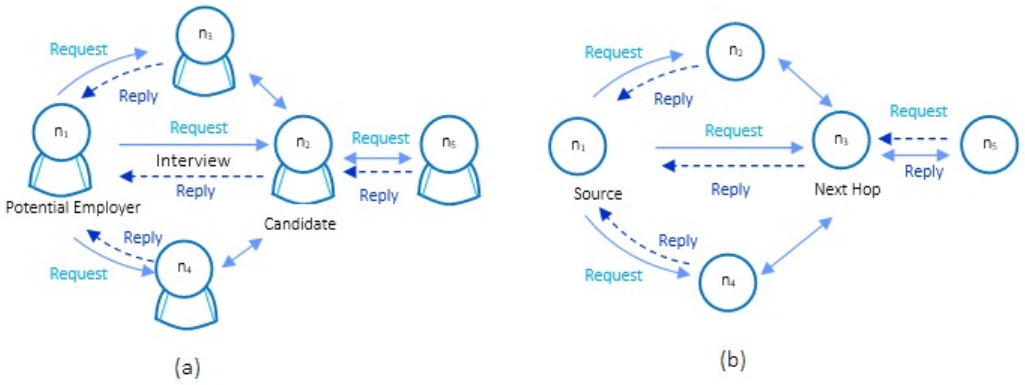

Figure 4.1: Similarities of a job application process and a wireless sensor network retrieving information from a third party.

Figure 4.1 compares a job application process (panel (a)) with a common scenario in the next-hop-node selection problem in WSNs (panel (b)). Both examples demonstrate how an evaluator seeks information from a third party when prior knowledge of the evaluated candidate is lacking. When a candidate applies for a job, the recruiter relies on information that is directly gathered through conversation during the interview, and on the information (experience, skills, interests, and educational background) contained in the candidateâs profile or resume. Indirect information can also be gained from the candidateâs previous employer or referees listed in the resume. The more information gathered about the candidate (through direct observation and third-party knowledge), the better the selection decision of the recruiter, despite the inherent risks (such as bias information) in the decision making.

(Figure 4.1b), demonstrates a similar situation that may exist in WSNs due to limited resources that nodes have in getting information about the whole network. The nodes in WSN rely on incomplete information provided by neighbouring nodes. Thus, information provided by surrounding neighbours play and important role. Like the applying for a job situation above, nodes in WSN too are facing with certain level of risks.

In many existing proposals, a node only elect the next-hop neighboring node to relay the data packet (by only considers the trustworthiness of its single-hop neighbors). This approach minimises the amount of information required for decision-

making by each node. The delivery to the sink is fully delegated to the next hop-node once the data packet is forwarded to the selected node, and the routing decision of the next-hop node is unknown to the source node.

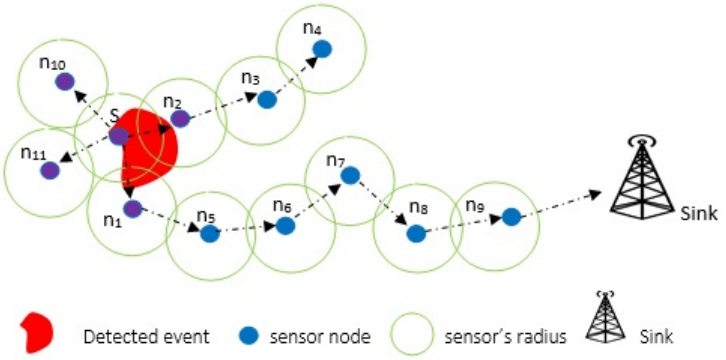

Figure 4.2: Possible scenarios of 1-hop nodes.

In the absence of global information and the dynamically changing behavior of the nodes, reliable node selection becomes nontrivial. For example, if the packets were sent to incapable nodes, re-transmissions may be required or the packets may be dropped. In Figure 4.2, an event is detected by the source node S. Node S can relay the node to any of the four nodes within its communication range, i.e., n_1, n_2, n_{10} or n_{11}. S will likely choose n_2 which has the highest capability among the nodes. Lacking information about further nodes, S must rely on its direct observations. The selection may not be suboptimal as the neighbour of n_2's (n_3, whose status is unknown to S) is connected to a neighbour (n_4) with no connection to the sink. Therefore, a packet sent via n_2 will never reach the sink. S is unlikely to choose n_1 although the neighbours of n_1 are connected to the sink. If S chooses either of n_{10} or n_{11}, a similar situation arises; the route leads to a dead end. Therefore, S can make a poor decision after evaluating 1-hop nodes only. On the other hand, when provided with information on more distant nodes, S may be able to make better decisions.

4.3.1 Definitions

Before explaining further, it is necessary to understand several important and related terms in ATRP. The network in ATRP is considered as a complex system consisting

of a number of sensor nodes (or agents).

Definition 1: The network: A WSN is defines as connected undirected weighted graph $G = (V, E)$, where V is group in the network comprises of agents, i.e. $V = a_0, a_1, a_2, ...a_n$ and $E = e_1, e_2, ...e_m$ is a set of edge in group. The edge, $e_k = (a_i, a_j)$ denotes the communication links between sensor a_i and sensor a_j (they are in each other's radio transmission range) [Khalid 2017].

Figure4.3 demonstrates types of nodes exist in the network. The source node S represents a node that sensed an event. The red circle expresses the sensing radius of source node S and denoted as r_s. The nodes that lie within r_s are called direct nodes and the nodes that lie within direct node's sensing radius, denoted as r_d are witness nodes for each direct node.

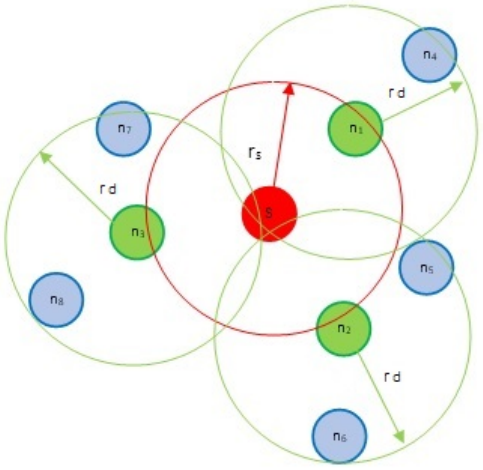

Figure 4.3: Types of nodes in network model: Source node S, direct nodes n_1, n_2 and n_3, witness node for direct node n_1, i.e. n_4, witness nodes for direct node n_2, which is n_5 and n_6 and witness nodes for direct node n_3, i.e. n_7 and n_8 respectively.

If the Euclidean distance between sensor node S and any sensor node n_i is not greater than r_s, then n_i is called direct node of sensor node S. If the Euclidean distance between direct node n_i and n_j is not greater than node n_i sensing radius r_s, then n_j is the witness node of direct node n_i.

Definition 2: Malicious node is defined based on packet forwarding ratio between node i (as sender) and node j (as receiver), i.e. $|\Sigma Fwd_{correctij}|$ / $|\sum Rcv_{packetij}|$, where $\Sigma Fwd_{correctij}$ is total number of correctly forwarded packet by node i and $\sum Rcv_{packetij}$ is total number of receive packets by j from i. A node is identified as malicious node if the value of packet forwarding ratio is less than the $Th_{FwdRatio}$,

where $Th_{FwdRatio}$ is threshold value of packet forwarding ratio.

Definition 3: Trust metrics: There are various criteria considered in ATRP. The criteria are classified as main criteria (MC) and sub-criteria (SC). The criteria are structured in hierarchical level (HL), where, in $HL_i \subset (MC_1, MC_2, ...MC_n)$ and each MC may consist SC, such that $MC_i \subset (SC_1, SC_2, ...SC_n)$. Each SC is associates or link with n alternatives. Thus, a hierarchy can be redefined as $HL_i \in (MC_1 \subset (SC_1, SC_2, ...SC_n), MC_2 \subset (SC_1, SC_2, ...SC_n), ..MC_n \subset (SC_1, SC_2, ...SC_n))$.

In ATRP, an assumption is made such as a node have a high degree of trust of it's peers. Peers in ATRP refers to a node's neighbours that are within the node's radius.

When S has data to send, it will send a request ReqD for relay service. The request will consists of several attributes or criteria together with its preferences, determined by the source node. The preference will depend on the type of data it senses. Thus, Request (ReqD) is defined as a 3 tuple: ReqD = <SID, ServType, ServDes>, where SID is the source ID and ServDes is details of the requested service. For each service type, ServType, a set of ServDes will be available. A service is represented by ServDes and is defined as 2-tuple: SerDes=<ServAttributes, SerfPerf>

However, as preferences on the attributes of the same service could be different for different requests, a preferences and attributes relationship can be represented by n attributes and their corresponding preferences, respectively such as:

ServDes = $$\begin{pmatrix} C_1 & C_2 & . & . & . & C_3 \\ w_1 & w_2 & . & . & . & w_3 \end{pmatrix}$$

, where C_1, C_2, C_3..., C_n are the attributes and w_1, w_2, w_3, ..., w_n are preferences for each attribute.

ATRP assumes that all nodes in the network use the same service description format. For example, upon receiving request ReqD from the source node, a direct nodes will check itself and provide information about itself together with it's witness information, through the reply, RlyD message. To gather information on the witness, direct node sends a request, Req_W to its direct neighbours as 4-tuple: Req_W=<DID, ServType, ServAttributes, Rep_D>, where DID is direct nodes' ID, ServType and ServAttributes as defined previously and Rep_D is the reputation of the direct node.

The reputation of the direct node is communication in the past between the witness and the direct node.

Prior to sending a reply to the source, the direct node will gather information from the witness. Witness information (WI) consists of 4-tuple defined as: WI=<WID, ServAttributes, ServType,Rep_D>, where WID, is witness ID, while ServAttributes, ServType and Rep_D is as defined previously.

Once a direct nodes receives a message from the witness, the direct node will compute witness trust (WT), using Equation 3.11 and send a reply message to the source node. Direct nodes will only forward witness that is in top rank. Finally, reply from the direct nodes is defined as 3-tuple, i.e.: RlyD=<DID, $ServAttributes_D$, WTSet>, where DID is direct nodes' ID, $ServAttributes_D$ is information (attributes of direct nodes) and WTSet is the set of witness trust computed by the direct trust.

When the source node receives RlyD from the direct nodes, it will compute total trust using Equation 3.13 and rank direct trust (with its witness). Selected direct nodes and their witnesses will be acknowledge and data will be sent through them.

Table 4.1 summarizes the message types used in ATRP. These messages are used in communication and information exchanges between nodes.

Table 4.1: Description of control messages.

Message	Description
ReqD	Tuple(SID, ServType, ServDes) (Source node request message from direct node)
ReqW	Tuple(DID, ServType, ServAttributes, Rep_D) (Direct node request message from witness)
RlyD	Tuple(DID, $ServAttributes_D$, WTSet) (Direct node reply to source)
RlyW	Tuple(WID, ServAttributes, ServType, Rep_D) (Witness reply to direct node)
DATA	Tuple(SID,DID,SinkLocation) (Data send from source to selected forwarder)

4.3.2 Structure of the Adaptive Trust-based Routing Protocol (ATRP)

ATRP discovers the neighbouring nodes during data transmissions, evaluates the trust of the transmission based on the monitored and gathered values, and disseminates the value and recommendation of the trust. In ATRP, these tasks are implemented by three units: the discovery, evaluation and dissemination units, as

shown in Figure 4.4. An additional control unit supports the implementation of ATRP in the WSN environment. These components are discussed in Subsections 4.3.2.1 to 4.3.2.3.

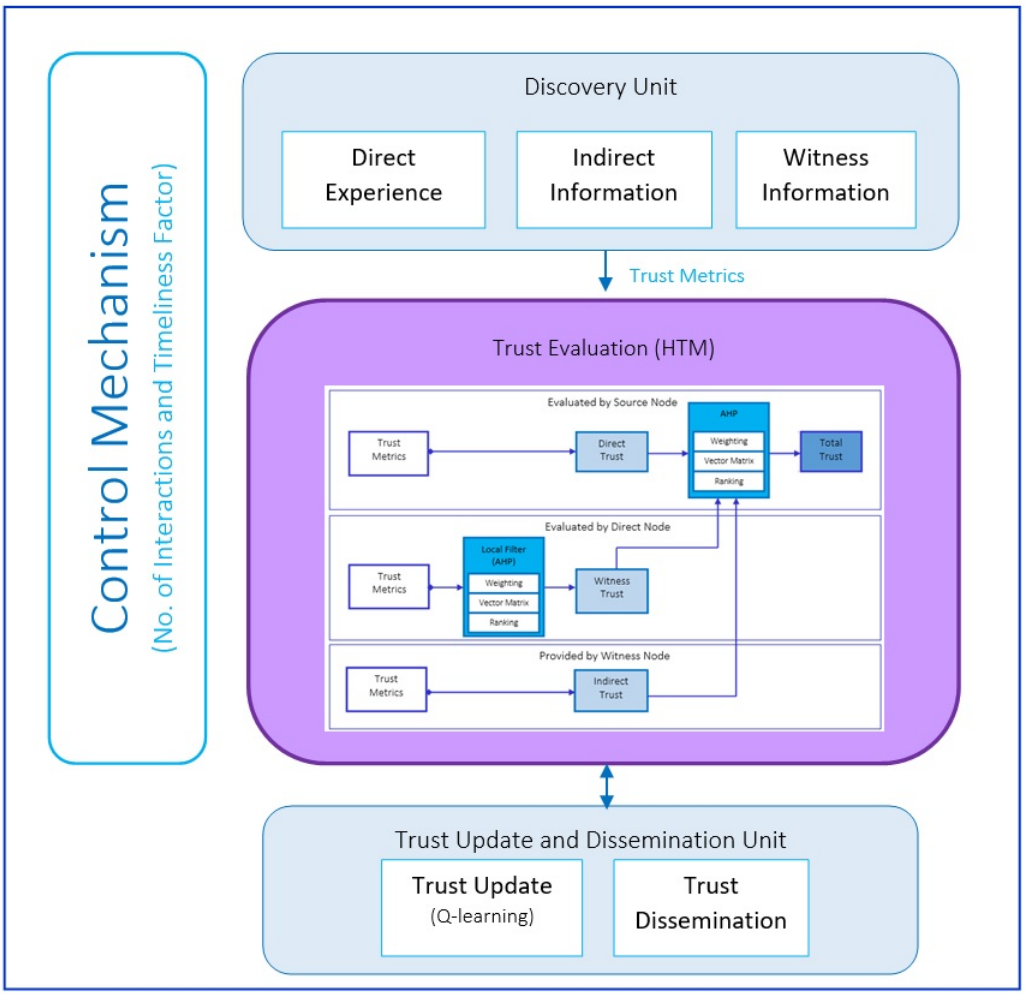

Figure 4.4: ATRP components and their relationships.

4.3.2.1 Discovery Unit

In the discovery unit, the nodes learn their neighbour's behaviours through direct observations and through recommendations by the third parties. The requesting nodes (evaluators) gather the information from their neighbours that is necessary for the selection decision. During monitoring, the related nodes may discover certain behaviours of its neighbours. The route discovery process of ATRP is shown in Figure 4.5.

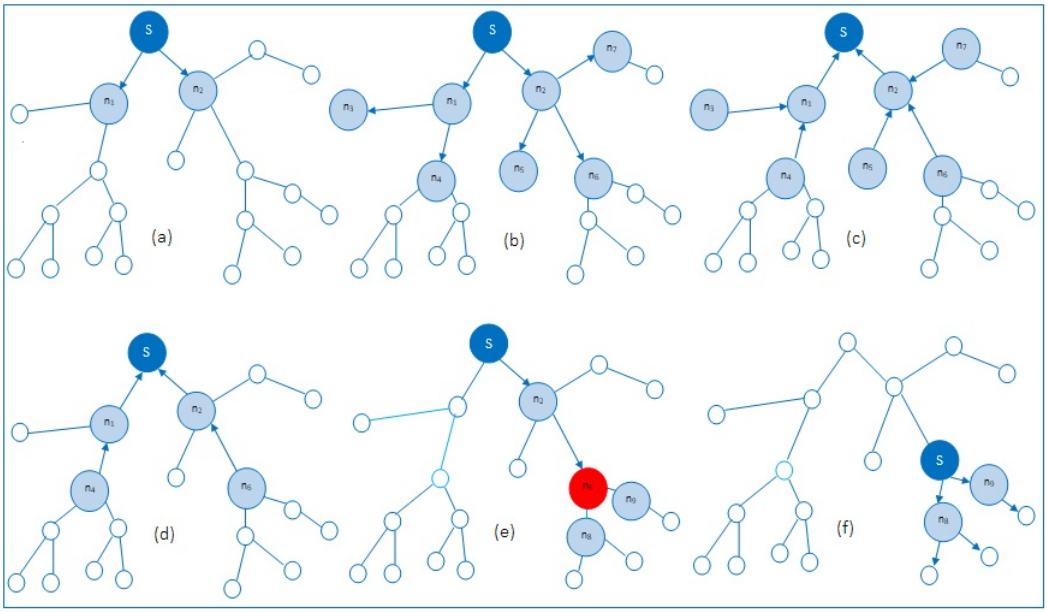

Figure 4.5: Construction of a hierarchy in ATRP.

Route discovery in ATRP proceeds by the following steps:

Step 1: The source node S will check for the route entry to the sink node D in its local routing table. A trust table may exist if the node has past experience as a decision maker (either as a source node or a direct node). If an entry for a route to D is found, the source node checks the current validity of the information in the trust table. In ATRP, information validity (recency) is tracked by an ageing mechanism, which applies only the recent information in the selection decision. Exponential distribution as in Equation 4.9 is used to reflect this. Thus, if valid information resides in the existing trust table, the source node S will pass the packet through that entry.

Conversely, if the entry for route D does not exist in the existing table, S will broadcast request packets (ReqD) to its direct nodes n_1 and n_2, initiating the node selection process (see Figure 4.5a).

In both cases, after sending the packet to the selected nodes, the source node updates its trust table for any successful or failed transmissions using Equation 4.1.

Step 2: When direct nodes n_1 and n_2 receive the ReqD, they check their capability (energy remaining for packet transmission and reception) to participate in the packet forwarding.

Suppose that nodes n_1 and n_2 in Figure 4.5b have sufficient capability to participate in the packet forwarding. Both nodes then check their route table for an

entry route to node D. If a valid route to D exists, the nodes will forward the packets through the existing routes. Otherwise, n_1 and n_2 will broadcast a request (ReqW) to their witness nodes, as shown in Figure 4.5, and wait for a reply from the witnesses (RlyW).

Step 3: The witness nodes send their replies to n_1 and n_2 (straight arrows pointing to n_1 and n_2 in Figure 4.5c). Node n_1 receives responses from two of its witness nodes (n_3 and n_4) and direct node n_2 receives responses from three of its witness nodes (n_5, n_6 and n_7).

Step 4: Upon receiving a RlyW from their witnesses, nodes n_1 and n_2 will compute and rank their witnesses accordingly. The ranking is based on the witness trust values. In the illustrated example, only one witness (n_4) is finally selected by n_1 (straight arrow from n_4 to n_1 in Figure 4.5d), and another witness (n_6) is selected by n_2. Nodes n_1 and n_2 will then forward their selected witnesses to the source node through RlyD packets, which additionally contain the information of the direct nodes' reputation. These values will be used by the source nodes in evaluating the total trust.

Step 5: Upon evaluation, the packet in this example is finally relayed to the destination node through nodes n_2 and n_6 (Figure 4.5e).

Step 6: A DATA message is routed through n_2 and n_6. The selected witness becomes the new source and begins discovering the route to D. Steps 1 to 5 are repeated until node D is reached (Figure 4.5f).

The process flows of the source, direct and witness nodes are shown in Figures 4.7 to 4.6, respectively. The ATRP algorithm of forwarder selection is demonstrated in Algorithm 4.1.

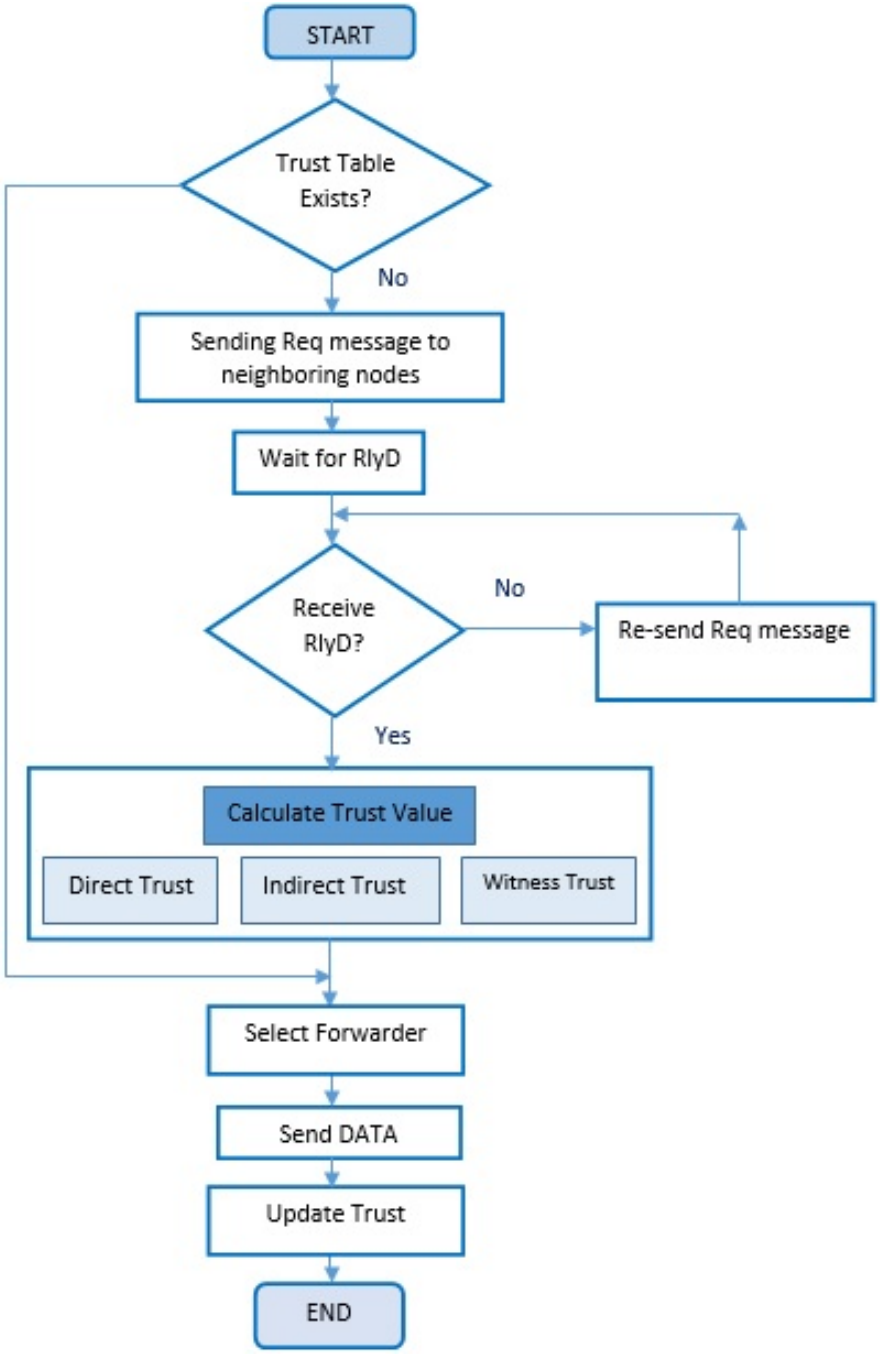

Figure 4.6: The process flow of source node in ATRP.

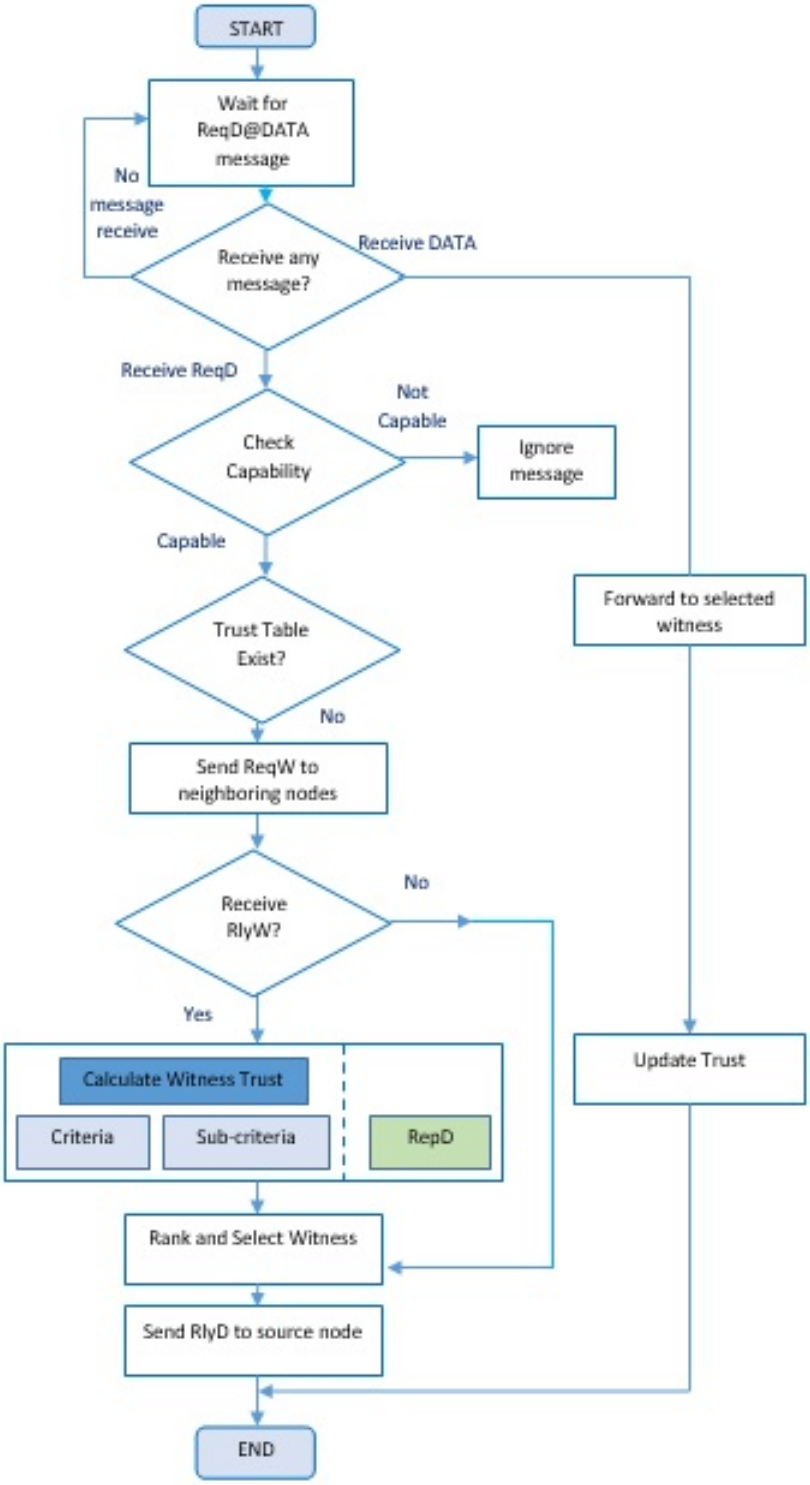

Figure 4.7: Process flow of a direct node in ATRP.

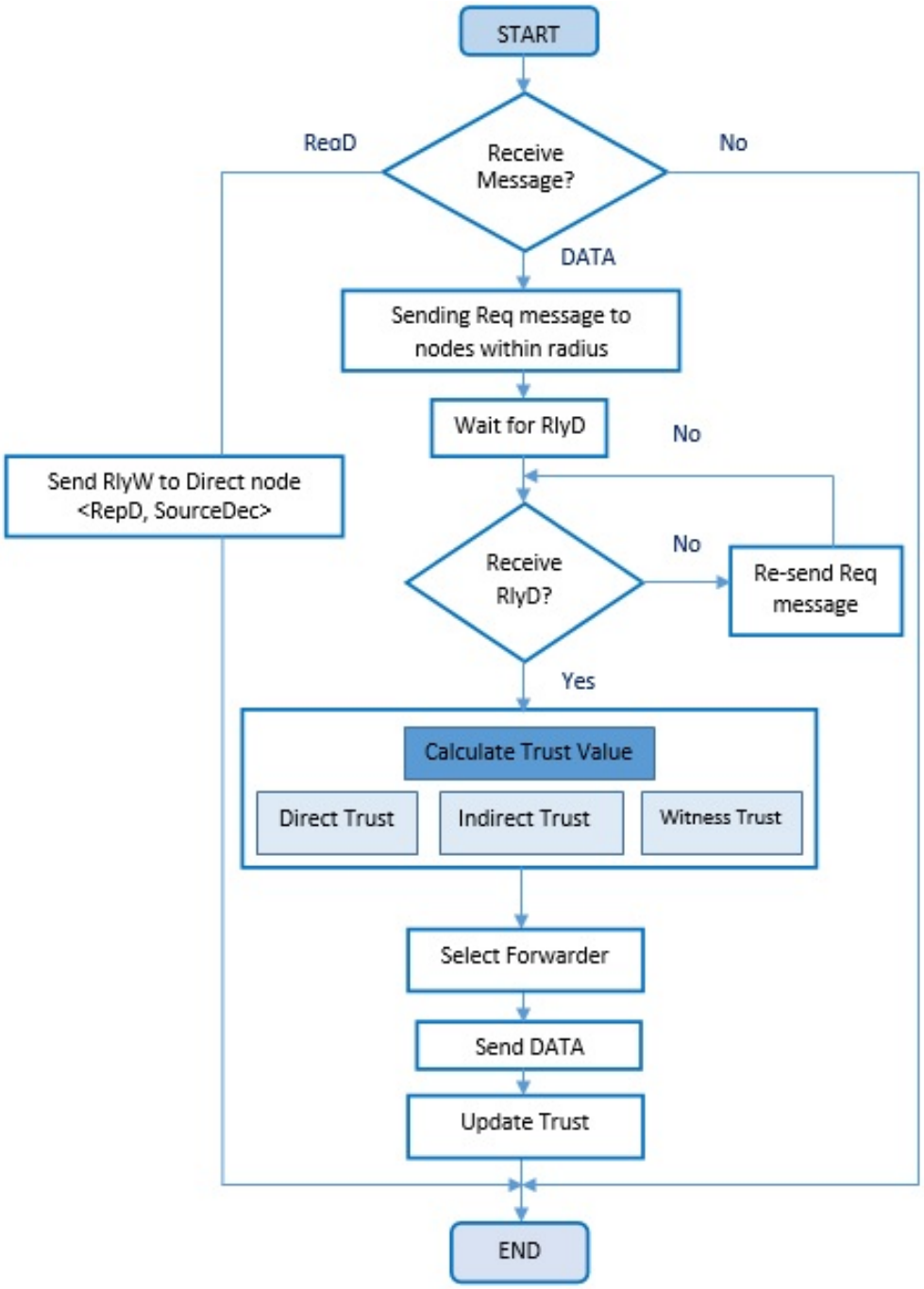

Figure 4.8: The process flow of witness node in ATRP.

Algorithm 4.1 The Forwarder Algorithm.

Input: Selection Metrics
Output: Ranked and Select Forwarder
for *For all episodes* **do**
  Source send ReqD to nodes in Radius ≤ RadiusSource
  Nodes at Radius ≤ RadiusSource , i.e., Direct Node check its Capability
  if *Capability* > *CapabilityThreshold* **then**
    Send ReqW to nodes in Radius ≤ RadiusDirectNode
    Wait for reply from N_{min} number of witness, i.e., RlyW
  end
  for *Received RlyW from witness* **do**
    Direct node compute witness trust (WT) for N_{min} nodes
    Sent RlyD < WT_i, Rep_{D-i}, $Direct_{Metric}$ > to Source
  end
  for *Receive RlyD from Direct node* **do**
    Source compute Trustworthiness
    Rank Forwarder in Decreasing order
    Send DATA to selected Direct nodes and its witness
  end
end

4.3.2.2 Trust Evaluation Unit

The second component of ATRP is the Trust Evaluation unit (Figure 4.4), which evaluates and integrates the trust levels and reputation values of the nodes. As previously mentioned, the output of the lower-layer evaluator in ATRP is input to the higher-layer evaluator, which makes the final selection decision.

To evaluate the trust and reputation, the Trust Evaluation unit embeds a hierarchical trust model (HTM) (refer Figure 3.2 for detail view of evaluation unit). As HTM was proposed and discussed in Chapter 3, this subsection will only explains the evaluation process in brief (see Figure 4.9 below):

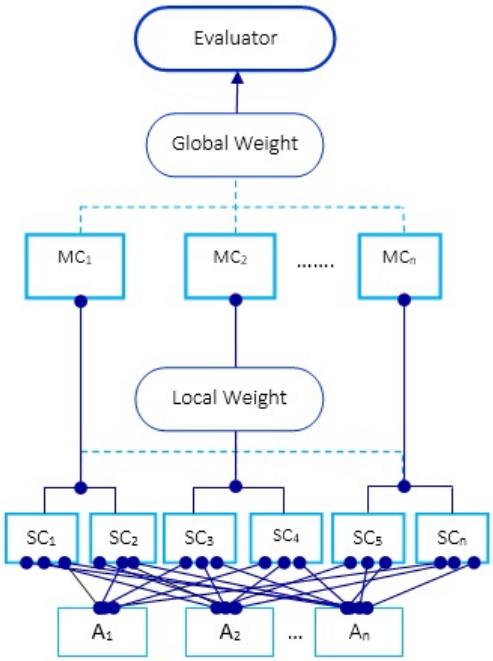

Figure 4.9: Trust evaluation demonstration on n alternatives involving various main criteria (MC_1 to MC_n) and sub-criteria (SC_1 to SC_n).

Figure 4.9 displays the hierarchies in ATRP. Each layer consists of several main criteria (MCs) and sub-criteria (SCs). Based on these criteria, n alternatives will be evaluated by pairwise comparison. In ATRP, the local weight generated for each sub-criterion is multiplied by the global weight assigned to the common main criterion. The alternative with the highest value is then selected as the next-hop node.

4.3.2.3 Trust Update and Dissemination Unit

The third component of ATRP is the Trust Update and Dissemination unit. Trust values are stored at each evaluating node's. As mentioned in Section 4.3.2.1, whenever an evaluator receives a packet to be transferred, it will either transfer the packet based on the route in its trust table (if it exists), or create a new trust table. When the trust table exists, the Trust Update and Dissemination unit is responsible for the packet transfer. The dynamic behavior is monitored by each nodes. The trust value is not periodically updated, but only when there is a change. Expired trust values are removed, and the up-to-date information (including node depletions and failed links) is sent either by the direct or indirect nodes whenever required by the source nodes. The trust value in ATRP is updated by the Q-learning technique,

explained in the next section.

4.4 Q-Learning implementation in gaining reputation

This section explains the mechanism used in gaining the nodes' reputation values. The nodes in a distributed network cannot monitor the current conditions or changes in the wider network. Node in this situation learn about its network based on the states and actions it takes previously. The ATRP adopts the Q-learning technique to capture the behaviour between two nodes in previous transmission. The level of believe that a node has on the other node is depends on the success or failure communication between them previously. The agent in Q-learning learns an action-utility function *Q(s, a)* that tells the value of performing action a in state s and the currently observed transition (s, a, s') is assumed as the only possible outcome. The Q-learning is implemented by Equations 4.1 to 4.2

$$Q*(s_t, a_t) = r_t + \gamma \sum_{s_{t+1} \in S} (P^{a_t}_{s_t s_{t+1}} max_a Q*(s_{t+1}, a)) \tag{4.1}$$

$$V*(s) = max_a Q*(s_{t+1}, a) \tag{4.2}$$

Thus, at each time step t, an action a is selected for the current state s, and the successor state (s') is observed.

Algorithm 4.2 The Q-learning Algorithm [Alpaydin 2014]

Input: Initialise all *Q(s, a)* arbitrarily
for *For all episodes* **do**
  Initalise S
  Choose a using policy derived from Q.
  State s' is observed for taken action, a,
  Update *Q(s, a)* using Equation 4.1.
  Until S is terminal state
end

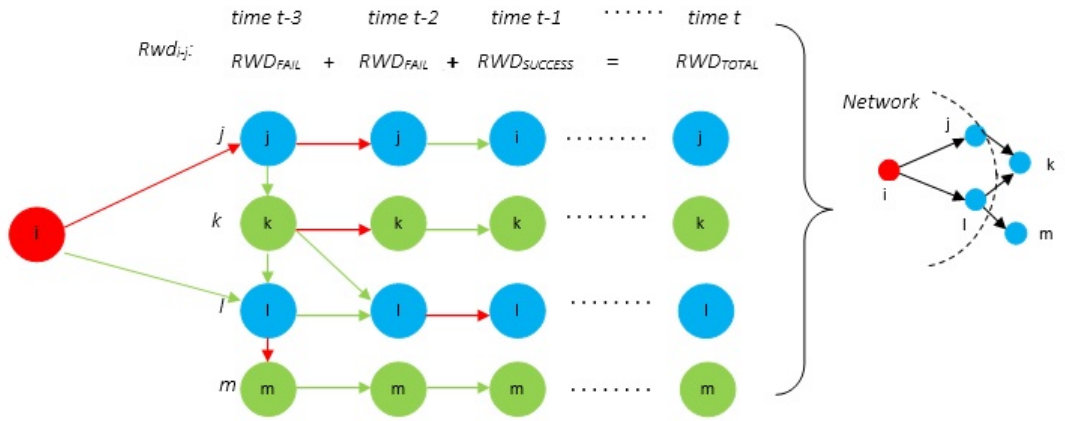

Figure 4.10: Direct and indirect relations among the reputation calculation of node i on its neighbors.

