TRUST COMPUTATIONAL MODELS FOR MOBILE AD HOC NETWORKS

A.R.M. SHABUT

PhD

UNIVERSITY OF BRADFORD

2015

Trust Computational Models for Mobile Ad Hoc Networks

Recommendation Based Trustworthiness Evaluation using Multidimensional Metrics to Secure Routing Protocol in Mobile Ad Hoc Networks

Antesar Ramadan M SHABUT

Submitted for the degree of

Doctor of Philosophy

School of Computing

Faculty of Engineering and Informatics

University of Bradford

2015

Abstract

Antesar Ramadan M SHABUT

Trust Computational Models for Mobile Ad Hoc Networks

Recommendation Based Trustworthiness Evaluation using Multidimensional Metrics to Secure Routing Protocol in Mobile Ad Hoc Networks

Keyword: Trust, Reputation, Trust management, Trust Models; Mobile Ad Hoc Networks; Recommendation Management, Dishonest Recommendation, Multidimensional Trust Metric, Social Trust, QoS Trust.

Distributed systems like e-commerce and e-market places, peer-to-peer networks, social networks, and mobile ad hoc networks require cooperation among the participating entities to guarantee the formation and sustained existence of network services. The reliability of interactions among anonymous entities is a significant issue in such environments. The distributed entities establish connections to interact with others, which may include selfish and misbehaving entities and result in bad experiences. Therefore, trustworthiness evaluation using trust management techniques has become a significant issue in securing these environments to allow entities decide on the reliability and trustworthiness of other entities, besides it helps coping with defection problems and stimulating entities to cooperate. Recent models on evaluating trustworthiness in distributed systems have heavily focused on assessing trustworthiness of entities and isolate misbehaviours based on single trust metrics. Less effort has been put on the investigation of the subjective nature and differences in the way trustworthiness is perceived to produce a composite multidimensional trust metrics to overcome the limitation of considering single trust metric. In the

light of this context, this thesis concerns the evaluation of entities' trustworthiness by the design and investigation of trust metrics that are computed using multiple properties of trust and considering environment.

Based on the concept of probabilistic theory of trust management technique, this thesis models trust systems and designs cooperation techniques to evaluate trustworthiness in mobile ad hoc networks (MANETs). A recommendation based trust model with multi-parameters filtering algorithm, and multidimensional metric based on social and QoS trust model are proposed to secure MANETs. Effectiveness of each of these models in evaluating trustworthiness and discovering misbehaving nodes prior to interactions, as well as their influence on the network performance has been investigated. The results of investigating both the trustworthiness evaluation and the network performance are promising.

Declaration

I hereby declare that this thesis has been genuinely carried out by myself and has not been used in any previous application for a degree. Chapters 4 to 6 describe work performed with me in the present of guides and support of my supervisors, Prof. K. P. Dahal and Prof. Irfan Awan. These chapters have been accepted for publication (as shown in the publication list). The invaluable participation of others in this thesis has been acknowledged where appropriate.

Antesar M. Shabut

Dedication

This thesis is dedicated to my beloved parents, whose love, help, support and prayers are the reason why I am where I am today. My wonderful husband, who provides me with love, support, and help. My beloved children Ahmed, Oriada, Lamar, and Mohamed whose make my life full of motivation and fun, this thesis is for you.

Acknowledgment

All praise and thanks to Allah the All-Merciful the All-Beneficent, for granting me the ability and strength to complete this doctoral thesis.

I am using this opportunity to express my gratitude to everyone who supported me throughout the course of this research. I am thankful for their invaluable guidance and friendly advice during the four years of this study. First of all, I would like to express my deepest appreciation to my supervisor Prof. Keshav Dahal who has supported me throughout my thesis and provided me with knowledge and guidance. His kindness, patience, encouragement, and endless support even when he has left the University of Bradford have a great impact on why I am where I am today. I would like to express my profound sense of reverence to my supervisor Prof. Irfan Awan for his constant guidance, support, motivation and help during the course of my PhD. I have been very lucky to have supervisors who concerned about my work, and responded to my questions and queries so promptly.

I would like to thank Dr. Sanat Bista for helping me in the publication of my Journal. Being a researcher in the same area of trust, I always find his comments, questions and suggestions in the journal manuscript very challenging and helpful in enhancing the writing and presentation of the journal paper.

I would like to express my appreciation to all the staff at the School of Computing, technical support office, as well as, Hub and the library. I would also like to express my warm thanks to my colleague Dr. Guzlan Miskeen who as a good friend provided me with valuable advice, fruitful discussions, suggestions, and cooperation.

I would like to express my profound gratitude to my husband Elsadek Abdelkarim for providing me with continuous love at all times. His support in pursuing my study is invaluable to me.

I am deeply indebted to my family, relatives and friends who offered me great encouragement and support throughout my studies. My heartfelt thanks go to my parents, my children, my sisters and my brothers for their constant love, prayers, continuous support, and patience.

Many thanks also go to all of my friends, who support and encourage me, in particular; Rehab, Rabha, Halima, Asma, Wafa, Fatma, Hind, and others for their continuous support.

Finally, I would like to gratefully acknowledge the provision of the scholarship from the Ministry of Higher Education in Libya and the Libyan Cultural Attaché bureau in London.

List of Contents

List of Figures

List of Tables

List of Acronyms

MANET	Mobile Ad hoc NETwork
B2B	Business to Business
B2C	Business to Consumer
C2C	Consumer to Consumer
P2P	Peer-to-Peer
IP	Internet Protocol
TTP	Trusted Third Party
DSR	Dynamic Source Routing
PDF	Probability Density Function
NS2	Network Simulator 2
Otcl	Object oriented tool command language
AWK	Alfred V. Aho, Peter J. Weinberger, and Brian W. Kernighan
RREQ	Route REQuest
RREP	Route REPly
CBR	Constant Bit Rate
MAC	Media Access Control
AODV	Ad hoc On-demand Distance Vector
BMA	Bad Mouthing Attack
BSA	Ballot Stuffing Attack
SMA	Selective Misbehaviour Attack
IBA	Intelligent Behaviour Attack
TDA	Time-Dependent Attack
LDA	Location-Dependent Attack
TMUC	Trust Management in Ubiquitous Computing
TLE	Trust Level Error
MSN	Mobile Social Network

SNA	Social Network Analysis
QoS	Quality of Service
TDSR	Trusted DSR
STDSR	Social Trusted DSR
IPD	Iterated Prisoner's Dilemma
DHT	Distributed Hash Table
TON	Trust Overlay Network
RPGM	Reference Point Group Mobility

Chapter 1 Introduction

This chapter introduces the work conducted by this thesis in terms of explaining the motivation behind the research, aims and objectives. The chapter also explores the contributions made by the research work and lists the instances of previous publication of the results and outcomes. Further, a brief description of the organisation of the thesis is provided to explore the content of subsequent chapters.

1.1 Introduction

In recent years, there has been tremendous growth in the use of mobile wireless networks and in access to various mobile applications and services on the Internet. Services such as information sharing, routing and location issues have found ways to operate in mobile environments. For these reasons, a mobile ad hoc network (MANET) system model is proposed which consists of a collection of wireless mobile nodes that are capable of communicating with each other in the absence of a fixed network infrastructure or centralised administration. MANET is considered to represent infrastructureless networking, in which nodes dynamically set up a network and establish routing among themselves to build their own network when needed [1]. MANETs' applications are practically emerging as a provider of a flexible method to establish communications in situations where geographical constraints demand a totally distributed system without fixed base stations: for example, for emergency rescue services in events such as hurricane and earthquake disasters, and for exchanging critical information on the battlefield through networking [2]. However, MANET's characteristics, including frequent changes in network topology due to mobility or discontinuous operation of nodes, open wireless medium, and constrained

capability, make it vulnerable to security issues in situations where a friendly and cooperative environment is not assumed [3].

In the context of MANETs, there have been a number of schemes based on cryptography to provide solutions in order to secure such networks. Cryptography models often seem unrealistic because of their fundamental assumption of the trustworthiness of the participating nodes and underlying networking system [4]. Researchers have recognised the significance of borrowing trust management concepts from the social network analysis (SNA) field to improve the performance of the network protocols [5]. This move towards social methods in securing MANETs facilitates identification of trust attributes of nodes such as level of cooperation, honesty and the manner of behaving, to establish and manage trust relationships between nodes in a distributed manner. Trust management technique is one of the approved mechanisms to improve security in MANETs, and which is utilised to deal with misbehaving nodes and stimulate them to cooperate [6]. Relying on social properties in modelling trust can offer an attractive security mechanism to monitor node behaviour, mitigate attacks, and filter out dishonest nodes.

Trust as a social concept can be defined as the degree of subjective belief about the behaviour of a particular entity [7]. Trust in MANETs is the opinion held by one node (known as the evaluating node) about another node (known as the evaluated node), based upon the node's past behaviour and on recommendations from other nodes in the network, known as recommending nodes. Very much as in the case of the human observation process, trust here is based on the accumulation of observations from various similar or dissimilar sources, to collect and combine the required information to decide on the trustworthiness of a perceived node. Trust is

time dependent, meaning that it grows and decays over time. Therefore, MANETs show close similarities to the human behaviour model, as a number of nodes which have never interacted before are able to acquaint themselves and communicate with each other based on trust developed over a period of time [8]. Besides, nodes' perceptions, motivations, and goals for interactions are different, and the presence of a selfishness concept and avoidance of being victimised by others are also other aspects showing similarity to human behaviour [9]. Consequently, it is vital for a useful trust model to be related to human patterns of behaviour, because these patterns can be used to increase the model's quality in terms of deducing the degree of friendship, level of honesty, privacy, and the correctness of information derived from direct interactions or by recommendations [10]. Despite the fact that researchers have different disciplines in operationalising trust [11], the trust model is being increasingly adopted as an important concept in designing and analysing security problems in distributed systems to guide decision making [12].

Existing trust management frameworks for MANETs can be categorised into two types. The first establishes trust relationships between nodes based on direct interactions only [13 , 14]. The second type is based on direct observations of the node itself and recommendations provided by other nodes in the network [15 , 16]. The use of a recommendation-based trust technique can be advantageous to nodes in discovering misbehaving nodes prior to interaction, thus avoiding a potential bad experience. Using recommendations, nodes in MANETs can make more informed decisions on the selection of routing paths even if they have not had any direct interactions in the past [15]. Acquaintance can be made with several distant nodes (not neighbours) by sending a single packet to them, and this could help in

saving energy [17]. Together with the advantages comes the challenge of handling dishonest recommendations in MANETs. A trust model with a multi parameter defence scheme to filter out attacks related to dishonest recommendations such as bad-mouthing, ballot-stuffing, and collusion for mobile ad hoc networks is needed to solve the problem of dishonest recommendation.

Most trust models designed to secure MANETs rely on a single evaluation parameter only, such as monitoring cooperation during packet forwarding in routing protocols. However, the monitoring only of packet transmission between nodes in the network is shown to be unable to represent the complexity and subjectivity of trust metrics [18 , 19 , 20 , 21]. Trust models that rely only on the experience of packet forwarding in MANETs can only identify routes with a certain measure of confidence and may not be secured from various attacks, as well as, lacking the consideration of dynamic characteristics, and multi-source information of trust [8 , 11]. Multidimensional factors such as social information and quality of communications should thus be considered while managing trust-based routing in MANETs.

1.2 Motivation

Due to the recent applicability and performance of mobile ad hoc networks in future paradigms, including vehicular and mesh networks, as well as many civilian and military services ranging from emergency rescue services to exchanging critical information on the battlefield or even home and personal area networking, MANET's security has been investigated in the literature using different techniques. The formation and sustained existence of MANET services is mainly based on an individual node's cooperation in packet forwarding. It is indeed a challenge to safeguard MANETs with a lack of infrastructure (i.e. pre-existing communication backbone) and central

authority (such as base stations or mobile switching centres) to establish and facilitate communication in the network against a wide range of attacks. Due to these unique characteristics and demands for use, MANETs are vulnerable to attacks launched by misbehaving nodes [22]. Trust management techniques are put forward as one of the approved mechanisms to improve security in MANETs to deal with misbehaving nodes and stimulate them to cooperate [6].

In recent years, different trust management models have been proposed to enhance security in MANETs to enable nodes to evaluate their neighbours directly or through recommendations from other nodes in the network. CORE [23], Context-Aware Detection [24], CONFIDANT [18], to name a few, are mechanisms which support cooperation in ad hoc networks by detecting and isolating malicious nodes. Although the proposed models have paid attention to the problem of misbehaving nodes, multi-dimensional trust metrics including social properties of trust to deal with situations like dishonest recommendations are still in their early stages. This is considered a research gap in which the focus of such models is directed toward a single parameter only in computing trustworthiness. Whether the trust models that have been applied consider changing behaviours of the nodes (due to time or mobility) based on investigating some social properties or not is the major question that remains unaddressed by the literature. Many of the existing models seem to be filtering untrustworthy nodes by only considering a packet forwarding metric for example in improving the overall performance in the network and are not efficient enough in handling other misbehaving nodes related to dishonest recommendations. Further, some models omit some important evaluation metrics such as quality of service and social properties in evaluating nodes' trustworthiness. By considering this problem, a

trustworthiness evaluation mechanism should be effective in encouraging cooperation between nodes, enhancing the false negatives and false positives in judging the behaviour of nodes by utilising multi- dimensional trust attributes.

This work has been proposed to include multiple parameters to compute the trustworthiness of nodes. Its main emphasis is on utilising social properties of trust in evaluating trustworthiness and investigating trust relationships between nodes. An enhanced trust model with a feedback and recommendation system has been proposed by using multiple parameters to filter out dishonest recommendations and investigate the similarity in nodes' behaviours. Further, the trust model is developed to include certain social and QoS properties of trust to enhance the nodes' evaluation process when interacting with other nodes. Additionally, the proposed models have been tested by simulating a network with a wireless mobile ad hoc setting and it has been shown that a multiple-parameter metric for computing trustworthiness can help enhance network performance in terms of throughput, packet drops and energy percentages. Besides, the model can enhance the error of evaluating the trustworthiness of other nodes in terms of false negative and false positive percentages.

1.3 Contributions

This work establishes the use of trust management techniques in distributed systems including their unique characteristics and uses MANET as an application by modelling interactions and establishing trust among nodes to test the validity of the proposed work. Since MANETs are by nature made of mobile nodes, this work has been extended to cover and analyse nodes' mobility in all the investigated scenarios. Both analytical and empirical investigations are used to validate the proposed work. The work investigates

the state of the art of trust and reputation management in four important distributed applications; E-Commerce and E-Market, Peer-to-Peer Networks, Social Networks, and Mobile Ad Hoc Networks. Besides this, three well known techniques to compute trustworthiness, namely Game Theory, Fuzzy Theory and Probability Theory, are investigated in such distrusted applications. As a result of the investigation process of the trust concepts, models, and techniques in the four mentioned distrusted applications, this thesis contributes to the knowledge of trust models in MANET in the following areas:

1. The problem of evaluating and computing trustworthiness is defined by exploring the important components that should be combined to work together in the proposed trust model. Model parameters and assumptions of MANETs' applications have been comprehensively investigated.
2. A recommendation based trust monitoring model for securing ad hoc routing protocols to include three parameters of nodes past history as direct experience, indirect experience, and the ability to judge the others' trustworthiness has been proposed to filter out unfair ratings and isolate misbehaving nodes.
3. A set of parameters related to trust have been considered to enhance the feedback mechanisms, propagation and aggregation of recommendations, as well as filtering out dishonest recommendations.
4. Security analysis on the countermeasures relevant to five attacks which aim to distort the correctness of the received recommendations has been provided.
5. The implications of various methods in dealing with the data sparsity problem in establishing the trust relationship has been investigated to fill in the missing values of trust when a MANET has just been established.

6. An introduction of the social feature of a friendship based trust model is proposed to investigate the degree of friendship and represent trust relationships between nodes as human behaviour.
7. More social properties of trust are considered by proposing a trust model which uses multidimensional composition of its trust metric to enhance the trustworthiness evaluation of MANET's nodes, including both social and QoS properties of trust.
8. The model of trust is enhanced by including two different stages of evaluation; peer to peer evaluation and path evaluation, when evaluating the trustworthiness of other neighbours to decide whether to interact with them or not.
9. Route optimisation has been investigated in order to select the best path among the available trustworthy paths by allowing source nodes to evaluate the entire path to the destination.

1.4 Publications

The work in this thesis has been published and presented at several international and local events. A list of publications is provided based on the category of the event or publication, to include international conferences, journals, and presentations, as follows.

Conferences

Shabut, A., Dahal K.P., Awan I., (2012). A Trust-Based Monitoring Model for Mobile Ad hoc Networks. Proceedings of International conference on Software, Knowledge, Information Management and Applications (SKIMA 2012), China, 2012 (Chapter 4).

Shabut, A., Dahal K.P., Awan I., (2013). Enhancing Dynamic Recommender Selection Using Multiple Rules for Trust and Reputation Models in MANETs. Proceedings of IEEE International Conference on Tools with

Artificial Intelligence (ICTAI) - 2013, Washington DC, 2013 (Chapter 5).

Shabut, A., Dahal K.P., Awan I., (2014). Friendship Based Trust Model to Secure Routing Protocols in Mobile Ad hoc Networks. Proceedings of IEEE International Conference on Future Internet of Things and Cloud (FICloud) - 2014, Barcelona, Spain, 2014 (Chapter 6).

Journals

Shabut, A.; Dahal, K.; Bista, S.; Awan, I., Recommendation Based Trust Model with an Effective Defence Scheme for MANETs, Mobile Computing, IEEE Transactions on , vol.PP, no.99 , pp.1,1. doi: 10.1109/TMC.2014.2374154 (Chapter 5).

Tutorials

Shabut, A., Dahal K.P., Awan I., (2013). A Recommendation-Based Trust Model for MANETs to Enhance Dynamic Recommender Selection Using Multiple Rules, Seventh International Open Conference HET-NETs 2013, UK, Ilkely, 2013.

Shabut, A., Dahal K.P., Awan I., (2013). A Trust-Based Monitoring Model to Secure Routing Protocol in MANETs Using Enhanced Trust Metric, Seventh International Open Conference HET-NETs 2013, UK, Ilkely, 2013.

Presentations

Shabut, A., Dahal K.P., Trust and Reputation Management in Distributed Systems, University of Bradford school of computing, School Research seminars (2011).

Dahal K.P., Shabut, A., Trust Management in Distributed Systems: Defense against Misbehaving Players, 8th International Conference on

Software, Knowledge, Information Management and Applications (SKIMA 2014), 18-20, December 2014, Dhaka, Bangladesh.

1.5 Thesis Organisation

This chapter (**Chapter 1**) introduces the work and explains the motivation behind it, and also presents the research contributions.

Chapter 2 reviews the notion of trust and reputation and surveys a number of existing trust models in a variety of applications, to include E-Commerce and E-Market, Peer-to-Peer Networks, Social Networks, and Mobile Ad Hoc Networks. Several popular techniques to build and compute trustworthiness among entities in such environments are also examined.

Chapter 3 illustrates the problem of trust and reputation, which has been considered as the basis of this work. The chapter describes the probabilistic trust model utilised, along with its components and parameters. Besides this, the adopted research methodology is explored by describing the simulator and assumptions used to build trust in MANETs.

Chapter 4 introduces the proposed trust model that is used to monitor the behaviours of nodes in MANETs and establish the trust relationship based on the historical experiences and recommendations. The model considers the problem of a multidimensional trust metric to compute trustworthiness by introducing the concept of *opinion trust,* which shows how honest a node is as a recommender in the trust and reputation system.

Chapter 5 examines the problem of utilising recommendations in trust and reputation models in MANETs, and explores various attacks related to dishonest recommendations. Therefore, this chapter introduces the proposed recommendation-based trust model with a suitable filtering algorithm to deal

with dishonest recommendations through combining three different techniques. Further, it presents the problem of data sparsity and lack of information in the recommendation filtering algorithms, and introduces the proposed effective defence scheme, which utilises a clustering technique to dynamically filter out attacks related to dishonest recommendations within a certain time based on number of interactions, compatibility of information and closeness between the nodes in MANETs.

Chapter 6 introduces a friendship-based trust management model for MANETs to reflect nodes' behaviour and cope with multiple misbehaving attacks. The model utilised the social property of friendship degrees that is based on combining two social metrics: honesty and confidence. Besides, this chapter develops a proposed trust model with more social properties, which utilises a composite multidimensional metric to compute trust by combining the social properties of trust with quality of service (QoS) trust properties. Social and QoS properties of trust are examined through appropriate parameters based on the behaviour and characteristics of the nodes in MANETs.

Chapter 7 summarises the contributions of this thesis and makes some recommendations for future work.

Chapter 2 Literature Review

This chapter provides a review of the literature to examine issues of trust and reputation system, their existing models, and some of the remarkable applications of these models. Firstly, this chapter attempts to understand trust and reputation systems by comparing and contrasting concepts of trust and reputation from different social and scientific disciplines. Secondly, trust linked problems and various solution methods in E-Commerce and E-Market places, Peer-to-Peer Networks, Social Networks, and Mobile Ad hoc Networks have been reviewed. Thirdly, well-known theories and techniques such as game theory, fuzzy theory and probabilistic technique have been illustrated, mostly because of the popularity of these concepts in trust and reputation management research.

2.1 Background of Trust and Reputation

Experience of trust can be plainly recognised in almost every aspect of human life, but trust is challenging to define because of its manifestation in different forms [25]. However, most of the literature is closely consistent about the origin of the concept of trust, which is first derived from social and psychological sciences and is inherent in human relationships [7 , 11]. In a social context, trustworthiness is evaluated in several ways, for instance using the past history of behaviours in previous interactions, word of mouth, and reliable third party certification [25 , 26 , 27 , 28]. Trust is a crucial concept for society because of its importance in building cooperation among entities and for humanity to be able to have meaningful relationships [9 , 11].

Trust is a highly complex concept, due to its subjective nature and differences in the way in which trustworthiness is perceived [7]. Trust is time-dependent [8], wherein it grows and decays over time, and further, trust is context-dependent [29], wherein it differs based on the given task. For

example, A and B may identify different levels of trust in relation to C due to their different experiences, and this illustrates the subjective aspect of trust. A may also trust B at different levels due to changes over time, illustrating the time-dependent aspect. Further, A may trust B as a technical expert but not as a car fixer, which illustrates the context-dependent aspect of trust.

Another aspect of trust is its multi-disciplinary nature, because of its diverse applicability as a decision making mechanism in varied disciplines such as sociology, economics, philosophy, psychology, organisational management, communications and networking [7 , 30 , 31]. Due to the importance of using trust for researchers in different disciplines, applications of trust in distributed systems such as mobile agents, mobile social networks, peer-to-peer networks and mobile ad hoc networks as a security mechanism become highly attractive. In such systems, trust has been considered as multidimensional based social concept to represent social relationships in communication and networking research [32 , 33].

Computational trust models are important for large-scale distributed systems to reflect the complexity of trust and enhance security, with an aim to enabling entities to evaluate their neighbour's trustworthiness directly or through recommendations from other nodes. The design of such models requires capturing trust properties such as subjectivity and differences in the way in which trustworthiness is perceived. Trust is utilised in such systems to conduct several tasks, including coping with defection problems of entities, ensuring authentication, securing routing against malicious intent and stimulating participants to cooperate. In the existing literature, trust is accompanied by the related concept of reputation, which is defined as referring to the perception that nodes form about a particular node [9]. Trust and reputation can be used interchangeably in most existing research, while

differentiation between the concepts is clearly stated in a smaller part of trust research [34]. In Human life, reputation is developed by aggregating trust information in order to use it in the prediction of others' actions based on the historical behaviours captured through personal interactions or shared knowledge with other persons [35]. The reputation concept has widely emerged as an important component in electronic markets and online communities. For example, eBay, Amazon.com and Yahoo auction use reviews and feedback to help their users decide whether to make transactions or not based on the available reputational information. Reputation has been developed to be used in distributed systems such as MANETs to allow nodes to evaluate others' trustworthiness based on rating each other after each transaction [36 , 37]. Duo to the lack of physical infrastructure and interpersonal evidence that humans use to determine trustworthiness, the reputation system for such distributed environments should not depend on a simple rating system similar to the one used in eBay. A set of guidelines and design patterns on the success of inferring trustworthiness using reputation mechanisms in such environments are needed based on the characteristics of the target distributed systems [38].

Another concept associated with trust is potential risk and how to estimate it. Risk is an important characteristic of trust, and emerges due to the subjectivity, uncertainty and unpredictability features of the trust concept, and from differences in estimating levels of trust. Consequently, these features result in miscalculation of the trustworthiness of an entity and thus increase the associated risk even in well-founded trust. Careful estimation of risk is closely related to the building of accurate trust relationships among participating entities in communities [7]. However, misplaced trust increases the chance that the trustworthiness value will be miscalculated in two

different ways. First, trustworthiness may be overestimated, and thus the chance of being deceived by an evaluated entity increases. Second, underestimation of the trustworthiness value results in a situation where an evaluating entity may fail to collaborate with potentially good participating entities. Because of the importance of clearly defining the level of risk when evaluating trust, risk and trust are two concepts which should be integrated as crucial aspects of decision-making [39]. The use of trust with social and multidimensional features makes it sensible in risky and uncertain environments such as distributed systems. More explorations have been made in the forthcoming chapters of the thesis in this line.

2.2 Definitions of Trust and Reputation

This section of the thesis explores some notable definitions given to trust in the literature. Trust can be defined based on different factors in terms of belief, risk, subjective probability, quality of services, transitivity relationship and other concepts [40].

Trust as belief: according to the Compact Oxford English Dictionary [41], trust is defined as "*firm belief in the reliability, truth, ability, or strength of someone or something*". This definition provides some context related to believing in an entity's behaviour, skills, knowledge, and competency to perform as expected, and yet this definition is not entirely helpful. Another definition of trust is as an individual's belief and willingness to act on the basis of the words, actions, and decisions of another.

Trust as risk: the definition given by Morton Deutsch [42] is widely accepted than other definitions, in which he states that *"(a) an individual is confronted with an ambiguous path, a path that can lead to an event perceived to be beneficial or to an event perceived to be harmful; (b) he perceives that the occurrence of these events is contingent on the behaviour of another person;*

and (c) he perceives the strength of a harmful event to be greater than the strength of a beneficial event. If he chooses to take an ambiguous path with such properties, he makes a trusting choice; else he makes a distrustful choice". An important concept in Deutsch's definition is the notion of vulnerability, the fact that the evaluating entity feels itself exposed to danger. Consequently, this leads to the idea of necessarily involving risks and uncertainty in the concept of trust and the action itself of trust relies on exposure to risks [43].

Trust as subjective probability: Gambetta [44] defines trust as "*the subjective probability by which an individual, A, expects that another individual, B, performs a given action on which its welfare depends*". The definition of Gambetta uses the term '*subjective probability*' which represents an indication of the existence of different levels of trust as a consequence of the evaluating entity's beliefs and theories about the world and other evaluated entities.

Trust as a transitivity relationship: Jøsang et al. [45] defines the trust transitivity relationship as a condition of: if A trusts B who trusts C, then A will also trust C based on the assumption that B actually tells A that it trusts C, which is called a recommendation, in the case of A and B having the same trust scope, which is a specific type(s) of trust assumed in a given trust relationship.

Trust as a composition of multiple attributes: Grandison and Sloman [46] define trust as "*the firm belief in the competence of an entity to act dependably, securely, and reliably within the specified context*". This definition regards trust as a composition of several different features: reliability, dependability, honesty, truthfulness, security, competence, and

timeliness. These attributes might require different consideration based on the environment in which trust is being utilised.

Trust as a QoS aspect: Chang et al. [47] define trust as "*the belief that the Trusting Agent has in the Trusted Agent's willingness and capability to deliver a quality of service in a given context and in a given Timeslot*". This definition deals with trust as a tool to judge on other entities' trustworthiness and its capability to provide the service at a specific level of quality. Besides this, it implies the context-specific and timeslot characteristics of trust.

Trust as a decision: to define trust as a decision Jøsang et al. [25] provide the definition of McKnight and Chervany, who see trust as *"the extent to which one party is willing to depend on something or somebody in a given situation with a feeling of relative security, even though negative consequences are possible*".

For the purpose of this research, trust is seen as a combination of multiple definitions based on Gambetta [44] and other definitions which are given above to be utilised to build on trust models proposed in the work context. This thesis defines trust as the subjective probability by which an entity, A, expects that another entity, B, is capable of performing a given action at a specific level of quality in a given timeslot and within a specified context, considering the risks and incentives involved based on A's views or through recommendations provided by C who trusts B at an acceptable level. This definition intends to deal with trust as the composition of multiple attributes to reflect the trust features of subjectivity, uncertainty, unpredictability which were explained in the previous section.

In the literature, reputation is a related concept to trust, which can be used interchangeably but is not to be confused with it. According to Abdel-Rahman et al. [28], reputation is defined as "*an expectation about an agent's*

behaviour based on information about or observations of its past behaviour". The definition implies that an entity's reputation is considered as a collective measure of trustworthiness in the sense of reliability based on its history of interactions or recommendation from other community members [25]. Reputation is an important concept existing in a community that monitors its members using a specific technique to reflect the possibility of positive and negative (success or failure) in future interactions. Reputational information is a vital tool to help make effective and informed trust decisions. Thus, a reputation system needs to be successful in gathering the required information to include both personal experience and recommendation by other members.

2.3 Review of Trust and Reputation Management Literature in Distributed systems

Trust management mechanisms have grown as a powerful tool for evaluating the trustworthiness of an entity in several distributed systems such as e-commerce and e-market places, peer-to-peer networks, social networks, and mobile ad hoc networks environments [48]. Designing trust and reputation models for such applications is an important research topic to help reduce risk and guarantee the completion of network activities. Trust management models with a flexible and effective design can sustain existing and reliable trustworthiness information for the diverse entities in a distributed system, besides they can be used to mitigate different attacks related to these systems. Table 2-1 shows the attacks related to trust and reputation management in distributed systems. Enhancements and new proposals continue to grow further and rapidly, considering more subtle problems in Trust and Reputation Management field. In this sub-section, different models

of trust evaluation and some related issues are presented for each of the following applications listed below:

I. E-Commerce and E-Market
II. Peer-to-Peer Networks
III. Social Networks
IV. Mobile Ad Hoc Networks

Table 2-1 Attacks Related to Trust Management Models of MANET

Attacks	**Description**
Blackhole attack	Nodes maliciously drop all the received packets and refuse to forward them
Greyhole attack	Nodes maliciously drop some selected packets with different percentages.
Selfish attack	Nodes behave badly by dropping packets when their energy level is below a certain threshold to conserve their energy and be available in the network
Bad Mouthing attack	Nodes propagate unfairly negative ratings of good nodes with an ill intent to tarnish their reputation in the network.
Ballot Stuffing attack	Nodes propagate unfairly positive ratings for some poorly performing nodes in the network.
Collusion attack	Nodes collude together to achieve a specific attack such as bad mouthing or ballot stuffing.

2.3.1 E-Commerce and E-Market

This sub-section refers to the literature concerning trust and reputation management mechanisms in e-commerce and e-market places. E-commerce is defined as a networked information system that provides an infrastructure over the Internet to enable buyers and sellers exchange information, undertake transactions, and achieve other related activities [49]. E-commerce includes Business to Business (B2B), Business to Consumer (B2C) and Consumer to Consumer (C2C) implementation of the business environments. E-commerce has increasingly grown over time and entered into every corner of social life [50]. Trust and reputation management is an essential concern

in almost any commerce involving monetary transactions. The issue of trust may be even more significant in e-commerce because seller and buyer might have never met and trustworthiness is thus vague for each. Insufficient information concerning the reputations of the seller and buyer raise the problems of uncertainty and mistrust. Such problems might have a negative impact on the e-market's economic competence [37].

Considerable research has introduced trust and reputation systems in e-commerce to allow users to be evaluated for each transaction they complete [51]. One of the possible solutions is to construct a centralised system, such as a credit history agency, in order to deal with users' reputations. Nevertheless, this approach may lack consideration of standards and personal preferences [37]. Electronic market places, online auctions and shopping sites like eBay, Amazon.com and OnSale Exchange use simple online reputation mechanisms to avoid cheat and fraud. eBay allocates sellers a rating of 1, 0, or –1 as a value for trustworthiness after involvement in an interaction, and a seller's reputation is computed as the aggregation of all the ratings obtained over the past six months, while a new user joining eBay is allocated a reputation of 0. The system in Amazon.com is as follows: both sellers and buyers are rated after each interaction, and reputation value is calculated as the average of all the feedback ratings obtained for the duration of the system's use. A new user to Amazon.com has no reputation value. OnSale permits users to rate sellers by submitting textual comments, and the overall reputation of a specific seller is made up of the average of all the ratings received from his/her customers. Like Amazon.com, newcomers joining OnSale have no reputation until someone rates them. However, these systems need users to cooperate in clearly providing their opinion regarding other users with whom they have interacted. Besides this, users can discard

their current identities and obtain new ones to re-enter the market when allocated low reputation ratings. To solve the problem of changing identity, Amazon.com and eBay apply the notion of pseudonyms in which new joiners must register with their important personal information, and consequently the reputation system is able to trace their real identities [52].

Zacharia et al. propose Sporas [53], which is a reputation mechanism for electronic communities. It has a reputation value within the range of (0, 3000) and the minimum value 0 is assigned to a newcomer, in which the reputation of a current user is always higher than a new one. Sporas accepts only the latest rating to help prevent the problem of two users deliberately raising their reputation value by repeated interactions. To evaluate a user's reputation, Sporas allocates more weight to the most recent ratings for the reason that they are closer to the user's present behaviour. The Sporas system is similar to a credit score evaluation system, where individuals at the beginning of their use of the system might have a low credit score, but their credit score will be raised as a result of enhancing their performance for a period of time. An initial low score does not have influence on the reputation value assigned to a user. The main drawback of Sporas is that a new user is assigned the lowest potential reputation value, and it takes a long period to increase this.

Ba and Pavlou [54] propose a feedback mechanism in electronic markets to examine the role of trust in the relationship between buyer and seller, the effect of positive and negative feedback, and how some risk factors play a role in trust formation. Using data from both an online experiment and an Internet auction market, they analyse the credibility type of trust. They show that credibility trust is a very important predictor of positive economic outcomes in online transactions and that trust leads to higher end prices.

DIRECT [55] is a distributed reputation framework proposed to prevent

dishonesty in e-commerce and web-based applications. DIRECT monitors and detects malicious attacks committed by dishonest users using statistical distribution techniques. To deal with the existing problem of dishonest feedback, DIRECT divides feedback into two groups; namely green and red, and only keeps the truthful reputation information obtained by the green group. This mechanism can reduce the effect of dishonest feedback to the minimum level.

To secure buyers in online marketplaces from cheating sellers, Kerr et al. [56] propose Trunits, which is a reputation model that is based on the aggregation of trust units. The model forces a seller to have an adequate number of trust units before achieving a transaction, which represents a score of all of the trust units obtained from all buyers to date. To enter a transaction, a seller is required to risk a sufficient quantity of trust units to cover the price of the good in sale. After a transaction, if a buyer is happy, the seller gains more trust units, but otherwise loses the risked trust units.

In the previously reviewed literature, users' trustworthiness is modelled on one scalar value: namely feedback rating or reputation, while others consider trust and reputation systems from the perspective of fraud. Fraud avoidance by automatic fraud detection is where the distinguished classification approaches can be applied and can play a very important role in enhancing e-market competence. Maranzato et al. [51] focus their research on identifying and evaluating features which can show fraud evidence in e-market reputation systems. They describe procedures which are used to extract these features. Their analysis is based on both the features of users and the negotiation procedures between buyers and sellers. They study and quantify the effect of each feature in normal and fraudulent behaviour in a real dataset. The authors believe that such a mechanism (i.e. features set)

might be beneficial to any reputation system of online services as a way to identify fraud and enforce credibility.

Simple feedback mechanisms used in e-commerce and e-market places such as eBay and Amazon have used to motivate the research of this thesis to enhance the feedback propagation, aggregation and computation of recommendation's problems and gabs in MANET. The investigation of risk factors and countermeasures of propagations of dishonest feedbacks to distort sellers or buyers has utilised to define a dynamic defence scheme to solve such problems in MANET.

2.3.2 Peer-to-Peer Networks

Peer-to-Peer (P2P) networks are distributed systems without centralised control or organisation. The interactions between peers are achieved directly and peers are considered both consumers and service providers. Besides this, peers frequently interact with anonymous entities whose trustworthiness is also anonymous. Such systems require trust management to guarantee cooperation and to mitigate the influence of misbehaving peers, such as free riding behaviour, in which peers obtain the services from the network but do not contribute back to the same degree to the network [57].

Peers should have the ability to identify reliable peers for communication in order to protect themselves, and this is considered a challenging demand in extremely dynamic P2P environments. Therefore, trust management and reputation systems have become an essential technique in securing large scale peer-to-peer networks. Several trust and reputation systems have been proposed to motivate peers to cooperate, incentivise the cooperated peers and punish the misbehaving peers. The utilisation of trust and reputation systems in P2P systems significantly decreases the number of malicious transactions in such networks [58]. These systems target a filtering out of

those peers who misbehave by offering trustworthiness values to peers. A peer who misbehaves will be considered untrustworthy and consequently assigned a bad reputation: for example, a peer with a bad reputation will not be chosen to operate as a downloading peer.

Trust management in pure peer-to-peer networks was first studied by Aberer and Despotovic [59], in which lying peers are identified by a complaint-based system. Their protocol is based on a decentralised storage method called P-Grid. The protocol only utilises the negative feedback, and a trustworthy peer cannot be differentiated from a newcomer. The evaluation process of trust classifies peers on a binary basis as either trustworthy or untrustworthy. A binary value would possibly be inadequate in a P2P environment in which all peers are untrusted. This approach also suffers from the fact that trust is only assessed by referrals from neighbours, and not on the basis of global information.