In ATRP, the Q-values is contributed by both successful and failed transmissions. As in [Hu 2010], the ATRP uses two functions: $Reward_j^i$ calculated by Equation 4.3 and $Penalty_j^i$ calculated by Equation 4.5. The agent will be rewarded if the packet-forwarding attempts from a_i to a_j is successful. Equation 4.3 denotes the reward function.

$$Reward_j^i = -g - \alpha(c(a_i) + c(a_j)) \tag{4.3}$$

In Equation 4.3, a constant cost, g of packet-forwarding by node a_i given a weight of 1 to reflect its high importance, and the weight α of the cost functions $c(a_i)$ and $c(a_j)$, denoting the residual energy costs of a_i and a_j respectively, is less than 1. The cost functions are calculated as:

$$c(a_i) = 1 - ERes_i/EInit_i \tag{4.4}$$

, where $ERes_i$ and $EIniti$ are the residual and initial energies of a_i, respectively. Conversely, the forwarding agent is penalized if the forwarding attempt from a_i to a_j fails. The $(Penalty_j^i)$ is defines using Equation 4.5

$$Penalty_j^i = -g - \beta c(a_i) \tag{4.5}$$

, where β is the (tunable) weight of the cost function. β can be set to less than 1.

The accumulated failures and successes of node i forwarding to node j is expresses as r^i_{tj}. From Equations 4.3 and 4.5, the total reward given by i to j is calculated as

$$r^i_{tj} = Reward^i_j + Penalty^i_j \tag{4.6}$$

4.5 Successful and Failed Transmission Detection

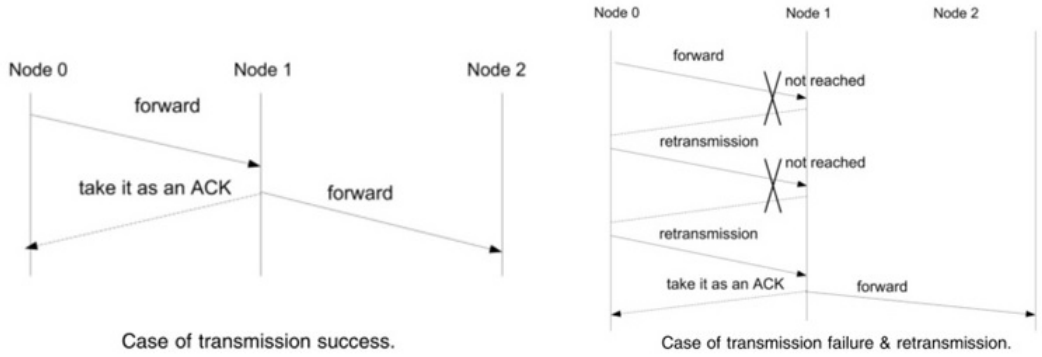

Figure 4.11: Case of successful (left) and failed (right) data transmissions [Hu 2010].

Packet delivery may be interrupted by noise in the channel, collisions or topological changes. Whether a packet has been successfully delivered to other nodes is assessed from the outgoing traffic of the receiver node. For this purpose, the receiving node stores the sent packet in memory for a certain time rather than removing it immediately from the buffer. The successfully received packet will be forwarded further by the next forwarder along the series of hops. Upon hearing the returning packet, the previous forwarder will take it as an acknowledgment, as shown in Figure 4.11. When a packet is successfully delivered to *Node 1* from *Node 0*, Node 0 will releases the memory of the packet upon hearing the ACK signal. Instead, a retransmission is triggered when the packet in the sender's memory is not be acknowledged after some time (if the transmission fails). As shown in Figure 4.11, this process is repeated up to the allowed number of re-transmissions, which is decided in advance (this mechanism was also used in [Hu 2010]).

4.6 Control Mechanism Unit

The Control Mechanism unit in the ATRP ensures the validity and reliability of the trust value. The control mechanism unit consists of three components: number of

interactions, decay time factor, and timeliness measurement.

4.6.1 Number of Interactions

The number of interactions between node pairs in a randomly deployed network cannot be determined. Due to the non-uniform deployment, more nodes may be connected to the evaluator (the source node or a direct node) in dense areas than in sparse areas. [Yu 2013] assumed that every trustee agent starts with no prior interaction experience with another trustee agent. The direct trust evidence gradually accumulates over time and the interactions are weighted by the level of confidence γ. The value of γ increases with the number of interactions with a trustee according to Equation 4.7:

$$\gamma = \begin{cases} \frac{N_C^B}{N_{min}}, & \text{if } N_C^B < N_{min} \\ 1, & \text{otherwise} \end{cases} \tag{4.7}$$

where N_C^B is the total number of direct observations of C's behaviour by a truster agent B, and N_{min} is the minimum number of direct observations to achieve a predetermined acceptable error rate ε and confidence level ϑ. N_{min} can be calculated by the Chernoff bound theorem, expressed as

$$N_{min} = -\frac{1}{2\varepsilon^2} ln \frac{1-\vartheta}{2} \tag{4.8}$$

Here, ε refers to the deviation of the estimator from the actual parameter, which can be assumed fixed, and ϑ is the confidence level. The number of interactions influence the trustworthiness of the nodes. Trust may not be established if the number of interactions is insufficient. On the other hand, if the number of interactions in dense areas is too high, excessive energy and resources will be consumed. In ATRP, the Chernoff bound theorem monitors the number of interactions between nodes by thresholding the number of interactions, thus balancing the consequences of the number of interactions in the network.

4.6.2 Decay Time Factor

The Control Mechanism unit of ATRP also determines the recency of the trust information. The historical trust values of a node indicate the current trustworthiness

of the node. The dynamic behaviors of the WSNs, such as node departures and additions resulting from battery depletions and other factors, are required for updating the trust values of the sensor nodes. However, the update frequency of the trust value should be controlled, as excessive updates can waste much energy. In contrast, an excessively long update cycle cannot efficiently reflect the current behaviors of the node.

As the trust value decreases over time, its relevance must be tracked by an appropriate mechanism. ATRP updates the trust value by an exponential decay time factor (γ) in Equation 4.9. The same mechanism was also adopted in [Duan 2013b].

$$\gamma = e^{\rho \times (t_c - t_{c-1})} \tag{4.9}$$

, where t_c and t_{c1} represent the current time and the time of the last interaction, respectively.

4.6.3 Measuring Timeliness

Timeliness is an important factor in applications involving resource-constrained nodes. The timeliness factors embedded in the Control Mechanism unit of the ATRP check whether the received packet is still meaningful. An interaction may be considered as a failure if no result is received after a predetermined deadline. The interactions' deadline performances can be tracked by a timeliness discount factor function in Equation 4.10:

$$f_{td}(T_{end}) = 1 - \frac{T_{end} - T_{start}}{T_{dl} - T_{start}} \tag{4.10}$$

, where T_{end} is the actual time at which the truster agent receives the interaction result. As T_{end} approaches the time of starting the interaction (T_{start}), the timeliness discount factor $f_{td}(T_{end})$ approaches 1. Conversely, as T_{end} tends to T_{dl}, the function $f_{td}(T_{end})$ approaches 0 [Yu 2013].

4.7 Simulation Results and Analysis

This section analyses the performance of the ATRP in a simulation conducted on the MATLAB software platform. One-hundred nodes were deployed over an area of

(1200 × 800) m^2. The initial energy and communication range of each node were set to 50 Joules and 30 m, respectively. The aims of the simulation were fourfold:
1) To observe the implementation of the simple weight assignment and weighting by pairwise calculation in AHP.
2) To observe the network performances under the control mechanisms.
3) To observe the ATRP performance in the presence of malicious nodes.
4) To compare the ATRP performance with those of other existing multi-criteria and single-hop node evaluation routing protocols (TERP and DTLSR).

4.7.1 Weight assignment using pairwise and simple weights

Most of the existing routing protocols in WSNs involving multi criterion decisions are based on simple weight assignment, where the weights of the individual criteria sum up or equivalent to 1. Instead, the ATRP weights the criteria by pairwise comparison. Section 4.7.1.1 compares the trust values generated by WSNs using these two weight mechanisms in three different scenarios (see Chapter 4).

4.7.1.1 Scenario 1

Scenario 1 is implemented on a dense network. For example, if the decision maker could choose from many available nodes (i.e. many interactions or coverage detection levels), the energy conservation preference could outweigh the density preference. In such a situation, the distance criterion is preferred over the capability criterion. Figure 4.12 plots the average indirect and witness trust values calculated by the source nodes in the network using pairwise comparison and the weighted sum in Scenario 1.

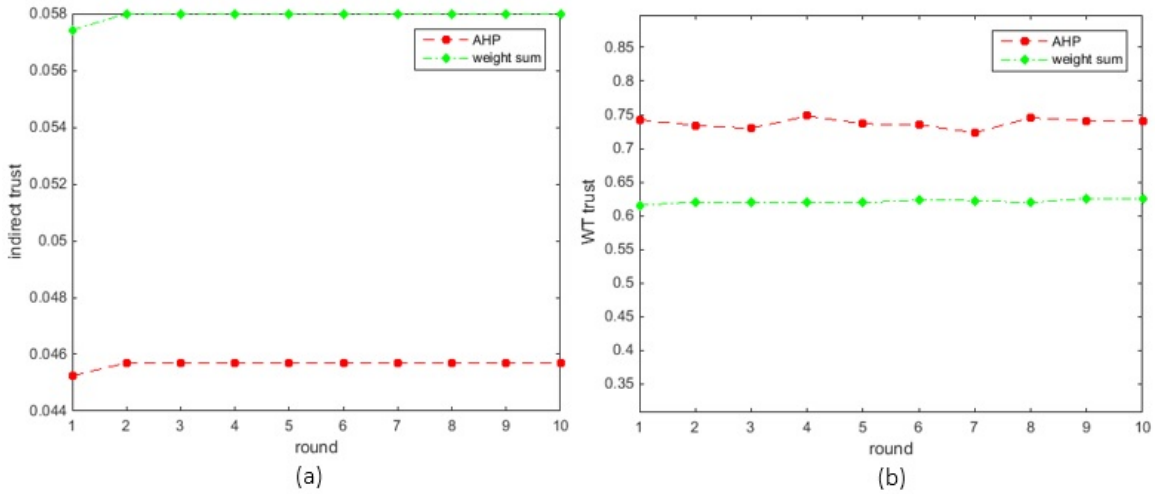

Figure 4.12: Trust values in WSNs based on weighting through AHP pairwise comparisons (red) and predetermined weights (green) in Scenario 1. Left: indirect trust; right: witness trust.

Figure 4.13 shows the trust values of the four main criteria used by the source nodes when assessing the trust values of direct nodes, and hence selecting the ATRP forwarder, in Scenario 1. The preference order of the criteria is Energy Efficiency (most important) > Reputation > Reliability > Coverage (least important). The preferences in this scenario are listed in Table 4.2 (also shown in Chapter 3). In terms of energy efficiency, the pairwise comparison and weighted sum methods improved the trust value by 0.32 and around 0.2, respectively. The gain in the reputation trust value was 0.13 in pairwise comparison and 0.132 in weighted sum. Meanwhile, the reliability and coverage trust values were improved by 0.034 and 0.03 respectively using pairwise comparison, and by 0.046 and 0.051 respectively using weighted sum.

Table 4.2: Comparison matrix for Scenario 1: When the decision maker sensed dense network.

	Energy	Reputation	Reliability	Coverage
Energy	1	3	5	7
Reputation	0.33	1	5	6
Reliability	0.2	0.2	1	3
Coverage	0.143	0.167	0.33	1

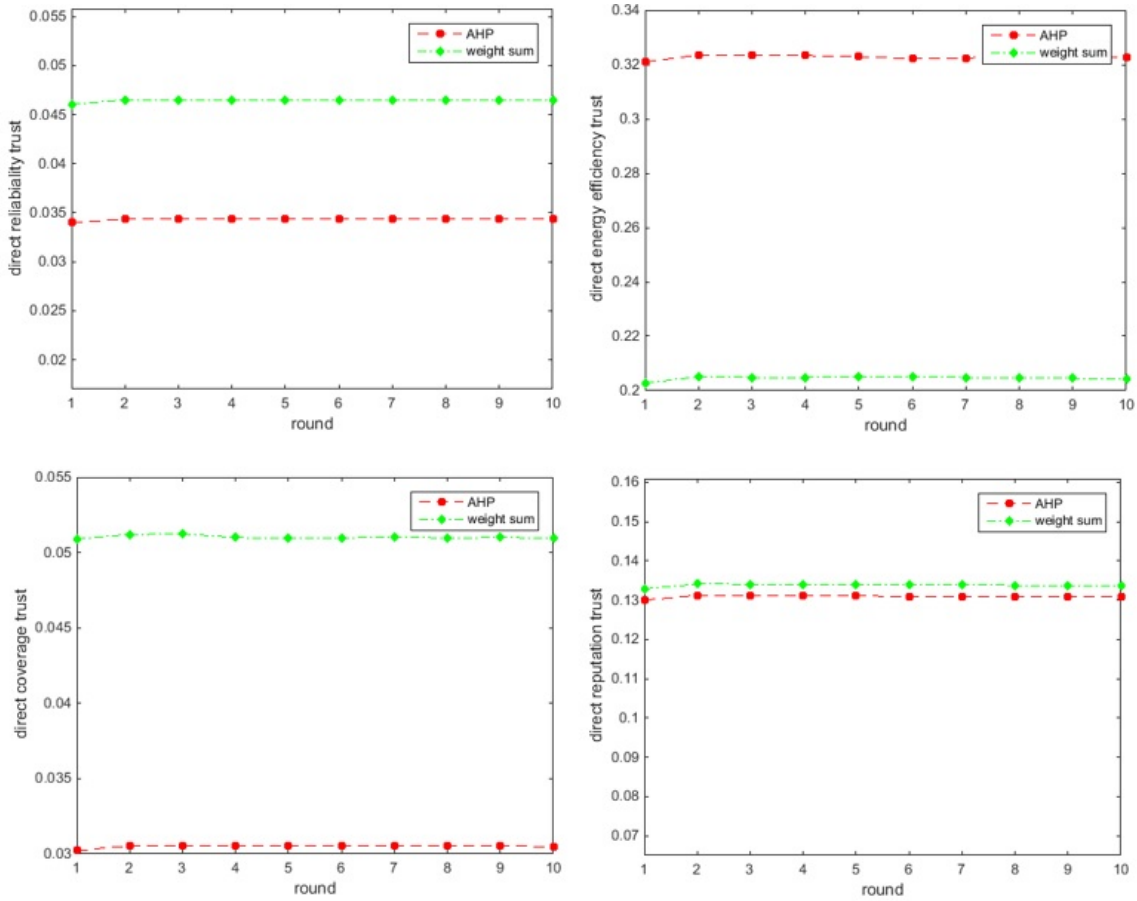

Figure 4.13: Direct trust values of direct nodes in WSNs with AHP-pairwise weighting (red) and predetermined weights (green) in Scenario 1.

Figure 4.14a shows the remaining energy of all participating nodes in the network after 500 seconds' simulation time. The energy consumed by the nodes was very similar in the pairwise comparison and weighted sum approaches. In both approaches, the weight assignment to the evaluated criteria incurred a computational cost. As most of the energy is consumed during transmission and communication, the energy cost of both weighting mechanisms is relatively small, indicating that in terms of energy, both mechanisms perform similarly. However, in terms of network throughput, pairwise comparison achieved a higher performance than the weighted sum method (Figure 4.14b). The pairwise comparison also increased the packet delivery ratio (Figure 4.14c), but lengthened the average network delay. However, the delay difference between the pairwise comparison- and weighted sum-based WSNs was small (0.3 ms; see Figure 4.14d).

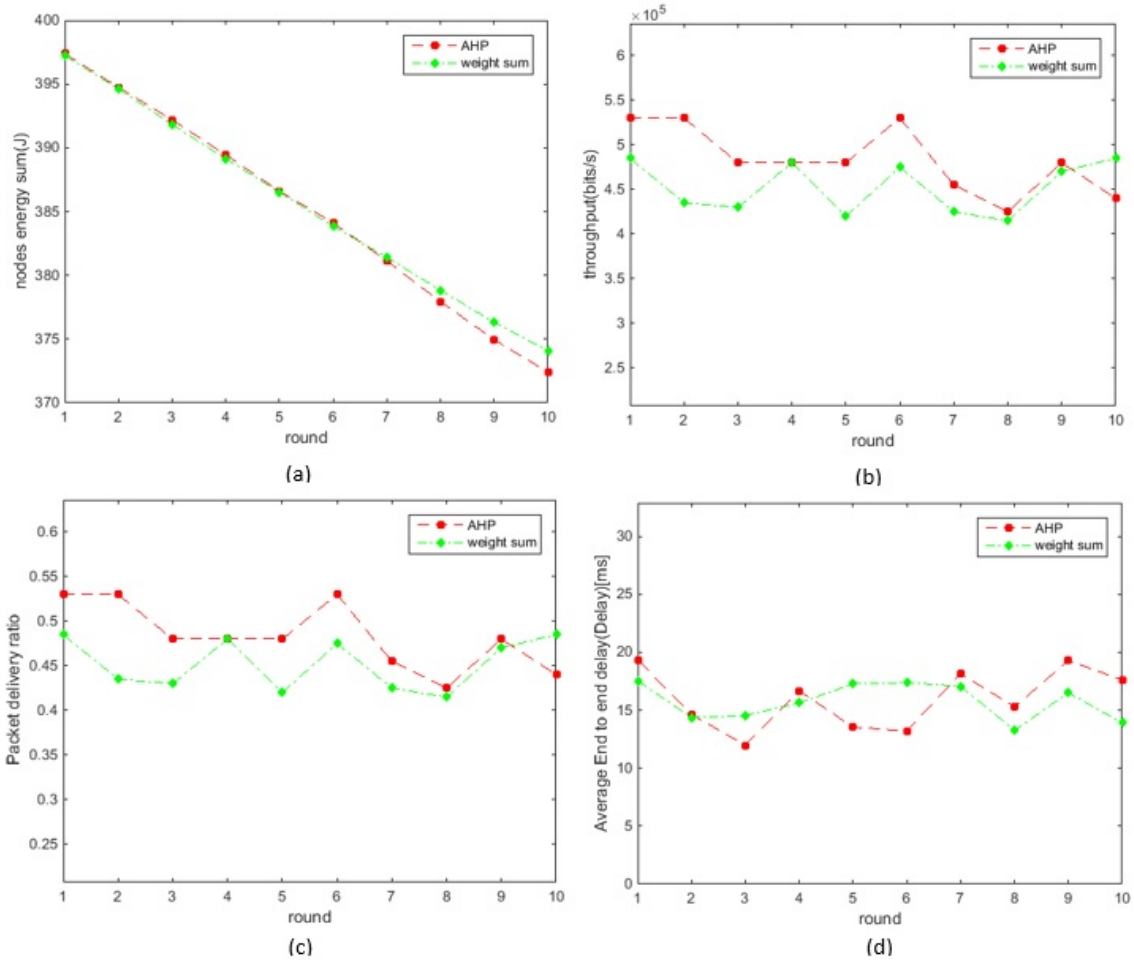

Figure 4.14: Energy consumption (a), throughput (b), packet delivery ratio (c) and delay (d) in WSNs based on AHP pairwise weighting (red) and predetermined weights (green) in Scenario 1.

4.7.1.2 Scenario 2

Table 4.3: Comparison matrix for Scenario 1: When Decision Maker (DM) sensed dense network.

	Energy	Reputation	Reliability	Coverage
Energy	1	0.33	3	5
Reputation	3	1	5	3
Reliability	0.33	0.2	1	3
Coverage	0.33	0.33	0.33	1

Figure 4.15 shows the trust values for the four main criteria used in assessing trust value of direct nodes by the source nodes for the selection of forwarder in ARTP, for Scenario 2. The preference would be Reputation > Energy Efficiency > Reliability > Coverage. The preferences in Table 4.3 (also shown in Chapter 3) is used for this scenario. The trust value gain in terms of energy efficiency using pairwise

comparison is 0.36 while using weighted sum, the value gained is around 0.2. The reputation trust value gained using pairwise is 0.03 and 0.13 using weighted sum. For Reliability, the trust value is 0.18 using pairwise comparison and 0.046 for weighted sum. In terms of coverage, the trust value is 0.098 using pairwise, while using weighted sum, the value is 0.05. The trust gained using either pairwise comparison or weighted sum follows the preferences sequences as assigned for Scenario 2.

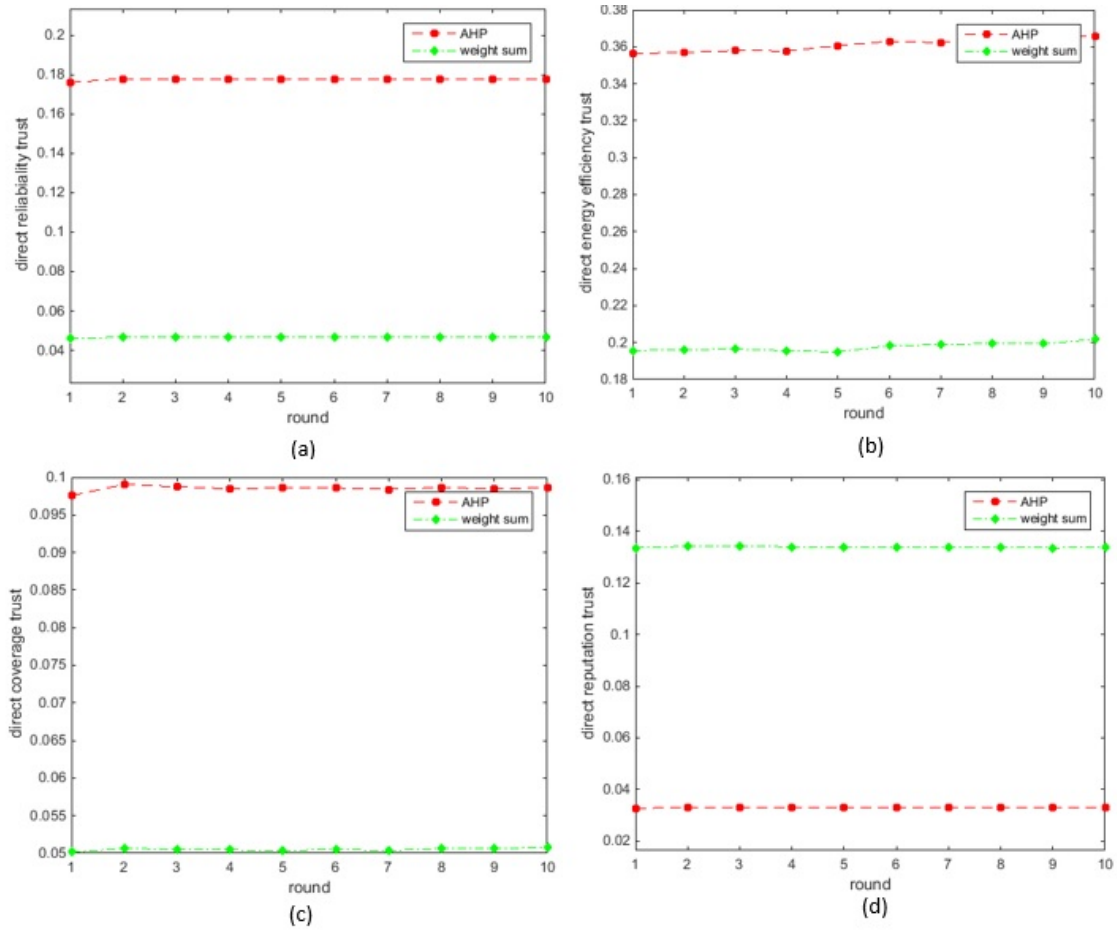

Figure 4.15: Direct trust values of direct nodes in WSNs with AHP-pairwise weighting (red) and predetermined weights (green) in Scenario 2: reliability trust (a), energy efficiency trust (b), coverage trust (c), and reputation trust (d).

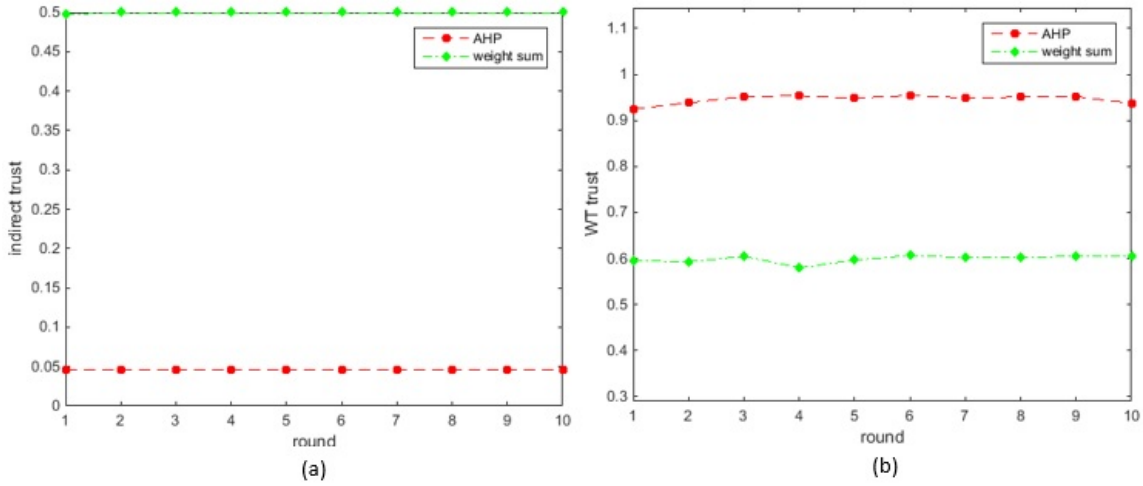

Figure 4.16: Trust values of nodes in WSNs with AHP-pairwise weighting (red) and predetermined weights (green) in Scenario 2. Left: indirect trust; right: witness trust.

Figure 4.17a shows the remaining energy of the participating nodes in the network after 500 seconds' simulation time. For the reasons discussed in Scenario 1 above, the energy consumed by the nodes was very similar in both weighting approaches. Also similarly to Scenario 1, the pairwise comparison improved the network throughput (Figure 4.17b) and the packet delivery ratio (Figure 4.17c), but slightly increased the average network delay (by 0.3 ms; see Figure 4.17d).

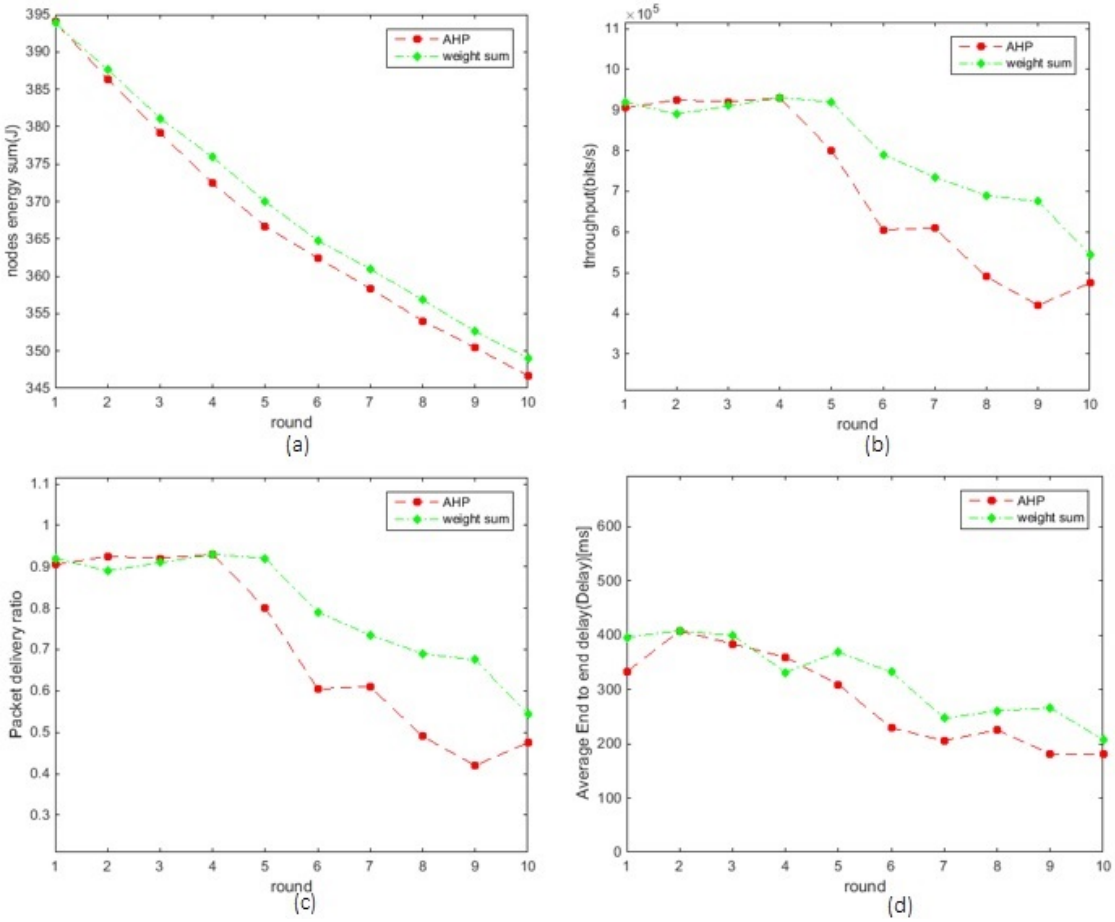

Figure 4.17: Energy consumption (a), throughput (b), packet delivery ratio (c) and delay (d) in WSNs based on AHP pairwise weighting (red) and predetermined weights (green) in Scenario 2.

4.7.1.3 Scenario 3

Table 4.4: Comparison matrix for Scenario 1: When Decision Maker (DM) sensed dense network.

	Energy	Reputation	Reliability	Coverage
Energy	1	5	3	0.25
Reputation	0.2	1	0.33	0.167
Reliability	0.33	3	1	0.25
Coverage	4	6	4	1

In some situations, for example, when the decision maker requires information about the wider network, improving the coverage area is preferred over improving the other trust criteria. In such situations, the coverage becomes the most important metric, and its preference value is set higher than for the other metrics. Figure 4.18 shows the trust values of the four main criteria used by the source nodes when assessing

the trust values of the direct nodes, and hence selecting the ATRP forwarder, in Scenario 3. The preference order is Coverage (most important) > Reliability > Energy Efficiency > Reputation (least important). The preferences in this scenario are listed in Table 4.4 (also shown in Chapter 3). In terms of energy efficiency, reputation, reliability and coverage, the trust value gains were decrease from 0.25 to 0.2, decrease from 0.13 to 0.12, between 0.048 and 0.052, and 0.032 respectively in the WSNs based on pairwise-comparison weighting, and decrease from 0.18 to 0.17, between 0.132 and 0.13, 0.065 to 0.7, and 0.045 respectively in the WSNs based on weighted sums. The trust gains of WSNs weighted by both methods followed the preference sequence assigned in Scenario 3.

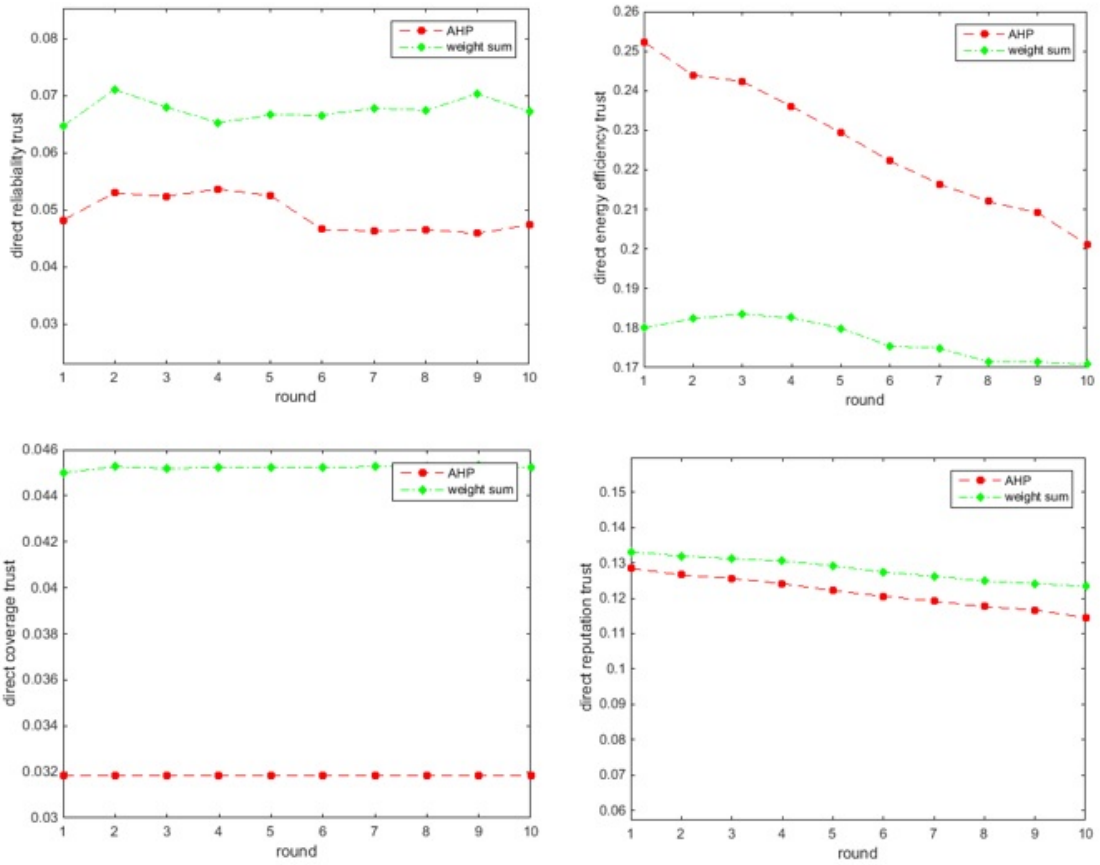

Figure 4.18: Direct trust values of direct nodes in WSNs based on AHP pairwise comparisons (red) and predetermined weights (green) in Scenario 3. Left: indirect trust; right: witness trust.

Figure 4.19a shows the remaining energy of the participating nodes in the network after 500 seconds simulation time. Again, the energy consumed by the nodes in the pairwise-comparison-weighted and weighted-sum WSNs was very similar. As ob-

served in Scenarios 1 and 2, the pairwise comparison improved the network throughput (Figure 4.19b) and the packet delivery ratio (Figure 4.19c) over the weighted sum, but lengthened the average network delay by approximately 0.3 ms (Figure 4.19d).

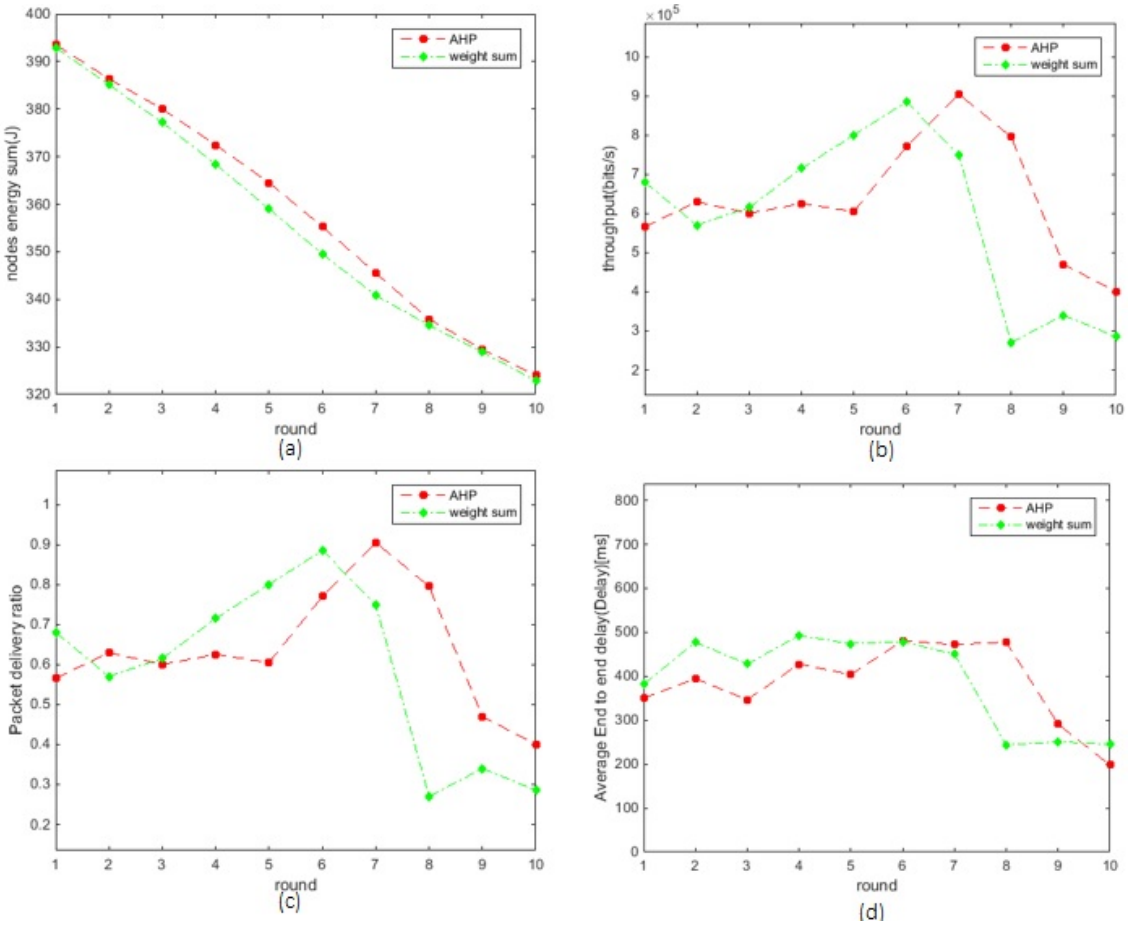

Figure 4.19: Energy consumption (a), throughput (b), packet delivery ratio (c) and delay (d) in WSNs based on AHP pairwise-weighting (red) and predetermined weights (green) in Scenario 3.

Most of existing routing protocols in WSNs involving multi criteria decisions are based on simple weight assignment, where the weights of the individual criteria sum up or equivalent to 1. The pairwise method is selected in ATRP decision making due to the benefits it provides such as the confidence level and consistency checking, the use of standardize scale, allows decision makers to weight coefficients and compare alternatives with relative ease, scalable, and can easily adjust in size to accommodate decision making problems due to its hierarchical structure. In Section 4.7.1, Figures 4.12 to 4.19 demonstrate the differences when using these two methods. Based on the results, two observations can be made: 1) even though the results plotted have

differences in the trust values and output they have generated, the results of both follows the same pattern (decreasing or increasing) and 2) in both methods, the results follow the preferences for the specified scenarios. However, in this thesis, the study on which method is more accurate is not covered and is out of the thesis scope.