TrustMe is an anonymous protocol proposed by Singh et al. [60] to maintain and access trust rating information in P2P networks. TrustMe utilises a random assignment of Trust-Holding Agent peers (THA) and Public Key cryptography mechanisms to provide security and prevent loss of anonymity in order to resist various attacks. Peers broadcast their global reputation about other peers using query messages and broadcast their feedback using reports. In the TrustMe protocol, the trust value of a peer is stored by other peers and a peer can securely access trust values of other peers. This mechanism requires a large number of messages to be produced in the network; besides, it may require a long time to broadcast peers' reports and to obtain a global reputation.

Kamvar et al. propose EigenTrust [36], which is a reputation algorithm used to decrease the number of downloads of inauthentic files in a P2P file-sharing

network. It assigns a global trust value based on the history of uploads for each peer in the network. A distributed and secure method is utilised to compute such global trust values using power iteration. In this algorithm, peers use these global trust values to select the peers from whom they download. Through use of simulations, the authors show that such a reputation system can identify malicious peers effectively and isolate them from the network even in the case of collusion amongst malicious peers. However, the algorithm lacks anonymity for peers due to its use of the IP address to identify peers, and places large overheads on network resources such as the consumption of large network bandwidth.

PeerTrust [61] is another reputation system for P2P networks that supports the utilisation of an adaptive trust model to quantify and compare the trustworthiness of peers. The computation of trustworthiness of a peer is based on three fundamental trust parameters and two adaptive factors. These parameters are feedback received by a peer from other peers, total number of transactions performed by a peer, and the credibility of feedback sources. The factors are defined as the transaction context and the community context. A general trust metric is defined to combine these parameters. PeerTrust adapts to different peers' behaviour and uses the notion of personalised similarities to rate the credibility of peers. It addresses the importance of identifying trust parameters and adaptive factors in a consistent way. Moreover, the problems of dishonest feedback and lacking of incentives are also addressed. A set of experiments is conducted to explore the feasibility and benefit of the system. One problem associated with this system is that it is not easy to implement in large scale P2P networks.

Zhou et al. [62] propose a reputation system called PowerTrust which utilises a trust overlay network (TON) to model local trust and reveal feedback

relationships among peers in large scale P2P networks. By examining over 10,000 transaction traces in eBay users, the authors discovered the importance of a power-law distribution in user feedback, and consequently model their system by leveraging the power-law distribution of peer feedback. By using a distributed ranking mechanism, PowerTrust dynamically chooses power nodes that are the most reputable based on the accumulation of the running history of the system. Power nodes are replaced dynamically in cases where they are inactive or show unacceptable behaviour, and they play an important role in both local and global scoring processes. By means of both experimental results and theoretical foundations, the system is validated to reveal its scalability in large-scale P2P applications, accuracy, robustness against malicious peers, and fast aggregation speed. PowerTrust has the disadvantage of lacking the consideration of some attacks like selfishness, and collusions of peers.

FuzzyTrust [63] is a P2P trust system based on fuzzy logic inferences, which can be used to handle uncertainty, fuzziness, and scarcity of information in peer trust reports. In this system, peer reputation is aggregated with a reasonable message overhead. There are two tables for each peer to maintain, namely transaction record and local score. A transaction record table is used to maintain transaction records with remote peers, and a local score table is used to maintain remote peers' evaluated trust scores. The system utilises distributed-hash-table (DHT) overlay networks to perform rapid and safe reputation propagation amongst peers. The authors compare their system with EigenTrust. They show that FuzzyTrust is slightly faster than the EigenTrust system and can detect more than 99% of malicious peers within four iterations. However, a drawback of the system is that it has

no particular techniques to tackle the misbehaviour of peers, such as in collusion attacks and free-riding.

By considering the concept of incentives, Wang et al. [58] propose the VCG-like reputation reward mechanism in order to motivate peers to honestly provide reputation feedback. The mechanism is designed based on a well-known economic model, and social features of trust networks. It considers reputation feedback as a particular sort of information, and that it is not free, and that reputation systems should incentivise peers to rate others and provide sufficient feedback. The authors classify trust into functional trust and referral trust, to consider the subjectivity of trust and reputation concepts. They also extend referral trust to include two factors: similarity and truthfulness, to efficiently reduce the trust inference error. Similarity is used to distinguish the personalised reputation feedback, while truthfulness is employed to assess the credibility of reputation feedback. From the entire trust network perspective, appropriate measures are proposed; global efficiency, local efficiency and cost to distinguish assured social characteristics of trust networks. The results of preliminary simulation show the benefits of such proposal and the emergence of certain social properties in a P2P network.

In addition to the concept of incentives, a punishment concept is introduced by Cascella and Battiti [64]. The authors extend the role of a reputation system to more than performing its basic functions of collecting, aggregating and disseminating of trust information to motivate peers to behave cooperatively and discourage malicious peers. In this context, they concentrate on incentives and punishment as two opposite functions which cope with both rational and malicious peers. They propose to use a Game Theory technique to design a trust economic model for P2P systems. The

authors also evaluate global reputation values for peers that are calculated according to first-hand opinions provided by the participants in transactions. These opinions are assigned weight on the basis of the credibility of the reporting peer and the attached quality value that decreases the impact of an opinion in the reputation function. Reputation values are disseminated in a distributed fashion by utilising compound trust administrators for each individual peer, which formulate the global trust of the peer and provide it to other peers upon a request.

The review of the literature in the domain of P2P networks shows that their characteristics of openness, distributed nature, and absence of centralised organisation require a robust monitoring technique to ensure the quality of services provided by the network. With the advantage of the flexibility of this environment, a great challenge is countered when interacting with dishonest and uncooperative peers. Trust and reputation based mechanisms have proved to be effective in assessing peers' trustworthiness and identifying malicious peers. Although, such mechanisms are utilised to evaluate trustworthiness among peers in order to guarantee cooperation and to mitigate the influence of misbehaving peers, they are still unable to handle tactful peers. However, in the context of this research, fully distributed models like PeerTrust, EigenTrust, and FuzzyTrust can be utilised to build reliable trust models for MANET with some improvements of the way the trust is viewed by nodes. As Nodes may interact with stranger entities whose trustworthiness is unknown, decentralized schemes, as well as, incentives, and punishment concepts have been borrowed from the field of trust in P2P systems. Free riding behaviour can also be considered as a problem for MANETs in which free-riders use other nodes to forward their own packets and refuse to forward packets to others.

2.3.3 Social Networks

The increasing attraction of the web in social networks (such as Facebook and MySpace), social media sites (such as YouTube and Flickr), and communities of large-scale information sharing (such as Wikipedia and Yahoo! Answers) demands construction of an online community platform that permits wide access to several diverse types of users [65]. The social network is considered as a research area that has a rich history and there is great interest in modelling such networks by understanding how efficiently people use their social networks and interact with others. The analysis of social networks includes the study of social relationships among individuals in a society and can be identified as a set of methods that is used to analyse social structures and allows the examination of relational characteristics of these structures [66]. In the presence of misbehaving participants who increasingly aim to exploit perceived social relationships among users and the probability of the disseminating of misinformation, lying, and misreporting, trust as a social phenomenon has been utilised to secure such networks and allow people to decide on the trustworthiness of others in the society.

The concept of using trust in a social network, which is called Social Trust, was introduced by Golbeck [33 , 67 , 68] by highlighting the importance of proposing a suitable trust model that is derived from a sociological viewpoint to identify the trustworthiness of user generated interactive contents over the web and identifying trust as a well-defined descriptor to represent security and encryption goals. Social trust is considered for sociable purposes which might include friendship degree, honesty, privacy, and social reputation or recommendation as a result of involving users in direct or indirect social interactions. Golbeck [33] introduces Tidal-trust, which is a trust metric proposed for semantic web or friend-of-a-friend networks. Each node is

statically assigned a local trust value that is utilised to infer trust levels between two nodes which have not directly connected on the social network. The inference process of such a trust algorithm is based on the recommendations provided by highly trusted nodes and via shorter paths which may give more precise information. The problem of the Tidal-trust algorithm is that it lacks the ability to dynamically update trust values. Besides this, observations based on direct experiences are not considered.

Maheswaran et al. [69] propose a gravity-based model for using trust in managing activities in social networks. The model uses two stages. For each user in the first stage, friendship strengths are computed with the extent of the trusted social neighbourhood, while in the second stage, the effective trust flow for users not in the social neighbourhood is computed using the social neighbourhood. An invocation of a distributed optimisation procedure is periodically used by each user on the social network to update the trust values on the connections. It is used to update the strengths of the social connections of the social neighbourhood. A simulation is conducted by the authors to present results in order to investigate the feasibility of the proposed scheme.

Another social trust model, called STrust, is proposed by Nepal et al. [70] for social networks to build trust communities using social capital and recommendation system social networks. The model is based on the concept of social science and derived using social capital. It splits the interactions in a social network into two groups, namely popularity and engagement based interactions. Such groups are used to recommend different things in the social network and to allow the capture of passive interactions such as reading comments without leaving any feedback. The popularity and engagement trust values are based on the trustworthiness of a member in

the community and are both computed by identifying and deriving metrics from the social capital (i.e. interactions). An analysis and potential benefits of the proposed model are presented.

In [71], authors use a trust model to assign trust levels for objects and subjects on social networks, to introduce a social access control, called SAC, to protect social data. The trust level of an object is identified by the creator, while the trust level of a subject is obtained as the average of the trust ratings provided by the community. Reading of a data object is controlled using the relative trust values of subjects and objects, and besides this, the SAC model supports the confidentiality of read-only data objects. Simulation is performed using traces from the flickr.com social network to evaluate the performance of certain issues in the design of the SAC model.

The review of utilising trust in social networks to study the social relationships among individuals in a society suggests that trust management mechanisms can be effective in handling misbehaving participants who aim to exploit perceived social relationships among users. Such mechanisms are utilised to decrease the probability of the dissemination of misinformation, lying, and misreporting. Social trust is identified as a method to analyse and study social structures and allow the examination of relational characteristics of these structures. As the case of all distributed systems, the study of trust is still in an early stage. It is still a challenge and open area in addressing various aspects of social trust such as collecting trust information, trust evaluation, and trust dissemination in social networks. The review of social properties of trust in social networks have led the research of this thesis to recognise the significance of borrowing trust management concepts from the social network analysis (SNA) field to improve the performance of trust models in MANET. This move towards social methods in securing MANETs

by defining social trust attributes of nodes such as level of cooperation, honesty, and manner of behaving to establish and manage trust relationships of nodes.

2.3.4 Mobile Ad hoc Networks

A mobile ad hoc network (MANET) is a proposed system model consisting of a collection of wireless mobile nodes that are capable of communicating with each other in the absence of a fixed network infrastructure or any centralised administration. MANET is considered to be infrastructureless networking, in which nodes dynamically set up a network and establish routing among themselves to build their own network when needed [1]. MANET's characteristics, including frequent changes in network topology due to mobility or discontinuous operation of the nodes, open wireless medium, and constrained capability, make it vulnerable to security issues if the situation of a friendly and cooperative environment is not assumed [3]. Therefore, in recent years, different trust and reputation models have been proposed to enhance security in MANETs to enable nodes to evaluate their neighbours directly or through recommendations from other nodes in the network. In this subsection, a literature review of important issues related to evaluating trustworthiness in mobile ad hoc networks is presented.

Michiardi and Molva [23] propose the CORE model, which has a watchdog component complemented by a reputation system that distinguishes between three types of information; subjective reputation by means of observations, indirect reputation by means of positive reports by others, and functional reputation by means of task-specific behaviour. The model only accepts positive recommendation by others. Consequently, this can lead to decreased efficiency of the system because nodes cannot exchange bad experiences from the misbehaving ones in the network. Also, CORE cannot

be resilient against a ballot-stuffing attack as it leaves ways for misbehaving nodes to collude and gain unfair high ratings.

Context-Aware Detection is the mechanism proposed by Paul and Westhoff [24] to relate nodes' accusations to a unique route discovery process and a specific time period. They use for monitoring a combination of un-keyed hash verification of routing messages, and misbehaviour detection by making a comparison between a cached routing packet and overheard packets, thereby detecting tampering from the route request header. This approach enables the detection of several types of attack and attacker, and also rejects ineffective route information at as early a stage as possible.

CONFIDANT [18] is a mechanism which supports cooperation in ad hoc networks by detecting and isolating malicious nodes using direct observations and recommendations. The model uses the personal experience mechanism to deal with the problem of dishonest recommendation. It applies the deviation test on the received recommendations and excludes those deviating above the threshold value. The reputation value of a recommending node is updated based on the results from the deviation test. The model cannot prevent the dissemination of false recommendation and negative recommendation is the only information exchanged between nodes [52]. Besides, it uses only single trust metric evaluation based on the cooperation of nodes in packet forwarding. The model omits some important evaluation metrics such as energy, delay and social properties in evaluating nodes' trust.

Authors in [72] propose RFSTrust, a trust model based on fuzzy recommendation similarity, which is presented to quantify and evaluate the trustworthiness of nodes. They use similarity theory to evaluate the recommendation relationships between nodes. That is, the higher the degree

of similarity between the evaluating node and the recommending node, the more consistent is the evaluation between the two nodes. In this model, only one type of situation is considered when a selfish node attack is present, and the performance of the model is not tested against other attacks related to recommendation.

Soltanali et al. [73], propose a model of trust to encourage cooperation between nodes by using direct observation and recommendation. This model only accepts the last opinion of a node, which is passed to a reputation manager system at the end of each interval. Considering only the last opinion is not insightful enough to recognise the fluctuation in a node's behaviour, as in on-off attack [74].

In an attempt to increase the honesty of utilising recommendations, Li et al. [16] include a confidence value in their evaluation by combining two values; trust and confidence, into a single value called trustworthiness. They utilise the trustworthiness value to put weight on recommendations in which a recommending node with a higher trustworthiness value is given more weight. Collusion attack in providing false recommendation is not considered by this work, and this may cause incorrect evaluation of the received recommendations [7].

Hermes [75] is a recommendation based trust model that uses an additional parameter known as an acceptability threshold (in relation to the confidence level). The notion of acceptability is used in the computation of recommendations to ensure that adequate observations of the behaviour of participating node have been obtained. However, the selection of acceptability is a trade-off between obtaining a more accurate trustworthiness value and the convergence time required to obtain it.

A recommendation exchange protocol (REP) is proposed by Pedro et al. [76] to allow nodes to send and receive recommendations from neighbouring nodes. It introduces the concept of relationship maturity, based on how long nodes have known each other. Recommendations forwarded by long term associates are weighted higher than those from short term associates. The maturity of relationship is evaluated on the basis of a single factor by considering only the duration of relationship.

Yu et al. [77] propose a clustering technique to filter out trustworthy recommendations from untrustworthy ones. They follow the majority rule by selecting the cluster with the largest number of recommendations as trustworthy. The authors tested their model against attacks such as bad mouthing and ballot stuffing. However, majority rule could be ineffective, as some nodes can collude to perform an attack, and not provide an honest judgment about other nodes.

TRUNCMAN is a trust based routing mechanism [21] used in order to isolate non-cooperative nodes during the path discovery process, to defend against many network layer attacks, including blackhole and greyhole attack (dropping packets). The proposed protocol is partitioned into two sections: the Suspicion Phase, which checks the route request broadcast and acknowledgement; and the Detection Phase, which details the detection of a non-cooperative node. Isolation and advertisement of the malicious behaviour in the network is propagated as social welfare. However, this model also evaluates the node's cooperation only based on packet forwarding without considering the dynamic characteristic of MANETs, besides quality of paths and social network attributes.

Cho et al. [78] propose a trust management protocol for group communication systems in MANETs. Their composite trust metrics combines

the social trust properties of the participating node with QoS trust. In this work, they consider honesty and intimacy to represent social trust properties, and unselfishness and energy as QoS trust properties. Subjective trust evaluation is undertaken, to consider the effect of trust chain length used by nodes to build acceptable trust levels. Besides this, objective trust evaluation is introduced as global knowledge to validate the subjective trust evaluation.

Yu et al. also consider the problem of proposing a composite trust metric [79]. They present a trust model with multiple decision factors, in which two types of trust: security trust and quality trust are incorporated in evaluating the trustworthiness of nodes in MANETs. Analytic Hierarchy Process (AHP) methodology is used to combine these two types. This work includes transmitting trust and energy trust, to evaluate the security trust of nodes, while it uses delay trust and delay jitter trust to evaluate the quality of trust. This work omits the social network properties in evaluating the trustworthiness of nodes in the network.

2.4 Trust Management Techniques

This section provides a summary of some known trust management techniques which are used to model and compute trust and reputation in various applications. In the previous section, an exploration of some important trust and reputation management models in E-Commerce, Peer-to-Peer networks, social networks, and Mobile Ad hoc Networks was given. However, most of the proposed approaches, including the above, are grounded in closed techniques which aim to allow entities in the community to observe each other's behaviour in order to construct a trust relationship representing the degree of trustworthiness one entity can place on another. These relationships are useful to help entities decide whether to interact with a specific neighbour or not. Trust metrics and their subsequent calculations in

most models are mainly based on three techniques, namely, game theory, fuzzy theory, and probability theory. Only the probability theory (beta probability) technique is used by this thesis to compute trust metrics because of its advantage and suitability for MANET's environment in terms of using less resource intensive (for more details on its advantages, the reader is referred to section 3.1.2 of chapter 3), while fuzzy, and game theories are in the scope of this review because of their importance and applicability.

2.4.1 Game Theoretic Trust Management Technique

A game-theoretic trust and reputation technique is applied to study cooperation between entities. It represents a powerful tool for modelling interactions and the prediction of an entity's cooperation in future transactions with usefulness functions, mathematical analysis, and numerical aggregation of past history [29].

In e-commerce and e-marketplaces, reputation formation has been broadly studied using the game theory technique [80]. It allows economists to build sophisticated models of individual entities' reasoning and preferences [81]. Ba et al. [82] use a game theoretic approach to propose an economic incentive model based on trusted third parties (TTP) to facilitate building trust in online environments, and to help reduce online fraud through the use of reputation. The model is used to serve the online auction communities and addresses both economic and technological aspects of online transactions by assigning a digital certificate to each participant. The model uses the Prisoners' Dilemma (PD) game to represent each non-repeated transaction (the stage game) and the TTPs to disseminate reputation information for the global online auction markets. Li [83] proposes an incentive mechanism using game theory, which aims to help buyers identify the sellers' types and to report on the quality of sellers, and consequently encourage sellers to

behave cooperatively. Besides, this rebate mechanism gives a chance to sellers to leave feedback about consumers' responses, such as on receiving payment.