4.7.2 Considering control mechanisms

4.7.2.1 Analysis on number of interactions

This subsection examines the performance of ATRP when the number of participants in the network is limited by the number of interactions. The nodes in WSNs have limited resources and are not rechargeable. In ATRP, the number of interactions is a control factor in an efficient control mechanism that utilizes the available resources. The importance of this factor was highlighted in Section 4.6.1; especially, the number of interactions should not be too large or too small.

By controlling the number of interactions, we reduce the communication and transmission costs of multiple nodes participating in the network. A dense network contains a large number of deployed nodes, all of which attempt to participate when a source node requires a relay service. Consequently, each interaction consumes many resources. To reduce the number of participants, the ATRP uses the Chernoff bound theorem (Equation 4.8).

The effects of number of interactions need to be observed, as the actual number of nodes interacting with other nodes is unknown. An appropriate number of interactions may optimise the trust values and the decision making. This subsection discusses the effect of varying the number of interactions in the ATRP. In order to observe the influence of number of interactions in ATRP, the number of allowable interactions is lower-bounded by the threshold (Equation 4.8), which specifies the minimum number of interactions by which the evaluators can assign the potential forwarders. For example, an accurate decision need to be made where the decision is expected to meet the 95% confidence level. In having such a high confidence level, more interactions is required. Figure 4.20 displays the total trust values at various confidence levels and when the number of interactions is not controlled (labeled as no interaction). Clearly, the total trust gained was higher at the 95% confidence

level than at the 35% and 50% confidence levels.

ATRP introduces a new features which is witness trust. Number of interactions act as input for witness trust, where in order to gain more accurate trust (let say 95% confidence level), more witness is required, which also means more interactions are involved. Figure 4.20 demonstrates the influence of number of interactions in terms of energy, throughput, packet delivery rate and delays.

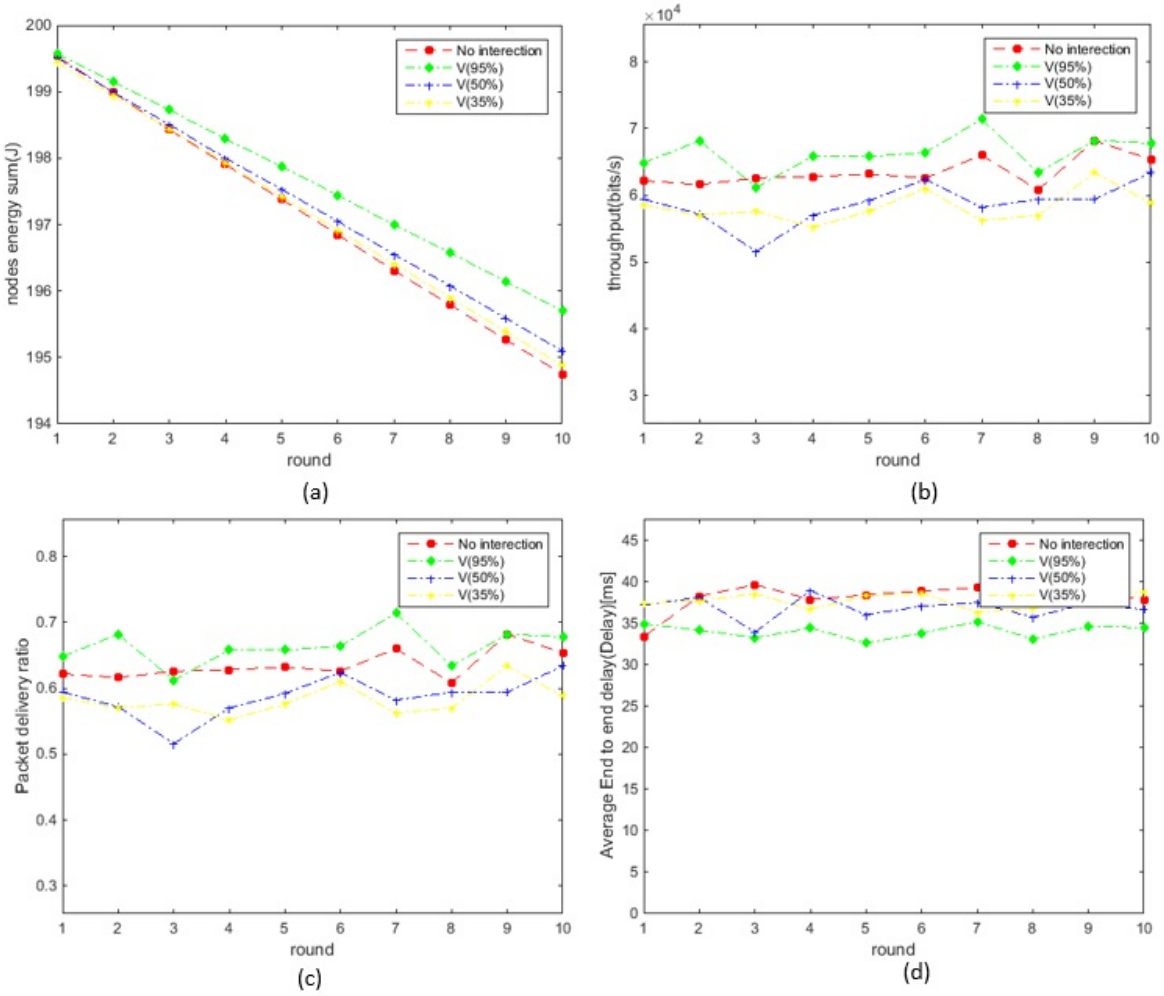

Figure 4.20: Network performance in terms of energy, throughput, packet delivery rate and delays when number of interactions is considered.

Figure 4.20 shows the network performance in terms of energy, throughput, packet delivery ratio and delay when different confidence level (35%, 50%, 95% and when there is there is no limitation set) is required. Base on Equation 4.8, for 95% confidence level, minimum number of interactions required is 11 interactions. This means that for source nodes, direct nodes that have minimum number of 11 witness is required. For direct nodes, witness that have at least 11 neighbors is may be selected.

In such situations, source nodes and direct nodes can limit number of nodes that they should consider in their decision making. Thus the network performance when 95% confidence level is higher as more information is available and is more accurate (provided by more witness) and at the same time, the number of interactions has limit (based on threshold value), instead of considering all nodes connected to either source or direct nodes.

In Figure 4.20a, when the confidence level is set to 95%, the energy consumed in the network is less compared to the others. The energy consumed when the confidence level is set to 35% and 50% is more than 95% confidence level but less than energy consumed by nodes in the network without any control in terms of number of interaction. The throughput is high when the confidence level is set to 95% compared to the scenario when the confidence level is set to 35% and 50%. The throughput when no control in number of interaction is the least (Figure 4.20b). Packet delivery rate in scenario with 95% confidence level is the highest, followed by scenario when no control mechanism is applied. The packet delivery rate is low when 35% and 50% confidence level is considered respectively (Figure 4.20c). In Figure 4.20d, the delay in least when 95% confidence level is utilised. The delay is highest when no control is set for the number of interactions and longer delay exists in the case when 35% and 50% confidence level is considered.

4.7.2.2 Analysis on timeliness factor

Figure 4.21 shows the results in terms of energy efficiency, throughput, packet delivery ratio and average delay, when timeliness factor is considered. The level of confidence determines the number of interaction required among nodes in the network. If higher level of confidence is required, more nodes will be involved, thus more communication will exist, causing higher energy consumption as shown in Figure 4.21a. The energy consumes decreases with number of interactions. In Figure 4.21b, the throughput is the highest when less communication exists due to lower confidence level (35%). The throughput decreases when more interactions involved. The packet delivery ratio is higher when 35% confidence level is set. Followed by 50% and 95% confidence levels. The packet delivery ratio is the least when number of interaction is not controlled Figure 4.21c. Less delay exists when less number of

nodes involve in an interaction. The protocol performs better when timeliness factor is considered. In fact, the delay when timeliness is considered is much less as shown in Figure 4.21d.

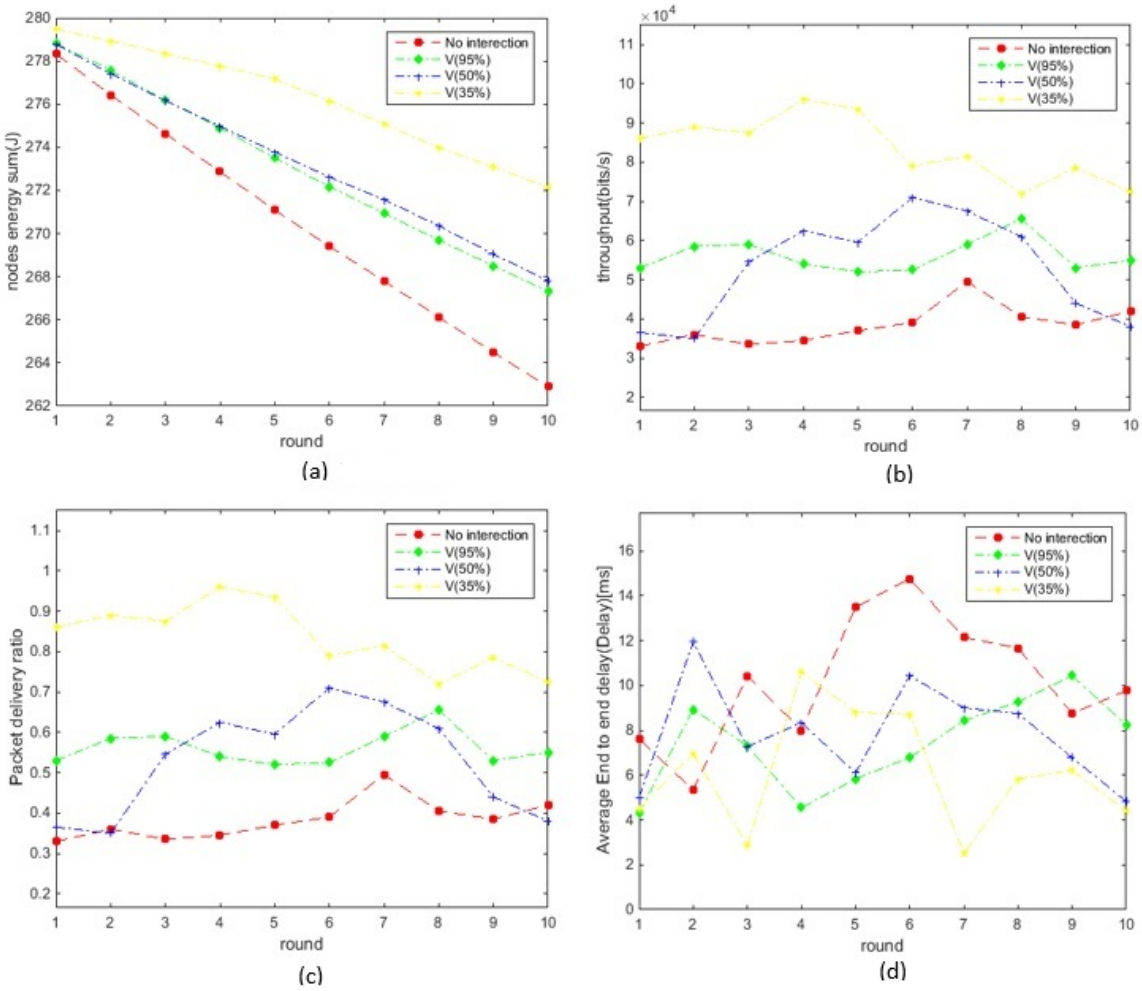

Figure 4.21: Network performance in terms of energy, throughput, packet delivery ratio and delay when timeless factor is considered.

4.7.3 Considering malicious nodes

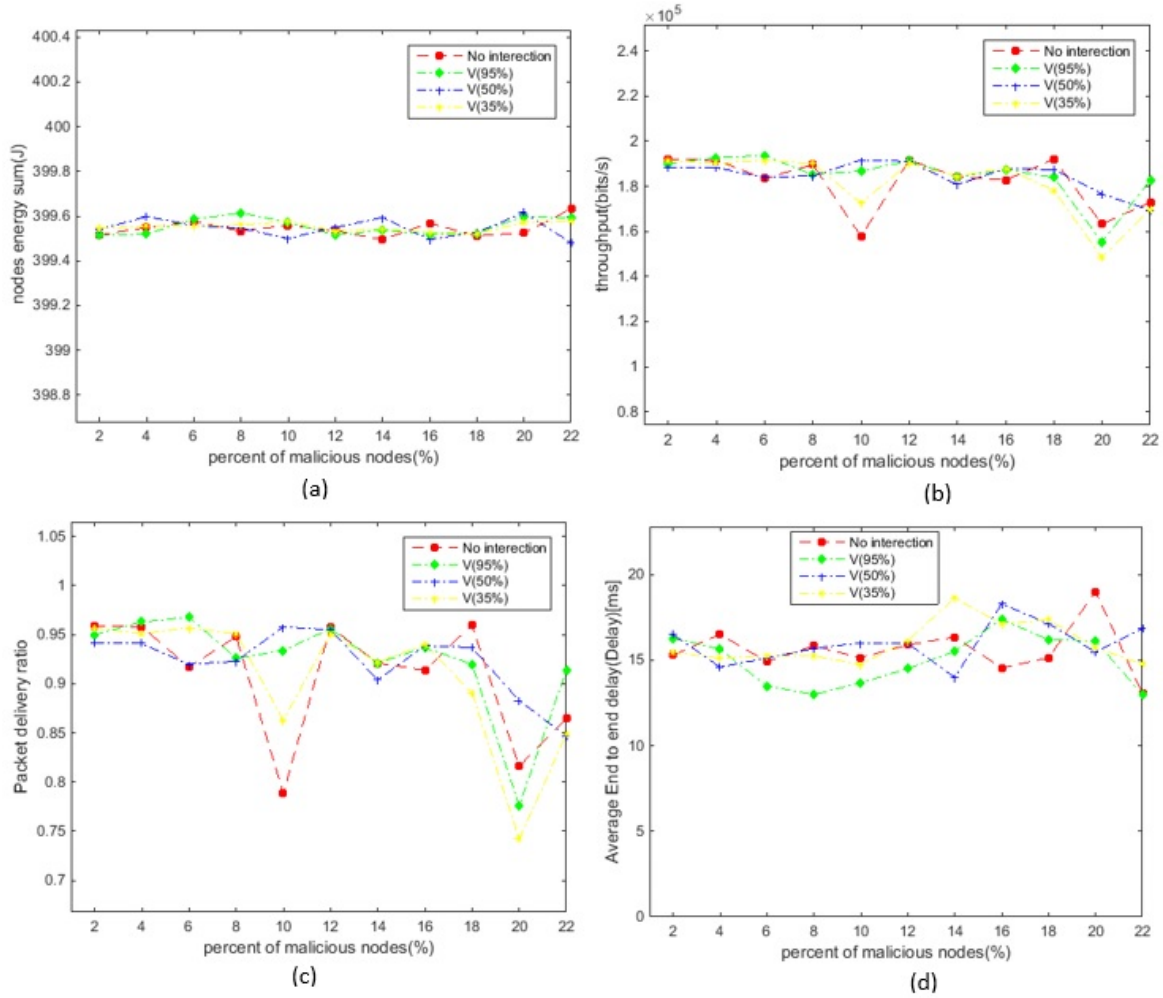

Figure 4.22: Network performances when different percentage of malicious nodes exist in the network.

Figure 4.22 shows the performances in terms of energy, throughput, packet delivery ratio and delay when certain percentage of malicious nodes exist in the network. A node is considered as malicious node if it's packet forwarding ratio is less than the packet forwarding ratio threshold value (Definition 2). Due to this, randomness of results is expected, especially in scenarios when the number of interaction is not controlled (labeled as no interaction in the figure) and when the level of the expected interaction expected is minimal (35%). This can be seen in Figure 4.22b and c. However, based on the results, it is observes that ATRP performs well even with the existence of malicious nodes. The selection criteria considered in ATRP enable it to detect and eliminate malicious nodes in the network.

4.7.4 Comparison with other existing protocols

This subsection presents simulation results of ATRP against TERP and DTLSR. The performance in terms of energy, throughput, packet delivery ratio and average end-to-end delay is evaluated by varying the number of nodes in the network, considering various network load, and considering the existence of malicious nodes in the network.

4.7.4.1 Considering different number of nodes

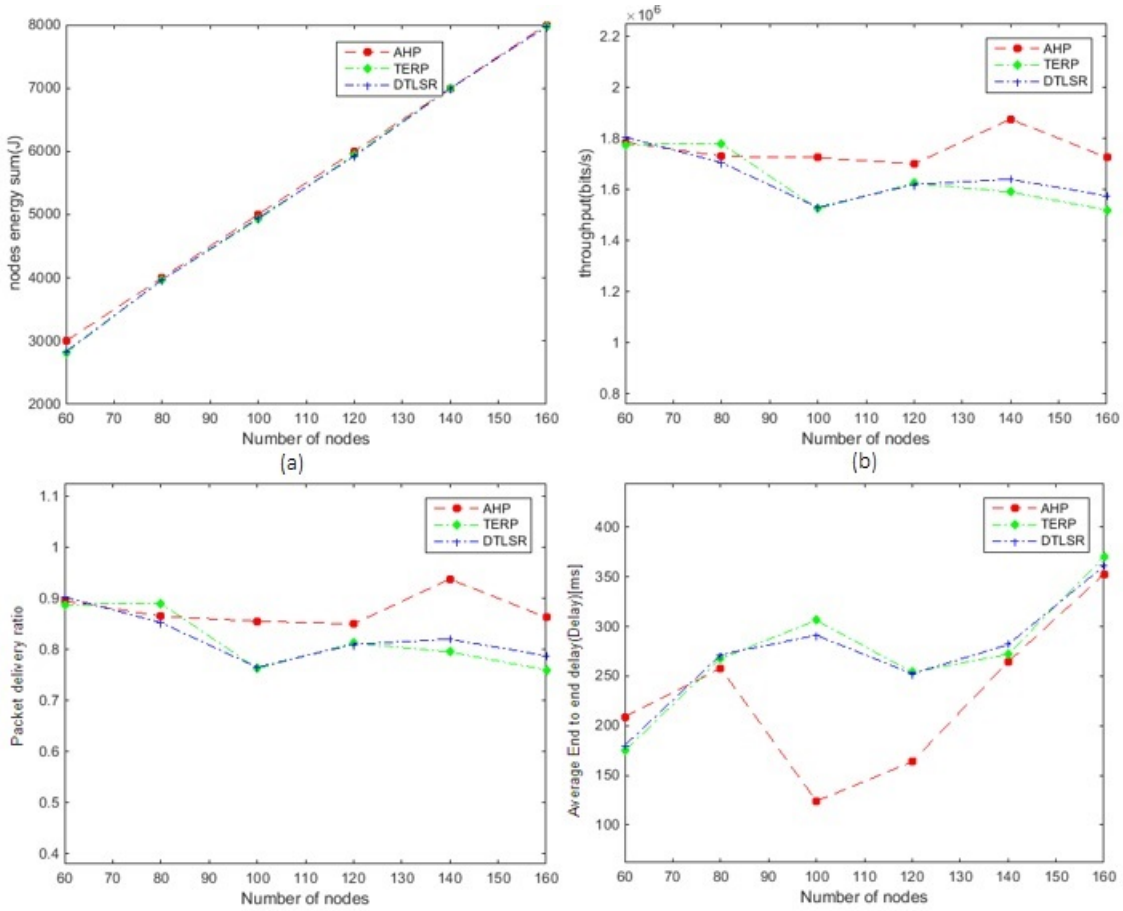

Figure 4.23: Performance comparison considering different number of nodes in A-TRP, TERP and DTLSR.

ATRP provide better and more accurate information by knowing few hops away nodes conditions. Packet drop due to unreliable and unavailable nodes to reach the sink can be avoided. The multi criterion used in ATRP provides better assistant in node selection. Node has the ability to determine whether it is capable to perform packet delivery or not. In addition, reputation given by other nodes may confirm the reliability of evaluated nodes.

ATRP is an adaptive protocol, that performs well even when large number of nodes were deployed, as shown in Figure 4.23. This is because they are selected based on its current conditions. When a frequently used nodes no longer performing better, source node will select other nodes that have higher capability. In Figure 4.23a, more energy is consumes when more nodes were deployed in the network. Figure 4.23b shows the throughput a higher throughput in ATRP compared to TERP and DTLSR. The throughput in ATRP is not much effected with the increase number of nodes. However, the throughput in TERP and DTLSR decreased with the increase number of nodes in the network. More packets are successfully delivered in ATRP Figure 4.23c compared to the other two protocols. However, the packet delivery ratio in ATRP is not much influenced by the increasing number of nodes. Instead, the packet delivery ratio in ATRP increases with the increase number of nodes, which is contrast to the other two protocols. The average delay in ATRP is less compared TERP and DTLSR and gradually increases when the number of nodes in the network increased. The delay in TERP and DTLSR are higher and increase with the number of nodes.

4.7.4.2 Performance evaluation under various network loads

Figure 4.24 shows the performances of ATRP, TERP and DTLSR in terms of energy, throughput, packet delivery ratio and delay under various network load. Based on Figure 4.24a, it is observes that in terms of energy consumption, DTLSR consumes the most, followed by TERP. The least energy is consumed in ATRP. In addition, the energy is uniformly consumed under the various network load (100 to 1000Kbps). A high throughput is observes in ATRP. DTLSR outperforms TERP with slight difference in terms of throughput (Figure 4.24b). Packet delivery ratio in ATRP is the highest among all. The performance of DTLSR in terms of packet delivery ratio is also higher than TERP when various network load is considered (Figure 4.24c). However, the performance of ATRP in terms of average end to end delay is higher than TERP and DTLSR as shown in Figure 4.24d.

Based on results in Figure 4.24, ATRP outperforms the TERP and DTLSR in terms of energy, throughput and packet delivery ratio, under various network load. ATRP selects the forwarder in an efficient way that allows the network load to

be distributed in more balance manner. Due to the fair load distribution among nodes, the packets are able to be delivered smoothly and successfully. The energy consumption is less due to its control mechanisms that reduce the flooding effects in the network.

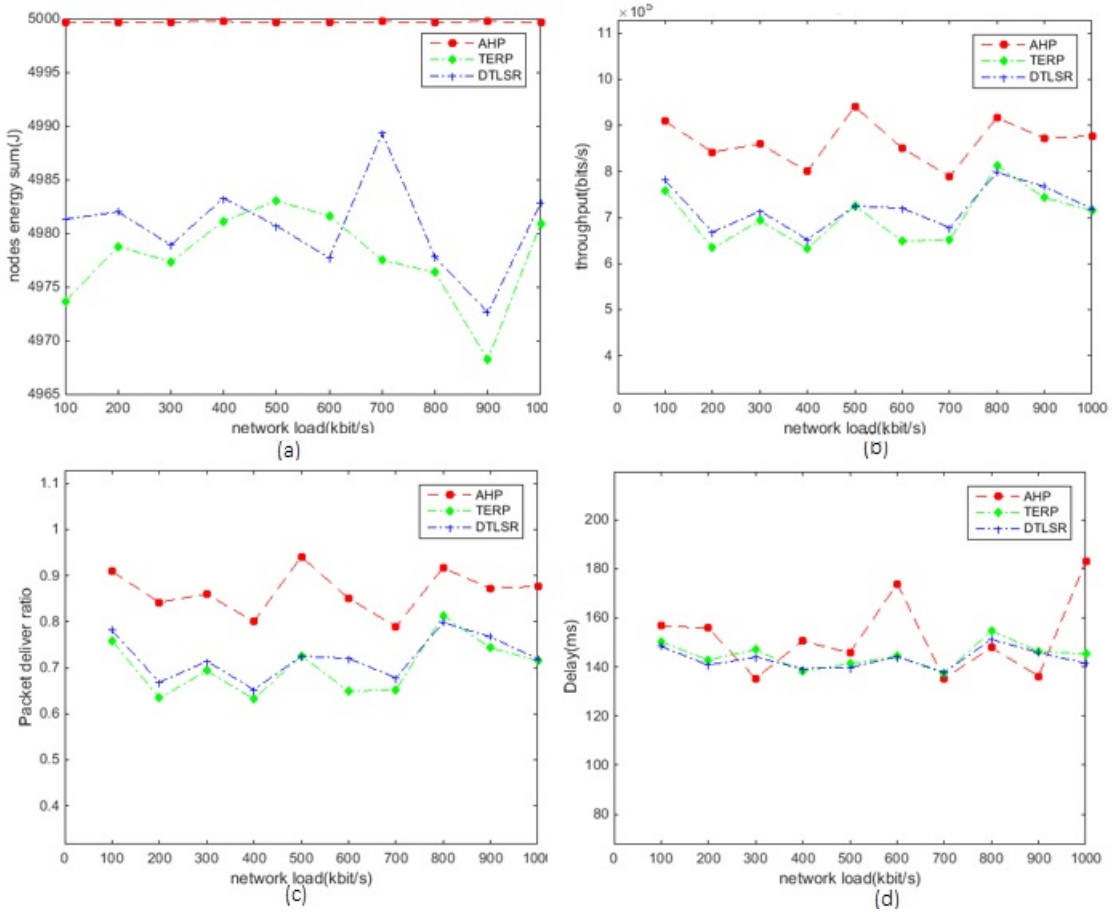

Figure 4.24: Performance comparison considering various network load (200 to 1000Kbps) in ATRP, TERP and DTLSR.

4.7.4.3 Considering existence of malicious nodes

Figure 4.25 presents the simulation results of ATRP against TERP and DTLSR, considering the existence of malicious nodes in the network.

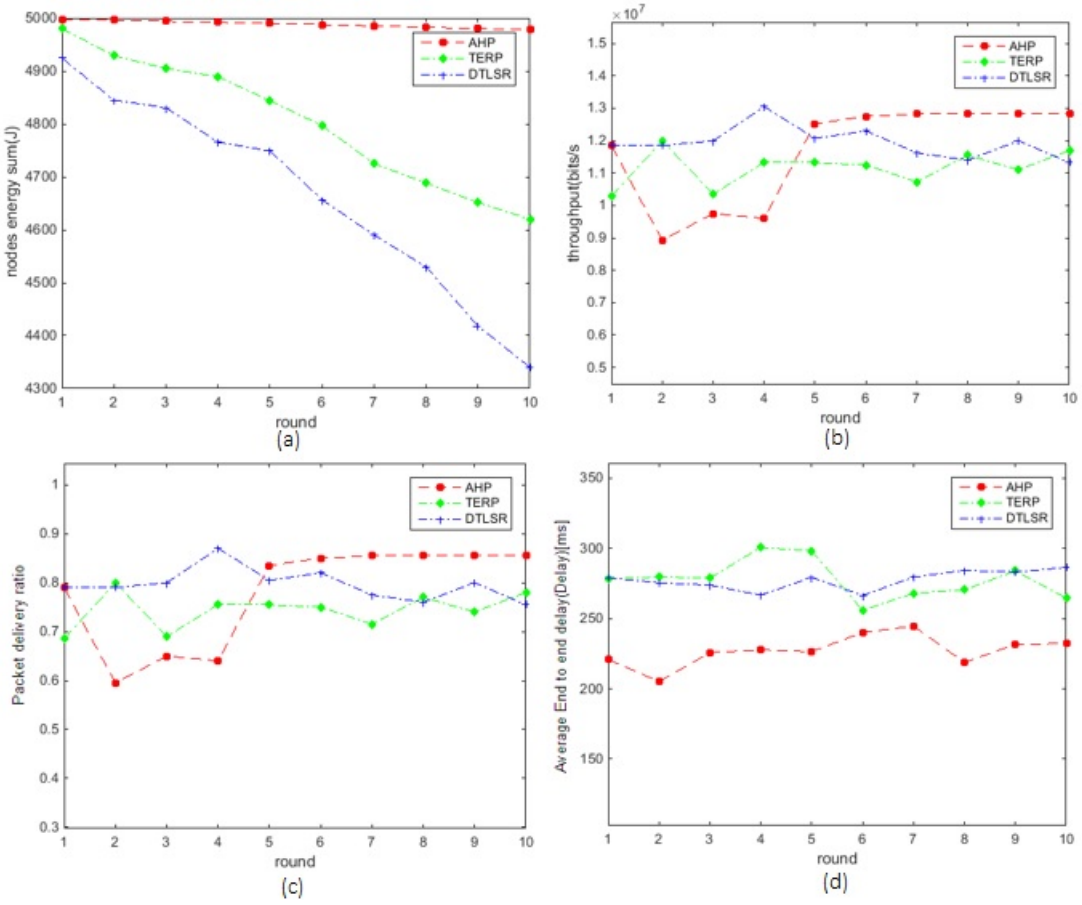

Figure 4.25: Performance comparison in 10 rounds when 10 malicious nodes exist in ATRP, TERP and DTLSR.

Figure 4.25a demonstrates the average of participating nodes remaining energy in the network. The higher the values for y-axis indicates more energy efficient the protocol is, i.e. less energy were consumed in routing packets from source to destination. Among the three schemes, ATRP performs better as the remaining energy is still high. Nodes remaining energy in TERP is higher than DTLSR. Energy is consumes when sending request and receives reply, due to re-transmission, computations and transmission of data.

ATRP outperforms the other two schemes due to its comprehensive considerations in its decision making process, besides considering factors considered in TERP and DTLSR, such as energy, distance (hop count) and trust. In these communications, ATRP provides several mechanisms such as control of number of interactions, local decision by direct and source nodes, multi criteria considerations and learning mechanism in its decision. These mechanisms helps in ensuring appropriate number of interactions required (more interactions may not be necessary and consume more

energy), lower layer decision reduces burden of higher layer decision maker and reduce the number of potentials to be evaluated, criteria used in selection considers several aspects allows nodes to avoid malicious nodes at the earliest and learning based reduce the number of request and reply required as nodes learn to make decision based on its existing local information rather than asking for information every time request is sent to them. More energy is consumes in DTLSR could due to its reliance on only direct trust even tough several factors were considered in evaluation of the direct trust.

In TERP, there is no control mechanism such as in terms of number of interactions. Thus more energy is consumes in interactions between nodes. In addition, for every error or changes in the route, route maintenance phase will be involved which requires messages to be sent to all related nodes and route discovery need to be re-initiated, thus, more energy is consumes.

Figure 4.25b shows the throughput in all three schemes. DTLSR demonstrates better throughput than followed by TERP and ATRP. However, the throughput decreases after several rounds. Contrary, the throughput in ATRP increases after several rounds. The trust estimation and attack capability in TERP is more accurate, incorporated several aspects such as probability for positive behaviour of nodes, the direct and indirect trust. TERP combines energy awareness with the concepts of trust in its route setup to allow selection of efficient trusted nodes which significantly increase the throughput. The result exhibits reduced throughput performance of DTLSR as it only relies on direct trust and overlook the energy preservation aspect. Thus, it also leads to the increased number of dead nodes. As the routing of these two protocols only rely on the trust values of one-hop neighbours, the probability of selecting the best path is low as they are unaware about the rest of the network topology.

In a dense network, ATRP are expose to more potential forwarder and yet only credible and reliable providers (considering several aspects and criteria). In ATRP, as the nodes learn the performance of their neighbours, malicious nodes can be detected and avoided earlier. Thus, packets are relayed through other reliable nodes. The throughput in ATRP is higher also due to evaluation mechanism provided for multiple hops rather than a single hop, i.e. by making decisions about several hops

away would be better rather than relaying through a single hop node which have no neighbours, would cause packet drop etc.

Figure 4.25d presents the evaluation results of all schemes in terms of average end-to-end delay. ATRP outperforms the other two schemes because the routing decision in ATRP requires nodes to select energy efficient, good coverage, reliable and good reputation nodes which allow the packets to be relayed smoothly through an optimal nodes, thus, minimizes the average end-to-end delay. In DTLSR, node is selected if it provides the highest reliability and also the shortest path. Also, the nodes with shortest path will be selected when the trust levels of all the nodes are equal. If there is no node within shortest distance between source and destination, longer paths may be selected. Thus, the end-to-end delay is increased as longer paths are more disposed to failure and require more route request and recoveries. These process cause network congestion that restrict the availability of bandwidth for data packets. In TERP, node selection is based on composite routing metrics that include energy efficiency, shortest and trusted routes which may keep a consistent flow of packets longer, thus, minimizes the average end-to-end delay. The performance in terms of average end-to-end delay in DTLSR and TERP are at almost similar range may due to similarity in selection metric chose in their decision, i.e., shortest path. Thus, in both schemes, the nodes chose among shortest path as their main criteria, thus keeps the value in a consistent range.

4.8 Conclusion

In this chapter, we have proposed an adaptive trust-based routing protocol, called ATRP. Our protocols consider several important issues with regards to multi hop decentralized and randomly distributed wireless sensor network. As a network consisting of resource-constraints nodes, energy-aware mechanism is a must factor to be considered. In homogenous network, flooding is the main aspect that consumes energy. In order to provide wider view of the network, we have proposed a hierarchical evaluations of node selection based on direct and indirect trust. By considering group of nodes in route selection, the possibility of chosen best node but having no inheritor can be avoided. In fact, the multi criterion factors considered in the trust metrics in ATRP performs well in decentralized and randomly distributed network.

This is proven based on its great performances in terms of lifetime, delay, packet loss and energy consumption.

Chapter 5

A Blockchain-based Protocol for Mobile Sink Coordination

5.1 Introduction

In Chapter 4, ATRP has been proposed to improve the routing protocol through an efficient forwarder selection mechanism. The approach helps by allowing longer node lifetime and balance load among the nodes by avoiding coverage hole due to the frequent used of the same nodes that are centred around the static sink. Apart from this, efficient mechanism to overcome coverage hole due non-uniform nodes distribution in randomly deployed network is nontrivial as it may cause inefficient routing when some abnormality or events at certain parts of the network cannot be detected. Existing work to tackle a coverage hole problem is by utilizing mobile sinks to collect and gather data from surrounding, aim either to maximize coverage area or to avoid hole that is centred around static sink. Some mobile sinks may fail to cover a certain area due to lack of information provided by the surrounding nodes. Without central controller, the nodes need to collaborate in a distributed way in determining efficient mobile sink mobility strategy.

Existing collaboration mechanisms elaborated in Chapter 2 include trust-based, learning-based, game theory-based, negotiation-based, consensus strategy, role-based, task-based allocation, and cluster formation. However, most of these collaboration mechanisms are not suitable for resource constrained environments, such as WSNs. In addition, most of the approaches used in the routing protocols of wireless sensor domains are based on decision making, which is aimed for individual decision maker but not necessarily for the whole network. Although a decision that benefits the whole network is practically infeasible, especially when global information is missing, a decision that benefits the larger parts of the network is a promising proposition.

An extensive review on distributed solutions involving mobile sink conducted in [Tunca 2014] revealed several challenges in the existing work with regards to

sink mobility such as hotspot problem around the constructed grid, outdated sink location, and energy consumption due to flooding. The distributed solutions for network controlled sink movements depend on the network conditions (such as the node energies and the node density in the regions [Basagni 2008]) for route management and decision making instead of relying on a central entity [Di Francesco 2011], [Liang 2010] may reduce the energy consumption and increase the lifetime of the network [Gandham 2003], [Luo 2005], [Papadimitriou 2005], [Faheem 2009], [Wang 2005]. However, there are only a few controlled sink mobility methods for distributed mobile-sink routing protocols exist [Tunca 2014]. In this chapter, a novel distributed routing protocol for WSNs called the Blockchain-based Protocol for Mobile Sink Coordination (BCRP) is proposed to assist mobile sinks relocation decision to ensure energy efficiency, updated dissemination on sink location and, more balance coverage among mobile sinks. BCRP exploits a recent distributed trust approach known as blockchain when making routing decision.

The trust in BCRP is defined as the belief that a node has on other node's decision, confined within a set of predetermined rules, which needs to be agreed among nearby nodes (sinks). The decision making in BCRP is determined by the coverage and redundancy levels, as the trust factors. Each participant will self-evaluate the request sent by a requestor and decide whether to accept or reject the request (via a vote). The ultimate decision is based on the vote, where the request with the highest positive votes is considered as the most trusted one.

This chapter is divided into several subsections. In Section 5.2, the motivations for BCRP development are highlighted. Section 5.3 explains the components and process flow in BCRP. The five modules in BCRP are explained in Subsections 5.3.3 to 5.3.7. Section 5.4 demonstrates the results of BCRP implementation. Finally, the conclusion of this chapter is presented in Section 5.5.

5.2 Motivation

- Coverage holes are created by the frequent use of nodes near the static sink and the non-uniform node distribution under random deployment. Leakages may cause mis-routing of the data packages. The coverage-hole problem is often treated by deploying mobile sinks that divert the traffic at frequently

used nodes, allowing those nodes to sustain longer [Basagni 2008]. Yet, many existing distributed mobile sink routing protocols that utilise cluster-based approach aim for energy efficiency still suffers from hotspot problems [Mir 2007], [Kweon 2009], and [Yuan 2011].

- The data packets may be lost if they are forwarded towards a sink position that is no longer exist or has changed. The sink relocation may also exposed to possibility of unexpected changes along data dissemination routes [Tunca 2014].

- In most of the existing works, mobile sink's position is commonly flood in periodic basis to advertise the sink's relocation position to all nodes in the network. Flooding comes with cost especially when all nodes in the network need to relay the routing control packets [Wang 2009], [Vecchio 2010]. Flooding also causes redundancy of packets along the data dissemination routes which increases the overall energy consumption [Ye 2005] and remain as a challenge in majority of existing distributed solutions.

- In most of existing distributed mobile sink routing protocols for WSNs, there is no mechanism to ensure the trustworthiness or validity of a decision or the decision provider. The source node calculates or estimates the relocation position and broadcast the information to all the nodes in the network. There is no guarantee that by relocating, other nodes will gain any benefits from it.

- The nodes in the network are characterised by their dynamic behavior. In cluster-based approach, reelection may be required when the current cluster head depletes its energy. However, selecting new cluster head consumes energy and increases in delay. A more flexible way is needed to allow the node to react accordingly without the need for such election or role-based assignment.

To resolve these deficiencies, BCRP is proposed as an efficient distributed mobile sink routing protocol based on blockchain strategy in assisting sink relocation decision for WSNs. BCRP aims to achieve following desirable goals:

1. Energy efficiency approach: BCRP reduces the energy consumption due to flooding and redundancy by partitioning and assigning a dedicated mobile sink for each partition.

2. Improving the coverage hole in the network: The sink mobility in BCRP is controlled by the network towards lower coverage level area.

3. Better decision on relocation position: The decision on relocation position is upon consensus among some mobile sinks. Thus, the problem due to outdated sink position can be avoided and may benefits larger parts of the network.

The contributions of this chapter are as follows. First, the routing efficiency in distributed and decentralized WSNs is improved by a novel blockchain-based routing protocol, which is assisted by mobile sinks. Second, unlike most of the existing routing decisions, the proposed protocol treats the coverage hole as an impact factor, thereby expanding the limited number of controlled mobility routing approaches. Instead of avoiding hotspots, our proposed protocol aims to cover areas which are insufficiently covered by the nonuniform deployment. Third, the protocol simultaneously considers both the resources constrained by the WSN nodes and the security requirements (which is feasible through verification and the consensus module).

5.3 Blockchain-based Routing Protocol with Mobile Sink (BCRP)

In a randomly distributed network, hole coverage is diminished by two mechanisms: the uneven node distribution (density in some areas and sparsity in others) and node depletion. In such a situation, the data reported to the sink may be inaccurate and deviant from the actual scenario.

The Blockchain-based Routing Protocol (BCRP) considers a network of static sensors, $S = s_1, s_2, ..., s_n$. Each s_i can monitor any point within its sensing range r_i, where r_i is a radius. In other words, if a location in A lies within the sensing range of s_i, it is covered by s_i. A network of mobile sinks, $MS = MS_1, MS_2, ...MS_n$, is deployed in a two-dimensional area A. Each mobile sink MS_i, $i = 1, ..., n$, is located at coordinates (x_i, y_i) inside A has a sensing range r_j, and is responsible for its own Voronoi polygon, meaning that only one MS_i exists in one polygon, and that each s_i within the polygon of MS_i is reported to MS_i.

5.3.1 Components in BCRP

The BCRP implements a contract, called the topology adjustment contract. As shown in Figure 5.1, the *topology adjustment contract* includes the participants, a distributed ledger (rules), and the verification components of the individual participants. Whenever a condition is met, the request is distributed among the other mobile sinks and normal nodes in the network. Whereas the centralised approach is vulnerable to a single point of failure, the distributed ledger exists across several locations or among multiple participants. The design eliminates the need for a central authority or intermediary to process, validate or authenticate a process. The content is stored in the distributed ledger only after consensus by the parties involved. The consensus principle ensures that the ledger is maintained by all participating nodes.

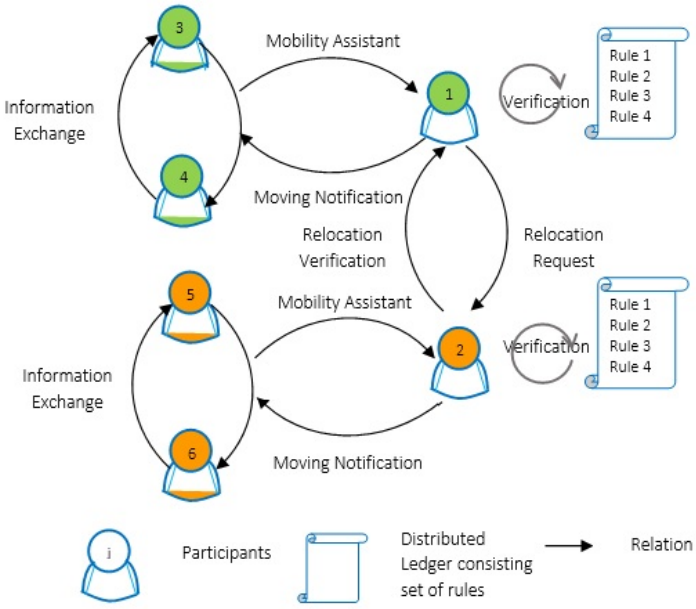

Figure 5.1: Components of the topology adjustment contract in BCRP: Rule 1: Coverage Detection; Rule 2: Relocation Rule; 3: Redundancy Check Rule; 4: Force-based Rule; 5: Consensus Rule.

5.3.1.1 Smart Contracts

Smart contracts are digital contracts that are self-enforcing or prohibitively expensive to break [Szabo 1997]. A smart contract refers to the computer protocols or programs that automatically execute or enforce the contract under a set of predefined conditions. The functions and conditions of smart contracts can be defined beyond the exchange of cryptocurrencies. For instance, they can validate assets

within a certain range of non-monetary transactions. Szabo [1993] defined the smart contract as a computerized transaction protocol that executes the terms of a contract. A smart contract can enforce or self-execute contractual clauses. The advantaged of smart contracts such as cost reduction, speed, precision, efficiency, and transparency have fostered new applications in various areas [Reyna 2018]. The blockchain consensus protocol ensures the correct execution of the contract.

Smart contracts (also called self-executing contracts, blockchain contracts or digital contracts), are preprogrammed computer instructions (codes) that must be agrees by all participants [Olivier 2018]. In e-commerce, smart contract enables two anonymous parties to trade and conduct mutual business operations (usually over the internet) without requiring a middleman.

5.3.1.2 Participants

The rules in the distributed ledger model of the blockchain-based approach are enforced by the participants. In Figure 5.1 above, the BCRP participants are the mobile sink (labeled 1 and 2) and the normal nodes (labeled 3, 4, 5 and 6). The mobile sinks are considered as potential participants because they communicate with each other at the beginning (initial construction of the region) and whenever a topology adjustment is needed, which may not involve all mobile sinks.

Each participant must obey four sets of rules. The first rule (the coverage detection rule), specifies that a request can only be sent under certain conditions (Section 5.3.4.1). The second rule (relocation rule) determines the new position (relocation) of a node by a vector-based approach (Section 5.3.4.2). The third rule (the redundancy check rule; see Section 5.3.5.1), stipulates that neighbouring mobile sinks should check for redundancy, and only approve new location that are not located in redundant sectors. Due to their distributed nature (physical obstacles), only mobile sinks nearby the requesting mobile sink can validate and approve a topology adjustment request. This localised decision making ensures that the movement is beneficial. The fourth rule (consensus rule) dictates the actual relocation after agreement from the majority of neighbours. The fifth rule (the balancing rule) ensures that the relocation distance and the existing mobile sinks are neither too close nor too far (Section 5.3.6).

The final decision of an individual is sent to the requestor, which determines the action based on the majority of agreed or disagreed results (i.e., the consensus vote) of the other participants.

5.3.1.3 Consensus

A common consensus defines the majority decision of several nodes voting on one node. If a node desires an update on one side, the other nodes must vote on whether the update is legitimate and secure. Once a consensus is reached, the old information is replaced by the most recent information, and the consensus updates are applied to all nodes.

The collaboration is set as a contract among the mobile sinks in the network. The contract (called the Topology Adjustment Contract) is setup when any mobile sink requires relocation (i.e., when triggered by a condition).

5.3.2 Process flow of BCRP

Figure 5.2 shows the overall process flow of the BCRP. The BCRP comprises four main modules; the setup module, the initialization module, the verification module and the consensus module. The details of these modules are given in Sections 5.3.3 - 5.3.5).

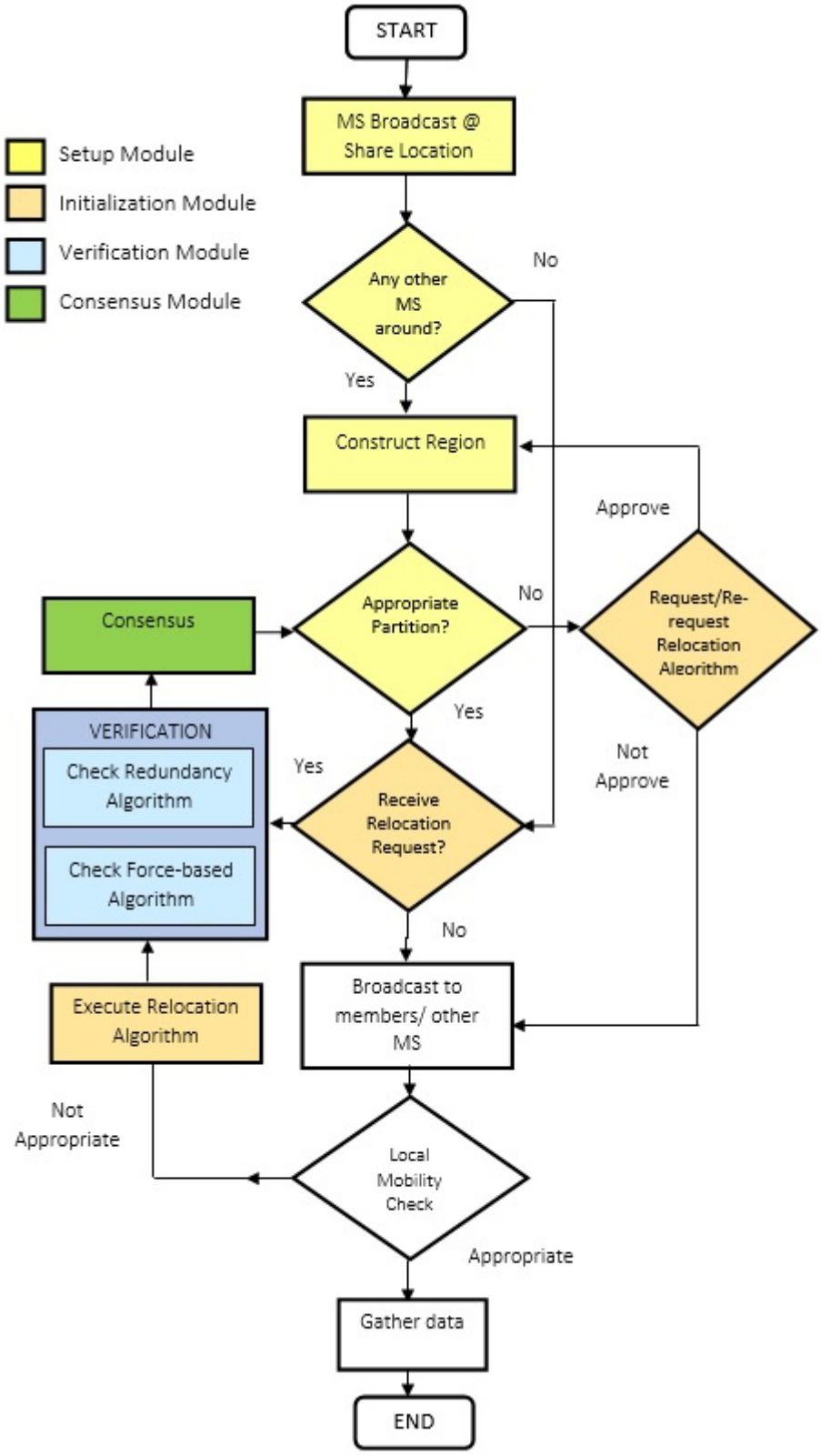

Figure 5.2: Flow diagram of the proposed blockchain based routing protocol (BCRP).

Step 1: Mobile sinks broadcast their location to other mobile sinks.

All mobile sinks share their location information with other mobile sinks. That is, each mobile sink broadcasts its location and requests the locations of other mobile sinks (REQ messages). Mobile sinks that receive a broadcast message send a reply (RLY message) informing their locations. Each mobile sink then stores information of its neighbours's location for partitioning purpose.

Step 2: A local mobility check is conducted in each region. This step detects any local coverage hole.

If a coverage hole exists in its region, the relocation will be conducted towards the coverage hole area. When a relocation request is executed, no mobile sink can move to any other position until the relocation is confirmed (by the mobile sink that initiated the request). After receiving confirmation, the mobile sinks must update the information in their records. During this phase, the nodes in the region continue reporting to their current mobile sinks. After consensus (by the module explained in Section 5.3.7), the mobile sinks inform their new locations to other mobile sinks. Each affected mobile sink updates this information, reallocates it, and broadcasts it to other members in the region. Consequently, all mobile sinks obtain the most recent information about all other sinks.

Step 3: Checking for a relocation verification request.

When a mobile sink receives a relocation verification request, it stars the verification process, which involves checking for redundancy and running the force-based algorithm. The verification module is explained in Section 5.3.5. If a mobile sink receives no relocation request, it either remains at its present location or moves to a low-coverage area within its region. After a move, the mobile sink broadcasts its new location to all surrounding nodes, which then repeat Steps 1 to 3.

5.3.3 Setup Module

The setup module is executed whenever a region in the network must be constructed, i.e., at the beginning of the deployment and whenever a topology adjustment contract is executed (as decided by the consensus module). This module aims to answer the following questions:

How do we construct the partitions and determine the participants in each partition?

In distributed networks such as WSNs, uncertainties are introduced by nodes

depletions and physical obstacles. These uncertainties cause coverage holes in some parts of the network, requiring a topological re-adjustment. Coverage is a fundamental and extremely important performance metric in sensor networks, as it reflects how well a field is monitored or covered by sensors [Wang 2011], [Huang 2005], [Wang 2006]. Thus, the BCRP considers the coverage holes as triggering factors for the protocol implementation.

5.3.3.1 Construction of the region

Partitioning a large network, into several regions extends the lifetime of the nodes in the network. If a single sink oversees each partition, several network performances (energy efficiency, network latency, packet loss and lifetime) are improved because the nodes can report to the sink that is closest to the nodes. The BCRP partitions the network into several Voronoi polygons. For efficient utilisation of the resources, each mobile sink monitors a designated region and collaborates with its neighbouring mobile sinks, achieving balanced adjustment of the covered region. In the initial setup module, each mobile sink construct its region by sharing its location with other mobile sinks in the network.

A Voronoi diagram describes the proximity information in a set of geometric nodes. The space around a collection of nodes is partitioned into polygons, such that every point in a given polygon is closer to the node in the polygon than any other node. A representative Voronoi diagram and Voronoi polygon are illustrated in panel (a) and (b) of Figure 5.3, respectively. The Voronoi polygon of node s_0 is defined as $G_0 = \langle \nu_0, \varepsilon_0 \rangle$, where ν_0 is the set of voronoi vertices of s_0, and ε_0 is the set of voronoi edges. In Figure 5.3(b), $\nu_0 = v_1, v_2, v_3, v_4, v_5$, and $\varepsilon_0 = v_1v_2, v_2v_3, v_3v_4, v_4v_5, v_5v_1$. The neighbours of s_0 is denoted as N_0, where $N_0 = s_1, s_2, s_3, s_4, s_5$ in Figure 5.3b. The vector bisectors of the line passing s_0 and its voronoi neighbours are the voronoi edges of s_0. In Figure 5.3b, the voronoi edges of v_1v_5 is $s_0s_1's$ bisector.

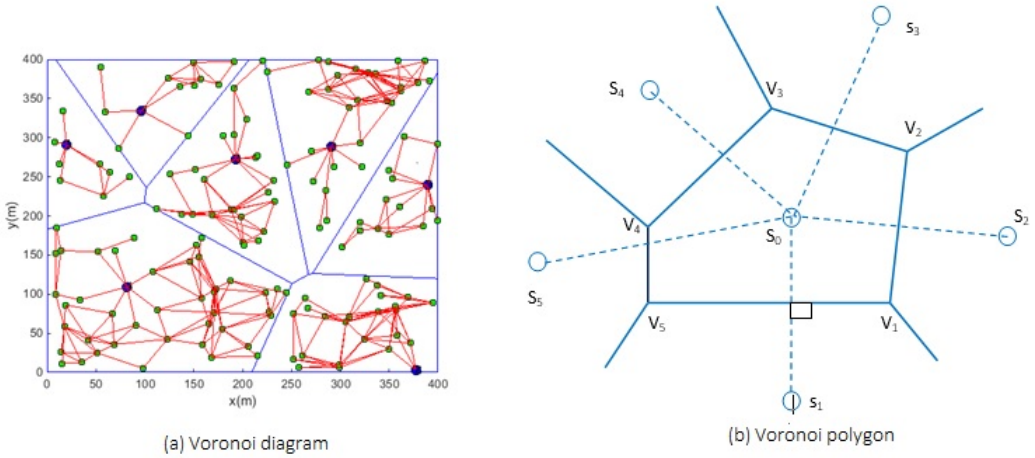

Figure 5.3: Example of a) a Voronoi diagram and b) a Voronoi polygon.

A Voronoi polygon is constructed by calculating the bisectors of the sensors and their neighbours. The bisectors and possibly the boundary of the target field are divisible into several polygons, and the smallest polygon encircling the sensor is the Voronoi polygon of that sensor. Each mobile sink senses its own Voronoi region (polygon) and detects the coverage level in that region. Each participant also shares its information (ID, location and coverage level) with its neighbours.

5.3.4 Initialisation Module

When detected coverage hole in the constructed polygon is less than a specified coverage threshold, the initialisation module initiates and triggers a topology adjustment of other mobile sinks. The sensors calculate the distance and angle of the movement. In the BCRP initiation module, a mobile sink sends a topology adjustment request. The topology of a distributed network, may require adjusting after node depletion (of either sensor nodes or mobile sinks), or may be necessitate by the random deployment. The topology change may affect the network. As the nodes in a distributed and decentralized network are not controlled by a central controller, their topology must be altered over time as the mobile sinks gravitate to regions with more holes than other regions. Movements of mobile sinks consume time and energy. In addition, mobile sinks may be restricted to certain capabilities (such as power or energy control). Thus, the usage and mobility of the mobile sinks must be adjusted accordingly. The initialisation module aims to: 1) Identify the conditions that initiate the protocol implementation and 2) calculate the required mobility

distance and angle.

To fulfill these aims, the BCRP initialisation module implements two rules: 1) coverage level detection and 2) mobile sink relocation (these rules are explained in Sections 5.3.4.1 and 5.3.4.2, respectively). Each mobile sink is bound by these rules when initialising a request and planning a relocation. Algorithm 5.1 shows the conditions and rules of the initialisation module.

Algorithm 5.1 Initialisation Rules: (Coverage level detection and relocation request)

Input: Location, coverage level, relocation position
Output: Relocation Position
for *For each round* **do**
  Check coverage level (Section 5.3.4.1) Broadcast position and coverage level
  if *Coverage level of region is low* **then**
    Request relocation
    if *dense(sparse) network* **then**
      Push(Pull) applying the force-based method to relocation position
    end
    else
      Determine the direction and angle by the vector-based method
    end
    Broadcast a relocation position (i.e. new location) request
    Wait for verification result
    if *Receive % of vote (consensus) is high* **then**
      Broadcast the relocation (new position)
    end
    else
      Remain in current position
    end
    Resend request
  end
end

5.3.4.1 Rule 1: Coverage Detection Algorithm

Topology changes are triggered by several conditions. The BCRP topology depends on the coverage conditions, and the protocol is executed when an inefficient coverage level is detected. Different applications may require different coverage levels. For example, battlefield monitoring may require full-area coverage, in which at least one sensor node must covers each location. Full coverage provides the best surveillance quality, but some applications (such as temperature and forest re-application moni-

toring) require only partial coverage (at least ¸ percent of the entire area) [Zhu 2012]. In the BCRP, partial coverage lowers the number of required sensor nodes in the deployment area, thereby reducing the node energy consumption and extending the network lifetime. The topology-changing conditions need to be detected to ensure efficient coverage of the network. In the existing works, coverage holes are detected by probabilistic coverage, perimeter coverage and cross-area coverage.

A sensing model is uniquely characterized by its sensing range, resolution and accuracy. The sensing area is determined by several factors: the strength of the signals generated at the source, the source-to-sensor distance, the propagation attenuation rate, and the desired confidence level of the sensing.

In BCRP, perimeter-coverage is used by each mobile sink to detect the coverage level of its Voronoi polygon (as proposed in [Huang 2005]), illustrated in Figure 5.4. The detection result determines whether the perimeter of the considered sensor is sufficiently covered or not. The perimeter-coverage is defines in Definition 4. A correct answer is obtained by collecting the coverage information from all sensors. Perimeter coverage is also applicable to irregular (non-circular) sensing regions [Huang 2005].

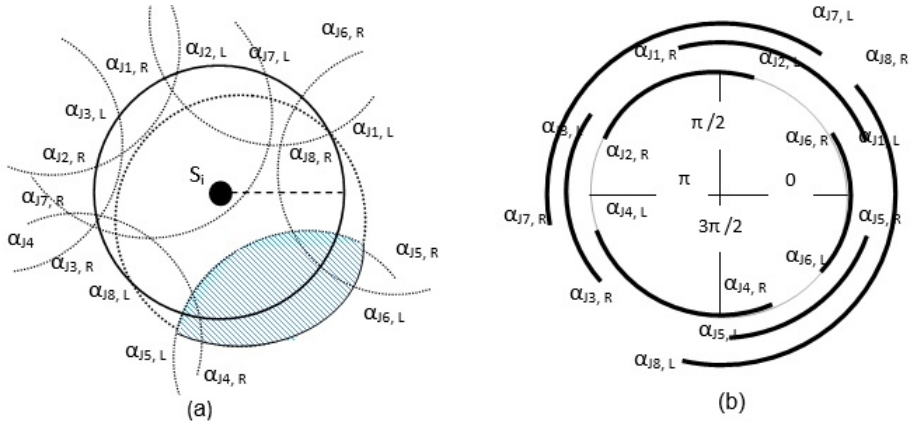

Figure 5.4: (a) The segment covered by s_j of s_i's perimeter and b) coverage of the s_i perimeter.

Definition 4: For any two nodes s_i's and s_j's, a point on the perimeter of si is perimeter-covered by s_j if it locates within the sensing range (r_s) of s_j.

The distance between two sensors s_i and s_j located at positions (x_i, y_i) and (x_j, y_j) respectively is given by:

$$d(s_i, s_j) = \sqrt{|xi - xj|^2 + |yi - yj|^2} \tag{5.1}$$

If the distance exceeds $2r_s$, s_j covers no part of s_i's perimeter. Otherwise, s_j covers a certain range of s_i's perimeter. Let $y_i = y_j$ and $x_i > x_j$. The angle α is computed as follows

$$\alpha = arccos(\frac{d(s_i, s_j)}{2r}) \tag{5.2}$$

Thus, the arc of s_i within the range $[\pi - \alpha, \pi + \alpha]$ is *perimeter-covered* by s_j.

When the detected coverage level is low, the mobile sink executes the relocation algorithm in Section 1.3.5.2, which determines the distance and angle of the required movement. If the coverage level is zero, the mobile sink remains stationary.

As mentioned previously, some coverage may be lost by random deployment and depletion of nodes in the network. When the nodes are randomly deployed, the coverage holes may be difficult to detect. The mobile sinks in BCRP are assume to have better capability and longer communication and sensing ranges than the normal network nodes.

5.3.4.2 Rule 2: Relocation Algorithm

Once a coverage hole is detected, the mobile sink will move towards and gather information from the coverage-hole area. However, as the central and global information is lacking, its mobility (distance travelled and orientation angle) must be assisted by other participants.

BCRP determines the mobility of a mobile sink by vector-based mechanisms, as proposed in [Sahoo 2010]. In addition, to ensure that the newly planned position (relocation) benefits the existing network, BCRP runs the verification and consensus modules explained in Sections 5.3.4.2 and 5.3.7, respectively.

Definition 5: *Close-worker* and *Co-worker*. Nodes S_i and S_j are *Close-workers* if $0 < d_{ij} \leq 2r_s$, and co-workers if $2r_s < d_{ij}$ r_s, where d_{ij} is the physical distance between the two nodes.

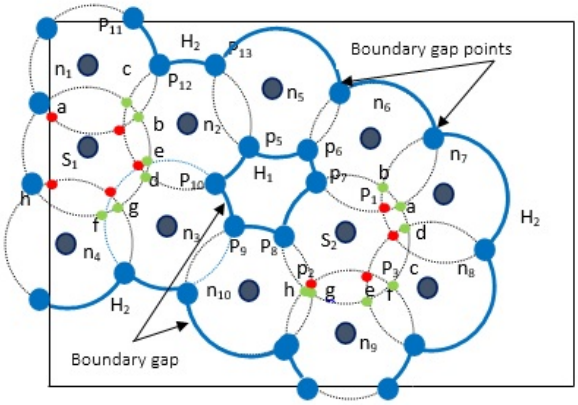

Figure 5.5: Coverage holes (open and close holes) in a random node deployment.

Definition 6: *Critical points* are the points of intersections of a source node (S) sensing disc with each of its connecting neighbours (*Close-workers*) sensing disc or with boundary of the monitoring region, called critical points of S. In Figure 5.5, p_1-p_4 are critical points for S_2.

Definition 7: Boundary gap points (p_{gp}) are the points of intersection of S sensing disc, with its connecting neighbours *Close-worker* sensing disc, S_i or with the boundary of the monitoring region. The boundary gap point (p_{gp}) is the point that lies only on the sensing disc of S_i and S or on the monitoring region's boundary. A boundary gap is the arc that is formed by joining the consecutive boundary gap points. For example, p_7 and p_8 in Figure 5.5 are the boundary gap points of S_2.

The S then connects its own location to the p_{gp} such that the head of the vector points towards a p_{gp}. The polygon laws of vector addition is then used to calculate the result vector upon constructing the vectors from the source node (mobile sink) to each of the p_{gp}.

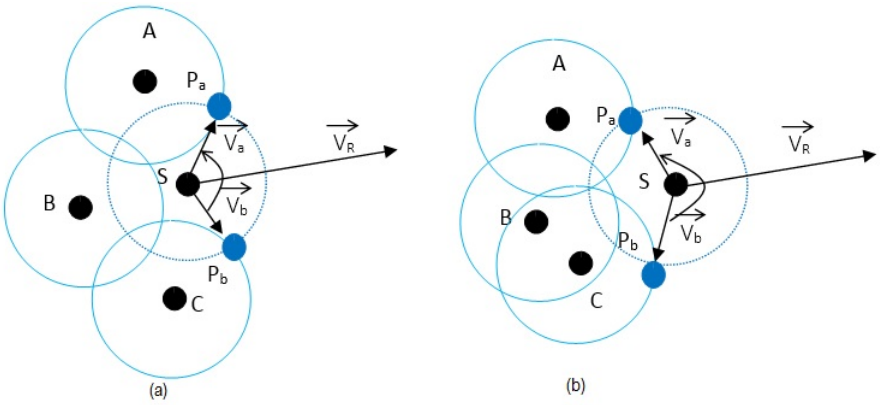

Figure 5.6: Determining angle of boundary gap.

Figure 5.6 demonstrates the angle of a boundary gap. In this figure, p_a and p_b are the boundary gap points of the source node S. Let, (x,y), (x_a, y_a), and (x_b, y_b) be the coordinates of S, p_a and p_b, respectively. From the distances between the source node S and p_a and p_b, we construct the boundary gap (θ) and $\overrightarrow{V_a}$ and $\overrightarrow{V_b}$. The vectors are calculated as follows:

$$\overrightarrow{V_a} = (x_a - x)\overrightarrow{i} + \overrightarrow{j} \tag{5.3}$$

$$\overrightarrow{V_b} = (x_b - x)\overrightarrow{i} + (y_b - y)\overrightarrow{j} \tag{5.4}$$

The resultant vector $\overrightarrow{V_R}$ is then computed by adding vectors $\overrightarrow{V_a}$, $\overrightarrow{V_b}$ using the triangle law.

Several strategies for relocating a mobile node have been proposed in the literature. In force-based mechanisms, the nodes are pushed from or pulled to a new location with higher or lower energy or coverage level than the current location, respectively . In the mechanism of [Wang 2006], the sensor moves to the midpoint between its current and target locations, provided that the move increases its local coverage. Alternatively, Wang et al. proposed a step-by-step movement of the sensor towards the coverage hole. Here, the maximum moving distance could not exceed one-half of the difference between the communication range and the sensing range.

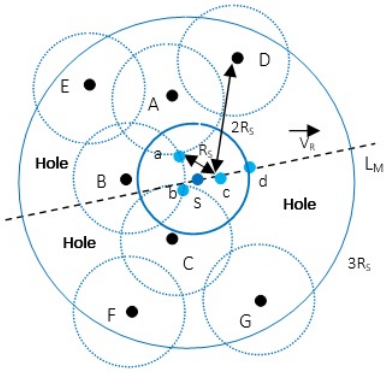

Figure 5.7: Finding the mobility distance of a mobile sink S.

In BCRP, the moving distance is calculated by the method of [Sahoo 2010]. The mobility-distance calculation of a mobile sink S is demonstrated in Figure 5.7. a and b are the critical points of S and $\overrightarrow{V_R}$ is the resultant vector which is determined using a resultant-vector construction algorithm. L_M is the equation of the straight line along $\overrightarrow{V_R}$, which passes through position S. All possible distances between S and its critical points are computed as follows:

1. The furthest critical point from S is determined (i.e., a).
2. A point on L_M (let say point c) is identified from a, so that $|ac| = r_s$ units.
3. Identify the nearest co-worker (i.e.,D) of S.
4. Mark a point (d) on L_M from D, such that $|Dd| = 2r_s$ units.
5. Determine the lesser of |Sc| or |Sd|.
6. The mobility distance of S is the minimum of (|Sc|, Sd|).

In Figure 5.7, the mobility distance of S is |Sc|.

5.3.5 Verification Module

Upon receiving a relocation request (a new location and angle as described in Section 5.3.4.2), the neighboring mobile sinks will individually determine the appropriateness of the new location based on the pre-agreed rules. A valid relocation position will be accepted and propagated, whereas an invalid one will be rejected. The

accepted information will be updated by each participant, meaning that each participant gains the updated version of all other participants. The verification module in BCRP ensures that moving to the new location will benefit the surrounding area. As moving a mobile sink incurs several costs (the communication cost of setting up a new partition or region, notifying the node changes in each region, and adjusting the relocations between mobile sinks), the relocation request needs to be verified by the surrounding mobile sinks. Algorithm 5.2 implements the sequence of rules followed by each mobile sink when verifying a relocation request.

Algorithm 5.2 Relocation Verification Rules

Input: Location, coverage level, relocation position
Output: Relocation Position Verification Results (Vote)
for *For each round* **do**
    if *Receive relocation request* **then**
        Check request relocation position (see Section 5.3.4.2)
        if *Redundancy Check idle* **then**
        end
        Send positive vote to request mobile sink
        Send Agreed Location
    end
    else
        Send Negative Vote
    end
end

Wait for consensus result: 1. consensus idle 2. consensus adjusted

Whenever a mobile sink is requested to relocate (move to a new location), its new location will be verified by the other participants. This module asks the mobile sinkâs neighbours participating in the voting to agree or disagree with the relocation. Based on the rules, the participating mobile sinks will send their results to the requesting mobile sink. In the verification module, the neighbouring mobile sinks consent to a request if the new location will not occupy a fully redundant area.

5.3.5.1 Redundancy Mechanism

In BCRP, the redundancy is a verification factor that determines the decisions of other mobile sinks. Redundancy checking ensures that the proposed location

(the new location calculated by the requesting mobile sink) is appropriate and non-overlapping with the regions of other mobile sinks, and that the movement is not unnecessary (as moving to a redundant location already covered by other mobile sinks will not improve the performance of the network). [Cărbunar 2006] proposed a redundancy elimination algorithm that reduces the number of redundant nodes. [Zhang 2005] minimized the overlapping area by controlling the density of WSNs.

Existing redundancy checks adopt several sensing disc coverage models based on geometric properties. These models include sponsor sectoring [Tian 2003], crossing coverage [Xing 2005], and Voronoi vertices and intersections [Cărbunar 2006]. Figure 5.8 demonstrates the coverage by Voronoi vertices and intersections for redundancy checking in BCRP. This redundancy check uses the approach of [Cărbunar 2006], to detect and eliminate the redundancy to improve the energy efficiency though preserving the network coverage. They assigned the covered nodes as redundant nodes that can be inactivated. In contrast, if the new location is redundant in BCRP, the request will be rejected by the participating mobile sinks.

BCRP follows the definition of sensor's coverage in [Cărbunar 2006] when determining the coverage of a sensor (Definition 8). The following definitions are applied when assessing a node as redundant or viable.

Definition 8: The coverage of a sensor s_i at location *(x, y)* and sensing range r is a disc of radius r_s centred at *(x, y)*. This disc is called the coverage or sensing disc. Its border is called the coverage or sensing circumcircle. A point p is covered by sensor s_i if $dist(s, p) \leq r$ and the union of all sensors coverage disks represents the coverage of the network.

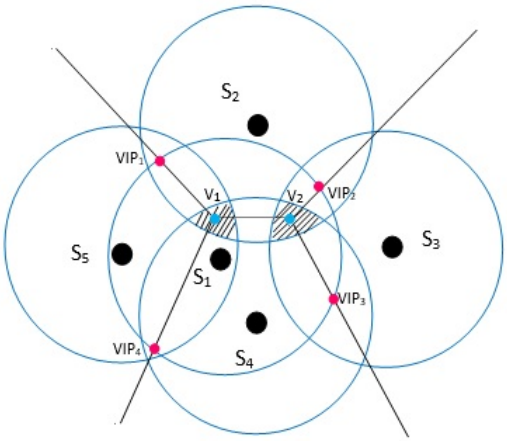

Figure 5.8: Example of a redundant sensor, s_1: points v_1, and v_2 are Voroni vertices of s_1, and $VIP_{1...4}$ are the Voronoi intersection points of s_1. Note that v_1 and $VIP_{1...4}$ are all covered by at least two Voronoi neighbours of s_1.

In BCRP, the new location is verified by the neighbours of the mobile sinks. If the new location is evaluated as redundant, the neighbouring mobile sink declines the movement, i.e. computes a negative vote. When deciding whether the new location is redundant or not, the definition given by [Cărbunar 2006] below is referred.

Definition 9: The Voronoi diagram of a sensor s_j is the Voronoi diagram of the Voronoi neighbours of s_j, excluding s_j itself. The Voronoi vertices (VV) of sensor s_j are the Voronoi vertices of the Voronoi diagram of s_j. A Voronoi intersection point (VIP) of s_j defines the intersection between an edge of the Voronoi diagram of s_j and the coverage circumcircle of s_j. A Voronoi edge (VE) of s_j is either a Voronoi edge between VIPs of s_j, or a Voronoi edge between a VV and a VIP of s_j.

In Figure 5.8, there are one VV (i.e., VV_1) and three VIPs (VIP_1, VIP_2, VIP_3). The redundancy rule by Voronoi diagram vertices and intersections is: s_1 is redundant if all the VVs and VIPs of a sensor s are covered by the Voronoi neighbours of s_1. In Figure 5.8, 2-Voronoi vertices and 2-VIPs and 2-VEs are covered by each sensor s_i that generates them (i.e., the voronoi neighbour of s_1 completely cover the partition associated them).

5.3.6 Force-based Mechanism

This module checks the distances between the new location and the other mobile sinks. To avoid the new location being too close or too far from the other mobile sinks, the BCRP balances the requested position of the mobile sink with the positions

of the surrounding mobile sinks by a force-based mechanism, a popular choice for solving coverage hole problems [Khou 2017]. In BCRP, the force-based mechanism enables a fair distribution with maximum coverage area of the multiple sinks in the network. The force-based mechanism balances the location partitioning of the sinks . A request for a topology change is assessed by a pre-agreed rule, which is implemented in all mobile sinks. The force-based mechanism in BCRP pushes two mobile sinks apart when they approach too closely, mimicking the actions of same-charged electromagnetic particles. Let, $d(s_i, s_j)$ be the distance between two sensors s_i and s_j, which equals d_{avg} on average. The virtual repelling force between s_i and s_j separates them by a distance $(d_{avg} - d(s_i, s_j)/2$. Forces are also exerted by the field boundary, denoted as $\overrightarrow{F_b}$. The virtual force exerted by s_j on s_i, denoted as $\overrightarrow{F_{ij}}$, acts from s_j to s_i. When a sensor approaches too close to the boundary, it is pushed inward by a distance $d_{avg}/2 - d_b(s_i)$, where $d_b(s_i)$ is the distance between s_i and the boundary. The overall force on s_i is the vector summation of the virtual forces from the boundary and all Voronoi neighbours.

5.3.7 Consensus Module

Before a new datum or transaction becomes part of the consensus-agreed ledger, it must be validated by some or all participants, depending on the network setup. In some private distributed-ledger networks, a subset of the participants rather than the entire ledger is sufficient for a consensus result. For example, a transaction may be invalid unless approved by at least three participants; that is, the new information is valid only when agreed by the relevant participants or by a majority of the participants. In other applications, a transaction involving certain assets (such as a central bank signing cash transactions) need only be signed by a specific portion of the participants.

Consensus is essential for the proper functioning of a blockchain, which determines the conditions to be reached in a distributed network without central authorities, and among participants who may not trust each other. Several authors have compared the consensus algorithms applied in permissioned and permissionless blockchains [Bano 2017], [Fernández-Caramés 2018]. Consensus mechanisms ensure the integrity of the information contained in the blockchain while defending against

double-spend attacks; hence they are an essential part of blockchain technology [Cachin 2017], [Baliga 2017], and [Tschorsch 2016]. Several alternative consensus methods are reviewed in [Fernández-Caramés 2018]. The practical Byzantine fault tolerance (PBFT) algorithm solves the Byzantine General Problem by consensual agreement in asynchronous environments [Castro 1999]. PBFT assumes that less than one third of the nodes are malicious. It accepts a decision when supported by at least 2/3 of all nodes, which must be known to the network. The stellar consensus protocol (SCP) implements a consensus method called federated Byzantine agreement (FBA) [Mazieres 2015]. The SCP is similar to PBFT, but whereas every node in PBFT queries all other nodes and waits for a majority agreement, only a subset of the participants (the important participants) reach consensus in SCP.

The participants in BCRP are the mobile sinks deployed in the network. In many WSN applications, these participants are distributed randomly, meaning that some participants are directly connected while others are indirectly connected via other intermediate participants. The information is imparted to all participants via broadcasting. In a large WSN network, obtaining consensus from all mobile sinks in the network is impractical, because of the large distance and uncertain nature (including physical obstacles) of the distributed network. In such situations, consensual agreement among all participants in the network is impossible. Instead, a certain number of verifications and approvals from neighbouring mobile sinks is required, and the decision of the involved participants is based on a distributed ledger (i.e. pre-agreed rules). In a large network, not all of the participants are required to verify, approve or reject a request sent by a mobile sink. Instead, a mobile sink is relocated after its request receives a certain percentage of positive votes. Moreover, 100% approval from all nodes would cause delays and incur high energy and other costs.