While peer-to-peer networks, [84] use game theory to study the interaction of strategic and rational peers. They propose a differential service-based incentive scheme in order to improve the system's performance by elimination of free riding and increased overall availability. Gupta et al. [85] studied peers' behaviour in peer-to-peer networks based on the game theoretic technique in the case of peers that receive services based on their reputation. Reputation is used as a mechanism to incentivise peers to share resources and provide services to others. Peers' reputation is calculated as the probability of a peer obtaining a service and their reputation is enhanced based only on serving others. Game theory is used by selfish peers to identify their optimal strategy for contribution level in the system. Besides, it provides a perception into the overall nature of peers' interactions and efficiency of the system. The proposed model is used to minimise the problem of free-riding and improve the efficiency of the system.

The design of an autonomic trust model that forms social network structures to incentive cooperation is proposed by Allen et al. [86]. They study a peer-to-peer data dissemination mechanism which is validated using an Iterated Prisoner's Dilemma (IPD) model based simulation. Social network properties of trust such as the ability of cooperative peers to prioritise and reciprocate inter actions, and consequently protect themselves from being compromised by uncooperative nodes is the basis of the proposed model. The similarity of interest (cooperation level and preference) between peers to identify pay-offs is used. Colombo et al. [87] design a pure trust based application of the IPD game in which each individual adjusts its behaviour and priorities based on

its direct experiences to construct social structures. The model aims to eliminate the effect of selfish behaviour and enhance system utility by providing greater levels of cooperation. Their implementation shows that the investigated system incentivises more cooperative behaviour over defection.

Various authors [88 , 89 , 90 , 91] based their trust models on using the game theory technique to evaluate nodes' cooperation in MANETs. Srinivasan et al. [88] suggest using a generous TIT-FOR-TAT model that is used by nodes to decide whether to accept or reject a relay request. Their work results in Nash equilibrium and leads the system towards an optimal operating point. Felegyhazi et al. [89] present a game theoretic model to investigate the conditions of equilibrium of packet forwarding mechanisms and take network topology characteristics of MANET into account based on game theory and graph theory. Yu and Liu (2007) suggest a game theoretic framework to investigate cooperation stimulation and security. Their results demonstrate that, in two-player game forwarding, the sole cheat-proof Nash equilibrium for each node is not to assist the opponent more than the opponent has assisted him/her. Bista et al in [90 , 92] propose to use the IPD model to examine the problem of trustworthiness evaluation by investigating the level of cooperation of nodes based on the weight of the feedback source being assigned on the basis of past interactions between players. They break feedback sources into different types based on acquaintance and dynamic computing weight accordingly. They argue that their work can support the evolution of cooperativeness in various disciplines compared with models which do not categorise feedback sources.

2.4.2 Fuzzy Trust Management Technique

Fuzzy logic or fuzzy inference is an important tool that has attracted several researchers to employ it in quantifying trust and reputation among nodes

because of its capability of quantifying imprecise data or uncertainty in measuring the trust and reputation metrics. Fuzzy logic inference rules are used to compute trust values, aggregation, and dissemination of trust information in communities which effectively handle imprecise linguistic terms [25]. The theory of fuzzy logic was first developed by Lotif Zadeh [76] and ever since, the fuzzy logic method has been applied in a considerable range of research to model uncertainties, vagueness and impreciseness of trust concepts, as well as risk analysis for interacting with strangers and decision making processes to identify trustworthy entities [93].

[94] use fuzzy logic to propose a trust model to evaluate trustworthiness in e-commerce based on information extracted from a vendor's website. They allow customers to rank trust parameters related to a particular transaction based on their own perception and experience. Existence, affiliation, policy and fulfilment are four major factors identified by the model to help customers decide whether to engage in a transaction or not. Wei et al. [95] utilise the theory of Fuzzy Cognitive Time Maps (FCTMs) to model and evaluate trust relationships in virtual enterprises. They show how relevant inter-organisational trust based on the sources and their credibility of trust. The model addresses trust related essential factors in such virtual environments by examining triple relations of trust including trustor, trustee and their surroundings. The model investigates the evolution of trust by considering the dynamic nature of trust to dynamically allow the trustor to form an opinion about another entity.

Song et al. [63], propose a FuzzyTrust model based on using fuzzy logic inference rules to compute local trust values and to aggregate global reputation in peer-to-peer networks. They utilise linguistic terms to handle trust and reputation information in order to achieve fast and secure

dissemination of reputation values among peers. Following the success of using fuzzy techniques of Song et al., in which there was an improvement in the ability of peers to handle uncertainty, fuzziness, and incomplete information in reports provided by peers, Chen et al. [96] present a fuzzy trust model for peer-to-peer networks. The model includes two phases; recommendation trust and direct trust. The main focus of the recommendation trust phase is on the extraction of the trust link and computation of recommendation trust degree using the fuzzy decision-making method. Various sets based on the fuzzy decision-making method are used to obtain a fuzzy trust evaluation metric, while the focus of the direct trust phase is mainly on updating the direct trust degree using peers' experience and recommendation.

[97] propose the utilisation of fuzzy linguistic terms to identify trust for social network users and allow users to decide on the trustworthiness of other users, who may not directly interact, in a trust graph. The algorithm depends on utilising linguistic expressions to represent the imprecise nature of the trust concept more than numbers. They show that their algorithm is able to provide more precise trust information than other algorithms when deeper paths are being searched. Li and Kao [98] propose TREPPS, a recommender system based on trust, to evaluate the quality and reliability of peer production services by computing trust values of peers in social networks. They apply a fuzzy inference system and fuzzy MCDM method to support decisions of service choice. By experiment, the authors show that their model is able to enhance the quality of peer production services and mitigate the overload problem, and besides this, a trust-based social news system is built to explore the model's applicability.

Luo et al. [72] present the RFSTrust model based on fuzzy recommendation similarly for MANETs to quantify and evaluate the trustworthiness of nodes using fuzzy theory and mathematical description of MANETs. Fuzzy logic is used to deal with uncertainty and inputs of imprecise data in evaluating trust, packet forwarding review, and adjustment of nodes' credibility. They utilise fuzzy relation theory to include five types of recommendation relationships in the trust system. The model is tested in the presence of selfish attack and a discussion of data sparsity problems is provided. In the case of securing routing protocols in MANETs, Xia et al. [99] propose FTDSR, which is a fuzzy trusted dynamic source routing protocol built on the basis of the standard dynamic source routing protocol (DSR) to secure MANETs. The proposed protocol evaluates the credibility of nodes using analytic hierarchy process theory and a fuzzy logic rules prediction method. Fuzzy dynamic programming theory is used in the trust routing protocol to isolate untrustworthy nodes in order to obtain a reliable route delivery.

2.4.3 Probabilistic Trust Management Technique

Probabilistic trust and reputation techniques are used to build trust models based on probability calculus using advanced statistical methods. Applying probability theory provides the advantage of providing simple models with a wide range of possible derivation methods [100]. Probability theory can offer better performance in comparison with deterministic trust models by enhancing security mechanisms and improving the quality of interactions [101].

Beta distribution and Bayesian inference technique have been heavily used by a variety of researchers to model trust and reputation. It deals with trust as binary ratings which takes two inputs (positive or negative), and is based on computing trust scores by means of statistical updating of beta probability

density functions (PDF) [25]. Jøsang et al. [102] propose a beta reputation system which is based on using the PDF functions to collect and combine feedback related to e-commerce transactions and consequently derive reputation ratings for the online agents. The reputation system is based on the statistical theory and is simple and flexible to use. Dong et al. [103] also use the probability theory to build a trust management model PTME for distributed e-commerce. The model is used to establish the trust relationships between buyers and sellers in e-commerce applications. The reputation of both buyers and sellers is based on direct and indirect observations and it is used to protect the e-commerce system from false accusation and collusion behaviour.

In peer-to-peer networks, Wang and Vassileva [104] use a Bayesian network to build a trust model based on recommendations exchanged between peers. They use the Bayesian networks to provide a flexible technique to present differentiated trust and combine different aspects of other peers' capability. Buchegger and Le Boudec [18] propose a fully distributed reputation system that can detect and isolate malicious nodes for both peer-to-peer networks and mobile ad hoc networks. It is used to cope with dissemination of false information by utilising a modified Bayesian approach, which is presented in their research. Another distributed reputation mechanism which is based on the probability theory is proposed in [105] to detect malicious and unreliable peers in peer-to-peer networks. In this model, peers' experiences of quality of service (QoS) is considered as probabilistic ratings in the interval [0, 1] and the main focus is on how to aggregate these ratings to decide whether to trust other peers or not.

In social networks, [106] propose SUNNY, which is a trust inference model based on an explicit probabilistic interpretation for confidence in social

networks. The model utilises a probabilistic sampling technique to estimate confidence in the trust information from different sources. Besides, it only estimates trust information from highly confidence sources. Liu et al. [107] propose the building of complex trust-oriented social network model which is based on an inferring trust mechanism using the Bayesian network. The model aims to deliver more realistic and accurate trust values that represent complex social relationships and recommendation roles in a social domain.

Trust based probabilistic technique is widely adopted in MANETs. The CONFIDANT model proposed by [18] is a distributed trust model for MANETs based on using the probability theory in the form of beta functions to compute two parameters of trust (i.e. success and failure interactions). OTMF in [108], and Hermes in [75] are proposed models that also use beta functions to compute success and failure interactions in packet forwarding as the mean value of the function. Besides this, they use the standard deviation to compute confidence value and to increase the robustness of the proposed models. Feng et al. in [109] use Bayesian inference and Beta distribution function to propose a certainty-oriented trust management system for MANET to isolate newcomers from misbehaviours and consequently certainty-based decisions can be made possible. They use the Beta function with its two continuously updated parameters to represent positive and negative interactions. Wei et al. in [110] use the probability theory expressed in Bayesian inference to derive direct trust values as a type of uncertain reasoning when the probability model is possible to be fully defined. They use reasoning based on uncertainty adopted from artificial intelligence community as a result of the development in the probability theory technique. They find that in the context of securing MANETs, these theories are very suitable for evaluating trust based on the trust interpretation in their research.

Bao et al. in [111] develop a probability model to propose a cluster-based hierarchical trust management protocol for securing wireless sensor networks in order to effectively mitigate the influence of selfish or malicious nodes. They use a novel probability model using a normal distribution, which is commonly used for statistical analysis to describe a heterogeneous environment that comprises a large number of nodes with different social and quality of service behaviours to validated subjective trust against objective trust of nodes.

2.5 Summary and Research Gap

In this chapter, a literature review related to trust models as applied in e-commerce and e-market places, peer-to-peer networks, social networks, and mobile ad hoc networks was presented. Some techniques that have been used in building these models, including game theory, fuzzy theory and probability theory approaches, were also described.

This review revealed that several trust models have been proposed in a wide range of domains with different computation techniques, such as CONFIDANT, PeerTrust, EigenTrust, PowerTrust, and FuzzyTrust to evaluate trustworthiness among entities. These models aim to enhance security in such environments by enabling entities to evaluate their neighbours directly or through recommendations from other entities in the network. However, the discussion conducted in the chapter highlights several limitations and gaps of the trust models in their abilities to shield nodes from malicious behaviour. Differences in behaviours of entities among time and location due to mobility characteristic, the use of all available sources of trust information (positive or negative information), false negative and false positive problems in evaluating trustworthiness, and dynamic weighting of trust parameters and factors are challenges that have not been tackled in the

literature. This thesis recognises the problem that most of the models have proposed in the literature in which they rely on a single parameter to compute trustworthiness. As trust is a very complex concept due to its subjective nature and differences in the way trustworthiness is perceived, this has been identified as a research gap, and the work in this thesis is conducted to fill this gap. This work has been designed to include multiple parameters to compute the trustworthiness of entities in MANET. The study underlines the importance of social properties in evaluating trustworthiness and uses this in investigating the trust relationships between entities and similarity in behaviour to help in:

1. Enhancing the trustworthiness evaluation of nodes in general.
2. Improving the network performance and quality of services.

Chapter 3 Problem Description

This chapter describes the trust and reputation management problem that is the basis for the research work. It illustrates the main concepts underlying a probabilistic trust model with rating and evaluation mechanisms to solve many problems like nodes' behaviour and recommender systems in the MANETs environment. Based on the definition of trust and reputation management problems in this chapter, more comprehensive trustworthiness evaluation models are presented in the subsequent chapters. Along with the problem model, the methodology for the investigations being carried out is also presented here. A network simulator with assumptions, data collection methods, and procedures for the experiment for each subsequent chapter is shown.

3.1 The Problem Definition and Model

This thesis considers the trust and reputation management model that is built upon the requirements and dynamic characteristics of mobile ad hoc systems. Findings could also be applied to any distributed systems such as peer-to-peer systems, social systems and open agent based systems. The aim of monitoring nodes' behaviour and trustworthiness evaluation in different distributed systems can be achieved in nearly the same manner despite the fact that each of these domains has its own requirements and characteristics. Assumptions such as self-policing, dynamic monitoring and diversity of information resources such as past history and recommendation mean that the underlying model suits many instances in such domains. To model the problem of monitoring and evaluating the trustworthiness of nodes in MANETs, this thesis considers a recommendation based trustworthiness evaluation model using the

probability theory technique. The model's components and assumptions are discussed in the subsections which follow.

3.1.1 Model Components

The aim of trust and reputation management models in MANETs is heavily focused on offering secure ad hoc routing by detecting and isolating misbehaving nodes (selfish or malicious) and encouraging collaboration among them to improve network throughput such as end-to-end packet delivery fraction. Typical trust and reputation management models are mainly characterised by the following components:

a. Evidence Manager: this component is used to collect evidence about the behaviour of each node in the network. Evidence may be anything that is generated by the node itself (direct observation) or received by others (recommendation) to build trust relationships.
b. Trust and Reputation Manager: this component includes a mathematical model to translate evidence into opinion, and then to use this to predict the behaviour of nodes in the future interactions. The mathematical model would be based on any mechanism such as probability theory, fuzzy logic, or bio-inspired model (refer to Chapter 2 for further detail on trust computation techniques).
c. Policy Manager: this component is used to identify the decision rules and policies to enable nodes making decisions. Policies are needed for example to deal with newcomers who are completely unknown and decide whether to ignore or permit any newcomer to become a part of the network. Redemption and recommender selection also requires rules and policies to enable the node to make effective decisions.
d. Evaluation Manager: this component allows nodes to evaluate the trustworthiness of an interacted node, making interaction decisions, and

evaluating nodes based on the interaction outcomes. Evaluation includes making a decision to interact with a node and collect evidence based on the outcome of the interaction.

The fundamental architecture of trust models is typically distributed and deployed at each node to provide ratings about other nodes in the networks to help in making subjective decisions. The important components which are combined together to build the basis for the trust and reputation models proposed in the next chapters are summarised in Figure 3-1.

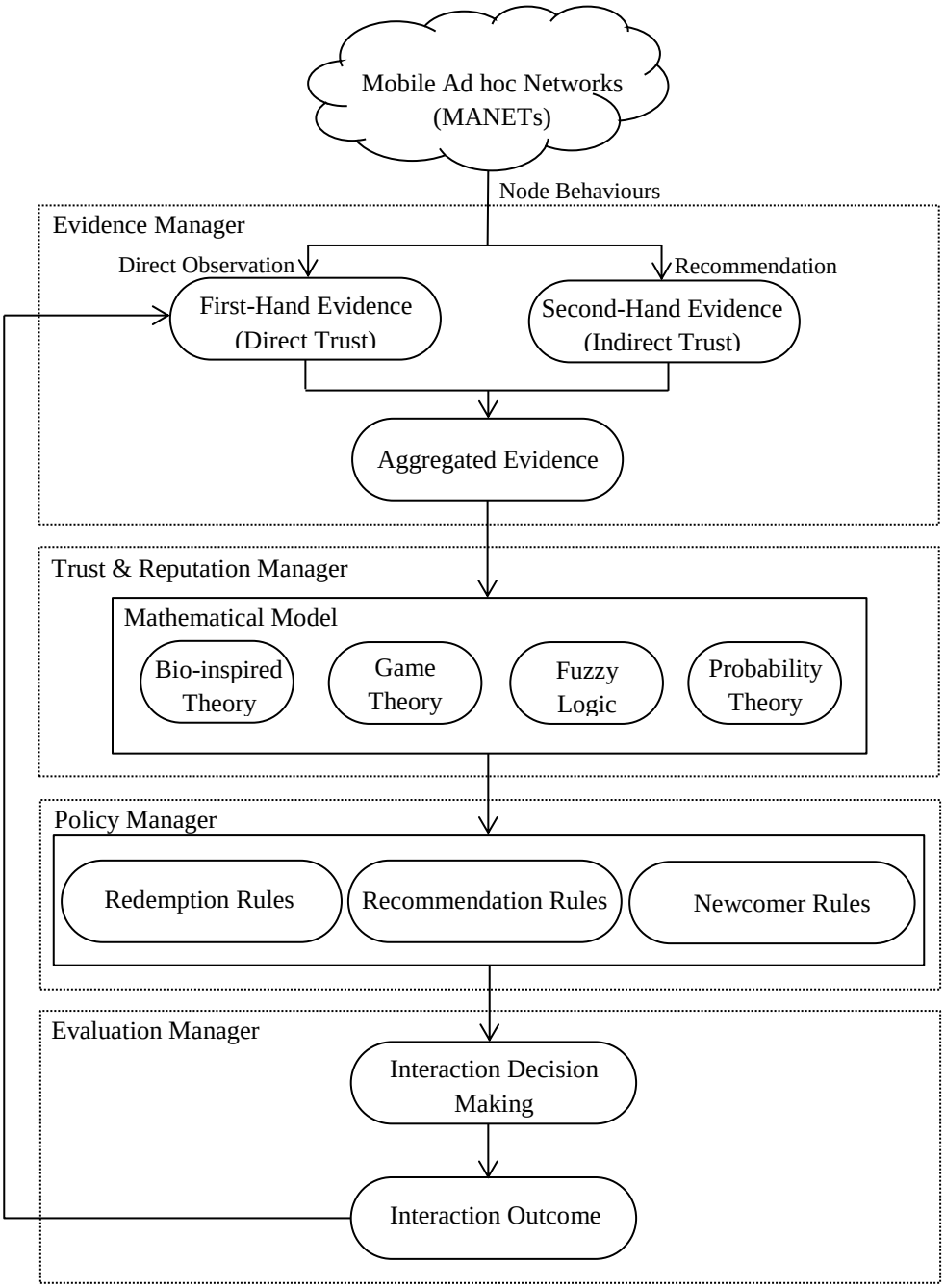


Figure 3-1 Trust and reputation model components.

3.1.2 Model Parameters

This thesis makes use of a Bayesian statistical approach similar to that used in [25] for computing trust values based on the assumption that they follow a beta probability distribution. This thesis uses a beta distribution

function in assessing nodes' trustworthiness for MANETs because of the following advantages [112]:

1. It represents a less resource intensive method to evaluate the trustworthiness of a node within two values (α, β) which is simple to store and compute. Therefore, it is suitable for MANET because of the constrained resources characteristic.
2. It forms a way to evaluate accumulated number of experiences a node can have during its network activities. The larger the numbers of experiences, the more a node is able to evaluate the trustworthiness of interacting nodes.
3. It enables the combination of experiences from different sources of direct experiences and recommendations received from others because of the addition property of the beta function.
4. It reflects the dynamic nature of trust, which is dependent on the accumulated number of experiences. A node can adjust its evaluation of others' trustworthiness with more experiences being accumulated by deriving the beta distribution after each observation has been made.
5. It captures the uncertainty property of trust because the beta function can give only a probabilistic estimation of future trust. Therefore, it is used to predict the future behaviour of nodes participating in networks' activities.