When verifying a request, the voting mobile sinks will check whether the requested location is appropriate or not. The appropriateness is decided by the two rules specified in the verification module. If most of the mobile sinks return a positive vote (agreement), the request is permitted and the requesting mobile sink will broadcast its decision. The other mobile sinks then update the information and broadcast it to other members.

5.4 Simulation Results

This section demonstrates the performance of the proposed blockchain-based routing protocol (BCRP) in terms of the five measures: number of dead nodes, energy consumption, delay, packet delivery ratio and percentage of coverage holes. The performances of different sink deployments, namely, static sinks, a single mobile sink, and multiple mobile sinks are compared, to observe the effect of sink deployment on the network performance. The simulations were conducted to observe the effect of varying the parameters: the number of mobile sinks was varied from 1 to 10, the number of normal nodes from 100 to 350, and the network size from 200 m^2 to 500 m^2. The performance of BCRP is then compared with those of existing protocols (random walk, GMRE and ETARP). BCRP adopts the energy dissipation model of [Anand 2016]. In BCRP, each node in BCRP is assigned an initial energy of 50 Joules, and its communication radius is 60 metres. The data packet size is set to 15 bytes and the effective coverage range of normal nodes is 30 metres. These values were chosen because they are commonly referenced in the literature.

5.4.1 Performance comparison of single static, single mobile sink and multiple sinks implementations

5.4.1.1 Considering different number of mobile sinks

This subsection presents the performance of BCRP and compare its implementation when single static sink, single mobile sink and multiple mobile sinks are considered.

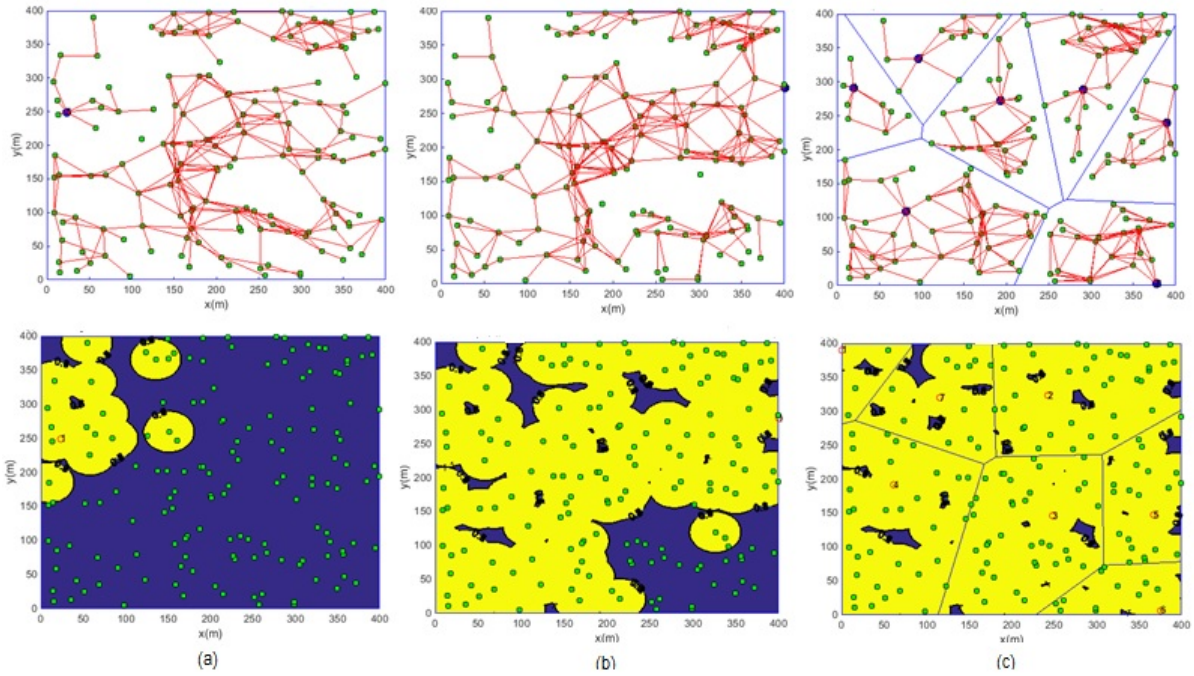

Figure 5.9: Coverage holes when deploying a) a single static sink, b) single mobile sink and c) multiple mobile sinks. The parameters are as follows: number of normal nodes (NN) = 250, number of mobile sinks (MS) = 1 to 10, area = $400m^2$.

Panels a to c of Figure 5.9 show the communications among the nodes in the network (top images), and the area coverages of the mobile sinks (bottom images). The network is partitioned into several regions, with one mobile sink in each region. The multiple mobile-sink deployment achieves the highest network coverage.

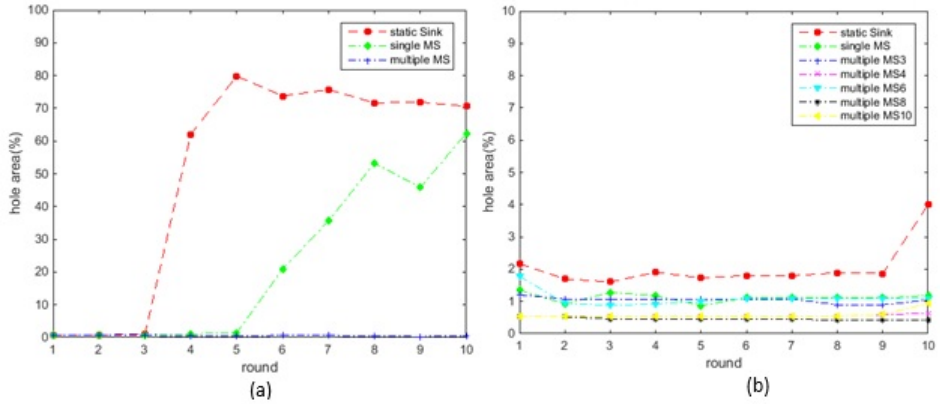

Figure 5.10: Coverage holes in the networks deploying a single static sink, a single mobile sink and multiple mobile sinks.

Figure 5.10a compares the percentages of coverage holes detected in networks utilising a static sink, a single mobile sink and multiple sinks. Deploying a single mobile sink in the network achieves higher coverage than the single sink deployment.

The high percentage of holes in the network with static sink deployment might be caused by node depletion and the non-uniform distribution of the random deployment (as a static sink cannot move to an uncovered area and gather its data). When multiple mobile sinks were deployed, the network was well covered with a small percentage of coverage holes. Figure 5.10b shows the percentages of the coverage holes in networks with different numbers of mobile sinks. Most of the network was covered when 8 or 10 mobile sinks were deployed. The percentages of coverage holes only slightly differed among the networks with fewer mobile sinks (1, 3, 4 and 6), but were consistently lower than in the static-sink network.

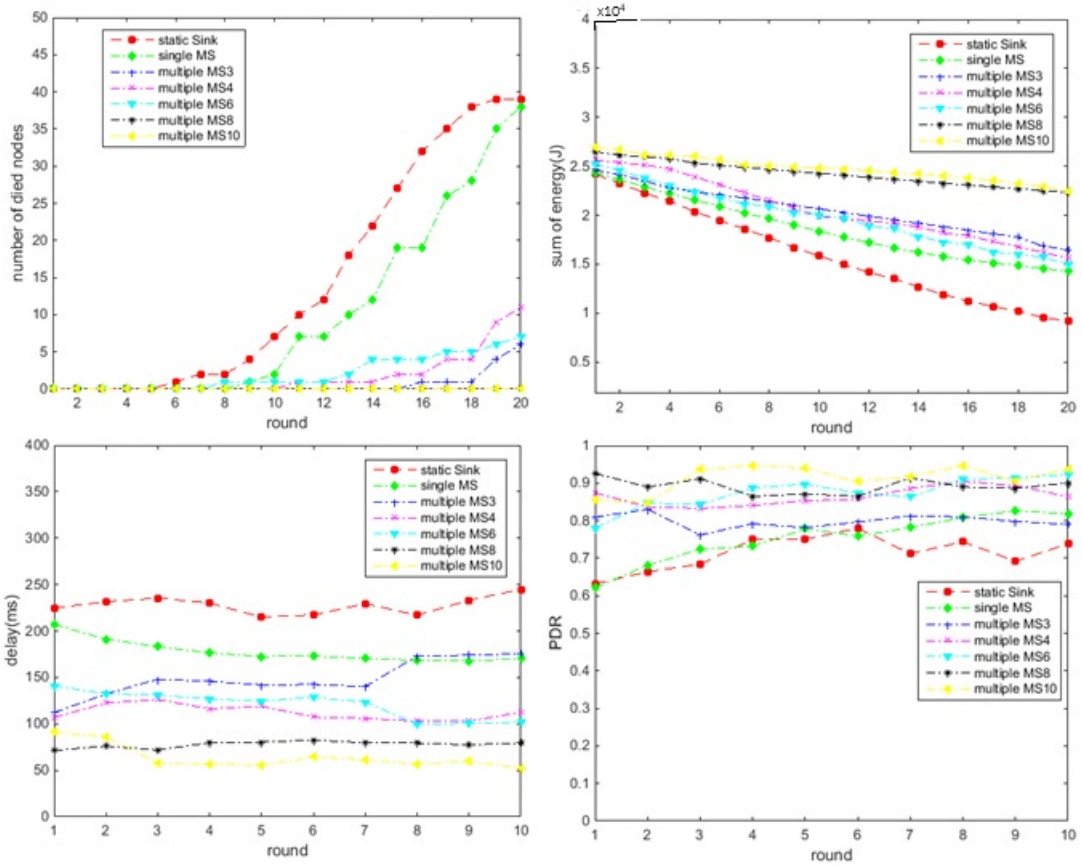

Figure 5.11: Number of dead nodes (top left), energy consumed (top right), delay (bottom left) and packet delivery rate (bottom right) in networks with a single static sink, a single mobile sink and multiple mobile sinks (3, 4, 6, 8 or 10). Here, NN = 250 and the area is 400m^2.

Figure 5.11a plots the evolution of the number of dead nodes in networks with a single static sink, a single mobile sink and multiple mobile sinks. The lowest number of dead nodes increased with network lifetime. In a network deploying random walks, the number of nodes began depleting at Round 6 and continually

decreased thereafter. In single mobile sink deployment, the start of node depletion was delayed to Round 9. The viable node performances of the protocols (from best to worst) were 10 MS > 3 MS > 6 MS > 4 MS > 1 MS > Static. The number of dead nodes did not significantly differ in the networks with 3, 4 and 6 mobile sinks, but was markedly reduced after deploying 10 mobile sinks. The multiple-sink networks achieved higher overall performances than the networks deploying a single static sink and a single mobile sink (as confirmed by the fewer number of dead nodes in the multiple-sink deployment). Figure 5.11b plots the summed energy in networks with different deployments of mobile sinks. Deploying a large number of mobile sinks (8 or 10) reduced the energy consumption of the network. Again, slight differences were observed in the networks deploying 3, 4 and 6 mobile sinks. The static sink deployment consumed the most energy, followed by the single mobile sink deployment. Moreover, the delay was high in the static- and single-mobile sink deployments, and was reduced by deploying many mobile sinks (8 to 10; see Figure 5.11c). This result might reflect the shorter required travel distance of the packet when deploying one static sink or few mobile sinks (meaning that the sink is reached after fewer hops). As shown in Figure 5.11d, more packets were successfully delivered in the multiple mobile-sink deployment. When multiple mobile sinks are deployed, the normal nodes need to only report to their nearby mobile sink. Deploying more mobile sinks divides the network into smaller areas, in which each mobile sink communicates with its close surrounding nodes. The high packet delivery rate in the many mobile-sink deployment relates to the less frequent use of the same nodes, as the relay-packet load to the sinks is distributed more fairly and is more balanced. Consequently, the node depletion (which is directly responsible for packet drop) is reduced.

5.4.2 Performance results of networks with different parameter values

5.4.2.1 Changing the number of normal nodes

This section compares the number of dead nodes, energy consumption, delay, packet delivery rate and percentage of coverage holes in networks with different numbers of nodes (ranging from 100 to 350). Here, the network area was 400 m^2, and the

number of mobile sinks was fixed as 7.

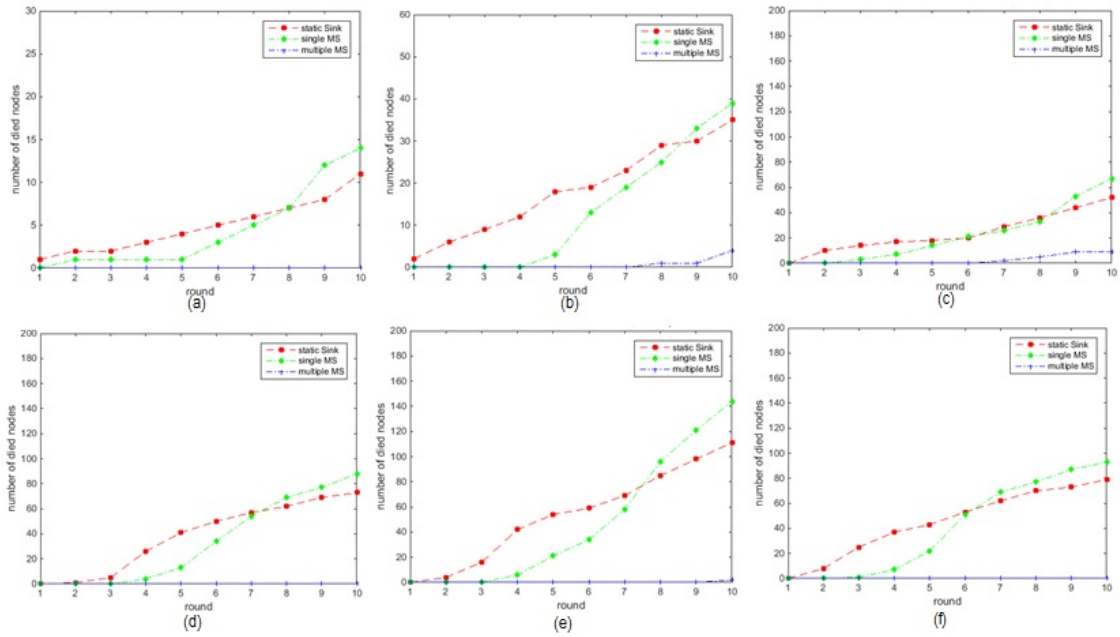

Figure 5.12: Number of dead nodes in networks deploying a single static sink, a single mobile sink and multiple mobile sinks with different network densities: a) 100, b) 150, c) 200, d) 250 nodes, e) 300 nodes and f) 350 nodes.

Panels a to f of Figure 5.12 plot the numbers of dead nodes in networks of different node densities deploying a single static sink, a single mobile sink and multiple mobile sinks. The number of nodes was varied from 100 to 300. In a randomly deployed network, nodes may die from several causes, such as energy depletion after frequent use of the same nodes, high communication cost when the source and sink are far apart, and physical destruction. In networks deploying a single static sink, the nodes around the sink are frequently used because the sink is spatially fixed, meaning that packets tend to be relayed through the same route. The number of dead nodes increased in later rounds, and (in the networks utilising the single static and single mobile sinks) with increasing number of deployed nodes. However, no dead nodes were observed in the network deploying multiple mobile sinks, even after 15 rounds. For a given node density (number of normal nodes in the network area), there was no significant difference between deploying a single mobile sink or a single static sink.

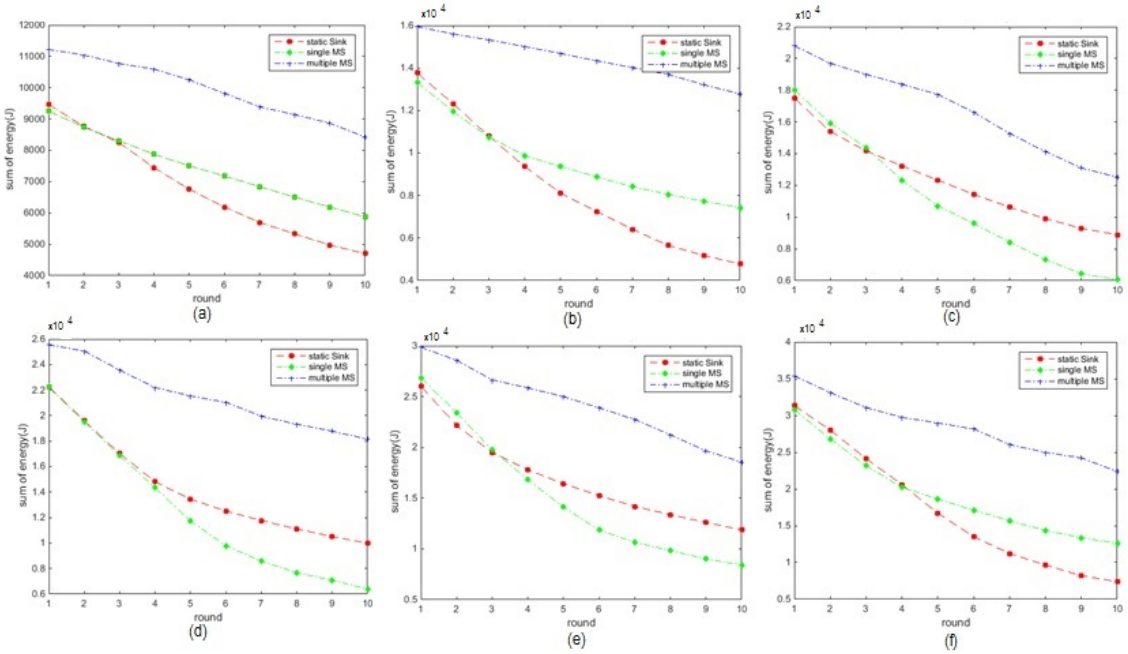

Figure 5.13: Summed energies when deploying a single static sink, a single mobile sink and multiple mobile sinks with different network densities: a) 100, b) 150, c) 200, d) 250 nodes, e) 300 nodes and f) 350 nodes.

Panels a to f of Figure 5.13 show the total energy consumed by networks with different node densities deploying a single static sink, a single mobile sink and multiple mobile sinks. Regardless of density, the network with multiple mobile sinks was more energy efficient than the other two networks. In less dense networks, the static sink deployment consumed more energy than the single mobile-sink deployment. However, when the node density increased, the energy consumption was higher in the network with the single mobile sink than in the network with the single static sink. In the high-density network (with 300 nodes), the network with the single static sink was more energy-efficient than the network using a single mobile sink. This reversal may be explained as follows. Because many nodes participate in the communication through a large network, the single mobile sink might incur high energy overheads in the frequent information exchanges (updating, requesting, and acknowledging of new locations). In some situations however, the energy overheads in the network with single static node is higher because more hops were involved.

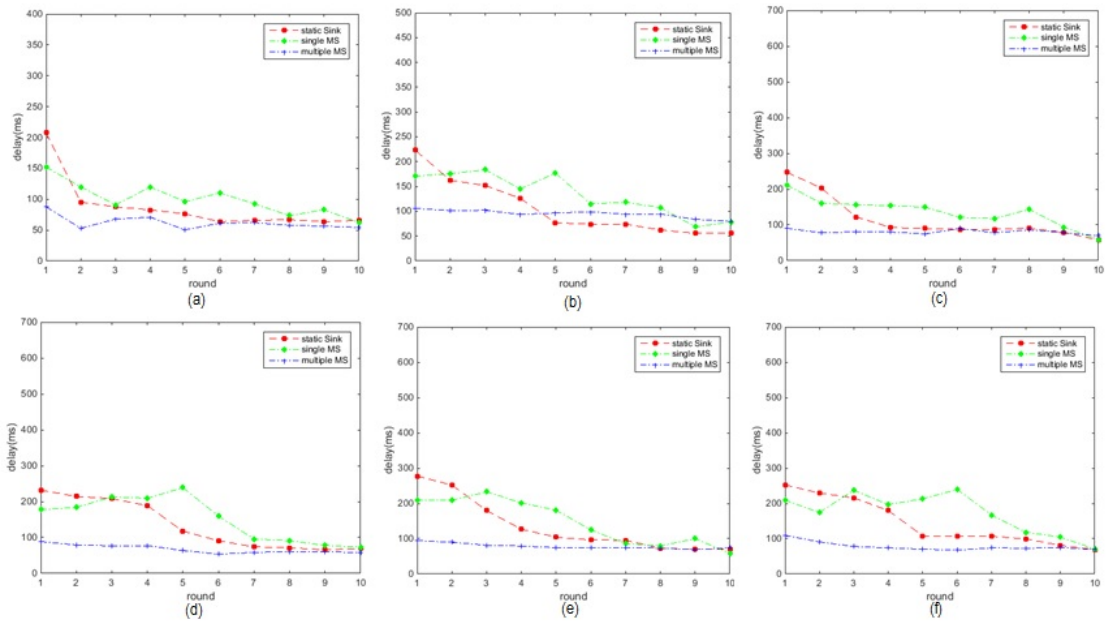

Figure 5.14: Delays in networks with different node densities deploying a single static sink, a single mobile sink and multiple mobile sinks: a) 100, b) 150, c) 200, d) 250, e) 300, and f)350 nodes.

Figure 5.14 shows the delays observed in networks with different node densities deploying a single static sink, a single mobile sink and multiple mobile sinks. In the multiple mobile-sink deployment, the delay was almost independent of network density, and smaller than in the other deployments at any network density (100 to 300 nodes). The lower and better balanced delay in the network with multiple mobile sinks than in the networks with a single static sink and a single mobile sink can be explained by the closer communication between the source and destination, as each node needs only to communicate with its own mobile sink. In the network utilising a single mobile sink, the delay is increased because the nodes must wait until the mobile sink is close enough for packet delivery. Meanwhile, the delay in static sink deployment is caused by the fixed distance between the (randomly located) source and the sink. Some sources will be located far from the sink.

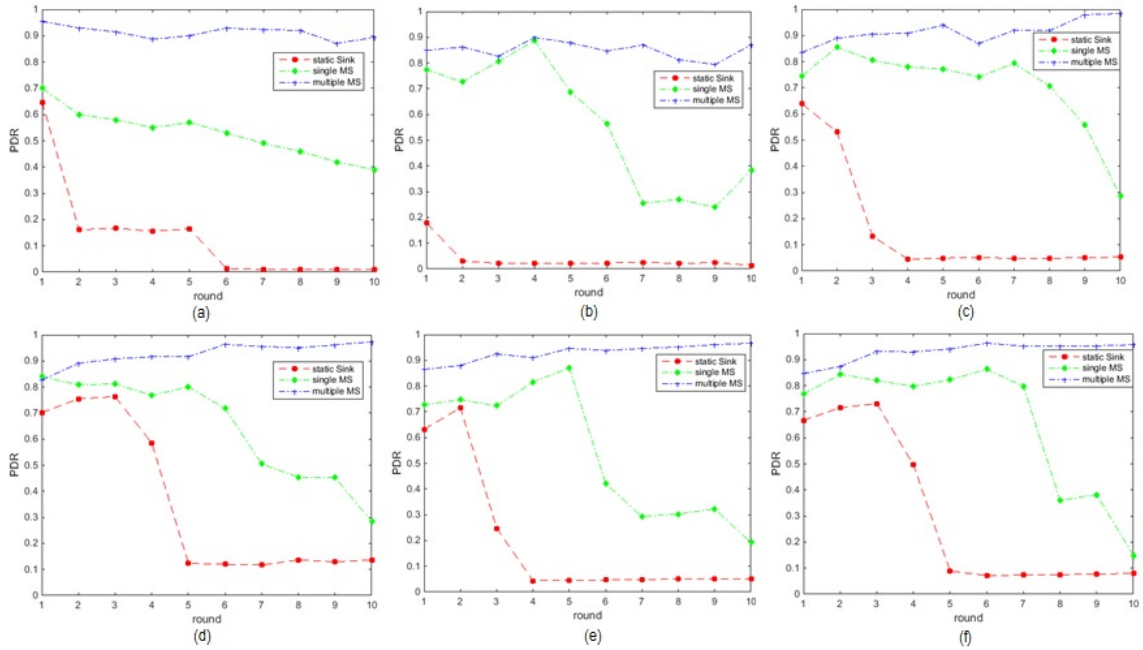

Figure 5.15: Packet delivery ratio in networks with different node densities deploying a single static sink, a single mobile sink and multiple mobile sinks: a) 100, b) 150, c) 200, d) 250 nodes, e) 300 nodes and, f) 350 nodes.

Figure 5.15 shows the packet delivery rates in the networks with different node densities and deployment configurations. The network with multiple mobile sinks provides a consistent packet delivery at all network densities. Because the single mobile sink moves randomly, the packet delivery rate in this deployment is little affected by the network density. In the single static-sink deployment, the packet delivery rate remained low in low-density networks, but was high in the initial stages of packet delivery in the high-density network. After 5 rounds, the packet delivery rate dropped, probably because of node depletion around the static sink or the frequent use of the nodes between the source and the sink.

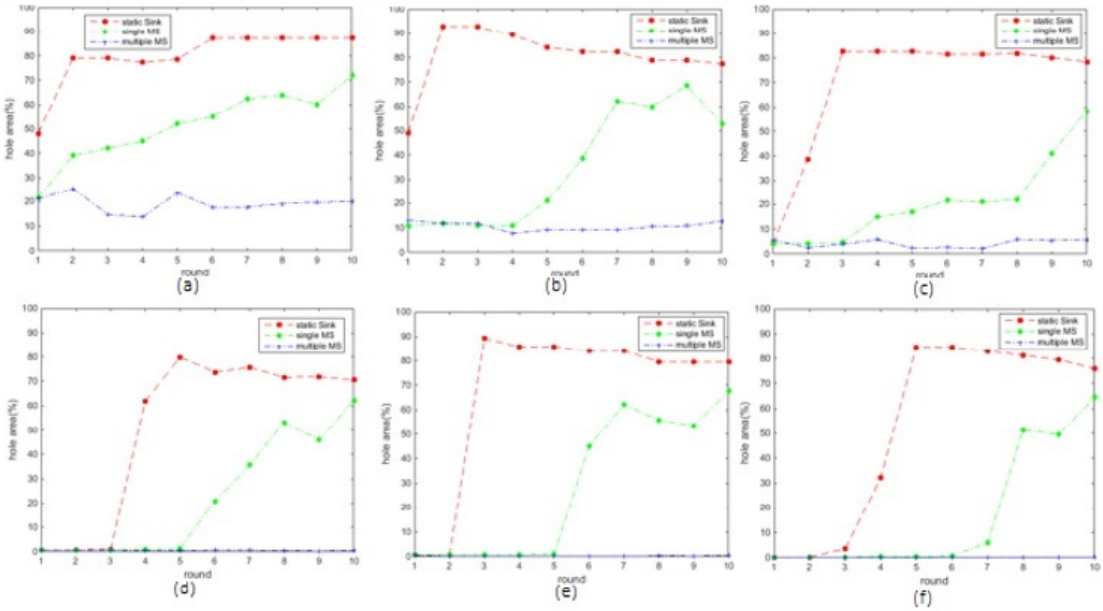

Figure 5.16: Coverage hole in networks with different node densities deploying a single static sink, a single mobile sink and multiple mobile sinks: a) 100, b) 150, c) 200, d) 250 nodes, e) 300 nodes and, f) 350 nodes.

Figure 5.16 shows the percentage of coverage holes in networks with different node densities in the single-sink, single mobile-sink and multiple mobile-sink deployments. The percentage of holes in the network deploying the single static sink was consistently high. As all nodes (sinks and normal nodes) are static (remain at the same position), the network coverage cannot be improved. The percentage of holes was also high in the network with a single mobile sink, although the coverage lack was less severe than in single static-sink deployment. In the network with multiple mobile sinks, holes were observed in the small networks (100 to 350 nodes), but the coverage holes were reduced in networks covered with more nodes (when each area in the network was serviced by a nearby mobile sink).

5.4.2.2 Varying the network size

This subsection presents the performance of network in three different network size (200 m_2, 300 m_2, and 500 m_2). Figure 5.17 shows the number of dead nodes in the three network deployment (single static, single mobile sink, and multiple mobile sinks). In Figure 5.17a, more nodes depleted in the network consisting single static sink after Round 5. Nodes start to deplete at later round (Round 9) in the network with single mobile sink. No node die during the 10 rounds in the network with

multiple mobile sinks. Number of dead nodes increases when larger network is considered in a single static sink and single mobile sink. The nodes in the network with multiple mobile sinks start to deplete when the network area is larger ($500m^2$). However, the number of dead nodes is very small compared to the other two. The nodes in the network with a single static sink and single mobile sink deplete earlier when the network size increases to ($500m^2$). The number of nodes with multiple mobile sinks deplete drastically in this area.

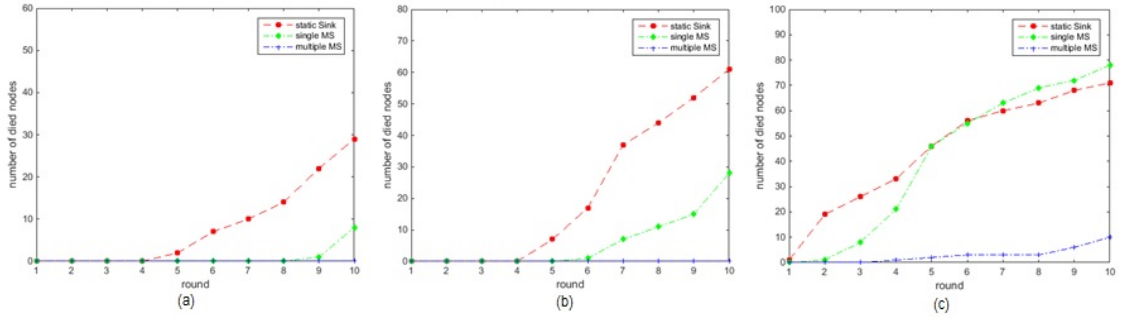

Figure 5.17: Number of dead nodes in networks deploying a single static sink, a single mobile sink and multiple mobile sinks: NN = 250, MS = 7, Area: a) $200m^2$, b) $300m^2$, and c) $500m^2$

Figure 5.18 shows the energy consumption in the network deploying a single static sink, a single mobile sink, and multiple mobile sinks in three different network sizes. The smaller the area, the less energy is consumed in all the three sink deployment type. In all the three cases (the three different network area), the least energy is consumed by the multiple mobile sinks, followed by the single mobile sink. The energy consumes in the single static sink is much higher compared to the other two.

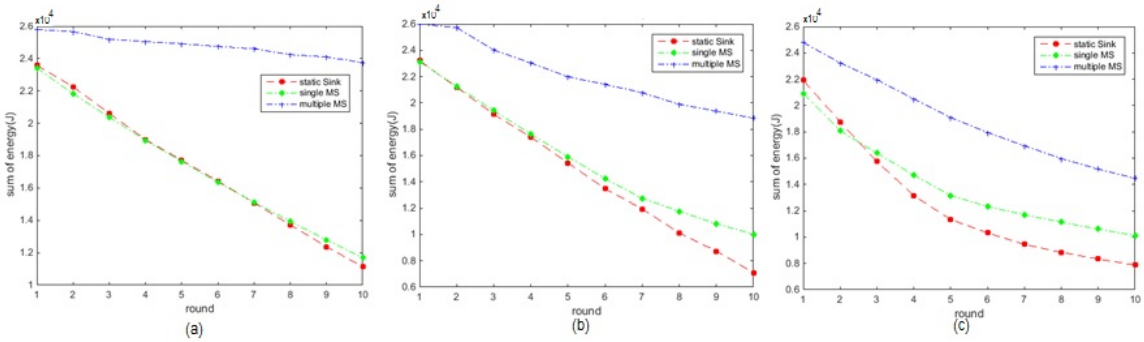

Figure 5.18: Summed energy consumption in networks deploying a single static sink, a single mobile sink and multiple mobile sinks: NN = 250, MS = 7, Area: a) $200m^2$, b) $300m^2$, and c) $500m^2$

In Figure 5.19, the delay in the networks deploying a single static sink, a single mobile sink and multiple mobile sinks: NN = 250, MS = 7, Area: a) $200m^2$, b) $300m^2$, and c) $500m^2$ are presented. More delay exists in larger network size. The least delay is observes in the network with multiple mobile sinks. The high delay in network with a single static sink is due to the larger distance between nodes and the sink. The delay in network consisting single mobile sink is slightly higher than the single static sink, as the mobile sink needs to move more to cover the larger network. The delay in the network with multiple mobile sinks is consistently low during all the 10 rounds.

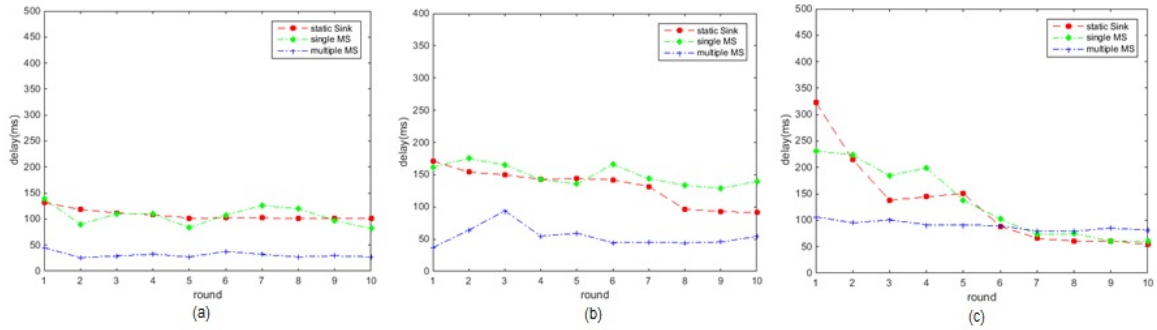

Figure 5.19: Delay in networks deploying a single static sink, a single mobile sink and multiple mobile sinks: NN = 250, MS = 7, Area: a) $200m^2$, b) $300m^2$, and c) $500m^2$

A higher packet delivery ratio is observes when multiple mobile sinks are deployed, as shown in Figure 5.20. Poor packer delivery ratio is observes when the network deploys a single static sink in a larger network size ($500m^2$).

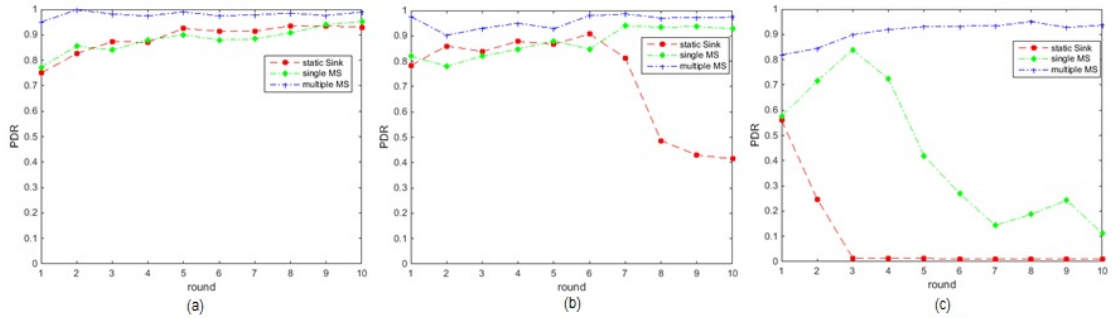

Figure 5.20: Packet delivery ratio in networks deploying a single static sink, a single mobile sink and multiple mobile sinks: NN = 250, MS = 7, Area: a) $200m^2$, b) $300m^2$, and c) $500m^2$

Figure 5.21 shows the coverage hole in networks deploying a single static sink, a single mobile sink and multiple mobile sinks in different network size. In Figure

5.21a, in the smaller area ($200m^2$) with 250 nodes, the network is densely covered. Thus, the no coverage hole detected in all the three deployment type (i.e., coverage level is higher than coverage threshold value). Coverage hole is detected when a single static sink is deployed in a larger network area ($300m^2$) Figure 5.21b. In Figure 5.21c, the highest coverage hole is observes in single static sink. The coverage hole was detected after several rounds in single mobile sink and it is gradually increased. A small coverage hole detected in the network deploying multiple mobile sinks.

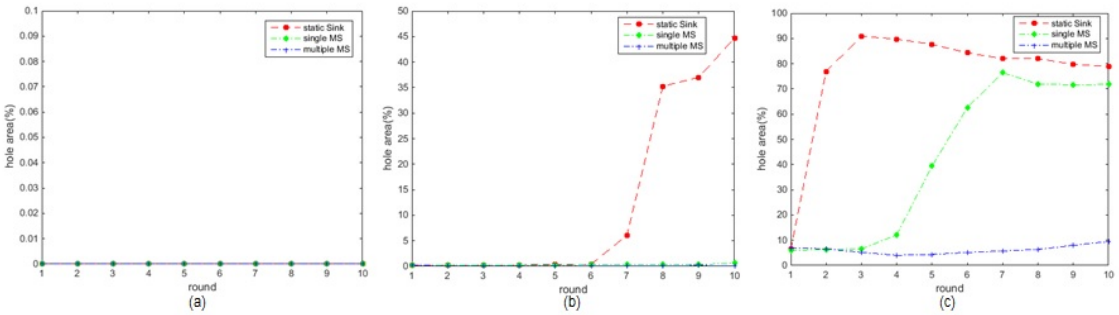

Figure 5.21: Percentage of coverage hole in networks deploying a single static sink, a single mobile sink and multiple mobile sinks: NN = 250, MS = 7, Area: a) $200m^2$, b) $300m^2$, and c) $500m^2$

5.4.3 Consensus consideration in BCRP

This subsection presents the network performance with and without consensus considerations. Figure 5.22 illustrates the coverage existence in the network with and without consensus among mobile sinks in the network. The effects of consensus is presented in Figure 5.23.