Beta distribution is estimated by using two parameters (α, β). These can be calculated by accumulating observations of forwarding and dropping packets where α represents the accumulation of positive observations (forwarded packets) and β represents the accumulation of negative observations (dropped packets). The beta distribution can be defined by gamma function [113] as in Eq. (3-1).

$$f(p|\alpha,\beta) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)}\, p^{\alpha-1}\,(1-p)^{\beta-1} \qquad (3\text{-}1)$$

where $0 \leq p \leq 1, \alpha, \beta > 0$ with a condition that $p \neq 0\, if\, \alpha < 1\, and\, p \neq 1$ if $\beta < 1$. Gamma function is defined by the integral: $\Gamma(x) = \int_0^\infty e^{-t}\, t^{x-1}\, dt$. Nodes in the network observe each other's behaviour in order to construct a trust relationship representing the degree of trustworthiness one node (known as an evaluating node) can place on another (known as the evaluated node) by evidence collected by the node itself or by other nodes (known as recommending nodes). The trust is measured as a real number in the range of 0-1, in which 0 denotes that the node is completely untrustworthy and 1 denotes that the node is completely trustworthy. These relationships are useful to help nodes decide whether to forward packets to a specific neighbour or not. The trust value of the problem is computed by giving the following information [18 , 108 , 114 , 115 , 116]:

- Number of positive observations (forwarded packets) α: it starts with the value 1, which is translated into complete uncertainty about the distribution of the parameter, which means no positive observation or evidence has been collected and would be calculated as $\alpha = \rho + 1$, where ρ represents the new positive observation.
- Number of negative observations (dropping packets) β: it starts with the value 1, which is translated into complete uncertainty about the distribution of the parameter, which means no negative observation or evidence has been collected, and would be calculated as $\beta = n + 1$, where n represents the new negative observation.
- Initial trust value: the trust model computation needs evaluating nodes to rate other evaluated nodes to find trustworthy neighbour to assign network activities. If nodes has no initial value to put on another node, trust

predictions cannot be made and this lead to the appearance of cold-start problem (which arises when nodes have no historical trust profile i.e., no interactions such as rating). To overcome the cold-start problem due to data sparsity, at time $t = 0$, $\alpha = \beta = 1$, which assigns a value of 0.5 to the initial trust held by a node about another.

- Trust value is updated after each positive or negative observation from these parameters as the expectation of beta distribution given by $\alpha/(\alpha + \beta)$.
- The computed trust value is utilised to detect misbehaving nodes based on the condition that $if\ \alpha/(\alpha + \beta) \leq Threshold$, then the node is classified as misbehaving.

The rationale of using α and β to represent a trust value or rating can be derived from the following analysis by plotting the beta probability density function $f(p|\alpha,\beta)$ for observation of some values of α and β as presented in Figure 3-2. The analysis starts with $\alpha = \beta = 1$, which makes the expectation value equal to 0.5, as shown in Figure 3-2(a). This initial belief is translated into complete uncertainty about the distribution of the parameter, which means no observations have been collected. The second case is when there are 9 observed successful interactions and 89 failed interactions, in which $(\alpha,\beta) = (10,90)$. As a result of this case, Beta$(p, 10,90)$ can be obtained, as in Figure 3-2(b). From this figure, it is observed that p converges to 0.1 which is a small constant and this can be translated into a node which performs more failed interactions and can be classified as untrustworthy. Meanwhile, the third situation, in which $(\alpha,\beta) = (50,50)$, presents the case where the number of observed successful interactions is the same as that of observed failed interactions. The result is obtained in Figure 3-2(c), where p is close to 0.5. In the last case, most

observed interactions are successful, in which $(\alpha, \beta) = (90,10)$ is plotted in Figure 3-2(d). It gives the result that p converges to 0.9 and this means that the node performs more successful interactions, and can be classified as more trustworthy than others who perform more failed interactions.

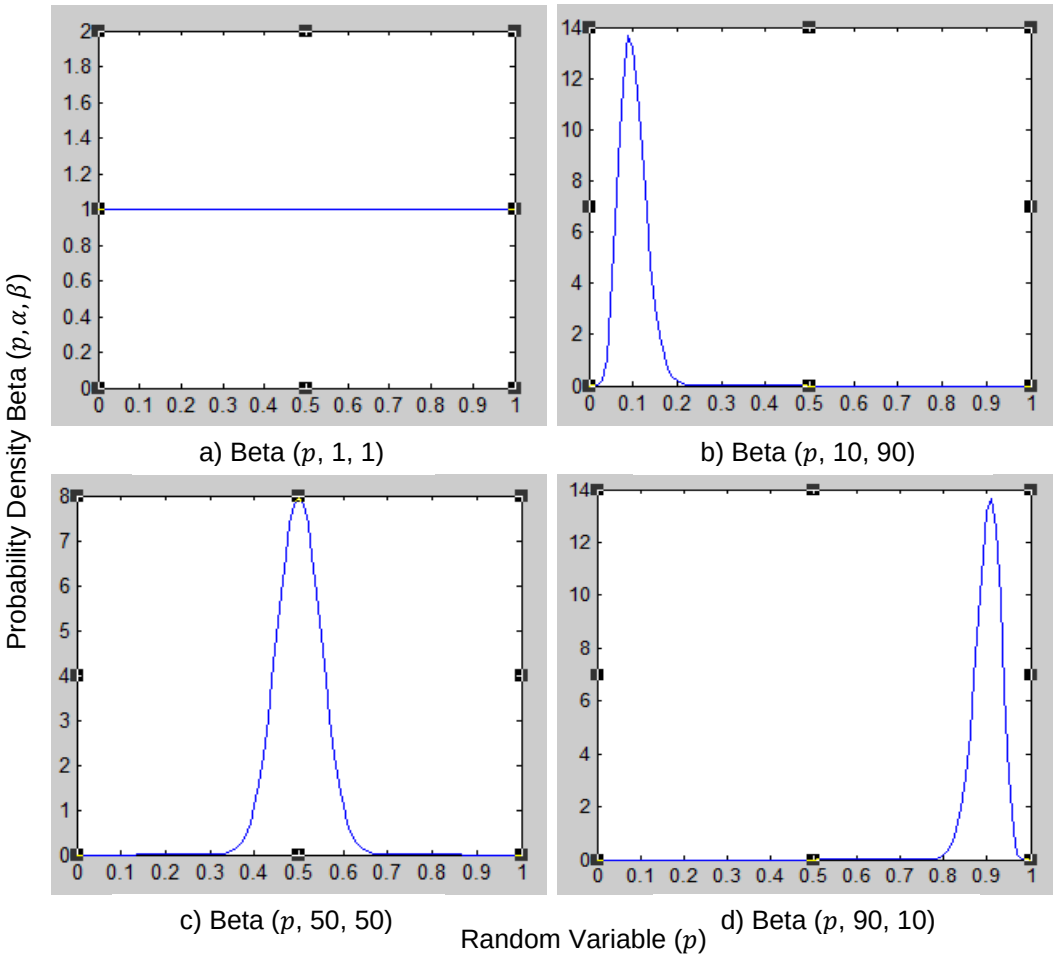


Figure 3-2 Typical beta plots for the random variables on the X-axes and Probability density on the Y-axes for the: a) ($\boldsymbol{\alpha}$=1, $\boldsymbol{\beta}$=1); b) ($\boldsymbol{\alpha}$=10, $\boldsymbol{\beta}$=90); c) ($\boldsymbol{\alpha}$=50, $\boldsymbol{\beta}$=50); d) ($\boldsymbol{\alpha}$=90, $\boldsymbol{\beta}$=10).

3.2 The Research Methodology

The research problem defined in Section 3.1 concerns collecting trust information and evidence by investigating the behaviour of nodes in mobile ad hoc networks. It evaluates the trustworthiness of nodes based on participating in network activities during the routing protocol activities, attacks models, and degree of hostility. In this context, there was a need to

have a realistic simulator that would produce a wireless network made up of autonomous and mobile nodes in order to evaluate the trustworthiness of nodes. Therefore, to conduct the research, NS2 simulator [117] is used. The underlying trust components which are described above (refer to Section 3.1.1) are added to the simulator to build the proposed models. Different components are added in each chapter to solve a specific problem. Chapter 4, Sections 4.2 and 4.3 explain in detail the design and the implementation of the experimental model. The opinion trust component, which evaluates the information received by the recommending node, is added. Besides this second chance components that evaluate the behaviour of nodes over time and give them another chance to contribute in network activities are also modelled. As the recommendation information is used in the model proposed in chapter 4, there is a need to extend the simulator to add a recommendation component and filtering algorithm, which is presented in Chapters 5. Further, Chapter 6 extends the simulation model by adding social and QoS components to test the influence of social properties on nodes' evaluation of trustworthiness. The configuration settings along with added components for each experiment are illustrated in Chapters 5 and 6, where the results of the experiments are analysed and conclusions drawn.

The following subsections give details about the research simulator, assumptions, and data collection used in this thesis.

3.2.1 NS2 Simulator

NS2 is an open-source discrete event simulator designed to support research in computer networking. It involves various modules to help test several network components such as packet, node, routing, application and transport layer protocol. It is implemented using two types of

languages, namely C++ and Otcl. Otcl script is used to manage parameters of protocols and C++ is used to implement models and algorithms. Although there are several network simulators with different features in different aspects, NS2 is the most popular simulator in academic research for its advantages of open source and useful library of different network components. Compare to commercial simulators like OPNET, NS2 has the advantages of being open and consequently individuals or organisations can contribute to it with maintenance, finding bugs, and future improvement. Besides, NS2 allows researchers to integrate existing codes and consequently takes advantage of their validity in previous wireless protocols. For these reasons NS2 is chosen to conduct this research. In this thesis, an extension has been made to Dynamic Source Routing (DSR) protocol [118] of the NS2 simulator to be used as an underlying routing protocol that supports MANET's architecture. DSR routing protocol is considered as an ad hoc on-demand protocol which is based on source routing technique. In the source routing technique, a sender of a packet determines the complete sequence of nodes through which to forward the packet and saves the available path in its route caches. The route discovery process is initiated when there is no path available from the sender of the packet to the destination. It contains two different phases, namely route request (RREQ), and route reply (RREP) in order to discover the available routes from source to destination. DSR is chosen in this thesis to test the trust models for its simplicity, and explicitly in stating routes in data packets. Besides, it is easy to launch attacks such as denial of service attack. However, the proposed models in this thesis can be applicable to any other routing protocols which are specifically designed for

mobile ad hoc networks such as Ad Hoc On-Demand Distance Vector Protocol (AODV) [119].

3.2.2 Assumptions

The proposed trust models in all subsequent chapters are based on improving the security of the network layer and do not depend on any tamper proof hardware, and there are no cryptography tasks required to transmit packets. However, the models can be used in conjunction with other security techniques for ad hoc routing such as cryptography or access control. The underlying assumptions used in testing the MANETs environment are commonly used in most MANETs' security area of research. Besides, these assumptions are critical to test the trust models proposed for MANETs, for example forwarding of packets is the most important behaviour because only cooperation of nodes can guarantee the exist of the network. Another example is giving a chance of bad behaving nodes to become good nodes and participate back in the network which may result in enhancing the network performance. The assumptions are illustrated as follows.

Assumption 1: All nodes have a unique ID and they are not able to change identity during the simulation time.

Assumption 2: Nodes are operating in promiscuous mode and they can listen to transmitting packets within their transmission range.

Assumption 3: Links between every two nodes are symmetric and omni-directional antennas.

Assumption 4: Correct forwarding of packets is the main behaviour to evaluate nodes' trustworthiness.

Assumption 5: Trustworthiness of nodes is based on a predefined threshold which is adjusted for each model in the subsequent chapters.

Assumption 6: Nodes can only monitor the behaviours of their one hop neighbours; consequently, they are able to evaluate their trustworthiness.

Assumption 7: Nodes can evaluate trustworthiness of two or more than one hop neighbours by using the monitoring information of other nodes which have interacted with them.

Assumption 8: Nodes can evaluate the future behaviour of each other based on past experiences of direct observations and recommendations.

Assumption 9: Trust among nodes is asymmetric and is not completely transitive.

Assumption 10: All nodes' behaviours are consistent with different percentages of hostility in some modeled attacks.

Assumption 11: Nodes' behaviours are independent from each other except for some attacks in which attackers collude together to achieve a specific attack.

Assumption 12: Redemption is utilised in order to give misbehaving nodes (due to network failure or environmental conditions) another chance to enhance their behaviours.

3.2.3 Mobility Model

The mobility model used in this thesis is the random way point which is the most commonly used model in ad hoc networking research [120]. It is feasible and movement could be considered as realistic which is very similar to the real world movement [121]. However, the proposed models in all subsequent chapters can fit any other type of mobility models like RPGM model [122].

3.2.4 Attack Model

The attack model is one of the important components that is utilised to represent the attackers' behaviour, which is modelled and added to the

simulator to test the validity of the proposed models. Different attacks are used in this thesis to fulfil the requirements of each model described in the following chapters. Similarly, nodes behaving badly such as blackhole, greyhole, and selfish attackers [22 , 123 , 124] are modelled and used with different percentages for all the proposed models in the subsequent chapters. For example, to model blackhole attack, nodes intend to maliciously drop all the received packets and refuse to forward them, while nodes in a greyhole attack also maliciously drop some selected packets with different percentages. Table 2-1 in the previous section shows the attacks modelled in this thesis to test the validity of the proposed models in the subsequent chapters.

3.2.5 Data Collection

This subsection provides information about the data collection and data sources used in this thesis. However, it is significant for large-scale simulation experiments to investigate the method of producing a flexible data collection and statistical analysis. Although NS2 has been considered as a leader among a vast number of network simulators [125], data collection aspects do not have adequate support and statistical analysis of the simulation results is most often performed by the users themselves using their local codes, which are not integrated in the simulator [126]. However, the only source of data collection in NS2 is represented by trace files. They record some important parameters such as generation, queuing, forwarding, and dropping of packets. Each line in the file represents information of an event related to the packet in terms of size, source and destination addresses, TCP/UDP port numbers, and some additional fields. In this thesis, a trace file of each simulation is used to analyse the proportion of packet loss and throughput. Additional information needed for

the research analysis, such as the number of misbehaving nodes and social values, is collected during the simulation and saved to text files. An AWK script [127], which is a programming language primarily designed for processing structured data records containing text, is written for each file to analyse the results.

3.3 Summary

An illustration of the problem of trust and reputation, which has been considered as the basis of this work is provided. The probabilistic trust model utilised in this thesis is described, along with its components and parameters. Further, the adopted research methodology is explored. An explanation of the simulator, assumptions, mobility model, attack model, and the way data is collected which are used to build trust in MANETs is provided.

Chapter 4 A Recommendation Based Trust Monitoring Model for MANETs

The reliability of delivering packets through multi-hop intermediate nodes is a significant issue in mobile ad hoc networks (MANETs). Monitoring based trust management has been proposed in the literature as a mechanism to filter out misbehaving nodes while searching for a packet delivery route. However, the building of a trust model that is designed to secure routing based on monitoring nodes' behaviour is vulnerable to the possible scarcity and uncertainty of information in the network, such as insufficient experience gained by an evaluating node. This chapter investigates the problems of building trust relationships between nodes to filter out attacks posed by misbehaving nodes while delivering packets in the existing trust models. A monitoring based trust model with a capability of utilising any available information within a certain time based on multiple sources of information: direct experience of a node itself, indirect experiences of other nodes, and opinion experience of recommending nodes is proposed in this chapter. The model is empirically tested and results are presented based upon a number of experiments. The experimental work of this chapter is carried out using an NS2 simulator.

4.1 Introduction

The trust based monitoring model of evaluating trustworthiness or reliability of nodes in MANETs has gained significant interest from researchers recently. Nodes tend to defect in the cooperation of packet delivery procedure by dropping packets or providing misleading information in order to extend their battery life or availability [22]. Recently, several trust and reputation management models have been proposed to secure MANETs and stimulate nodes to cooperate. However, some deficiencies have been

observed which might be trivial but can degrade the efficiency and performance of these environments. MANETs are distributed systems with unique characteristics; consequently, technical challenges are arising due to these characteristics, such as resource-constraints, openness to eavesdropping, high vulnerabilities, increased hostile environments, rapid topology changes due to node mobility or failure, and the inherent unreliability of communications over a wireless medium [75].

Most of the existing trust management mechanisms do not model trust in MANETs based on all these unique characteristics. It is critical in building such models in a dynamic environment like MANETs to carefully define the concept of trust based on their characteristics [7]. Trust in MANETs can be defined as the reliability, timeliness, and integrity of message delivery to a node's intended next-hop [128]. Due to MANETs' unique characteristics, nodes' collaboration in forwarding packets is vulnerable to misbehaving nodes. In the absence of proper countermeasures, MANETs' performance can significantly decrease due to selfish nodes, malicious attacks, and random failures. To overcome these limitations, a fully decentralised trust based monitoring model is proposed where trust scores are collected by the trust management system from all MANET participating nodes as ratings. The trust management system computes and updates these ratings to build trust relationships amongst nodes. The model aims to detect packet drop by selfish or malicious nodes, taking into account most of the MANETs' unique characteristics such as constrained resources in terms of time and energy. Another aim is to save these limited resources by simplifying or eliminating unnecessary computations of the trust values such as helping nodes to reduce the energy consumption and increase their lifetime in the network. The main contribution of this chapter is the use of any available information in

the network to construct the trust relationships between any two nodes that would like to interact. An important component is added to the proposed model, namely opinion trust that expresses a node's opinion about how honest a node is as a recommender. This value is used in calculating the overall trust value of a particular node in addition to direct and indirect trust with various different weights.

4.2 The Trust-Based Monitoring Model

This subsection outlines the parameters that would be used as a basis to measure trust values in a MANET environment. The choice of these parameters has been directed by the use of the beta distribution function outlined in Chapter 3. A wireless MANET scenario is considered, where a node monitors its neighbours for packet forwarding service and chooses a trustworthy neighbour in terms of packet forwarding based on a trust value assigned by the trust model. The main component of the model is the trust management system that is run by each node in the network to maintain a trust value for all other nodes with which it has interacted in the past. Each node initiates a trust relationship with other nodes based on accumulating the successful and failed transactions (positive and negative observations) from the monitoring components. After each observation, a trust value of the evaluating node is updated regarding the evaluated node. The evaluation process is not only based on past experiences: it also has the opportunity to share other nodes' experience by means of recommendations. The trust is measured as a continuous valued variable in the range of $[0, 1]$, in which 0 denotes that the node is completely untrustworthy, 1 denotes that the node is completely trustworthy, and 0.5 denotes complete uncertainty. A continuous valued variable can effectively represent uncertainty property of trust better than a binary variable [7]. The following parameters, listed and detailed

below, summarize the characteristics of the Trust Based Monitoring Model in the scenario explained above:

A. Direct Trust T_{ij}^{direct}

In MANETs, direct trust is obtained when two nodes have already initiated a trust relationship and they can immediately interact with each other (at least for a specific period of time, when they are within the same range, because of nodes' mobility), without requiring a third-party opinion or recommendation. The direct trust value is updated based on whether the previous interactions between two nodes have been successful or not. The observation is represented by two variables ρ and n describing the number of positive and negative interactions respectively. The calculation of ρ and n would be as $\rho = \rho + 1$ when observing normal behaviour (forwarding packets) and $n = n + 1$ when observing misbehaviour (dropping packets) where ρ and $n \geq 0$. Then α_{ij} which represents the accumulated positive interactions between node i and j is calculated as $\alpha_{ij} = \alpha_{ij} + \rho_{ij}$, while β_{ij} which represents the accumulated negative interactions is calculated as $\beta_{ij} = \beta_{ij} + n_{ij}$. Direct trust value is considered to be accurate and its computation invulnerable to dishonest attacks. The calculation is based on the beta-function by applying the values of α_{ij} and β_{ij} in Eq. (4-1).

$$T_{ij}^{direct} = \frac{\alpha_{ij}}{\alpha_{ij} + \beta_{ij}} \qquad (4\text{-}1)$$

B. Indirect Trust $T_{ij}^{indirect}$

Indirect trust needs to be considered when two nodes have not established a previous trust relationship through exchange of packets or any other form of communication. In such cases, the evaluating node does not have sufficient experience to judge the trustworthiness of the other node being evaluated. Indirect trust is also calculated using the beta-function, similarly to the way in

which direct trust was computed earlier. Indirect trust actually comprises the direct observations obtained by one node about its neighbours, which can be used by another node as second-hand information. Node k 's direct observations of node j could be indirect or second hand information to another node i (given that node i and j have not interacted in the past). Therefore, indirect trust value is calculated using (α'_{ij}, β'_{ij}) and updated by two variables: ρ', describing the number of positive interactions, and n', describing the number of negative interactions. Further, α'_{ij} and β'_{ij} are calculated as $\alpha'_{ij} = \alpha'_{ij} + \rho'_{ij}$ and $\beta'_{ij} = \beta'_{ij} + n'_{ij}$. If the evaluating node i receives N recommendations for the evaluated node j denoted by $k = 1, 2, \dots, N,$ indirect trust $T_{ij}^{indirect}$ of node i about j is calculated according to the Eq. (4-2).

$$T_{ij}^{indirect} = \sum_{k=1}^{N} \frac{\alpha'_{kj}}{\alpha'_{kj} + \beta'_{kj}} \quad (4\text{-}2)$$

C. Opinion Trust $T_{ij}^{opinion}$

Opinion trust is the trust value that expresses a node's opinion about how honest a node is as a recommender in the trust and reputation system. In other words, this information represents whether a node's recommendations are likely to be accepted by the evaluating node and considered as true. In a similar way to direct and indirect trust, opinion trust value is also calculated based on (α''_{ij}, β''_{ij}) and updated by two variables: ρ'', describing the number of positive interactions; and n'', describing the number of negative interactions. Further, α''_{ij} and β''_{ij} are calculated as $\alpha''_{ij} = \alpha''_{ij} + \rho''_{ij}$ and $\beta''_{ij} = \beta''_{ij} + n''_{ij}$. Consider the same scenario expressed above: k is a recommending node would provide information about evaluated node j by the evaluating node i. Opinion trust is updated only when a recommendation

is received from node k. If the recommendation is accepted, this is interpreted as a positive interaction (i.e. $\rho'' = 1$); otherwise, this is interpreted as a negative one (i.e. $n'' = 1$) between the evaluating node i and the recommender k. Opinion trust $T_{ik}^{opinion}$ of node i about k is calculated according to Eq. (4-3).

$$T_{ik}^{opinion} = \frac{\alpha_{ik}^{''}}{\alpha_{ik}^{''} + \beta_{ik}^{''}} \quad (4\text{-}3)$$

D. Deviation Test D

Indirect trust information is very important to incorporate in a trust model for MANETs because of its advantages in providing information about unknown nodes by the evaluating node. However, involving this kind of information can leave the model vulnerable to intentionally generated untrustworthy recommendations. It is significant to check the honesty of this information to mitigate the influence of wrong evaluation by the trust model. Assume that the evaluating node i would like to calculate the trust value of its neighbour node j using receiving recommendation provided by recommending node k. Node i first checks the opinion trust value of the node k. If the opinion trust value held by node i about node k, which is denoted by $T_{ik}^{opinion}$, is more than a certain trust threshold $T_{ik}^{opinion} > Opinion\_threshold$, then the k is trusted without further tests and indirect trust is updated for node j. This technique permits fast trust convergence, which is vital in MANETs, where nodes have limited battery and resources to observe the trust of other nodes. As a result of trusted node k, node i updates the opinion trust value of node k accordingly. If the above test is false, node i first performs a deviation test to check if the information received from node k is compatible with the information held by node j using $\left|T_{ij}^{direct} - T_{kj}^{indirect}\right| \leq D$, which indicates the deviation threshold. If the above test is positive, then the information provided

is regarded as compatible and indirect trust information is used to update trust value node j.

E. Decay Factor μ

The influence of past experiences changes over time in a dynamic environment. It is thus important for a trust model to consider this change in influence. The proposed model incorporates a decay factor (μ) to gradually decrease the influence of past experience over time, prior to aggregation with new trust values. Forgetting of past experiences is carried out by adjusting the time frame of observations while recording the positive or negative experience. However, trust decays over time even during inactive periods and it is thus important to consider the diminishing impact of trust over time. The first situation is when a node observes an additional new positive or negative interaction between time t_c and t_{c+1} denoted as ρ^{new} and n^{new} . In this case, the updated ρ and n should be reduced by the decay factor μ before merging them with the new values. Therefore, at time t_{c+1}, ρ and n is updated respectively according to the formula in Eq. (4-4).

$$\rho = \rho^{old} * \mu + \rho^{new} \ , \ n = n^{old} * \mu + n^{new} \qquad (4\text{-}4)$$

where $0 \leq \mu \leq 1$. The second situation is when there is no observed new positive and negative interaction between time t_c and t_{c+1}. Then, at time t_{c+1}, ρ and n are updated respectively as in Eq. (4-5).

$$\rho = \rho^{old} * \mu \ , \ n = n^{old} * \mu \qquad (4\text{-}5)$$

F. Trust Value T_{ij}

For each node in the network, trust value T_{ij} is calculated by combining direct, indirect and opinion trust values with different weights, denoted by w_{direct}, $w_{indirect}$, and $w_{opinion}$ respectively. Trust value T_{ij} is computed according to Eq. (4-6),

$$T_{ij} = w_{direct}T_{ij}^{direct} + w_{indirect}T_{ij}^{indirect} + w_{opinion}T_{ij}^{opinion} \quad (4\text{-}6)$$

where $0 \leq w_{direct} \leq 1, 0 \leq w_{indirect} \leq 1, 0 \leq w_{opinion} \leq 1, and \;\; w_{direct} + w_{indirect} + w_{opinion} = 1$. Different weights are incorporated in the proposed model because of their significant impact on diminishing the possibility of wrong trustworthiness evaluation of trust information provided by nodes. In the proposed model, higher weight is usually given to direct information, as it is less prone to dishonest evaluation. It is fixed per each simulation and manually changed when needed. However, MANETs' characteristics such as mobility and frequent change in topology make it difficult to completely trust the source of information, even if it is the node's self-assessment. Therefore, the weighting problem is considered in subsequent chapters and dynamically calculated based on the quantity and quality of interactions observed by evaluating nodes.

G. Example of Calculating Trust.

Assume that the evaluating node i would like to calculate the trust value of its neighbour node j using direct trust and indirect trust (recommendation provided by recommending node k). node i has observed 89 positive interactions $\alpha = 90$ and 9 negative interactions $\beta = 10$ at time t. Therefore, the direct trust is calculated using Eq. (4-1).

$$T_{ij}^{direct} = \frac{\alpha_{ij}}{\alpha_{ij} + \beta_{ij}} = \frac{90}{90 + 10} = 0.90$$

Indirect trust is calculated based on the sum of received recommendation in the form of ratings (α, β). Assume node i receives recommendations from node $k_1 = (80,20)$, $k_2 = (100,15)$, $k_3 = (89,10)$, and $k_4 = (7,79)$. Based on the received recommendation node i will perform the deviation test and accept only the recommendations from nodes k_1, k_2, and k_3 and

exclude the recommendation received from node k_4. Therefore, indirect trust is calculated according to Eq. (4-2).

$$T_{ij}^{indirect} = \sum_{k=1}^{N} \frac{\alpha'_{kj}}{\alpha'_{kj} + \beta'_{kj}} = \frac{80 + 100 + 89}{(80 + 100 + 89) + (20 + 15 + 10)} = 0.86$$

Opinion trust is calculated based on the positive and negative interactions of node j held by node i as a result of being honest recommender. Assume that node i has observed 49 positive interactions $\alpha = 50$ and 2 negative interactions $\beta = 3$ at time t. Therefore, the opinion trust is calculated using Eq. (4-3).

$$T_{ik}^{opinion} = \frac{\alpha''_{ik}}{\alpha''_{ik} + \beta''_{ik}} = \frac{50}{50 + 3} = 0.94$$

The overall trust now is calculated using Eq. (4-6) with a weight of 50%, 40%, and 10% is given to direct, indirect, and opinion trust values respectively.

$$T_{ij} = w_{direct} T_{ij}^{direct} + w_{indirect} T_{ij}^{indirect} + w_{opinion} T_{ij}^{opinion}$$

$$T_{ij} = 0.50 * 0.90 + 0.40 * 0.86 + 0.1 * 0.94 = 0.83$$

4.3 Simulation and Analysis

An experiment to test the components and functionality of the trust model is conducted. A wireless MANET environment with two types of nodes which act as intermediate nodes is simulated. The first type of node comprises good nodes which behave normally in the service of forwarding packets, while the other type behaves badly by dropping all or some packets (blackhole and greyhole attack). The main aim of the experiment is to consider the contribution of the model in detecting and avoiding the bad nodes and consequently enhancing network performance in terms of throughput and packet loss.

4.3.1 Experimental Setting

The simulation is conducted by the NS2 simulator. In a network with 50 random placed nodes in an area of 700×700, several nodes are randomly selected as misbehaving by dropping data packets and this attack is simulated. There are 15 source-destination pairs and each source transmits 2 packets per second with a Constant Bit Rate (CBR). The packet size is 512 bytes and the simulation time is 900s. Table 4-1 shows the parameters used in configuring the network for this experiment.

Table 4-1 Network configuration

Parameter	**Value**	**Parameter**	**Value**
Nodes	50	**Application**	CBR
Area	700 X 700 m	**Packet size**	512 B
Speed	10 m/s	**Simulation time**	900 s
Radio Range	250 m	**Opinion_threshold**	0.6
Movement	Random waypoint	**Trust_threshold**	0.3
Routing Protocol	DSR	**Publication timer**	10 s
MAC	802.11	**Decay timer**	10 s
Transmitting capacity	2 Kbps, 4 Kbps	**Deviation threshold *D***	0.5

4.3.2 Experimental Results

In this section, results and analysis on the computation of three components of the trust model, namely the direct trust, indirect trust, and opinion trust values, are presented. A discussion of the values and their relationship to the overall trustworthiness value is also provided. The simulation results are shown in Figures 4-1 to 4-3. The ability of the model to allow a node to classify other nodes in the network as bad and good nodes and successfully judge their trustworthiness in a short time is also considered in figure 4-4 and 4-5. The model extends the standard DSR routing protocol with the trust model. Therefore, comparisons between the standard DSR and DSR with trust model performance on both throughput and packet loss are also presented in Figures 4-6 and 4-7.

To produce the results, a highly connected node which has a great number of neighbours in the network is picked at random and its interactions and trust relationships with other nodes is analysed. Because of the mobility issue in MANETs, a single node's data is used in the analysis to confine the results.

Firstly, an analysis of the impact of the three components on the overall trustworthiness of a good node (node 4 in this case) is considered by looking at the values of direct, indirect, and opinion trust values over the time of the simulation. A weight of 50%, 40%, and 10% is given to these values respectively which are identified by practice as the best weights to increase the ability of nodes to assess trustworthiness of other neighbours in the network. A value of 0.5 is given as a starting trust value for all nodes in the network. It is obvious from the comparable results in Figure 4-1 and Figure 4-2 that the direct trust values and indirect trust values are consistent. This is because of the fact that the proposed model only accepts recommendations which do not deviate too much from the direct trust being held by the evaluating node and used to update the indirect trust values. Meanwhile, in Figure 4-3, opinion trust starts at a value of 0.5 when the node provides recommendations, and this increases gradually whenever the node provides honest recommendations, and its value then differs from the overall trustworthiness in the early time of simulation. Its value increases to nearly the same value as trustworthiness in the second half of the simulation time.

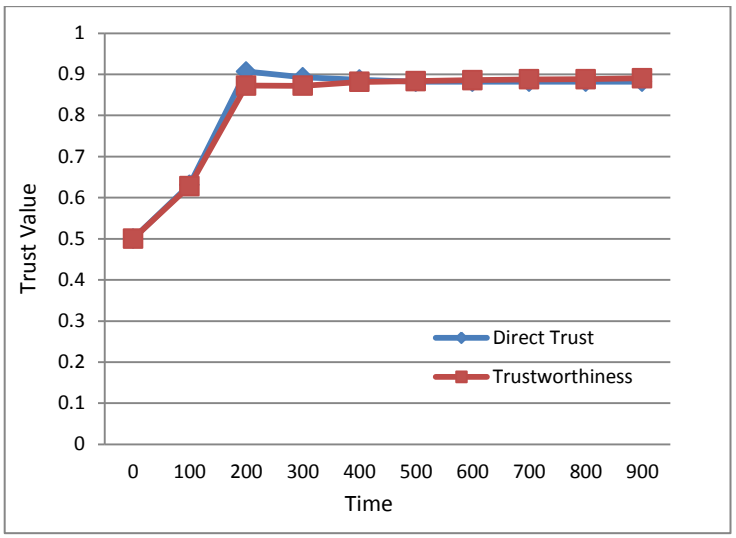


Figure 4-1 The impact of direct trust component in the trustworthiness computation of node 4 by other nodes in the network

Figure 4-2 The impact of indirect trust component in the trustworthiness computation of node 4 by other nodes in the network

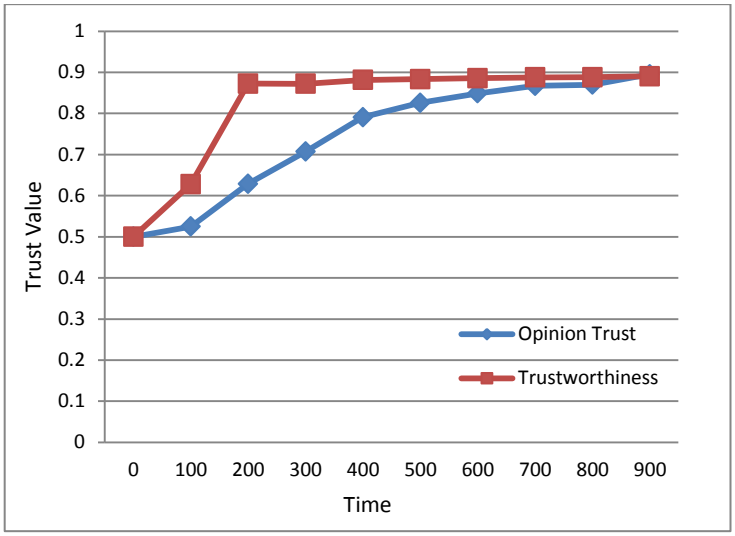


Figure 4-3 The impact of opinion trust component in the trustworthiness computation of node 4 by other nodes in the network

In Figures 4-4 and 4-5, an important evaluation metric is also examined to look more closely at whether the nodes are correctly classified as good and bad nodes. The classification of nodes should happen quickly in the early phase of the simulation as nodes are forced to make early decisions about other nodes' trustworthiness. Figure 4-3 shows the trustworthiness of node 4 by other nodes at different numbers of interactions which starts from 0 to 100 interactions in the presence of 40% bad nodes. It is obvious that nodes are able to judge the others' trustworthiness by gaining more experience over time (i.e. increasing the number of interactions). In the early stages, once there is no enough experience, good and bad nodes are intermixed and there is no clear separation between them as the bad nodes have trust values more than the trust threshold. The classification of nodes is improved by an increase in the number of interactions. Good nodes move towards the upper right corner in which the trust value converges to 1, while the bad nodes move towards the upper left corner in which the trust value converges to 0.

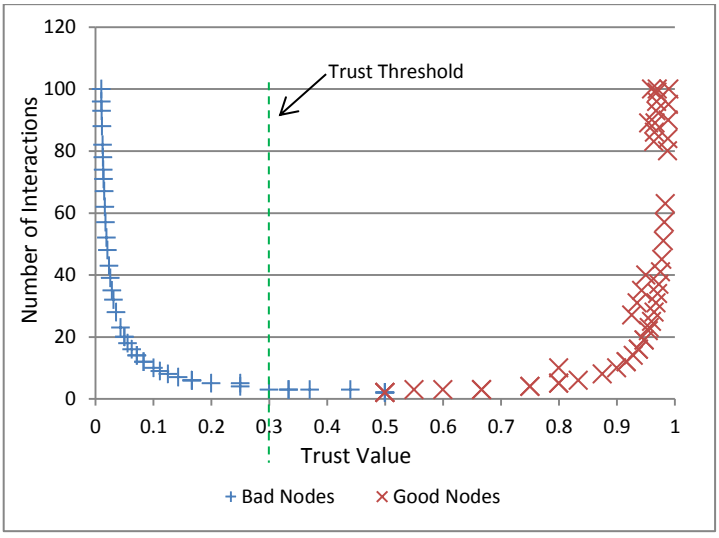


Figure 4-4 The impact of experience (number of interactions) in the classification of other nodes by node 4 in the present of 40% bad nodes

Figure 4-5 shows the classification of nodes by two nodes: 4 and 9. It shows that the percentage of nodes classified by both nodes 4 and 9 increases with the time of the simulation and is above 60% by the end of simulation. This percentage depends on the number of bad nodes and the degree of connectivity (neighbours). However, the proposed model is able to allow nodes to successfully classify others even when 40% of nodes are behaving badly.