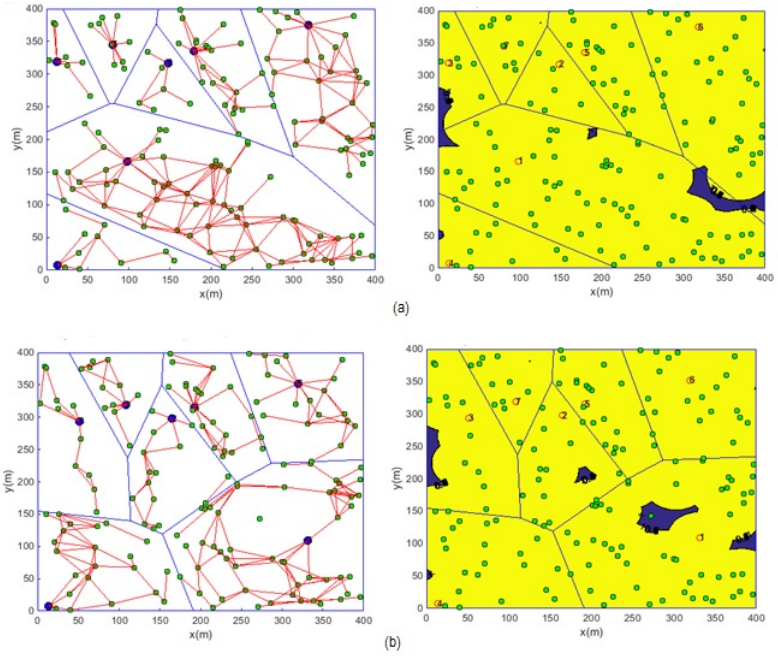

Figure 5.22: MS_1 moves to a new position after consensus agreement among MS_1, MS_3, MS_7, MS_2, MS_5, and MS_6. When MS_1 moves, the other voting nodes move under the rules of the force-based algorithm on MS_1.

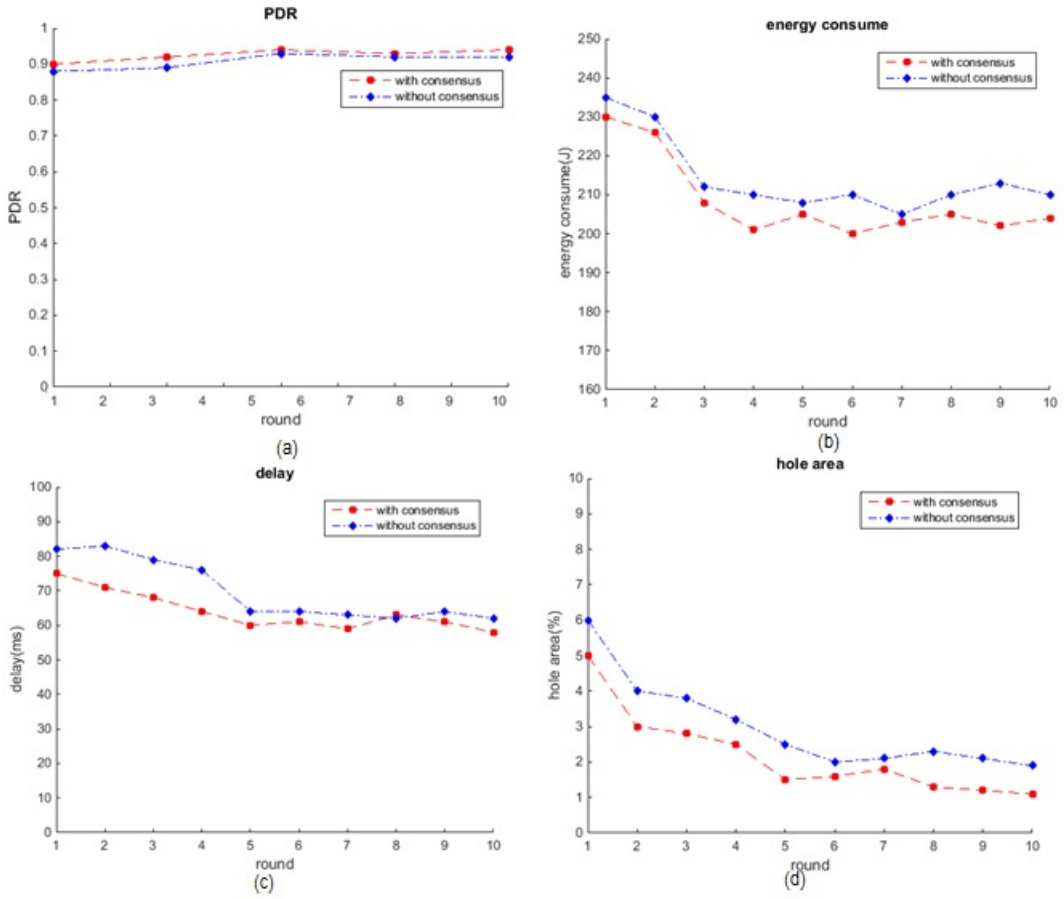

Figure 5.23: Performance results of networks with consensus (red) and without consensus (blue).

Panels a to d of Figure 5.23 compare the performance measures (packet delivery rates, energy consumptions, delays and percentage coverage holes) of networks employing and not employing the consensus mechanism. After consensus agreement among the neighbouring mobile sinks, the packet delivery rate was higher than without the consensus strategy. After several rounds, the packet delivery rate in both cases had slowly increased and the energy consumption was higher. However, the consensus lowered the energy consumption in each round (Figure 5.23b). The delay was also reduced by the consensus mechanism, as the distribution was better balanced and the expected area was divided fairly, reducing the delay between the source and the sinks. Meanwhile, the lower percentage of holes in the network with consensus (Figure 5.23d) can be explained by the agreement and verification process, which enables better local coverage of each mobile sink.

5.4.4 Performance comparison of BCRP and other protocols

5.4.4.1 Performances in networks with different numbers of mobile sinks

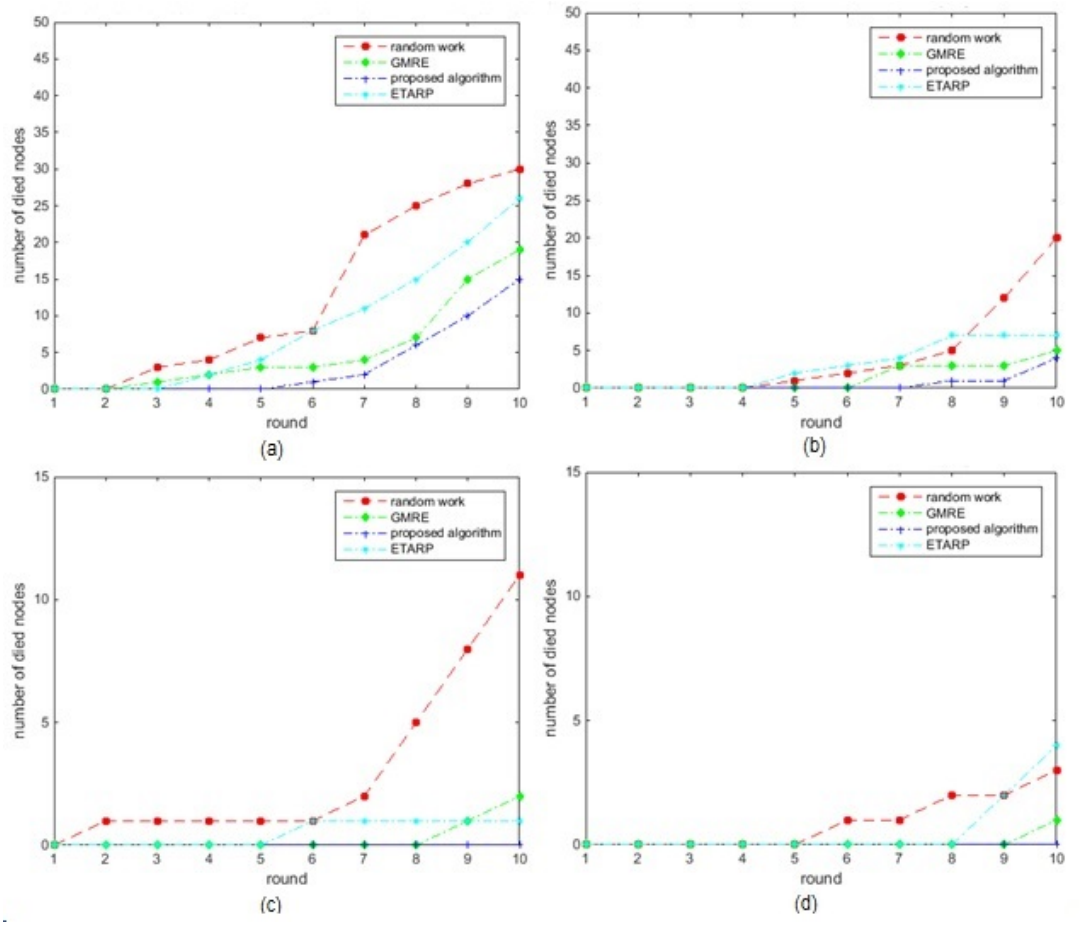

Figure 5.24: Number of dead nodes in networks deploying different numbers of mobile sinks: a) 3 MS, b) 5 MS c) 7 MS, and d) 9 MS.

Panels a to d of Figure 5.24 show the number of dead nodes in networks with different protocols deploying different numbers of mobile sinks. As shown in Figure 5.24a, the nodes began depleting later (Round 6) in BCRP than in the other protocols. The number of dead nodes was also lower in BCRP than in the other protocols (Figure 5.24b). In GMRE and ETARP, the nodes began deleting at Round 4, but in later rounds, the number of dead nodes was higher in ETARP than in GMRE. Most of the nodes died in the network with random walk deployment, and the die-off began earlier than in the other three protocols. Increasing the number of mobile sinks from 5 to 9 reduced the number of dead nodes in BCRP, ETARP and GMRE (Figure 5.24c, d).

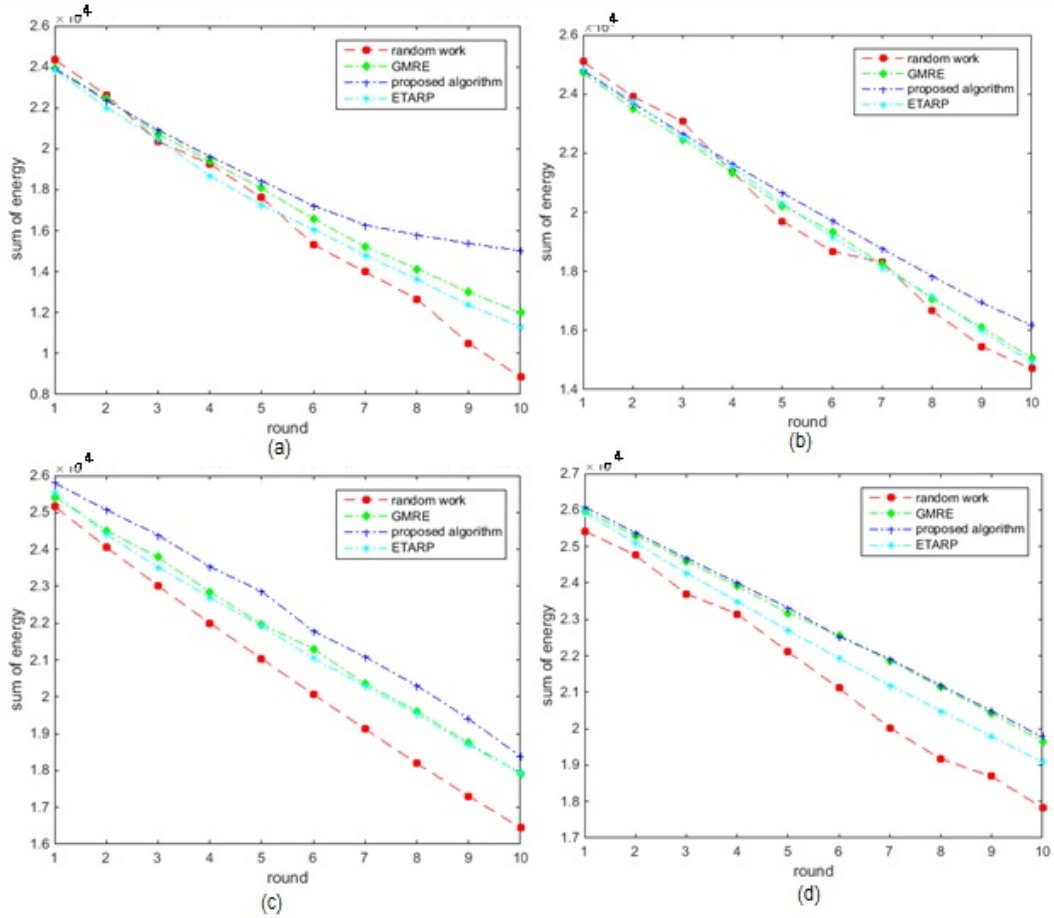

Figure 5.25: Energy consumed in networks deploying different numbers of mobile sinks: a) 3 MS, b) 5 MS, c) 7 MS, and d) 9 MS.

Figure 5.25 shows the summed energy consumed in the BCRP, ETARP, GMRE and random walk networks deploying different numbers of mobile sinks. The energy consumption was lowest in the BCRP networks deploying 3, 5 and 7 mobile sinks. However, when 9 mobile sinks were utilised, the energy consumptions of BCRP and GMRE were very similar. In networks with different numbers of mobile sinks, the energy efficiency decreased in the order: BCRP, GMRE, ETARP random walk. Less energy was consumed when more mobile sinks were deployed in the network.

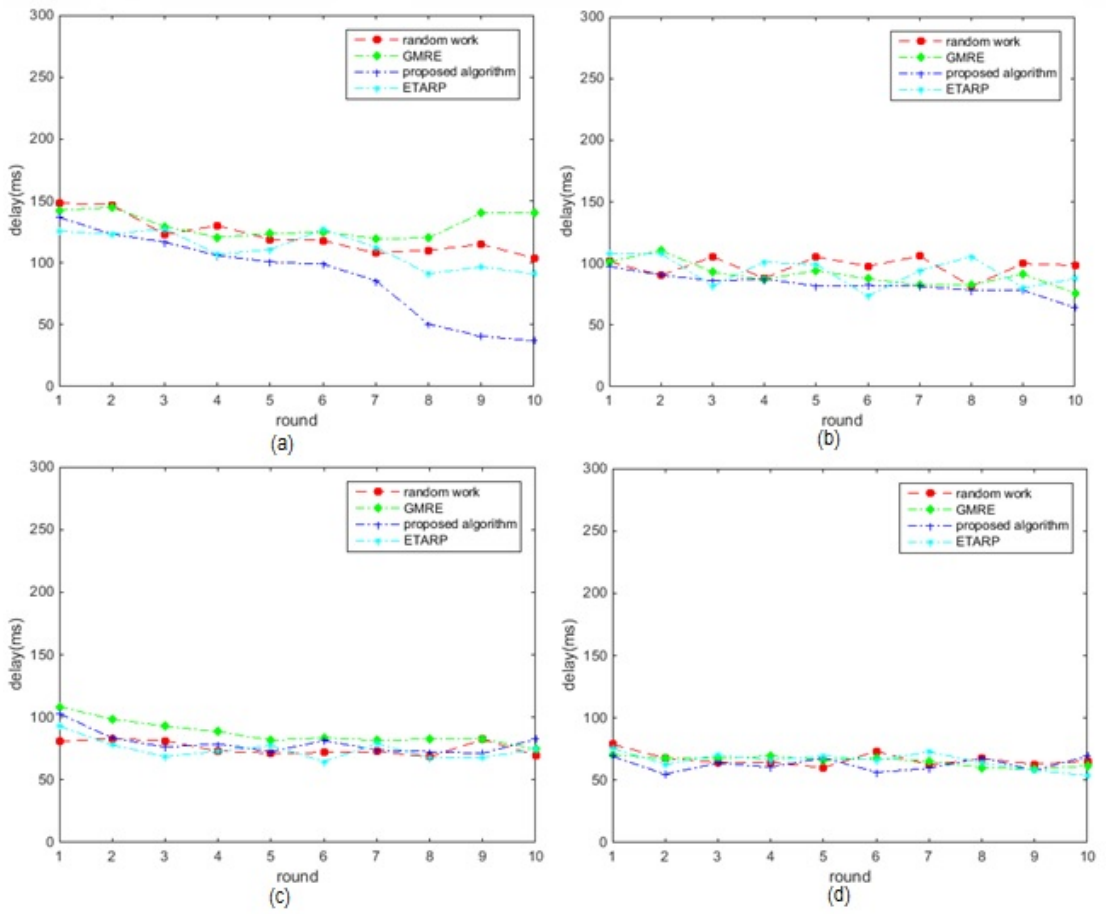

Figure 5.26: Delay in networks deploying different numbers of mobile sinks: (a) 3 MS, b) 5 MS, c) 7 MS, and d) 9 MS.

Figure 5.26 plots the delays in the BCRP, ETARP, GMRE and random walk networks with different numbers of mobile sinks. Although BCRP outperformed the other three protocols, the delay differences between BCRP and the other protocols are less obvious when more mobile sinks are deployed (7 and 9). The delay in BCRP possibly reflects the need to communicate and wait for replies from the many mobile sinks. In all protocols, increasing the number of mobile sinks reduced the delay.

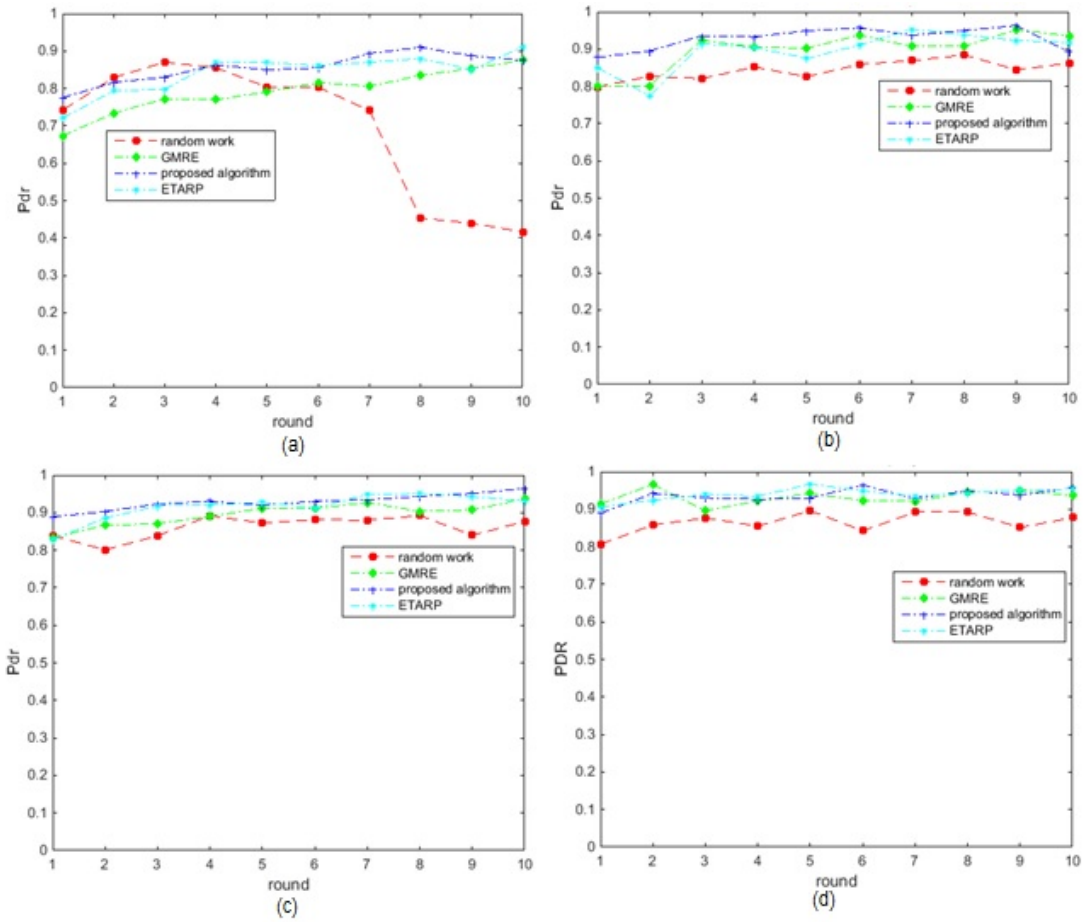

Figure 5.27: Packet delivery ratio in networks deploying different numbers of mobile sinks: a) 3 MS, b) 5 MS, c) 7 MS, and d) 9 MS.

Figure 5.27 shows the packet delivery ratio in networks with different protocols deploying different numbers of mobile sinks. The packet delivery ratio was lower in the network utilising random walk than in the other three protocols. ETARP and BCRP both performed well, with only slight differences in their delivery ratio. The packet delivery ratio increased with increasing number of mobile sinks in GMRE and ETARP, but was almost independent of mobile sink number in the network with random walk deployment.

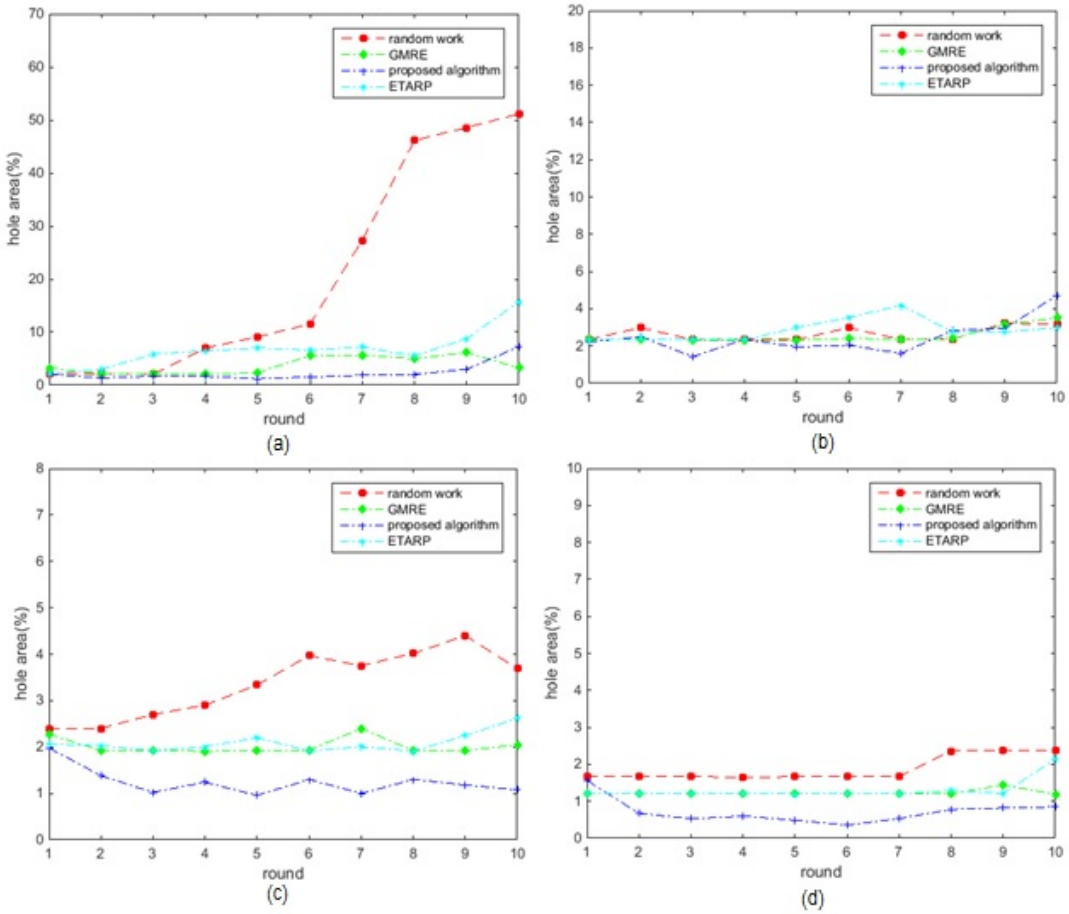

Figure 5.28: Percentage coverage holes in networks deploying different numbers of mobile sinks: a) 3 MS, b) 5 MS, c) 7 MS, and d) 9 MS.

In networks with few mobile sinks, the number of coverage holes was much higher in the random walk protocol than in the other three protocols (Figure 5.28a). The percentage of coverage holes was lowest in BCRP for any number of mobile sinks, but decreased as the number of mobile sinks increased. The percentage coverage holes in the networks utilising GMRE and ETARP were very similar, with only minor deviations in each case.

5.4.4.2 Performances of networks with different numbers of deployed nodes

Figures 5.29 to 5.33 compare the performances (numbers of dead nodes, energy consumptions, delays, packet delivery rates and percentage coverage holes) of BCRP, ETARP, GMRE and random walk). The network area was 400 m^2, and the number of mobile sinks was fixed at 7.

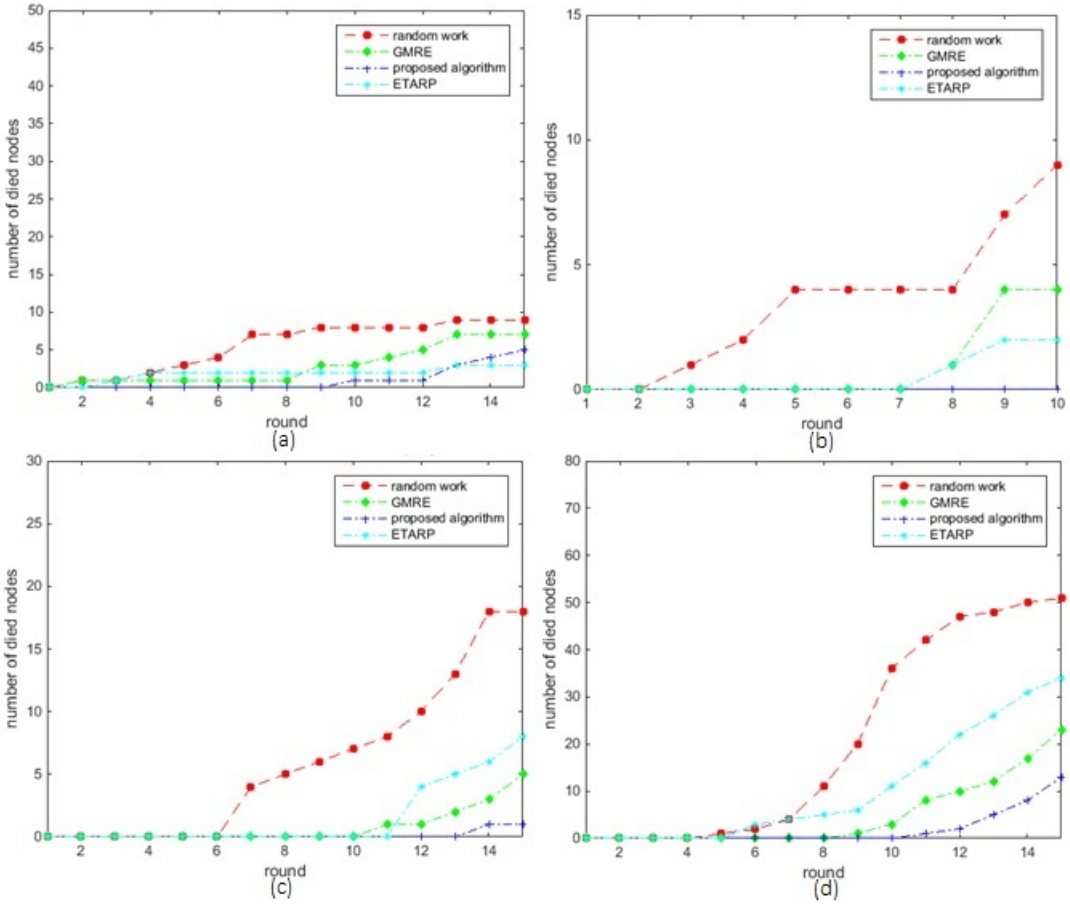

Figure 5.29: Number of dead nodes in the BCRP, random mobility, GMRE and ETARP networks with a) 150 nodes, b) 200 nodes, c) 250 nodes, and d) 300 nodes.

Figure 5.29 plots the number of dead nodes in the BCRP, random mobility, GMRE and ETARP with different numbers of deployed nodes. The network lifetime is defined as the time before energy depletion (death) of the first node. The number of dead nodes was generally lower in BCRP than in the other three protocols. The exception was the 150 node network, in which the number of dead nodes was also minimized in ETARP, followed by GMRE and random walk. However, when more nodes were deployed (200 to 300), the number of dead nodes was higher in ETARP than in GMRE. In the random walk protocol, the nodes began depleting sooner than in the other three protocols, and the number of dead nodes increased with increasing node number. On the other hand, the number of dead nodes in BCRP remained low as more nodes were deployed in the network.

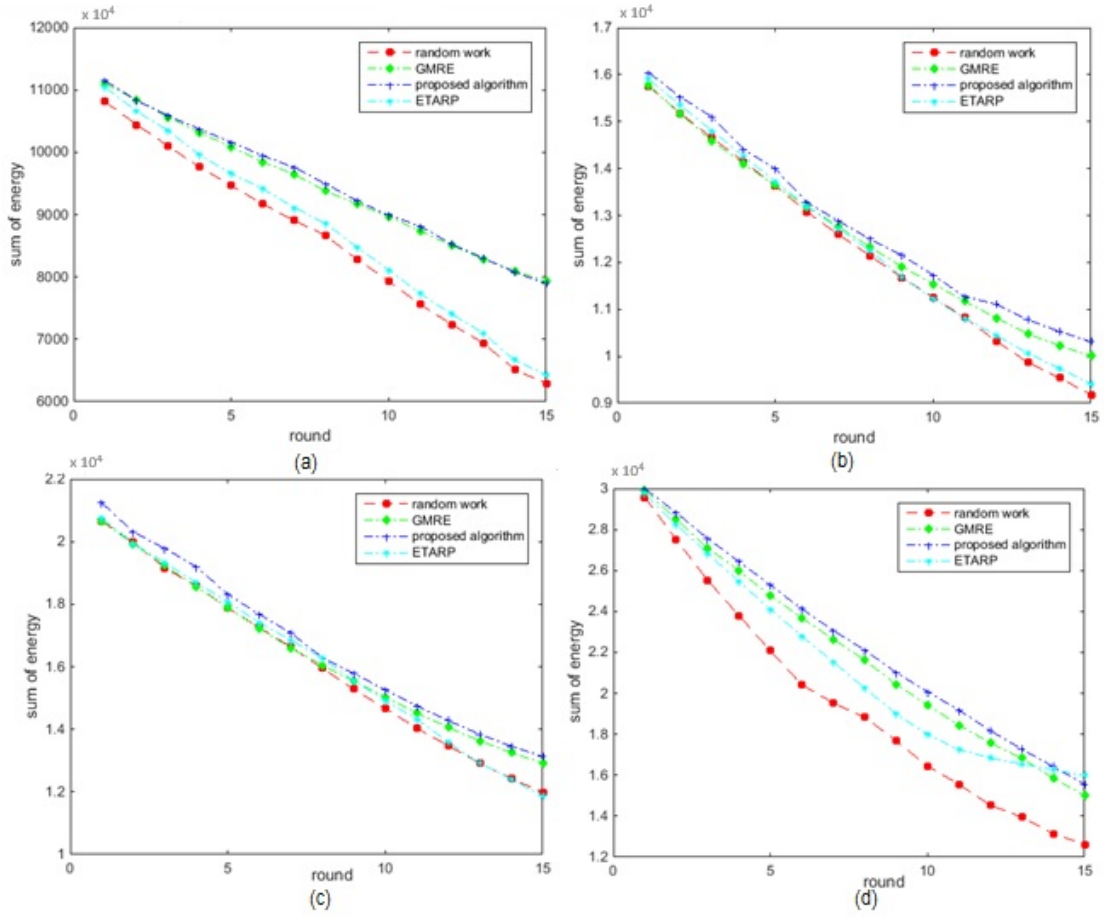

Figure 5.30: Energy consumptions in the BCRP, random mobility, GMRE and ETARP networks with a) 150 nodes, b) 200 nodes, c) 250 nodes, and d) 300 nodes.

Figure 5.30 shows the summed energies (residual energy per node over time) consumed in the networks with different mobility schemes. The BCRP consumed the least energy among the protocols, followed by GMRE, ETARP and random walk. The energy consumption depended on the number of nodes in the network (panels a to d of Figure 5.30).

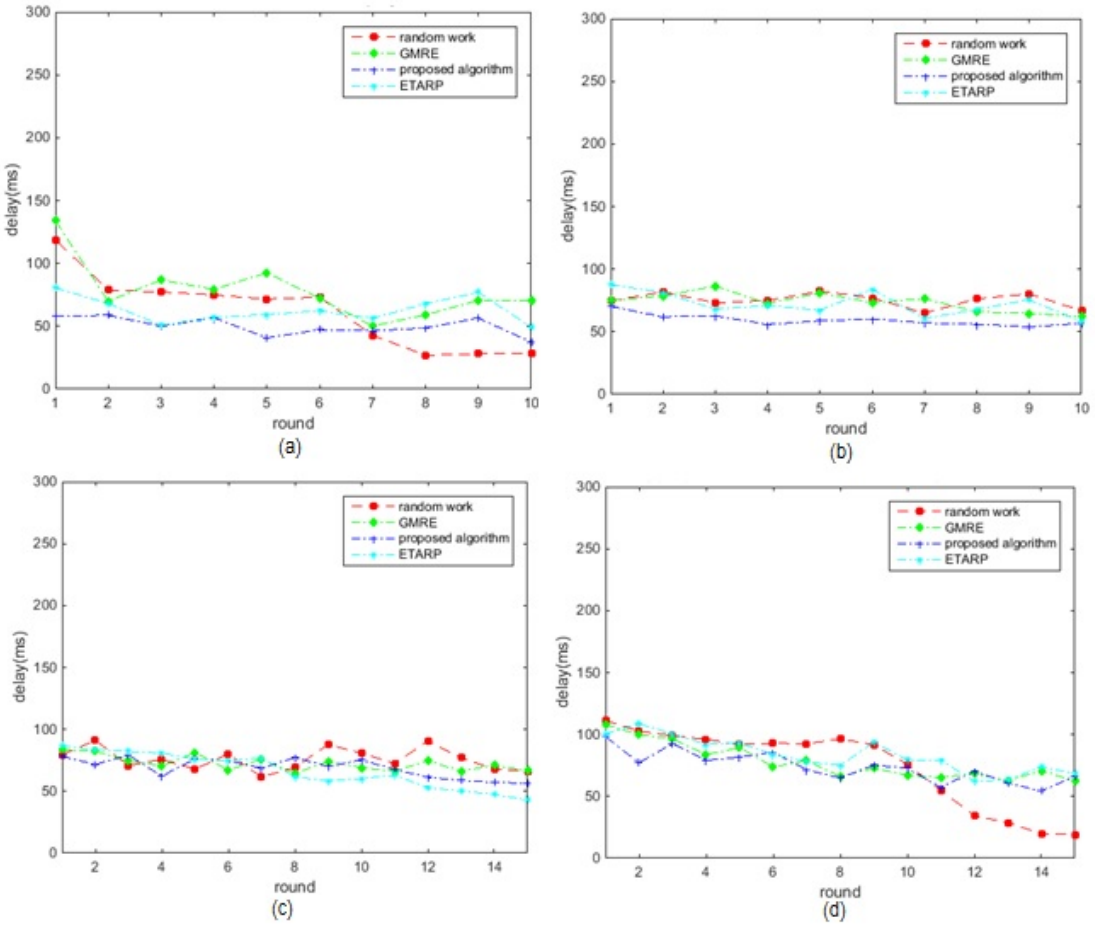

Figure 5.31: Delays in the BCRP, random mobility, GMRE and ETARP networks with a) 150 nodes, b) 200 nodes, c) 250 nodes, and d) 300 nodes.

Figure 5.31 shows the delay performances of the networks when different number of nodes were considered. The delay defines the time from packet generation at a sensor node to the successful delivery of that packet at the destination sink [Basagni 2008]. The delays in BCRP were almost independent of number of rounds in networks of all sizes.

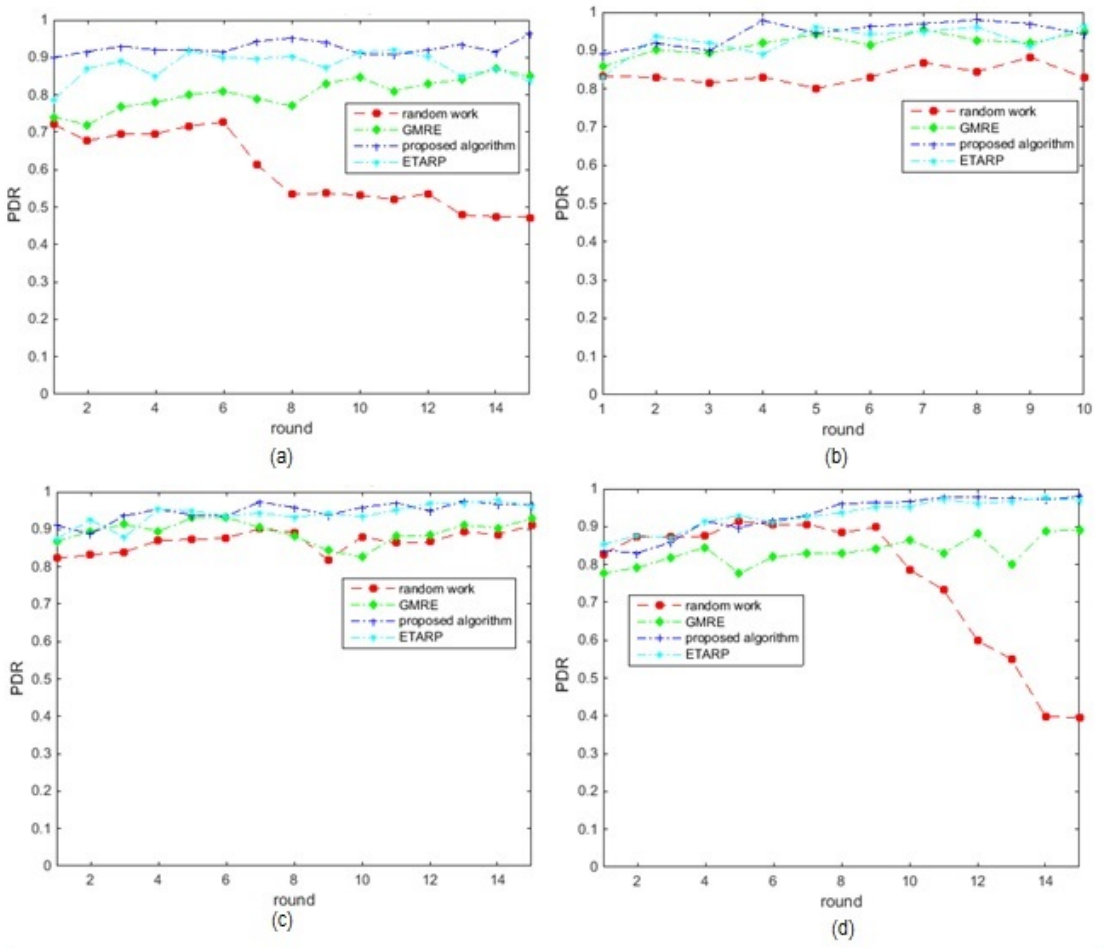

Figure 5.32: Packet delivery ratio in the BCRP, random mobility, GMRE and E-TARP networks with a) 150 nodes, b) 200 nodes, c) 250 nodes, and d) 300 nodes.