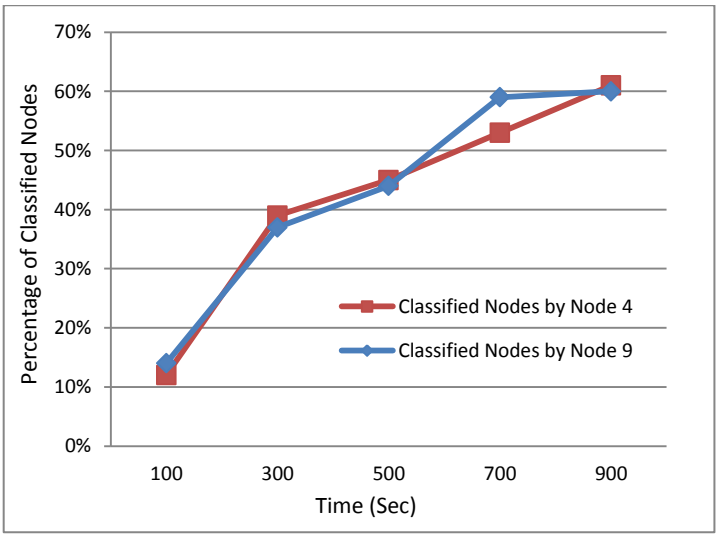


Figure 4-5 Percentages of the nodes classified by node 4 and node 9 of other nodes in the presence of 40% bad nodes

Another evaluation metric is to consider the adaptation of the proposed model in routing protocols such as DSR or AODV and check its applicability and impact on the network performance, as shown in Figures 4-6 and 4-7. Figure 4-6 displays on the x-axis the number of misbehaving nodes, ranging from 0, which means all nodes are behaving normally, to 20 misbehaving nodes. The y-axis shows the percentage of the network throughput of both standard and trusted DSR. The figure shows that the throughput for the proposed trust mechanism gradually drops as the number of misbehaving nodes increases but it remains at nearly 60%. Meanwhile, standard DSR falls below 50% at the same time and same number of misbehaving nodes.

Figure 4-7 displays the percentage of the packet loss of both standard and trusted DSR, with the same percentage of misbehaving nodes, which ranges from 0 to 20 misbehaving nodes. It shows an improvement in the ratio of packet loss over the standard DSR in all the cases considered.

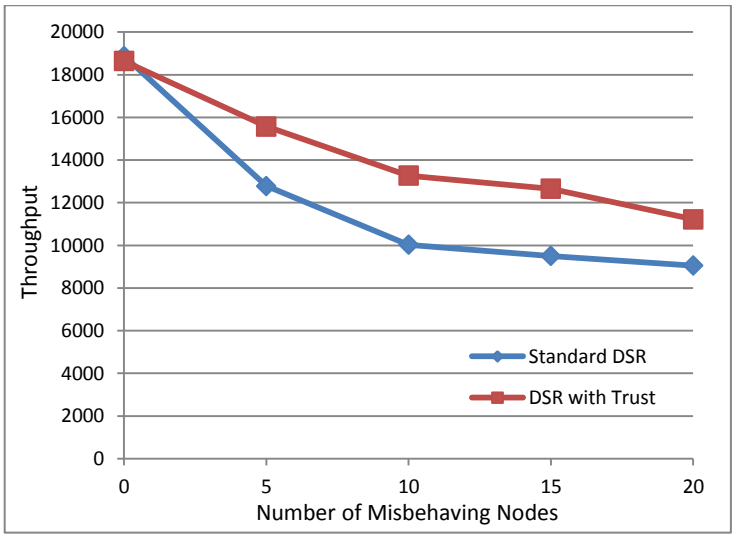


Figure 4-6 Network throughput

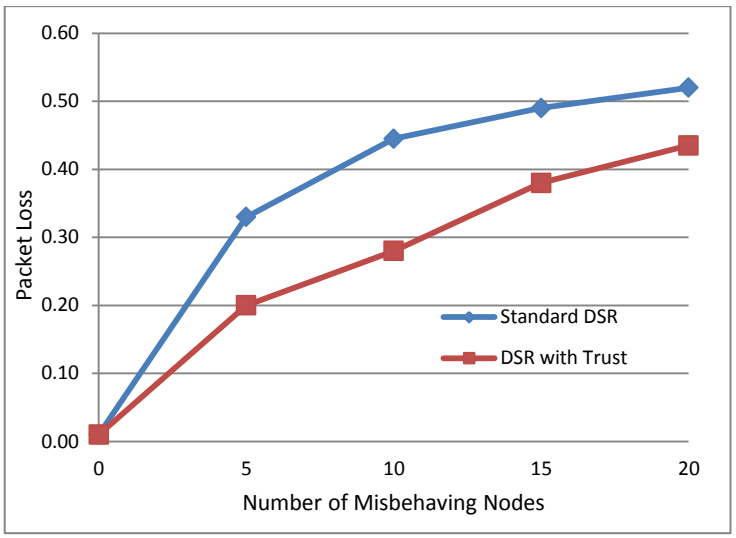


Figure 4-7 Packet loss

4.4 Summary

In this chapter, a trust model was built to monitor misbehaving nodes in ad hoc routing protocol, their harmful influence was mitigated and they were avoided by nodes in selecting a reliable routing path. Trust evidence, including direct trust, indirect trust and opinion trust are evaluated. All the available information needed for calculating trustworthiness is gathered and used as appropriate. The model is totally decentralised and depends on the nodes' experience gained in previous interactions, giving greater importance to recent experiences. The node can use its own evidence (direct trust) or can use external evidence or recommendations by other nodes (indirect trust). These forms of evidence are used with appropriate weighting to reflect the fact that direct evidence is more valuable than other evidence, which may be subject to dishonest recommendations. A deviation test was used to deal with untrustworthy nodes in hostile environments like MANETs and this test was sufficient, as no attacks related to providing dishonest recommendations are considered. Extensive work on finding effective solutions to the problem of dishonest recommendations is considered in subsequent chapters. A

second chance for misbehaving nodes which are isolated from the network is given to deal with the problem of false evaluation due to insufficient experience to determine the honesty of a node. The problem of short-term experience is solved in the next chapters by using the confidence value, which indicates that the node has sufficient experience to determine the honesty of other nodes.

Chapter 5 Recommendation Based Trust Model with an Effective Defence Scheme

This chapter proposes a recommendation based trust model that adopts recommendations by other nodes in the network which is a challenging problem due to the risk of dishonest recommendations like bad-mouthing, ballot-stuffing, and collusion. This chapter investigates the problems of attacks posed by misbehaving nodes while propagating recommendations in the existing trust models. It proposes two methods to tackle this problem. First, a dynamic recommender selection, which utilises three different rules: (i) majority rule based; (ii) personal experience rule based; and (iii) service reputation rule based. Second, a robust and effective defence scheme to select the recommending node based on three factors: (i) number of interactions with the evaluated node; (ii) unity of view with the evaluating node; and (iii) closeness to the evaluating node. Clustering technique is adopted in both methods to dynamically filter out recommendations between certain timeframe.

5.1 Introduction

Recommendation based trust management has been proposed in the literature as a route security mechanism to establish trust between nodes and filter out the misbehaving nodes [15 , 129]. Prior to interaction, the use of recommendation based trust technique can help nodes in discovering misbehaving nodes, consequently avoiding a potential bad experience. Nodes in MANETs can make more informed decisions on the selection of routing paths using recommendations by sending a single packet to them, and consequently use less resources and could help in saving energy [17].

Together with the advantages comes the challenge of handling dishonest recommendations in MANETs. A cold-start problem due to data sparsity,

which arises when nodes have no historical trust profile results in a particular node might not be well informed to make an assessment of trustworthiness of another node. In such cases, the evaluating node solicits recommendations from the evaluated node's neighbours (acquaintances) with whom it has a history of interaction. However, to maximise the gain of individuals and their acquaintances, nodes could resort to dishonest behaviours through attacks such as ballot stuffing, bad-mouthing and collusion. Such attacks could eventually lead to trust framework malfunction [123]. Solutions proposed to tackle these problems are limited and not adequately effective [10 , 15 , 17 , 114].

One of the approaches [10] judges the honesty of the recommending node by considering the majority opinion between recommendations and excluding any recommendation out of the majority. In such case, filtering out dishonest recommending nodes becomes a serious problem when recommending nodes collude with each other to accomplish a malicious goal. Another approach is the service reputation [114] by referring to their trust values in which a recommending node with a high trust value is preferred and seen as a trustworthy one. However, a node can be trustworthy in terms of packet forwarding but could be a bad node as a recommending node. An experience based approach [15] is also used to filter out dishonest recommending nodes whose opinions are considered as incompatible with the opinions of the evaluating node. This approach could be unfruitful when the evaluating node has no prior experience with the evaluated node. These limitations may result in a confusing and misleading trust model in judging the nodes' trustworthiness.

The main contribution of this chapter is the proposal of a recommendation based trust model with a defence scheme, which utilises clustering

techniques to dynamically filter out attacks related to dishonest recommendations between certain timeframes based on two ways. First, the consideration of all three types of rules described above to come with an integrated measure to address the problem of dishonest recommendations: the majority rule to ensure the consistency of recommendations among time and location, the personal experience based rule to ensure the consistency of the received recommendation with the information held by the evaluating node, and the service reputation based rule to ensure the honesty of recommender by the services provided over time. Second, an effective defence scheme is proposed using three parameters to compute the trustworthiness of recommenders: number of interactions (using confidence value), compatibility of information with the evaluated node (through deviation test), and closeness between the nodes. The defence scheme underlines the importance of social properties in evaluating trustworthiness and uses it in investigating the relation between closeness of nodes and similarity in behaviour. The use of proof of time and location missing in the current literature is considered by the proposed model. False negative and false positive problems in evaluating the recommendation's trustworthiness and their impact on the network performance are thoroughly investigated. Different nodes are chosen in the evaluation procedure to test the performance of the filtering algorithm against various mobile topologies and neighbourhoods.

5.2 Attacks Related to Recommendation Management in Trust and Reputation Frameworks

It is indeed a challenge to safe guard a network against a wide range of attacks. Recent focus of research in this area has been on the problems associated with misbehaving nodes in the context of packet forwarding, like

blackhole or wormhole attack [130]. For quality assurance, it is important that trust management frameworks be resilient to attacks [16]. Although several researchers have put considerable effort to protect the propagation and aggregation of recommendations in a trust model, research is still in its early stages [74]. The following attacks, namely, bad mouthing attack, ballot stuffing attack, selective misbehaviour attack, intelligent behaviour attack, time-dependent attack and location-dependent attack (see Figure 5-1 for the classification of attacks), are targeted at the propagation and aggregation of recommendation [16 , 74 , 131] Location-dependent attack is used for the first time in this thesis. The attack behaviours are summarised below:

I. Bad Mouthing Attack (BMA). In this type of attack, conspiring nodes propagate unfairly negative ratings of good nodes with an ill intent to tarnish their reputation in the network. Such collusive behaviour may lead to the blocking of valid paths in the network by confusing the trust and reputation management mechanism.
II. Ballot Stuffing Attack (BSA). Propagation of unfairly positive ratings for some poorly performing nodes by collusive nodes in the network lead to ballot stuffing attack. The intention of collusive nodes is to mislead the trust mechanism and cause it to malfunction in accurately reporting the trustworthiness of the assessed node.
III. Selective Misbehaviour Attack (SMA). This attack victimises some trusted nodes by propagating false ratings for them, while at the same time acting normal to other nodes. This type of behaviour can be very difficult to detect for the trust mechanism.
IV. Intelligent Behaviour Attack (IBA). This attack selectively provides recommendation with high or low ratings according to the trust threshold.

This kind of attack can cause malfunction to the trust framework by dynamically responding to the trust threshold and behaving based on it.

V. Time-dependent Attack (TDA). This attack makes participating nodes change their behaviour by time. Nodes can behave normally for a period of time and can misbehave by providing unfair ratings at other times. This attack also has its roots in the subjective property of trust.

VI. Location-dependent Attack (LDA). This attack exploits mobility property of MANETs, where a node behaves differently according to its location. This attack originates from the subjective property of trust where behaviours at one location cannot affect evaluating trustworthiness of nodes at another location.

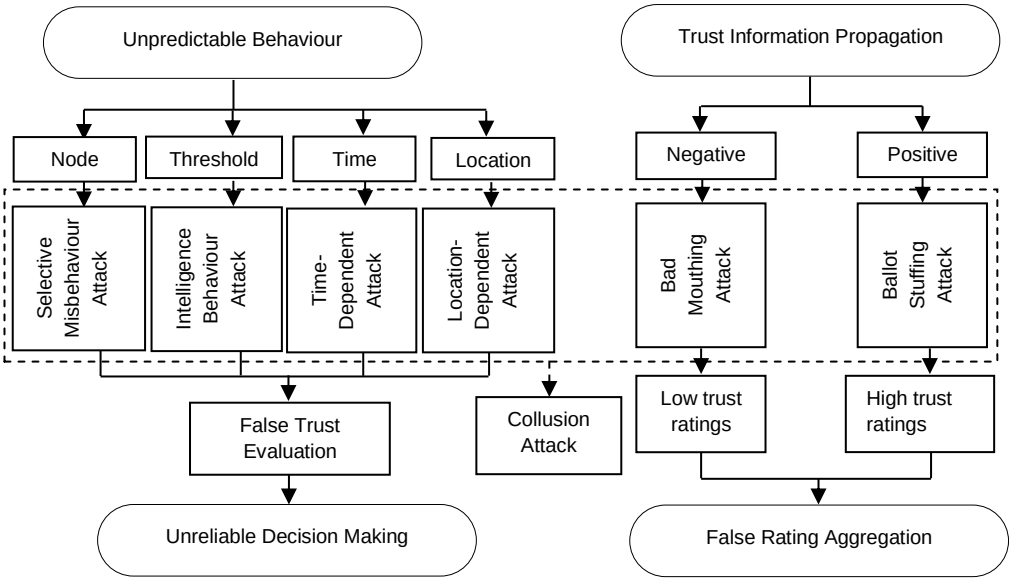


Figure 5-1 Attacks Related to Misbehaviour Problems in Recommendation Management of Trust and Reputation Frameworks

The summarised attacks belong to two categories: false rating (BMA, BSA, and SMA), and inconsistent rating based on the trust threshold, time, or location (IBA, TDA, and LDA). Some of the countermeasures illustrated below can be used for both categories or being specifically designed for one category. For example, [23] proposes the use of only positive

recommendations, while [18] uses only negative recommendations and this can countermeasure attacks like ballot stuffing and bad mouthing. This kind of defence can be harmful to trust information because nodes cannot report their complete experiences. Statistical methods like Bayesian theory to accurately compute the correctness of recommendations can be a robust solution to both categories [131]. Proof of sufficient interactions [75], and specifying a certain threshold of negative and positive recommendation, besides, the majority opinion technique [77] could also be used to mitigate the effect of false and inconsistent rating. Comparison between a recommendation list and proof of time and location of the recommendation provider is also a promising solution to time and location-dependent attacks. The method of comparing time and location is considered for the first time in the proposed algorithm.

What follows from the above discussion is that the recommending nodes' trustworthiness cannot be assessed by just a single scheme. It should be supported by using many behaviour and social properties (such as, the closeness between nodes, and proof of time and location) which are missed in the literature. In order to improve accuracy and robustness of the trust model, the influence of the untrustworthy recommendations should be mitigated to overcome the problem of false negative and false positive.

5.3 The Recommendation-Based Trust Model

This subsection describes the recommendation-based trust management model that is utilised to secure the routing protocol between source and destination nodes based on the trust value of each node in the path. The model considers the problem of the attacks discussed earlier due to some misbehaving nodes in MANETs. The model uses the Bayesian statistical approach similar to that used in chapter 3 and 4 for computing trust values

based on the assumption that they follow a beta probability distribution by using two parameters (α, β). They can be calculated by accumulating observations of forwarding and dropping packets where α represents the accumulation of positive observations (forwarded packets) and β represents the accumulation of negative observations (dropped packets). We model two types of attacks related to the dishonest recommendation problem, which are bad-mouthing and ballot-stuffing to test the model functionality. The model has three components deployed to evaluate trust as in Figure 5-2.

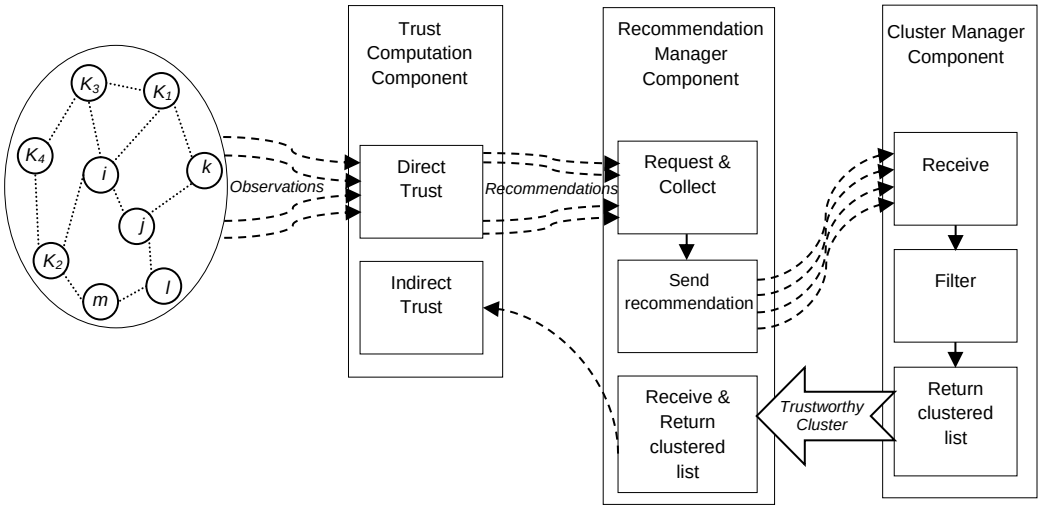


Figure 5-2 Recommendation trust model components

A) Trust Computation Component

The computation component uses direct as well as indirect (second hand) trust information. It obtains direct trust value from two nodes that have already initiated a trust relationship. The proposed model incorporates a decay factor (μ) to gradually decrease the influence of past experience over time, prior to the aggregation with new trust values. The trust computation component needs to consider indirect trust when two nodes have not established a previous trust relationship through exchange of packets or any other form of communication. In such cases, the evaluating node does not

have enough experience to judge the trustworthiness of the other node being evaluated. Indirect trust is also calculated using the beta-function, similarly as in chapter 4. While indirect trust information is important to incorporate in a trust model for MANETs, involving this kind of information can be vulnerable to intentionally generated dishonest recommendations. For each node in the network, overall trust value T_{ij} is calculated by combining both direct and indirect trust values with different weights.

B. Recommendation Manager Component

The recommendation manager component in the proposed model requests and gathers recommendations for a node from a list of recommending nodes. It works as an intermediate component between indirect trust computation and cluster manager components. It helps in detecting and eliminating false recommendations. The recommendation manager has three important roles: (1) send recommendation request to the evaluating node's neighbours; (2) collect received recommendation and send it to the cluster manger which runs the filtering procedure; (3) receive the filtered recommendation and send it back to the trust computation component. The recommendation manager requests and gathers a recommendation list for an evaluating node i about node j from a list of recommending nodes $\{k_1, k_2, k_3, \ldots., k_N\}$ between time t_i and $t_{i+1}$and send it to the cluster manager to run the filtering algorithm. After filtering, it receives the trustworthy clusters as a list of honest recommendations denoted as $\{k_1^{Tr}, k_2^{Tr}, k_3^{Tr}, \ldots, k_N^{Tr}\}$. The final task is to send the trustworthy cluster $C^{Trustworthy}$ to the requesting node. Algorithm 5-1 illustrates the recommendation manager algorithm.