Figure 5.32 shows the packet delivery ratio in the BCRP, ETARP, GMRE and random walk-based when different number of nodes were considered. The packet delivery ratio defines the percentage of packets generated at the sensor nodes that are successfully delivered to the sink [Basagni 2008]. In BCRP, the data packets were always successfully transmitted, and the packet delivery rate was high regardless of network density. ETRP also performed well, but was slightly inferior to BCRP. Whereas increasing the node density little affected the BCRP, it degraded the packet delivery ratio of random walk and GMRE, possibly because these protocols make more frequent moves when more nodes are involved. Also, the frequent changes of sink position may cause inaccurate reporting when the nodes send information to an outdated sink location. This error is responsible for packet drop. On the other hand, the verification and checking mechanisms in ETARP and BCRP require confirmation and consensus; the mobile sink cannot decide to move without consulting

its neighbours.

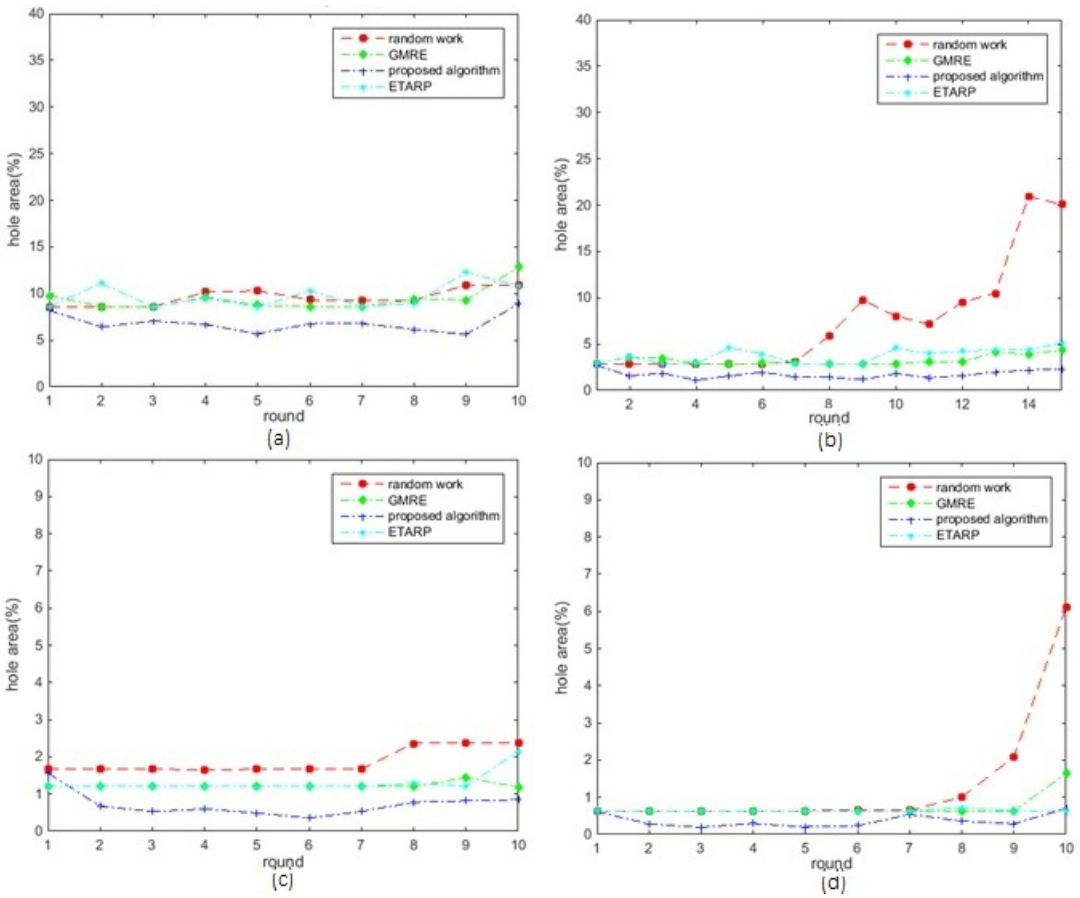

Figure 5.33: Percentage of coverage holes in the BCRP, random mobility, GMRE and ETARP networks with a) 150 nodes, b) 200 nodes, c) 250 nodes, and d) 300 nodes.

Figure 5.33 shows the coverage hole in the BCRP, ETARP, GMRE and random walk-based. As the nodes in the networks are randomly deployed, the coverage holes are expected to be larger or commoner in sparse networks (Figure 5.33a) than in dense networks (Figure 5.33c and d). In networks of all densities, BCRP outperformed the other protocols while the performances of ETARP and GMRE were very similar. The high performance of BRCP is attributable not only to its sink mobility, but also to its partitioning and balancing mechanisms.

5.4.4.3 Performances of networks with different network areas

Figures 5.34 - 5.38 compare the performance results (numbers of dead nodes, energy consumptions, delays, packet delivery ratio and percentage coverage holes) of the BCRP, ETARP, GMRE and random walk-based networks covering differently sized

areas. The number of mobile sinks was fixed at 7.

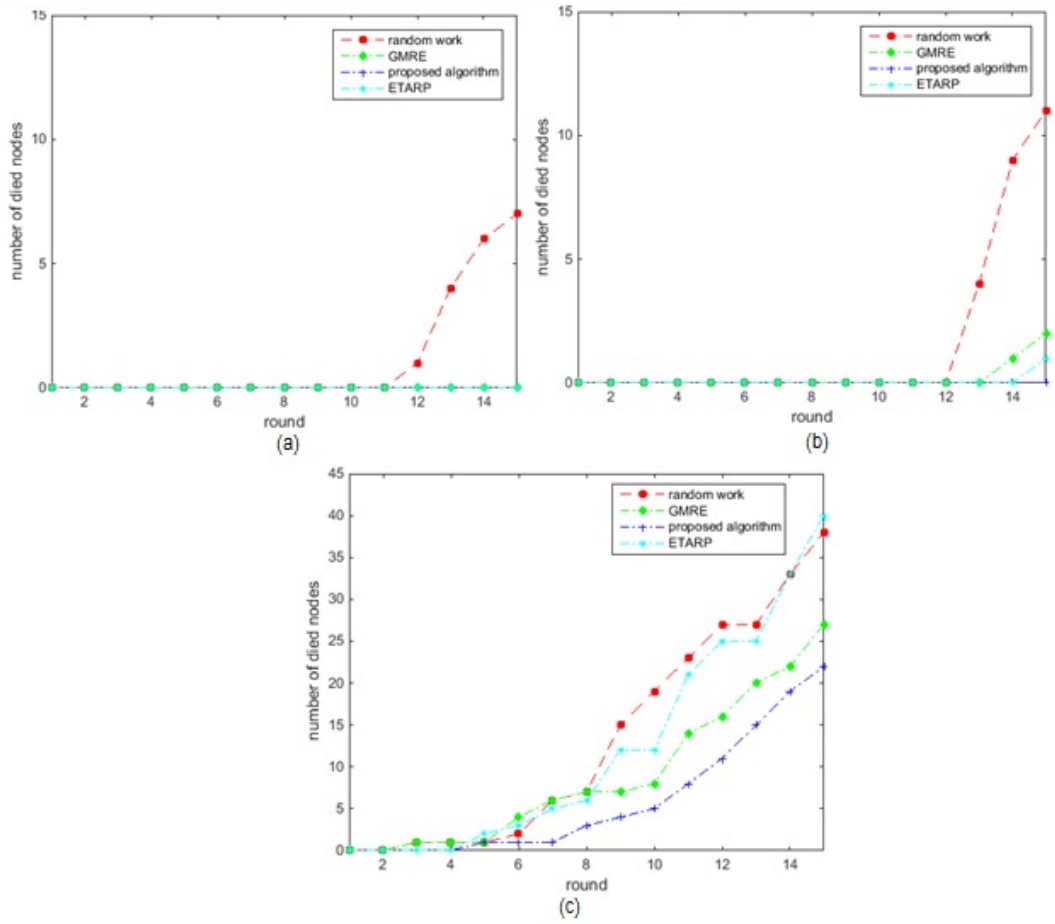

Figure 5.34: Delay in BCRP and other protocols deployed over different network areas: a) 200 m^2 b) 300 m^2 and 500 m^2.

The nodes in random walk began depleting in Round 12 of the network covering 200 m^2 (Figure 5.34a) whereas those in GMRE and ETARP began depleting in Rounds 13 and 14 of the 300 m^2 network, respectively. The number of dead nodes increased when the network area expanded from 300 m^2 to 400 m^2. In terms of number of dead nodes, the network performance decreased in the order BCRP (best)→ GMRE→ ETARP→ Random walk (worst). The performance degradation in larger areas may be attributable to the increased number of coverage holes, because the number of deployed nodes is fixed. Moreover, frequently used nodes may die off, and the nodes will be further separated, increasing the energy consumption over a larger area. In BCRP, node depletion is diminished by the verification mechanism, reduced mobile sink movement, partitioning and balancing. The ETARP and B-GRP performed similarly, as both protocols reduce the node movement and employ

checking mechanisms.

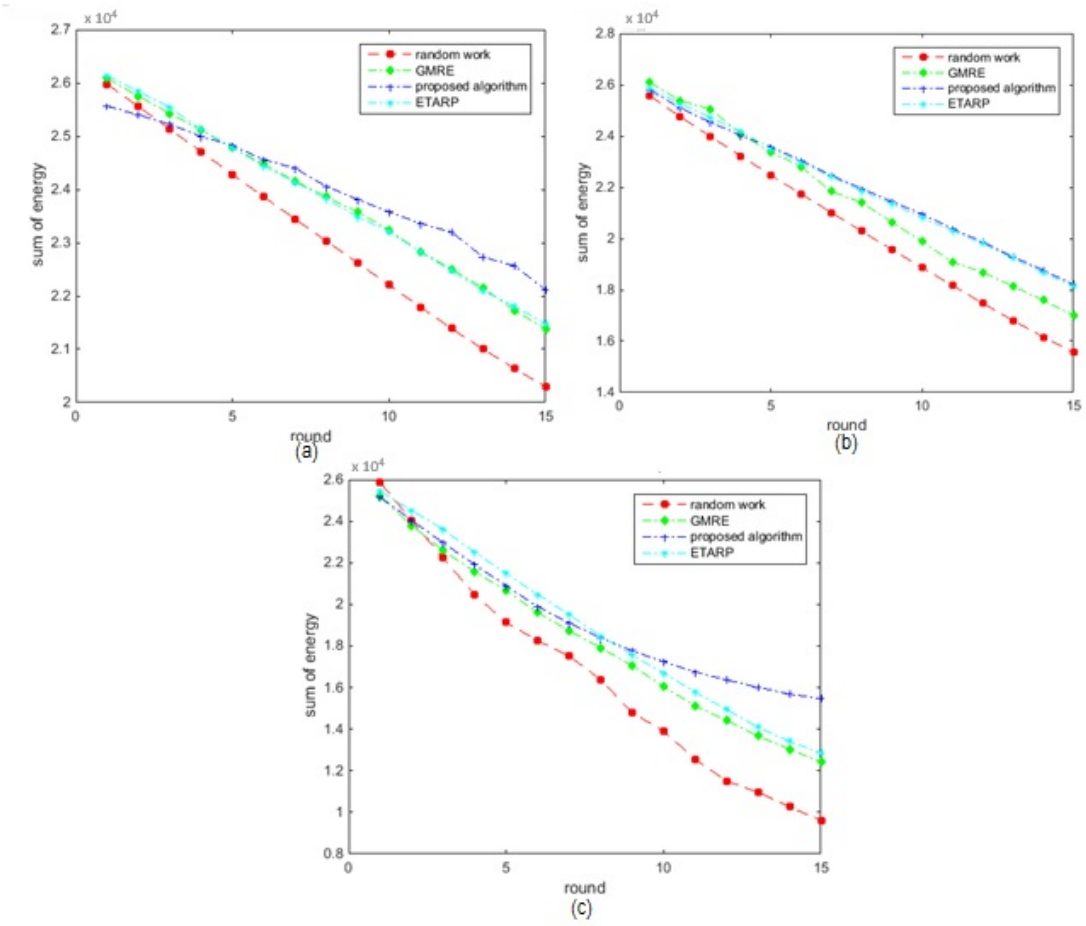

Figure 5.35: Energy consumed in BCRP and other protocols deployed over different areas: a) 200 m^2, b) 300 m^2 and, c) 500 m^2.

Figure 5.35 shows the energy consumption of the BCRP, ETARP, GMRE and random walk-based deployed over different areas. Energy is consumed during data transmission and reception, so the energy demands are data which is in influenced by distance and number of nodes involved in the communication.

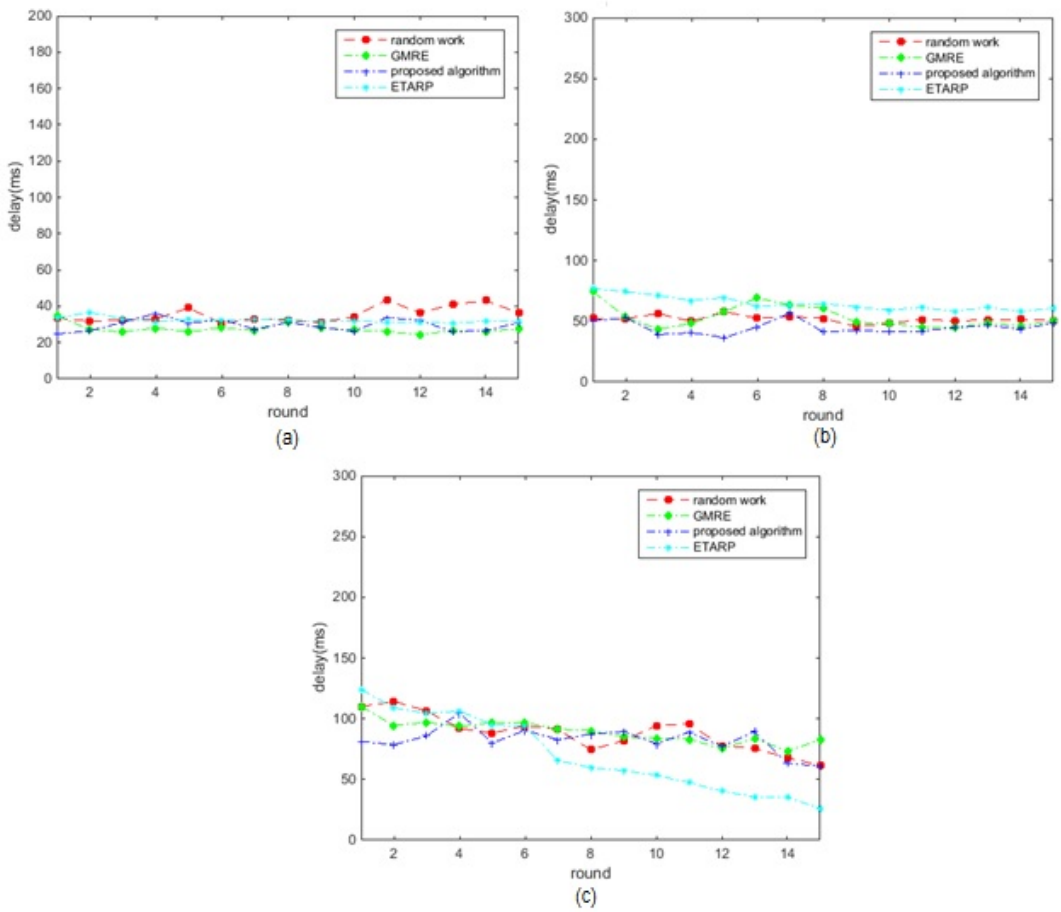

Figure 5.36: Delay in BCRP and other protocols deployed over different areas: a) 200 m^2 b) 300 m^2 and c) 500 m^2.

Figure 5.36 compares the delays in the BCRP, ETARP, GMRE and random walk-based networks deployed over different areas. The delay in the four protocols ranged from 20 to 40 ms. The BCRP outperformed the other three protocols except in the largest area deployment, when it was eclipsed by ETARP. This outcome may be explained by the verification and consensus process in BCRP, which delays the decision to deliver packets through the network.

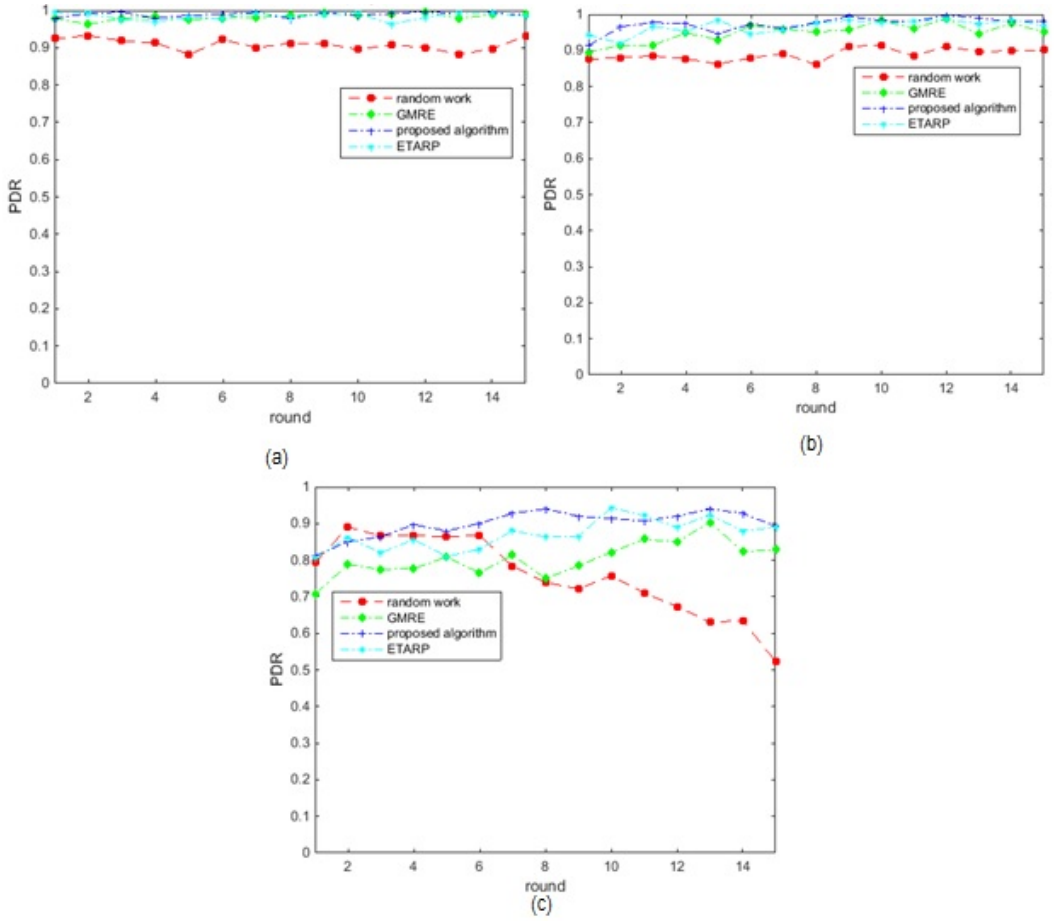

Figure 5.37: Packet delivery ratio in BCRP and other protocols deployed over different areas: a) 200 m^2, b) 300 m^2 and c) 500 m^2.

As shown in Figure 5.37, increasing the area of the network coverage reduced the packet delivery ratio of all protocols. In the smallest area, almost 100% of the packets were successfully delivered in ETARP, GMRE and BCRP. As the area increased, the reduction in the packet delivery rate became more obvious in GMRE and random walk than in BCRP and ETARP (Figure 5.37b). In the largest area (Figure 5.37c), the packet delivery rates were reduced in all protocols, especially in random walk. In terms of the packet delivery rate, the performance decreased in the order of BCRP (best) ETARP GMRE random walk (worst).

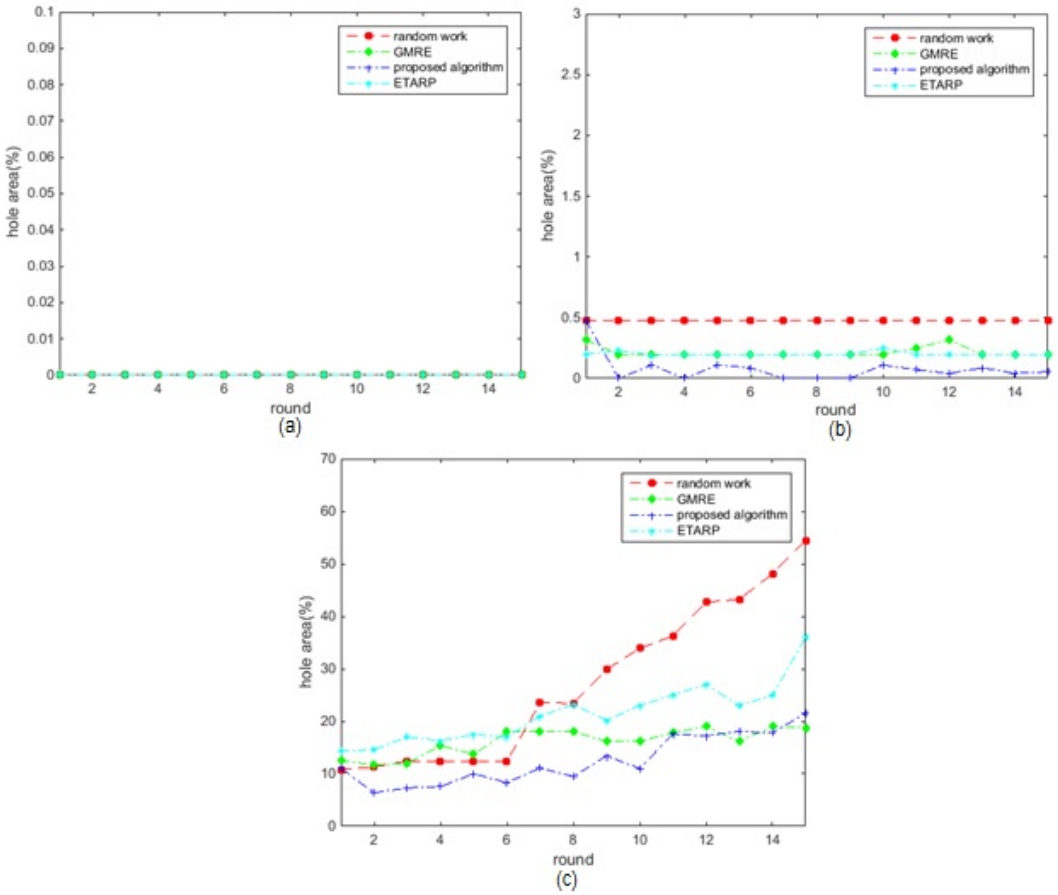

Figure 5.38: Percentages of coverage holes in BCRP and the other protocols deployed over different areas: a) 200 m^2 b) 300 m^2 and c) 500 m^2.

Figure 5.38 shows the percentage coverage holes of the BCRP, ETARP, GMRE and random walk-based networks deployed over different areas. In the smallest area, the coverage of all protocols was 100% (Figure 5.38a). Coverage holes emerged when the network was spread over a larger area (5.38b). As BCRP treats the coverage as a factor, this protocol outperformed the other three protocols. The percentage of coverage holes detected by BCRP was almost balanced (i.e., independent of number of rounds), by virtue of the consensus mechanism.

5.5 Conclusions

This chapter proposed and evaluated a novel protocol called the blockchain-based routing protocol (BCRP) for distributed WSN. The BCRP utilises multiple mobile sinks for efficient routing in a distributed manner. The proposed protocol is a controlled mobility type, meaning that the movements of the mobile sinks are guided

by the other nodes in the network. Such mobility approaches are rarely considered in existing works. Most of the existing works guide the mobile sinks or node mobility by an energy factor. Although BCRP can potentially accommodate more factors and (or) alternative factors, it currently determines the mobility of mobile sinks by the coverage, focusing on the nonuniform distribution of random deployment.

The proposed protocol is intended for a distributed network, uncertain environment, limited knowledge, nonuniform distribution and collaborative mechanisms. In a distributed and randomly distributed network where the information is shared only by nearby nodes, the reliability of the participating nodes or sinks is not guaranteed. In most of the existing protocols, the nodes decide to satisfy their own utilities rather than those of the wider network. Accordingly, mechanisms that can provide verification and consensus among nodes are needed.

The recently proposed blockchain concept can support these needs, but its application to WSNs is very limited at present. The BCRP integrates the blockchain concepts in the decision making of the mobile sinks with assistance by the surrounding nodes. The BCRP integrates five modules (setup, initialisation, relocation, verification and consensus). In simulation studies, its performance was quantified by five performance metrics: number of dead nodes, energy consumption, delay, packet delivery ratio and percentage of coverage holes.

We evaluated the performances of the static sink, single sink and multiple mobile sink configurations. The scalability of the BCRP was confirmed by its high performance in three different settings (varying the number of mobile sinks, number of nodes and the network area).

In comparative simulations, the BCRP far outperformed the other tested routing protocols (GMRE, ETARP and random walk). The collaboration among nodes and mobile sinks, and among the mobile sinks themselves, improved the routing efficiency of the network. In addition, the mobility assistance provided by the normal nodes through the vector-based approach improved the coverage of holes in the network. Collaboration among the mobile sinks and verification before the decision making balanced the network performance. Overall, the BCRP demonstrated higher coverage, more efficient routing, more balanced distribution, and longer network lifetime.

Chapter 6

Conclusion and Future Work

6.1 Conclusions

This chapter concludes the research work that has been done for the research objectives discussed in Chapter 1. This chapter also highlights the concluding remarks about the solution to the research problems and research questions as expressed in Chapter 1.

In this thesis, the challenges in decentralised and randomly distributed network were discussed. The routing challenge has been extensively discussed when involving resource constrained nodes as most of the energy is consumed when routing the packets in the network. Reviews on existing traditional routing protocols have been conducted to observe the state of the art. More recent approaches involving trust-based routing protocols were further investigated. The reviews reveal the need for efficient distributed and decentralised decision making to assist nodes in the decentralised and randomly distributed wireless sensor network. Through the literatures, the limitations exist in current approaches were identified, and the solutions to overcome and reduce the gaps were determined. In distributed and decentralised network, the routing efficiency lies in the provided information and the information provider which play the important role in a decision making. The nodes were treated as agents, having the capability of being self-configurable and taking actions autonomously.

Two types of network have been considered, involving one with static sink, and the other with mobile sinks. This research has successfully demonstrated the use of distributed decision making in the 1) forwarder selection and 2) the relocation of mobile sinks for the two types of network. The main objective of this research was to propose a distributed and decentralised trust-based decision making particularly in routing, by adaptively considers multiple criteria as its trust factors.

To observe whether the research has achieve the specified objectives, the objectives in Chapter 1 are re-visited. The main objective of this research is to propose a

distributed and decentralised decision making particularly in routing to distributed. In this research we have proposed two distributed solutions for forwarder selection decision and relocation decision for mobile sinks.

In achieving our main objectives, we have identified the research gap based on extensive literature reviews conducted in Chapter 2. Upon investigating the existing solution for distributed decision making, only some are relevant for WSNs. This include the trust-based mechanisms that has been represented as the level of reliability that a node has on another node. The factors that contributes to the reliability level in our approach is determined and being considered in the trustworthiness values. Upon deciding on the factors, processes and mechanisms, we have proposed a Hierarchical Trust Model (HTM), Adaptive Trust-based Routing Protocol (ATRP), and Blockchain-based Routing Protocol (BCRP).

HTM introduces a multiple nodes evaluation instead of the single node evaluation that is commonly considered in most of existing distributed routing protocols. The evaluations not only evaluate the target node but also the nodes evaluating the target nodes.

In traditional routing protocols, the forwarder selection is based on certain factors, which mostly are resources related, especially in terms of energy consumption. On the other hand, the trust-based routing has been introduced that focusing on security factors in the decision making. More recent, there are researches that integrate both factors in their forwarder selection decision. However, the number of such work is very limited. ATRP integrates both aspects in its trustworthiness consideration. The trust in ATRP has been defined as the level of reliability of a node has on the other node, where the trust values are contributed by four criteria: energy, reliability, reputation and throughput. As ATRP employs HTM in its selection decision, thus the trustworthiness values involve multiple criteria, and multiple node evaluations.

The BCRP introduces in this thesis has taken into consideration several blockchain features in determining the relocation position of mobile sinks. The mobile sinks in BCRP were able to make decisions automatically based on a set of rules that are agreed by all mobile sinks. However, the relocation decision making requires consensus from other mobile sinks. In such a way, many challenges in distributed

mobile sink routing can be overcome such as in term of outdated position of mobile sink and better decision that benefits larger parts of the network.

Several methods have been adapted and embedded in the proposed approaches. Analytical Hierarchy Process (AHP), a well known multi criteria analysis strategy that is commonly used in domains other than WSNs, has been applied in computing the trustworthiness in HTM and ATRP. Q-learning was adopted in calculating the nodes reputation values in ATRP while the force-based mechanism is used in BCRP to balance the coverage level in partitioned network.

The proposed methods were than being evaluated and compared to the existing protocols for several network performance metrics (energy consumption, throughput, packet delivery ratio, average delay and coverage level). The performance of ATRP (that embeds HTM in its strategy) is compared to two other existing protocols, the Trust and Energy Aware Routing Protocol for WSNs (TERP) and Direct Trust Dependent Link State Routing Protocol Using Route Trusts for WSNs (DTL-SRP), while the performance of BCRP is compared to ETARP, Greedy Maximum Residual Energy (GMRE) and random walk. ATRP was evaluated in the existence of malicious nodes, when control mechanism such as number of interactions and timeliness factor were considered and being compared with the other existing protocols for various network loads and different number of deployed nodes in the network. BCRP performance was evaluated by varying the number of nodes, network size and number of mobile sinks. The network performances when a single static sink, a single mobile sink and multiple sinks were also observed. MATLAB has been used to simulate the proposed approaches. The performances of ATRP and BCRP outperformed the other existing protocols in all the five metrics. The multi criteria considerations, multiple nodes evaluations and the distribution of load through hierarchical structure had contributed to the outstanding performance of ATRP. The features considered in BCRP allow each mobile sink to react and decide locally in distributed manner, causes less energy consumption. BCRP had shown itself as a scalable protocol upon its outstanding performances when vary number of nodes were deployed and performed well in large network area when tested with different network size. The decision that requires consensus from other mobile sinks had created a fairer distribution among mobile sinks.

6.2 Recommendations and Future Research

In conclusion, this research has successfully accomplished its specified objectives. Extensive simulations have been conducted in the research, considering several parameters to observe the performances of proposed methods in terms of important network performance metrics (energy consumption, throughput, packet delivery ratio, delay and coverage level). Results gained from the simulations indicated that proposed solutions outperform the existing comparable protocols, which could lead to the development of real implementations and open to almost unlimited number of potentials for future research.

- Potential applications: The proposed protocols could be implemented and tested on real applications. It could be divided into two types of applications: large scale and smaller scale applications. As a distributed solution, the proposed methods have great potentials in many applications that require decision making to be made in a distributed manner such as in military applications, wildlife, human mobility, moving or relocatable goods etc. However, this may require cost and effort to make it feasible. In order to realise its implementation, financial support or permission from the user is needed.

  The AHP method proposed in HTM and ATRP can be implemented in the decision making in WSN where multiple factors are available. For example, in the network that consists of multiple types of sensors where each sensor is responsible to gather specific data, these data can be aggregated at the higher level for a better decision making.

- Experiment based: The implementation of this proposed methods can be further observed in real world through experiment or real data. To find the real data to validate the concept is a challenge and need to be further explored.

  The algorithms in proposed protocols could be conducted into experimental-based. For small scale applications for example, several sensors can be embedded on a Zigbee Arduino board and programmed to coordinate the movement among multiple devices. It can also be tested by using other protocols such as Z- Wave or LoraWAN, for larger type of applications.

- Limitation based on assumptions: In reality, the performance may not be reflecting similarly due to certain simulation assumptions. In BCRP, the blockchain-based idea is borrowed to represent the distributed decision making. This new consideration can be further studied considering more complex situation in the distributed WSNs, including making use of the existing blockchain platform such as Ethereum.

- Embedding proposed solutions in existing technologies: Several existing techniques were embedded in proposed approaches. The proposed protocols can also be integrated with other technologies. For example, the current consideration of Zigbee protocol can also be tested on LoRAWAN, where some part of the WSN may be connected to IoT via LoRaWAN gateway, in the case of tracking object in the military or fire notification system in the jungle (due to its long range capabilities).

- Performance measures: In the research, the performance metrics that are considered include energy consumption, throughput, packet delivery ratio, delay and coverage rate. Other performance metrics can be used to measure the implementation of proposed solutions. This includes the measures in terms of communication packet volume and the computational complexity. Packet size optimization is also an important issue in energy constrained WSNs. Such measures can be formulated to a certain extend to evaluate the operations on an actual device (for example in microcomputers, such as Arduino and mbed). The impact of communication packet volume (i.e. the packet size which could be a fixed value or adaptive to the channel availability), in terms of energy efficiency and lifetime can be further tested. However, as the packet size is mostly depended on the type of the data that is disseminated to the destination, the application needs to be identified in order to gain such performance measures. The knowledge involving packet size optimization may be required for such deployment. In terms of computational complexity (i.e. the amount of resources required for running the algorithm), several experimental setups could be further explored. For example, network with various number of nodes that are linked to different number of criteria input can be implemented to further observe the effect of the number of the criteria and accuracy of such

setup to the network performances.

Bibliography

[Abedin 2012] Fahmida Abedin, Kuo-Ming Chao and Nick Godwin. *An agenda based multi issue negotiation approach.* Journal of Ambient Intelligence and Humanized Computing, pages 1–19, 2012.

[Abusaimeh 2009] Hesham Abusaimeh and Shuang-Hua Yang. *Dynamic cluster head for lifetime efficiency in WSN.* International journal of automation and computing, vol. 6, no. 1, pages 48–54, 2009.

[Ahmed 2015] Adnan Ahmed, Kamalrulnizam Abu Bakar, Muhammad Ibrahim Channa, Khalid Haseeb and Abdul Waheed Khan. *TERP: A trust and energy aware routing protocol for wireless sensor network.* IEEE Sensors Journal, vol. 15, no. 12, pages 6962–6972, 2015.

[Ahmed 2016] Adnan Ahmed, Kamalrulnizam Abu Bakar, Muhammad Ibrahim Channa and Abdul Waheed Khan. *A secure routing protocol with trust and energy awareness for wireless sensor network.* Mobile Networks and Applications, vol. 21, no. 2, pages 272–285, 2016.

[Akkaya 2005] Kemal Akkaya and Mohamed Younis. *A survey on routing protocols for wireless sensor networks.* Ad hoc networks, vol. 3, no. 3, pages 325–349, 2005.

[Akl 2011] Ahmed Akl, Thierry Gayraud and Pascal Berthou. *A metric for evaluating density level of wireless sensor networks.* In Wireless Days (WD), 2011 IFIP, pages 1–3. IEEE, 2011.

[Akyildiz 2002a] Ian F Akyildiz, Weilian Su, Yogesh Sankarasubramaniam and Erdal Cayirci. *A survey on sensor networks.* Communications magazine, IEEE, vol. 40, no. 8, pages 102–114, 2002.

[Akyildiz 2002b] Ian F Akyildiz, Weilian Su, Yogesh Sankarasubramaniam and Erdal Cayirci. *Wireless sensor networks: a survey.* Computer networks, vol. 38, no. 4, pages 393–422, 2002.

[Al-Karaki 2004] Jamal N Al-Karaki and Ahmed E Kamal. *Routing techniques in wireless sensor networks: a survey.* Wireless Communications, IEEE, vol. 11, no. 6, pages 6–28, 2004.

[Al-Obaisat 2007] Yazeed Al-Obaisat and Robin Braun. *On wireless sensor networks: architectures, protocols, applications, and management.* 2007.

[Alan 1988] H Alan. *Bond, Les Gasser, Distributed Artificial Intelligence*, 1988.

[Alpaydin 2014] Ethem Alpaydin. Introduction to machine learning. 2014.

[An 2008] Bo An, Kwang Mong Sim, Liang Gui Tang, Chun Yan Miao, Zhi Qi Shen and Dai Jie Cheng. *Negotiation Agents' Decision Making Using Markov Chains.* In Rational, Robust, and Secure Negotiations in Multi-Agent Systems, pages 3–23. Springer, 2008.

[An 2011] Bo An, Victor Lesser and Kwang Mong Sim. *Strategic agents for multi-resource negotiation.* Autonomous Agents and Multi-Agent Systems, vol. 23, no. 1, pages 114–153, 2011.

[Anadozie] NU Anadozie, CO Ohaneme, ACO Azubogu and KC Okafor. *Performance Evaluation and Optimization of Key Performance Indicators of WSN Metrics.* network, vol. 3, page 4.

[Anand 2016] Veena Anand, Deepika Agrawal, Preety Tirkey and Sudhakar Pandey. *An energy efficient approach to extend network life time of wireless sensor networks.* Procedia Computer Science, vol. 92, pages 425–430, 2016.

[Babu 2011] Shaik Sahil Babu, Arnab Raha and Mrinal Kanti Naskar. *A Direct trust dependent link state routing protocol using route trusts for WSNs (DTLSRP).* Wireless Sensor Network, vol. 3, no. 04, page 125, 2011.

[Badica 2011] Costin Badica, Mihnea Scafes, Sorin Ilie, Amelia Badica and Alex Muscar. *Dynamic Negotiations in Multi-Agent Systems.* ICT in Education, Research and Industrial Applications: Integration, Harmonization and Knowledge Transfer, page 8, 2011.

[Baliga 2017] Arati Baliga. *Understanding blockchain consensus models.* Persistent, 2017.

[Bano 2017] Shehar Bano, Alberto Sonnino, Mustafa Al-Bassam, Sarah Azouvi, Patrick McCorry, Sarah Meiklejohn and George Danezis. *Consensus in the age of blockchains.* arXiv preprint arXiv:1711.03936, 2017.

[Barto 1998] Andrew G Barto. Reinforcement learning: An introduction. MIT press, 1998.

[Basagni 2007] Stefano Basagni, Alessio Carosi and Chiara Petrioli. *Controlled vs. uncontrolled mobility in wireless sensor networks: Some performance insights.* In Vehicular Technology Conference, 2007. VTC-2007 Fall. 2007 IEEE 66th, pages 269–273. IEEE, 2007.

[Basagni 2008] Stefano Basagni, Alessio Carosi, Emanuel Melachrinoudis, Chiara Petrioli and Z Maria Wang. *Controlled sink mobility for prolonging wireless sensor networks lifetime.* Wireless Networks, vol. 14, no. 6, pages 831–858, 2008.

[Bernon 2006] Carole Bernon, Vincent Chevrier, Vincent Hilaire, Paul Marrow*et al.* *Applications of self-organising multi-agent systems: An initial framework for comparison.* Informatica (Slovenia), vol. 30, no. 1, pages 73–82, 2006.

[Birk 2000] Andreas Birk. *Boosting cooperation by evolving trust.* Applied Artificial Intelligence, vol. 14, no. 8, pages 769–784, 2000.

[Brzostowski 2008] Jakub Brzostowski and Ryszard Kowalczyk. *Experimental evaluation of possibilistic mechanism for negotiation partners selection.* In Rational, Robust, and Secure Negotiations in Multi-Agent Systems, pages 127–145. Springer, 2008.

[Buskens 1998] Vincent Buskens. *The social structure of trust.* Social networks, vol. 20, no. 3, pages 265–289, 1998.

[Cachin 2017] Christian Cachin and Marko Vukolić. *Blockchains consensus protocols in the wild.* arXiv preprint arXiv:1707.01873, 2017.

[Cărbunar 2006] Bogdan Cărbunar, Ananth Grama, Jan Vitek and Octavian Cărbunar. *Redundancy and coverage detection in sensor networks.* ACM Transactions on Sensor Networks (TOSN), vol. 2, no. 1, pages 94–128, 2006.

[Castro 1999] Miguel Castro, Barbara Liskov*et al. Practical Byzantine fault tolerance.* In OSDI, volume 99, pages 173–186, 1999.

[Chakrabarti 2003] Arnab Chakrabarti, Ashutosh Sabharwal and Behnaam Aazhang. *Using predictable observer mobility for power efficient design of sensor networks.* In Information Processing in Sensor Networks, pages 129–145. Springer, 2003.

[Chen 1995] Tongwen Chen and Bruce Francis. *Optimal Sampled-Data Control Systems (errerta).* 1995.

[Chen 2007] Haiguang Chen, Huafeng Wu, Xi Zhou and Chuanshan Gao. *Agent-based trust model in wireless sensor networks.* In Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2007. SNPD 2007. Eighth ACIS International Conference on, volume 3, pages 119–124. IEEE, 2007.

[Chen 2012] Shenlong Chen, Yuqing Zhang, Qixu Liu and Jingyu Feng. *Dealing with dishonest recommendation: The trials in reputation management court.* Ad Hoc Networks, vol. 10, no. 8, pages 1603–1618, 2012.

[Cheng 2009] Long Cheng, Yimin Chen, Canfeng Chen and Jian Ma. *Query-based data collection in wireless sensor networks with mobile sinks.* In Proceedings of the 2009 international conference on wireless communications and mobile computing: connecting the World wirelessly, pages 1157–1162. ACM, 2009.

[Cho 2011] Jin-Hee Cho, Ananthram Swami and Ray Chen. *A survey on trust management for mobile ad hoc networks.* IEEE Communications Surveys & Tutorials, vol. 13, no. 4, pages 562–583, 2011.

[Choi 2010] Seong-Yong Choi, Jin-Su Kim, Jung-Hyun Lee and Kee-Wook Rim. *REDM: Robust and energy efficient dynamic routing for a mobile sink in a*

multi hop sensor network. In Communication Software and Networks, 2010. ICCSN'10. Second International Conference on, pages 178–182. IEEE, 2010.

[Cobo 2015] Luis Cobo, Harold Castro and Alejandro Quintero. *A location routing protocol based on smart antennas for wireless sensor networks.* Indian Journal of Science and Technology, vol. 8, no. 11, 2015.

[Das 2015] Bijoy Das, Suman Sankar Bhunia, Sarbani Roy and Nandini Mukherjee. *Multi criteria routing in wireless sensor network using weighted product model and relative rating.* In Applications and Innovations in Mobile Computing (AIMoC), 2015, pages 132–136. IEEE, 2015.

[de Oliveira 1999] Eugénio de Oliveira, José Manuel Fonseca and Adolfo Steiger-Garção. *Multi-criteria negotiation on multi-agent systems.* CEEMAS'99, page 190, 1999.

[del Carmen Delgado-Roman 2013] M del Carmen Delgado-Roman and Carles Sierra. *A multi-agent approach to energy-aware wireless sensor networks organization.* In Agreement Technologies, pages 32–47. Springer, 2013.

[Devillé 2011] Maarten Devillé, Yann-Aël Le Borgne, Ann Nowé, P De Causmaecker, J Maervoet, T Messelis, K Verbeeck and T Vermeulen. *Reinforcement learning for energy efficient routing in wireless sensor networks.* In Proceedings of the 23rd Benelux Conference on Artificial Intelligence, pages 89–96, 2011.

[Di Francesco 2011] Mario Di Francesco, Sajal K Das and Giuseppe Anastasi. *Data collection in wireless sensor networks with mobile elements: A survey.* ACM Transactions on Sensor Networks (TOSN), vol. 8, no. 1, page 7, 2011.

[Dimarogonas 2009] Dimos V Dimarogonas and Karl Henrik Johansson. *Event-triggered control for multi-agent systems.* In Decision and Control, 2009 held jointly with the 2009 28th Chinese Control Conference. CDC/CCC 2009. Proceedings of the 48th IEEE Conference on, pages 7131–7136. IEEE, 2009.

[Duan 2013a] Junqi Duan, Deyun Gao, Chuan Heng Foh and Hongke Zhang. *TC-BAC: A trust and centrality degree based access control model in wireless sensor networks.* Ad Hoc Networks, vol. 11, no. 8, pages 2675–2692, 2013.

[Duan 2013b] Junqi Duan, Dong Yang, Sidong Zhang, Jing Zhao and Mikael Gidlund. *A trust management scheme for industrial wireless sensor networks.* In Industrial Electronics Society, IECON 2013-39th Annual Conference of the IEEE, pages 5576–5581. IEEE, 2013.

[Durfee 1989] Edmund H. Durfee, Victor R. Lesser and Daniel D Corkill. *Trends in cooperative distributed problem solving.* Knowledge and Data Engineering, IEEE Transactions on, vol. 1, no. 1, pages 63–83, 1989.

[Edalat 2012] Neda Edalat, Chen-Khong Tham and Wendong Xiao. *An auction-based strategy for distributed task allocation in wireless sensor networks.* Computer Communications, vol. 35, no. 8, pages 916–928, 2012.

[Elmakias 2008] David Elmakias. New computational methods in power system reliability, volume 111. Springer, 2008.

[Faheem 2009] Yasir Faheem, Saadi Boudjit and Ken Chen. *Data dissemination strategies in mobile sink wireless sensor networks: A survey.* In Wireless Days (WD), 2009 2nd IFIP, pages 1–6. IEEE, 2009.

[Fatima 2002] Shaheen S Fatima, Michael Wooldridge and Nicholas R Jennings. *Multi-issue negotiation under time constraints.* In Proceedings of the first international joint conference on Autonomous agents and multiagent systems: part 1, pages 143–150. ACM, 2002.

[Fatima 2004] Shaheen S Fatima, Michael Wooldridge and Nicholas R Jennings. *An agenda-based framework for multi-issue negotiation.* Artificial Intelligence, vol. 152, no. 1, pages 1–45, 2004.

[Feng 2011] Renjian Feng, Xiaofeng Xu, Xiang Zhou and Jiangwen Wan. *A trust evaluation algorithm for wireless sensor networks based on node behaviors and ds evidence theory.* Sensors, vol. 11, no. 2, pages 1345–1360, 2011.

[Fernández-Caramés 2018] Tiago M Fernández-Caramés and Paula Fraga-Lamas. *A Review on the Use of Blockchain for the Internet of Things.* IEEE Access, 2018.

[Forster 2009] Anna Forster and Amy L Murphy. *CLIQUE: Role-free clustering with Q-learning for Wireless Sensor Networks.* In Distributed Computing Systems, 2009. ICDCS'09. 29th IEEE International Conference on, pages 441–449. IEEE, 2009.

[Fredrick 2015] Fredrick. *Modelling Performability Evaluation of WSN.* PhD dissertation, School of Science and Technology, 2015.

[Fuentes-Fernández 2009] Rubén Fuentes-Fernández, María Guijarro and Gonzalo Pajares. *A multi-agent system architecture for sensor networks.* Sensors, vol. 9, no. 12, pages 10244–10269, 2009.

[Gan 2004] Long Gan, Jiming Liu and Xiaolong Jin. *Agent-based, energy efficient routing in sensor networks.* In Proceedings of the Third International Joint Conference on Autonomous Agents and Multiagent Systems-Volume 1, pages 472–479. IEEE Computer Society, 2004.

[Gandham 2003] Shashidhar Rao Gandham, Milind Dawande, Ravi Prakash and Subbarayan Venkatesan. *Energy efficient schemes for wireless sensor networks with multiple mobile base stations.* In Global telecommunications conference, 2003. GLOBECOM'03. IEEE, volume 1, pages 377–381. IEEE, 2003.

[Garcia 2013] Eloy Garcia, Yongcan Cao, Han Yu, Panos Antsaklis and David Casbeer. *Decentralised event-triggered cooperative control with limited communication.* International Journal of Control, no. ahead-of-print, pages 1–10, 2013.

[Gautam 2009] Navin Gautam, Won-Il Lee and Jae-Young Pyun. *Dynamic clustering and distance aware routing protocol for wireless sensor networks.* In Proceedings of the 6th ACM symposium on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks, pages 9–14. ACM, 2009.

[Gong 2010] Wei Gong, Zhiyang You, Danning Chen, Xibin Zhao, Ming Gu and Kwok-Yan Lam. *Trust based routing for misbehavior detection in ad hoc networks.* Journal of Networks, vol. 5, no. 5, page 551, 2010.

[Gowrishankar 2008] S Gowrishankar, TG Basavaraju, DH Manjaiah and Subir Kumar Sarkar. *Issues in wireless sensor networks.* In Proceedings of the World Congress on Engineering, volume 1, 2008.

[Goyal 2012] Deepak Goyal and Malay Ranjan Tripathy. *Routing protocols in wireless sensor networks: A survey.* In Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on, pages 474–480. IEEE, 2012.

[Grammalidis 2011] Nikos Grammalidis, Enis Çetin, Kosmas Dimitropoulos, Filareti Tsalakanidou, Kivanc Kose, Osman Gunay, Benedict Gouverneur, Dino Torri, Ercan Kuruoglu, Saverio Tozzi*et al. A multi-sensor network for the protection of cultural heritage.* In Signal Processing Conference, 2011 19th European, pages 889–893. IEEE, 2011.

[Gupta 2010] Anuj K Gupta, Harsh Sadawarti and Anil K Verma. *Performance analysis of AODV, DSR & TORA routing protocols.* International Journal of Engineering and Technology, vol. 2, no. 2, page 226, 2010.

[Han 2014] Guangjie Han, Jinfang Jiang, Lei Shu, Jianwei Niu and Han-Chieh Chao. *Management and applications of trust in Wireless Sensor Networks: A survey.* Journal of Computer and System Sciences, vol. 80, no. 3, pages 602–617, 2014.

[Hassan 2008] Jahan Hassan, Harsha Sirisena and Björn Landfeldt. *Trust-based fast authentication for multiowner wireless networks.* IEEE Transactions on Mobile Computing, vol. 7, no. 2, pages 247–261, 2008.

[Heinzelman 2000] Wendi Rabiner Heinzelman, Anantha Chandrakasan and Hari Balakrishnan. *Energy-efficient communication protocol for wireless microsensor networks.* In System Sciences, 2000. Proceedings of the 33rd Annual Hawaii International Conference on, pages 10–pp. IEEE, 2000.

[Henningsson 2008] Toivo Henningsson, Erik Johannesson and Anton Cervin. *Sporadic event-based control of first-order linear stochastic systems.* Automatica, vol. 44, no. 11, pages 2890–2895, 2008.

[Hu 2010] Tiansi Hu and Yunsi Fei. *QELAR: a machine-learning-based adaptive routing protocol for energy-efficient and lifetime-extended underwater sensor networks.* Mobile Computing, IEEE Transactions on, vol. 9, no. 6, pages 796–809, 2010.

[Huang 2005] Chi-Fu Huang and Yu-Chee Tseng. *The coverage problem in a wireless sensor network.* Mobile networks and Applications, vol. 10, no. 4, pages 519–528, 2005.

[Huynh 2006] Trung Dong Huynh, Nicholas R Jennings and Nigel R Shadbolt. *An integrated trust and reputation model for open multi-agent systems.* Autonomous Agents and Multi-Agent Systems, vol. 13, no. 2, pages 119–154, 2006.

[Intanagonwiwat 2000] Chalermek Intanagonwiwat, Ramesh Govindan and Deborah Estrin. *Directed diffusion: a scalable and robust communication paradigm for sensor networks.* In Proceedings of the 6th annual international conference on Mobile computing and networking, pages 56–67. ACM, 2000.

[Jadidoleslamy 2013] Hossein Jadidoleslamy. *AN INTRODUCTION TO VARIOUS BASIC CONCEPTS OF CLUSTERING TECHNIQUES ON WIRELESS SENSOR NETWORKS.* International journal, 2013.

[Jennings 1998] Nicholas R Jennings and Michael Wooldridge. *Applications of intelligent agents.* In Agent technology, pages 3–28. Springer, 1998.

[Jennings 2001] Nicholas R Jennings, Peyman Faratin, Alessio R Lomuscio, Simon Parsons, Michael J Wooldridge and Carles Sierra. *Automated negotiation: prospects, methods and challenges.* Group Decision and Negotiation, vol. 10, no. 2, pages 199–215, 2001.

[Jiang 2015] Jinfang Jiang, Guangjie Han, Feng Wang, Lei Shu and Mohsen Guizani. *An efficient distributed trust model for wireless sensor networks.*

IEEE transactions on parallel and distributed systems, vol. 26, no. 5, pages 1228–1237, 2015.

[Kaler 2010] Er Barjinder Singh Kaler and Er Manpreet Kaur Kaler. *Challenges in wireless sensor networks.* Proc. of ISCET, 2010.

[Kamath 2013] H Srikanth Kamath. *Energy Efficient Routing Protocol for Wireless Sensor Networks.* International Journal of Advanced Computer Research, vol. 3, no. 2, pages 95–100, 2013.

[Karp 2000] Brad Karp and Hsiang-Tsung Kung. *GPSR: Greedy perimeter stateless routing for wireless networks.* In Proceedings of the 6th annual international conference on Mobile computing and networking, pages 243–254. ACM, 2000.

[Khalid 2017] Nor Azimah Khalid and Quan Bai. *Adaptive Forwarder Selection for Distributed Wireless Sensor Networks.* In Multi-agent and Complex Systems, pages 95–107. Springer, 2017.

[Khan 2012] Wazir Zada Khan, NM Saad and Mohammed Y Aalsalem. *An overview of evaluation metrics for routing protocols in wireless sensor networks.* In Intelligent and Advanced Systems (ICIAS), 2012 4th International Conference on, volume 2, pages 588–593. IEEE, 2012.

[Khoufi 2017] Ines Khoufi, Pascale Minet, Anis Laouiti and Saoucene Mahfoudh. *Survey of deployment algorithms in wireless sensor networks: coverage and connectivity issues and challenges.* International Journal of Autonomous and Adaptive Communications Systems, vol. 10, no. 4, pages 341–390, 2017.

[Klein 2008] Mark Klein*et al. A Multi-Issue Negotiation Protocol Among Nonlinear Utility Agents: A Preliminary Report.* In Rational, Robust, and Secure Negotiations in Multi-Agent Systems, pages 25–38. Springer, 2008.

[Kweon 2009] Kisuk Kweon, Hojin Ghim, Jaeyoung Hong and Hyunsoo Yoon. *Grid-based energy-efficient routing from multiple sources to multiple mobile sinks in wireless sensor networks.* In Wireless pervasive computing, 2009. ISWPC 2009. 4th international symposium on, pages 1–5. IEEE, 2009.

[Lai 2006] Guoming Lai, Katia Sycara and Cuihong Li. *A decentralized model for multi-attribute negotiations.* In Proceedings of the 8th international conference on Electronic commerce: The new e-commerce: innovations for conquering current barriers, obstacles and limitations to conducting successful business on the internet, pages 3–10. ACM, 2006.

[Lai 2008a] Guoming Lai, Cuihong Li and Katia Sycara. *A general model for pareto optimal multi-attribute negotiations.* In Rational, Robust, and Secure Negotiations in Multi-Agent Systems, pages 59–80. Springer, 2008.

[Lai 2008b] Guoming Lai, Katia Sycara and Cuihong Li. *A decentralized model for multi-attribute negotiations with incomplete information and general utility functions.* In Rational, Robust, and Secure Negotiations in Multi-Agent Systems, pages 39–57. Springer, 2008.

[Le 2012] Thao P Le, Timothy J Norman and Wamberto Vasconcelos. *Adaptive negotiation in managing wireless sensor networks.* In Principles and Practice of Multi-Agent Systems, pages 121–136. Springer, 2012.

[Lee 2010] Wang-Chien Lee. *Uncertainty in wireless sensor networks.* In Workshop on AFRL, 2010.

[Leligou 2012] Helen-Catherine Leligou, Panagiotis Trakadas, Sotirios Maniatis, Panagiotis Karkazis and T Zahariadis. *Combining trust with location information for routing in wireless sensor networks.* Wireless Communications and Mobile Computing, vol. 12, no. 12, pages 1091–1103, 2012.

[Li 2010a] Qiao Li, Lingguo Cui, Baihai Zhang and Zhun Fan. *A low energy intelligent clustering protocol for wireless sensor networks.* In Industrial Technology (ICIT), 2010 IEEE International Conference on, pages 1675–1682. IEEE, 2010.

[Li 2010b] Yukun Li, Zhipeng Gao, Yang Yang, Zhili Guan, Xingyu Chen and Xuesong Qiu. *A cluster-based negotiation model for task allocation in Wireless Sensor Network.* In Network and Service Management (CNSM), 2010 International Conference on, pages 112–117. IEEE, 2010.

[Li 2011a] Changle Li, Hanxiao Zhang, Binbin Hao and Jiandong Li. *A survey on routing protocols for large-scale wireless sensor networks.* Sensors, vol. 11, no. 4, pages 3498–3526, 2011.

[Li 2011b] Tao Li, Minyue Fu, Lihua Xie and Ji-Feng Zhang. *Distributed consensus with limited communication data rate.* Automatic Control, IEEE Transactions on, vol. 56, no. 2, pages 279–292, 2011.

[Li 2013] Zhongkui Li, Wei Ren, Xiangdong Liu and Lihua Xie. *Distributed consensus of linear multi-agent systems with adaptive dynamic protocols.* Automatica, 2013.

[Liang 2010] Weifa Liang, Jun Luo and Xu Xu. *Prolonging network lifetime via a controlled mobile sink in wireless sensor networks.* In Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE, pages 1–6. IEEE, 2010.

[Lunze 2010] Jan Lunze and Daniel Lehmann. *A state-feedback approach to event-based control.* Automatica, vol. 46, no. 1, pages 211–215, 2010.

[Luo 2005] Jun Luo and J-P Hubaux. *Joint mobility and routing for lifetime elongation in wireless sensor networks.* In INFOCOM 2005. 24th annual joint conference of the IEEE computer and communications societies. Proceedings IEEE, volume 3, pages 1735–1746. IEEE, 2005.

[Manjeshwar 2002] Arati Manjeshwar and Dharma P Agrawal. *APTEEN: A Hybrid Protocol for Efficient Routing and Comprehensive Information Retrieval in Wireless Sensor Networks.* In ipdps, volume 2, page 48, 2002.

[Mazieres 2015] David Mazieres. *The stellar consensus protocol: A federated model for internet-level consensus.* Stellar Development Foundation, 2015.

[Mcknight 1996] DH Mcknight and NL Chervany. *The meanings of trust: University of Minnesota, Technical reports*, 1996.

[Melese 2010] Desalegn Getachew Melese, Huagang Xiong and Qiang Gao. *Consumed energy as a factor for cluster head selection in wireless sensor net-*

works. In Wireless Communications Networking and Mobile Computing (WiCOM), 2010 6th International Conference on, pages 1–4. IEEE, 2010.

[Meng 2013] Xiangyu Meng and Tongwen Chen. *Event based agreement protocols for multi-agent networks.* Automatica, 2013.

[Minet 2009] P Minet. *Energy efficient routing.* Ad Hoc and Sensor Wireless Networks: Architectures: Algorithms and Protocols, 2009.

[Mir 2007] Zeeshan Hameed Mir and Young-Bae Ko. *A quadtree-based hierarchical data dissemination for mobile sensor networks.* Telecommunication Systems, vol. 36, no. 1-3, pages 117–128, 2007.

[Naderan 2013] Marjan Naderan, Mehdi Dehghan and Hossein Pedram. *Sensing task assignment via sensor selection for maximum target coverage in WSNs.* Journal of Network and Computer Applications, vol. 36, no. 1, pages 262–273, 2013.

[Nakamoto 2008] Satoshi Nakamoto. *Bitcoin: A peer-to-peer electronic cash system.* 2008.

[Nayak 2016] Padmalaya Nayak and Anurag Devulapalli. *A fuzzy logic-based clustering algorithm for wsn to extend the network lifetime.* IEEE sensors journal, vol. 16, no. 1, pages 137–144, 2016.

[Nguyen 2009] Dang-Quan Nguyen, Louise Lamont and Peter C Mason. *On Trust Evaluation in Mobile Ad Hoc Networks.* In MobiSec, pages 1–13. Springer, 2009.

[Niemann 2009] Christoph Niemann and Florian Lang. *Assess Your Opponent: A Bayesian Process for Preference Observation in Multi-attribute Negotiations.* In Advances in Agent-Based Complex Automated Negotiations, pages 119–137. Springer, 2009.

[OâDwyer 2015] Rachel OâDwyer. *The Revolution will (not) be Decentralized: Blockchains.* Commons Transition, vol. 11, 2015.

[Olivier 2018] Frédéric Olivier. *Solutions for Integrating Photovoltaic Panels Into Low-voltage Distribution Networks.* PhD thesis, Université de Liège,â Liège,ââ Belgique, 2018.

[Pantazis 2013] Nikolaos A Pantazis, Stefanos A Nikolidakis and Dimitrios D Vergados. *Energy-efficient routing protocols in wireless sensor networks: A survey.* IEEE Communications surveys & tutorials, vol. 15, no. 2, pages 551–591, 2013.

[Papadimitriou 2005] Ioannis Papadimitriou and Leonidas Georgiadis. *Maximum lifetime routing to mobile sink in wireless sensor networks.* In Proc. SoftCOM, 2005.

[Park 1997] Vincent Douglas Park and M Scott Corson. *A highly adaptive distributed routing algorithm for mobile wireless networks.* In INFOCOM'97. Sixteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Driving the Information Revolution., Proceedings IEEE, volume 3, pages 1405–1413. IEEE, 1997.

[Patil 2012] VP Patil. *Effect of traffic type on the performance of table driven and on demand routing protocols of manet.* International Journal Of Computational Engineering Research (ijceronline. com) Vol, vol. 2, 2012.

[Pereira 2016] Vasco Nuno Simões Pereira. *Performance Measurement in Wireless Sensor Networks.* PhD thesis, 2016.

[Pinyol 2013] Isaac Pinyol and Jordi Sabater-Mir. *Computational trust and reputation models for open multi-agent systems: a review.* Artificial Intelligence Review, vol. 40, no. 1, pages 1–25, 2013.

[Qu 2013] Chuanhao Qu, Lei Ju, Zhiping Jia, Huaqiang Xu and Longpeng Zheng. *Light-weight trust-based on-demand multipath routing protocol for mobile ad hoc networks.* In Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on, pages 42–49. IEEE, 2013.

[Raja 2016] B Raja, R Rajakumar, P Dhavachelvan and T Vengattaraman. *A survey on classification of network structure routing protocols in wireless sensor networks.* In Computational Intelligence and Computing Research (ICCIC), 2016 IEEE International Conference on, pages 1–5. IEEE, 2016.

[Ramchurn 2004] Sarvapali D Ramchurn, Dong Huynh and Nicholas R Jennings. *Trust in multi-agent systems.* The Knowledge Engineering Review, vol. 19, no. 01, pages 1–25, 2004.

[Rani 2014] V Uma Rani and K Soma Sundaram. *Review of trust models in wireless sensor networks.* Int. J. Comput. Inf. Syst. Control Eng, vol. 8, pages 371–377, 2014.

[Raval 2016] Siraj Raval. Decentralized applications: Harnessing bitcoin's blockchain technology. " O'Reilly Media, Inc.", 2016.

[Ren 2011] Wei Ren and Yongcan Cao. *Overview of recent research in distributed multi-agent coordination.* In Distributed Coordination of Multi-agent Networks, pages 23–41. Springer, 2011.

[Reyna 2018] Ana Reyna, Cristian Martín, Jaime Chen, Enrique Soler and Manuel Díaz. *On blockchain and its integration with IoT. Challenges and opportunities.* Future Generation Computer Systems, 2018.

[Saaty 1980] Thomas L Saaty and Luis G Vargas. *Hierarchical analysis of behavior in competition: Prediction in chess.* Behavioral science, vol. 25, no. 3, pages 180–191, 1980.

[Saaty 1991] Thomas Lorie Saaty and Luis Gonzalez Vargas. Prediction, projection, and forecasting: applications of the analytic hierarchy process in economics, finance, politics, games, and sports. Kluwer Academic Pub, 1991.

[Sabater 2001] Jordi Sabater and Carles Sierra. *Regret: A reputation model for gregarious societies.* In Fourth workshop on deception fraud and trust in agent societies, volume 70, 2001.

[Sadagopan 2003] Narayanan Sadagopan, Bhaskar Krishnamachari and Ahmed Helmy. *The ACQUIRE mechanism for efficient querying in sensor networks.* In Sensor Network Protocols and Applications, 2003. Proceedings of the First IEEE. 2003 IEEE International Workshop on, pages 149–155. IEEE, 2003.

[Sahoo 2010] Prasan Kumar Sahoo, Jang-Zern Tsai and Hong-Lin Ke. *Vector method based coverage hole recovery in Wireless Sensor Networks.* In COMSNETS, pages 1–9, 2010.

[Senouci 2014] Mustapha Reda Senouci, Abdelhamid Mellouk and Amar Aissani. *Random deployment of wireless sensor networks: a survey and approach.* International Journal of Ad Hoc and Ubiquitous Computing, vol. 15, no. 1-3, pages 133–146, 2014.

[Shah 2002] Rahul C Shah and Jan M Rabaey. *Energy aware routing for low energy ad hoc sensor networks.* In Wireless Communications and Networking Conference, 2002. WCNC2002. 2002 IEEE, volume 1, pages 350–355. IEEE, 2002.

[Shah 2003] Rahul C Shah, Sumit Roy, Sushant Jain and Waylon Brunette. *Data mules: Modeling and analysis of a three-tier architecture for sparse sensor networks.* Ad Hoc Networks, vol. 1, no. 2-3, pages 215–233, 2003.

[Shah 2007] Kunal Shah and Mohan Kumar. *Distributed independent reinforcement learning (DIRL) approach to resource management in wireless sensor networks.* In Mobile Adhoc and Sensor Systems, 2007. MASS 2007. IEEE Internatonal Conference on, pages 1–9. IEEE, 2007.

[Shah 2011] Kunal Shah, Mario Di Francesco, Giuseppe Anastasi and Mohan Kumar. *A framework for resource-aware data accumulation in sparse wireless sensor networks.* Computer Communications, vol. 34, no. 17, pages 2094–2103, 2011.

[Shah 2012] Kunal Shah, Mario Di Francesco and Mohan Kumar. *Distributed resource management in wireless sensor networks using reinforcement learning.* Wireless Networks, pages 1–20, 2012.

[Sharma 2016] Vikrant Sharma, RB Patel, HS Bhadauria and D Prasad. *Deployment schemes in wireless sensor network to achieve blanket coverage in large-scale open area: A review.* Egyptian Informatics Journal, vol. 17, no. 1, pages 45–56, 2016.

[Simon 1996] Herbert A Simon. The sciences of the artificial. MIT press, 1996.

[Singh 2015] Surjit Singh and Rajeev Mohan Sharma. *Some aspects of coverage awareness in wireless sensor networks.* Procedia Computer Science, vol. 70, pages 160–165, 2015.

[Su 2010] Xing Su, Minjie Zhang, Yi Mu and Kwang Mong Sim. *Pbtrust: A priority-based trust model for service selection in general service-oriented environments.* In Embedded and Ubiquitous Computing (EUC), 2010 IEEE/IFIP 8th International Conference on, pages 841–848. IEEE, 2010.

[Sun 2012] Yan Sun, Hong Luo and Sajal K Das. *A trust-based framework for fault-tolerant data aggregation in wireless multimedia sensor networks.* IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 6, pages 785–797, 2012.

[Szabo 1997] Nick Szabo. *Formalizing and securing relationships on public networks.* First Monday, vol. 2, no. 9, 1997.

[Tian 2003] Di Tian and Nicolas D Georganas. *A node scheduling scheme for energy conservation in large wireless sensor networks.* Wireless Communications and Mobile Computing, vol. 3, no. 2, pages 271–290, 2003.

[Tscheikner-Gratl 2017] Franz Tscheikner-Gratl, Patrick Egger, Wolfgang Rauch and Manfred Kleidorfer. *Comparison of multi-criteria decision support methods for integrated rehabilitation prioritization.* Water, vol. 9, no. 2, page 68, 2017.

[Tschorsch 2016] Florian Tschorsch and Björn Scheuermann. *Bitcoin and beyond: A technical survey on decentralized digital currencies.* IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pages 2084–2123, 2016.

[Tunca 2014] Can Tunca, Sinan Isik, Mehmet Yunus Donmez and Cem Ersoy. *Distributed mobile sink routing for wireless sensor networks: A survey.* Communications Surveys & Tutorials, IEEE, vol. 16, no. 2, pages 877–897, 2014.

[Tyagi 2012] Sudhanshu Tyagi and Neeraj Kumar. *A systematic review on clustering and routing techniques based upon LEACH protocol for wireless sensor networks.* Journal of Network and Computer Applications, 2012.

[Tzeng 2011] Gwo-Hshiung Tzeng and Jih-Jeng Huang. Multiple attribute decision making: methods and applications. Chapman and Hall/CRC, 2011.

[Van Dyke Parunak 1997] H Van Dyke Parunak. *" Go to the ant": Engineering principles from natural multi-agent systems.* Annals of Operations Research, vol. 75, pages 69–101, 1997.

[Vecchio 2010] Massimo Vecchio, Aline Carneiro Viana, Artur Ziviani and Roy Friedman. *DEEP: Density-based proactive data dissemination protocol for wireless sensor networks with uncontrolled sink mobility.* Computer Communications, vol. 33, no. 8, pages 929–939, 2010.

[Vinyals 2011] Meritxell Vinyals, Juan A Rodriguez-Aguilar and Jesus Cerquides. *A survey on sensor networks from a multiagent perspective.* The Computer Journal, vol. 54, no. 3, pages 455–470, 2011.

[Voulkidis 2013] Artemis C Voulkidis, Markos P Anastasopoulos and Panayotis G Cottis. *Energy efficiency in wireless sensor networks: A game-theoretic approach based on coalition formation.* ACM Transactions on Sensor Networks (TOSN), vol. 9, no. 4, page 43, 2013.

[Wang 2005] Z Maria Wang, Stefano Basagni, Emanuel Melachrinoudis and Chiara Petrioli. *Exploiting sink mobility for maximizing sensor networks lifetime.* In System Sciences, 2005. HICSS'05. Proceedings of the 38th Annual Hawaii International Conference on, pages 287a–287a. IEEE, 2005.

[Wang 2006] Guiling Wang, Guohong Cao and Thomas F La Porta. *Movement-assisted sensor deployment.* IEEE Transactions on Mobile Computing, vol. 5, no. 6, pages 640–652, 2006.

[Wang 2009] Guojun Wang, Tian Wang, Weijia Jia, Minyi Guo and Jie Li. *Adaptive location updates for mobile sinks in wireless sensor networks.* The Journal of Supercomputing, vol. 47, no. 2, pages 127–145, 2009.

[Wang 2011] Bang Wang. *Coverage problems in sensor networks: A survey.* ACM Computing Surveys (CSUR), vol. 43, no. 4, page 32, 2011.

[Wang 2014] Bo Wang, Xunxun Chen and Weiling Chang. *A light-weight trust-based QoS routing algorithm for ad hoc networks.* Pervasive and Mobile Computing, vol. 13, pages 164–180, 2014.

[Wen 2013] Guanghui Wen, Zhongkui Li, Zhisheng Duan and Guanrong Chen. *Distributed consensus control for linear multi-agent systems with discontinuous observations.* International Journal of Control, vol. 86, no. 1, pages 95–106, 2013.

[Wood 2014] Gavin Wood. *Ethereum: A secure decentralised generalised transaction ledger.* Ethereum project yellow paper, vol. 151, pages 1–32, 2014.

[Wu 2009] Mengxiao Wu, Mathijs de Weerdt and Han La Poutré. *Efficient methods for multi-agent multi-issue negotiation: allocating resources.* In Principles of Practice in Multi-Agent Systems, pages 97–112. Springer, 2009.

[Wu 2011] Mengxiao Wu, Mathijs de Weerdt, Han La Poutré, Chetan Yadati, Yingqian Zhang and Cees Witteveen. *Multi-player Multi-issue Negotiation with Complete Information.* In Innovations in Agent-Based Complex Automated Negotiations, pages 147–159. Springer, 2011.

[Wüst 2017] Karl Wüst and Arthur Gervais. *Do you need a Blockchain?* IACR Cryptology ePrint Archive, vol. 2017, page 375, 2017.

[Wüst 2018] Karl Wüst and Arthur Gervais. *Do you need a Blockchain?* In 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), pages 45–54. IEEE, 2018.

[Xie 2009] Guangming Xie, Huiyang Liu, Long Wang and Yingmin Jia. *Consensus in networked multi-agent systems via sampled control: fixed topology case.* In American Control Conference, 2009. ACC'09., pages 3902–3907. IEEE, 2009.

[Xing 2005] Guoliang Xing, Xiaorui Wang, Yuanfang Zhang, Chenyang Lu, Robert Pless and Christopher Gill. *Integrated coverage and connectivity configuration for energy conservation in sensor networks.* ACM Transactions on Sensor Networks (TOSN), vol. 1, no. 1, pages 36–72, 2005.

[Yao 2006] Zhiying Yao, Daeyoung Kim and Yoonmee Doh. *PLUS: Parameterized and localized trust management scheme for sensor networks security.* 2006.

[Ye 2005] Fan Ye, Gary Zhong, Songwu Lu and Lixia Zhang. *Gradient broadcast: A robust data delivery protocol for large scale sensor networks.* Wireless Networks, vol. 11, no. 3, pages 285–298, 2005.

[Ye 2011] Dayong Ye, Minjie Zhang and Quan Bai. *A composite self-organisation mechanism in an agent network.* In Web Information System Engineering–WISE 2011, pages 249–256. Springer, 2011.

[Yu 2007] Fang Yu, Yun Li, Fei Fang and Qianbin Chen. *A new TORA-based energy aware routing protocol in mobile ad hoc networks.* In Internet, 2007. ICI 2007. 3rd IEEE/IFIP International Conference in Central Asia on, pages 1–4. IEEE, 2007.

[Yu 2012] Chao Yu, Minjie Zhang and Fenghui Ren. *Exploiting independent relationships in multiagent systems for coordinated learning.* In PRICAI 2012: Trends in Artificial Intelligence, pages 686–697. Springer, 2012.

[Yu 2013] Han Yu, Zhiqi Shen, Cyril Leung, Chunyan Miao and Victor R Lesser. *A survey of multi-agent trust management systems.* IEEE Access, vol. 1, pages 35–50, 2013.

[Yuan 2011] Xun-Xin Yuan and Rui-Hua Zhang. *An energy-efficient mobile sink routing algorithm for wireless sensor networks.* In Wireless communications, networking and mobile computing (WiCOM), 2011 7th international conference on, pages 1–4. IEEE, 2011.

[Yun 2010] YoungSang Yun and Ye Xia. *Maximizing the lifetime of wireless sensor networks with mobile sink in delay-tolerant applications.* IEEE Transactions on mobile computing, vol. 9, no. 9, pages 1308–1318, 2010.

[Zahariadis 2013] Theodore Zahariadis, Panagiotis Trakadas, Helen C Leligou, Sotiris Maniatis and Panagiotis Karkazis. *A novel trust-aware geographical routing scheme for wireless sensor networks.* Wireless personal communications, vol. 69, no. 2, pages 805–826, 2013.

[Zhan 2010] Guoxing Zhan, Weisong Shi and Julia Deng. *Tarf: A trust-aware routing framework for wireless sensor networks.* Wireless Sensor Networks, pages 65–80, 2010.

[Zhang 2005] Honghai Zhang and Jennifer C Hou. *Maintaining sensing coverage and connectivity in large sensor networks.* Ad Hoc & Sensor Wireless Networks, vol. 1, no. 1-2, pages 89–124, 2005.

[Zhu 2012] Chuan Zhu, Chunlin Zheng, Lei Shu and Guangjie Han. *A survey on coverage and connectivity issues in wireless sensor networks.* Journal of Network and Computer Applications, vol. 35, no. 2, pages 619–632, 2012.