Algorithm 5-1: Recommendation Manager Algorithm

1. ***For*** *each recommendation request* ***Do***
2. ***Send*** *request to neighbours*
3. ***Collect*** *received recommendation*
4. ***Construct*** $L = \{k_1, k_2, k_3, \ldots, k_N\}$
5. ***Send*** L *to the cluster manager for processing*

6. ***Receive*** *trustworthy cluster* $C^{Trustworthy} = \{k_1^{Tr}, k_2^{Tr}, k_3^{Tr}, \dots, k_N^{Tr}\}$
7. ***Send*** $C^{Trustworthy}$ *to the requested node*
8. ***End*** *For*

C. Cluster Manager Component

The proposed trust model uses a clustering technique in order to maximise the consistency of receiving recommendations. For example, recommendations from a misbehaving node can have a range of multiple different ratings for the evaluated node. These ratings may be inconsistent in which they can differ from each other in a short period of time, a malicious act of the misbehaving node to confuse the trust model. Dynamic clustering of the recommendations over a period of time can filter out deviated ratings from the list of recommendations, thus decreasing the influence of false estimations in computing a trust value.

Cluster manager receives a list of recommendations from the recommendation manager and processes it through a clustering technique. The clustering algorithm is performed by the evaluating node on all the reports from the recommendation list which is denoted by $L = \{k_1, k_2, k_3, \dots, k_N\}$. The k-means clustering technique similar to [77] is applied on weighted trust values provided by recommenders which are considered as data for the clustering operation. The clustering approach divides the trust values from the recommenders into a predefined number of clusters denoted as K. Each trust value is initially considered as a cluster, and then two clusters with the shortest Euclidean distance are merged together to produce a new cluster. The clustering process is repeated by merging two clusters from the previous iteration with the shortest Euclidean distance to produce another cluster until the predefined number of clusters K is reached.

It is difficult to decide on selecting an optimal clustering algorithm to cluster a set of received recommendations based on a specific timeframe. However, k-means technique is selected because it is a very common used algorithm and well defined for euclidean distance which is the main function used to cluster recommendations. It satisfies the requirements for MANET environment in terms of the following features.

- *Scalability*: the algorithm is scalable to different numbers of clusters specified dynamically by the cluster manager when the evaluating node receives a list of recommendations. The algorithm shows good results in both cases of small number of recommendations and big number of recommendations in the later time of the network simulation or when most of nodes are active in providing recommendations.
- *Diversity*: the algorithm is capable to deal with different criterion and characteristics expressed in the different rules that combined together to cluster recommendations.
- *Runtime*: k-means is classified as Flat clustering algorithm which is usually more efficient run-time than the hierarchical clustering algorithm which may be slow because of making several decisions of merging or splitting clusters.
- *Complexity*: k-means usually characterised by low memory usage feature than other clustering algorithms such as hierarchal clustering algorithm. Complexities of calculations as well as memory requirements for the k-means are efficiently reduced by using the dynamic selection of the number of recommendations based on a period of time.

5.4 Dynamic Selection of Recommender Using Three Rules

In this proposed algorithm, nodes are clustered based on three values, namely, majority rule, personal experience rule, and service reputation rule.

These rules are combined and used to cluster recommendations from a list of recommenders in order to filter out dishonest recommendations.

5.4.1 Component of the Dynamic Selection of Recommender Using Three Rules Filtering Algorithm

The computation, recommendation, and cluster manager components work as outlined in section 5-3 of this chapter. Recommendation manger follows the same roles in algorithm 5-1 above. The following subsections will explain these values and give an overview of the clustering process and its algorithm.

A. Majority Rule

In the majority rule based technique, the trust and reputation schemes compute the majority opinion across all recommendations and classify those recommendations that deviate too much from the majority opinion as untrustworthy, and consequently exclude them from calculation.

B. Personal Experience Rule

The personal experience based technique aims to filter out any recommendation that is considered as incompatible with the opinion of the evaluating node. This filtering algorithm applies the deviation test to the receiving recommendations and excluding any that deviate too much from the opinion held by the evaluating nodes using a deviation threshold.

C. Service Reputation Rule

The service reputation based technique assumes that there is a consistency between the trustworthiness of a node as a service provider and a recommender. The evaluating node gives more weight to recommendations received from highly reputed nodes for service providing and treats them as trustworthy recommenders.

D. Cluster Procedure

The cluster procedure follows the same roles illustrated in the previous section. It consists of two levels of iterations. This first level iteration technique aims to merge trust value with the closest similarity. At the second level, the clustering process continues merging recommendations by calculating the average of the deviation value d_{ik}^{Avg} of the cluster's members. Then it merges any two clusters with the deviation average less than the deviation threshold D. The second level process aims to merge clusters with the closest deviation value compatible with the evaluating node i. The proposed cluster process works as shown in Algorithm 5-2 to filter out dishonest recommendations and send out trustworthy cluster to the evaluating node.

Algorithm 5-2: Cluster Manager Algorithm for the Dynamic Selection of Recommender Using Three Rules

1. ***For*** *each recommendation list* L ***Do***
2. ***For*** *each rating vector in the list* (α^r, β^r) ***Do***
3. ***Calculate*** *trust value for the recommender as* $T_{kj}^r = \frac{\alpha_{kj}^r}{\alpha_{kj}^r + \beta_{kj}^r}$
4. ***Calculate*** *deviation value as* $d_{ik} = |T_{ij}^d - T_{kj}^r|$
5. ***Weight*** T_{kj}^r *as* $TW_{kj}^r = T_{kj}^r * w_{kj}$ *based on* d_{ik} *value*
6. ***End*** *For*
7. ***Initialize*** *each vector as a unique cluster*
8. ***Repeat***
9. ***For*** *each vector* ***Do***
10. ***Merge*** *two clusters with the shortest Euclidean distance*
11. ***End*** *For*
12. ***Until*** *number of clusters =* K
13. ***For*** *each cluster* C_i *appeared in the previous iteration* ***Do***
14. ***Calculate*** *the average of the deviation value* d_{ik}^{Avg}
15. ***If*** $(d_{ik}^{Avg} \leq D)$ ***Then***
16. ***Merge*** C_i *and* C_{i+1}
17. ***End*** *If*
18. ***End*** *For*
19. ***Apply*** *the majority rule*
20. ***Select*** *trustworthy cluster with the highest* TW_{kj}^r
21. ***Return*** *trustworthy cluster* $C^{Trustworthy}$
22. ***End*** *For*

5.4.2 Experimental Setting

Experiment in this section is conducted to test the validity and the importance of the dynamic selection based on three rules filtering algorithm used to

mitigate the influence of dishonest recommendation. A wireless MANET environment in the present of false rating information which is propagated in the network using bad-mouthing and ballot-stuffing attacks is simulated. This experiment mainly aims to consider the contribution of the model in safely incorporate recommendation and enhance the dynamic selection of recommender in terms of the evaluation of trustworthiness of bad and good recommenders in the present of attacks. This experiment extends the simulation by adding the required components to NS2 simulator in order to filter out dishonest recommendation. This integrated simulator is used to test the ability of the algorithm to reach a reasonable level of trust among unacquainted network nodes. As in Table 4-1 in section 4.3, a network with 50 randomly placed nodes is simulated in an area of 700X1000m. Several nodes were randomly selected to provide false rating information in bad-mouthing and ballot-stuffing attacks. The maximum bad-mouthing and ballot-stuffing attack percentage used in the simulation scenario is 50% misbehaving nodes. We use the optimistic scheme in choosing the trust threshold value at 0.4 in which all nodes are initially expected to be trusted and normally behaving. Table 5-1 shows the parameters used in the network configuration for the experiment. Results in this experiment are based on multiple runs and we notice negligible variation.

Table 5-1 Network configuration

Parameter	**Value**	**Parameter**	**Value**
Nodes	50	**Transmitting capacity**	2 Kbps
Area	700 m X 1000 m	**Application**	CBR
Speed	20 m/s	**Packet size**	512 B
Radio Range	250 m	**Simulation time**	500 s
Movement	Random waypoint model	**Trust threshold**	0.4
Routing Protocol	DSR	**Publication timer**	30 s
MAC	802.11	**Fading timer μ**	10 s
Source-destination pairs	15	**Deviation threshold *D***	0.5

5.4.3 Experimental Results

As discussed earlier, there are several types of attacks which distort recommendations exchanged by nodes of trust models in the network. This work considers the proposed model under bad-mouthing, ballot-stuffing attacks, and collusion attack. These attacks are appropriate to test the performance of the model to show its ability to mitigate the influence of dishonest recommendations. The model investigates the average of the trust level held by other nodes in the network of a good node (node 10 in this case) and a bad node (node 1 in this case). The simulation is conducted several times with the filtering algorithm enabled and disabled against bad-mouthing and ballot-stuffing attacker nodes that range from 0% (no attacker nodes) to 50% (half of the nodes are attackers). The comparison of the calculated trust value with and without the filtering algorithm in the presence of varied attack percentages is considered against the expected trust value. The expected trust value is calculated based on conducting simulations under normal behaviour of the nodes in the network (the simulations' ground truth). The results collected from the conducted simulation are plotted in Figures 5-3 and 5-4.

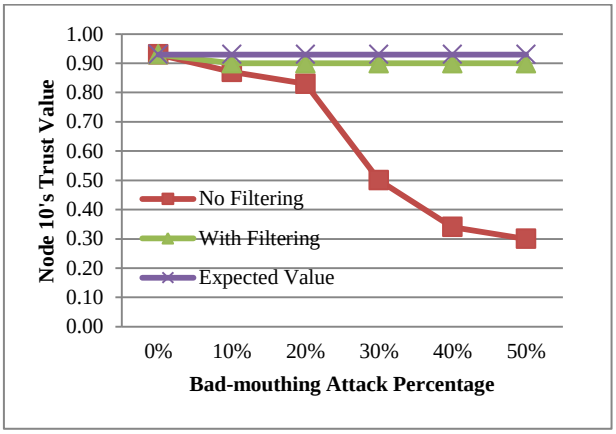


Figure 5-3 Good-node: 10's trust value in the presence of a bad-mouthing attack

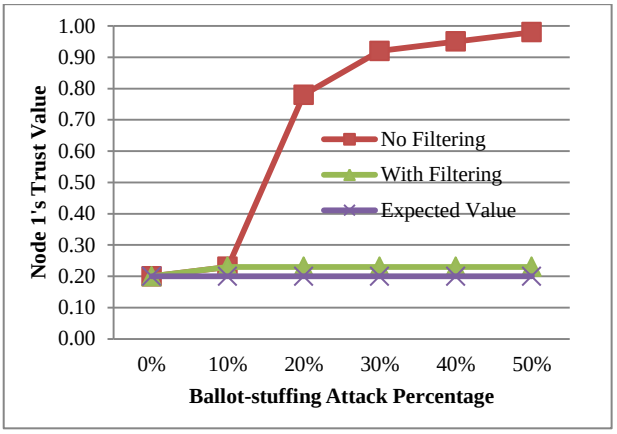


Figure 5-4 Bad-node: 1's trust value in the presence of ballot-stuffing attack

The x-axis in figure 5-3 represents the percentage of bad-mouthing attacker nodes, and this ranges from 0% to 50% attacker nodes. The y-axis shows the average of the trust value of a good node (node 10) by other nodes which have interacted with it. From this figure, it can be seen that the increased percentage of attackers distorts the value of the trust value of node 10 held by other nodes in the network when there is no filtering algorithm incorporated. By increasing the number of dishonest recommenders, more untrustworthy ratings are propagated in the recommendations provided by neighbour nodes. Meanwhile, the proposed filtering algorithm is able to keep the trust value close to the expected level even if half of the nodes in the network are regarded as bad-mouthing attackers.

The effects of the ballot-stuffing attack are shown in Figure 5-7. The x-axis represents the percentage of nodes act as ballot-stuffing attackers, which also varies between 0 and 50%. The y-axis shows the value of trust calculated for a bad node (node 1) when the dishonest recommenders are absent, which represents the expected value of the system; when the filtering algorithm is working; and when the filtering algorithm is not working. From the figure, it is observed that attacker nodes propagate more dishonest information in their recommendations in order to mislead nodes in the

network in their assessment of node 1. Consequently, this can mislead the decision made by other nodes to trust it to more than 90% when the attackers increase to 50%, instead of deciding not to trust this bad node. At the same time, the proposed model, which is equipped with a filtering algorithm that aims to filter out dishonest recommendations, may be more capable of mitigating the influence of dishonest recommenders.

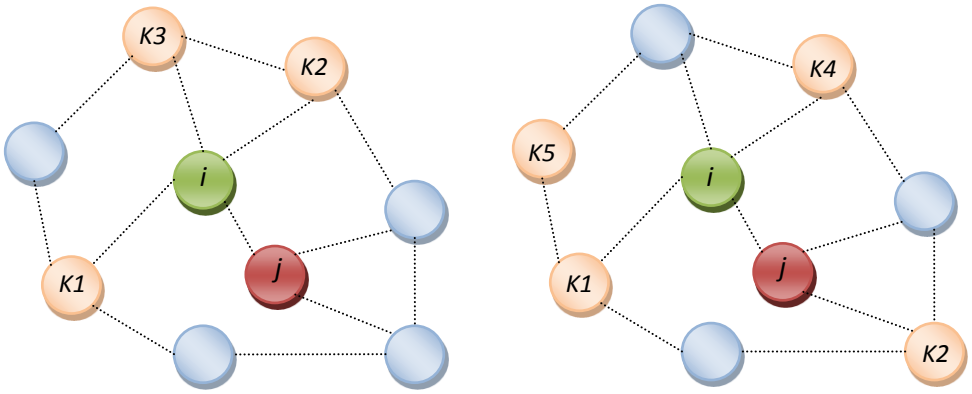
5.5 The Effective Defence Scheme

In previous subsections, a filtering algorithm to filter out recommendation is proposed based on the combination of the majority opinion, personal experience, and quality of service approaches. The algorithm enhances the selection procedure of the recommending nodes and keeps the evaluation near to ground truth value. However, this algorithm needs to be reconsidering based on the MANETs characteristics like level of experience, scarcity of knowledge, data sparsity, and how close the recommender to the evaluating node. The algorithm can give good results when the percentage of attacks is 50% or less, while the algorithm is not able to correctly filter untrustworthy recommendations when the attacks increase more than 50%. From this point there was a need to build a capable defence scheme to overcome these limitations. Therefore, this section proposes a robust and effective defence scheme to filter out attacks discussed in section 5.2 of this chapter to select the recommending node based on three factors: number of interactions with the evaluated node, unity of view with the evaluating, and closeness to the evaluating node.

5.5.1 Components of the Defence Scheme

The proposed defence scheme takes into consideration the dynamic characteristics of MANETs that change over time. The honesty of recommending nodes is evaluated over a period of time to mitigate the

influence of bad behaviour of the same node over time. Figure 5-5 shows the dynamic topology of MANETs. Consider that, a node i wants to evaluate another node j by requesting recommendations from its neighbours. The evaluating node i receives a list of recommending nodes referred as $\{k_1, k_2, k_3, \dots, k_N\}$. At time t_c (refer Figure 5-5(a)), the location and number of recommending nodes differ from the recommending nodes at time t_{c+1} as shown in Figure 5-5(b).



(a) Recommending nodes at time t_c

(b) Recommending nodes at time t_{c+1}

Figure 5-5 Recommendation by time

With the increase of mobile nodes and resources in MANETs, the difference in rating scale between different nodes becomes an issue which has led to a data sparsity problem. Data sparsity in a recommendation-based trust model occurs in a situation of lacking or insufficient interaction experience in the early time of establishing the network, or when most of the nodes are inactive in recommendation. It is considered as one of the main challenges for the high quality of recommendation in trust research field for MANETs. Several solutions have been proposed to overcome the problem of data sparsity in MANETs. This can be categorised as: a) methods that utilise similarity metrics to enhance the selection of recommendations from similar neighbours [72 , 132], b) methods that implement aggregation techniques to

integrate the ratings given by all the neighbours [132], and c) methods using data imputation to improve the selection of missing or insufficient ratings of neighbours [133]. To overcome this problem, the proposed scheme uses a clustering technique similar to [77] to impute ratings and reduce the sparsity. Besides, it can improve the consistency of received recommendations of the filtering algorithm. For example, recommendations from a misbehaving node can have a range of multiple different ratings for the evaluated node. These ratings may be inconsistent in which they can differ from each other in a short period of time, a malicious act of the misbehaving node to confuse the trust model.

In this subsection, an analysis of the functionalities of the defence scheme that includes three components: computation, recommendation and cluster manager is illustrated which work as outlined in previous sections. It explains the three factors used in the algorithm and gives an overview of the clustering process and its algorithm.

A) Confidence Value V_{ij}^{conf}

The notion of confidence was introduced in [134] where confidence value and trust value are combined together to derive a single trustworthiness value of a node. Following that, trust models in [16 , 75 , 135] have also considered the confidence value as a desired parameter to achieve a single trust value to represent the trustworthiness of nodes. Confidence value can be used to solve the problem of short-term and long-term observations. That is, nodes may have the same level of trust with different number of observations. For example, the trust value of a node at the initial time with $\alpha = \beta = 1$ is 0.5, and after a sequence of positive and negative interactions in which $\alpha = \beta = 50$, the node has the same trust value of 0.5 about the evaluated node (see Table 5-2 for more information). Confidence value starts from 0 in case of no

observations between nodes and increases gradually with the number of recorded observations. Relying only on the trust value can raise the problem of short-term and long-term observations. Nodes in the network can have nearly the same level of trust though they may have different levels of observations. Consequently, this can lead to wrong estimation in judging the ability of nodes to be honest recommending node.

The proposed filtering algorithm clusters recommending nodes based on the level of confidence for two reasons. Firstly, the nodes with higher confidence value (those having sufficient interactions with evaluated node) are desirable because the higher number of interactions will offer rich information that would help in choosing better recommending nodes. Secondly, the recommending nodes with very high trust value in the early rounds in the network (when there are no enough interactions) are more likely to be attackers. Consequently, it may lead to exclusion of dishonest nodes from the recommendations list in early stages. The confidence value is computed as the variance of the beta distribution with some modifications as in [16] and [75]. Nodes use the confidence value to make a correct decision about the trustworthiness of recommending nodes taking into account the number of observations accumulated by each node. Suppose that i is an evaluating node that received recommendations from a recommending node k about the trustworthiness of an evaluated node j , V_{ij}^{conf} value refers to the confidence of node i in the experience of the recommending node k with evaluated node j at time t and is calculated as in Eq. (5-1).

$$V_{ij}^{conf} = 1 - \sqrt{12}\sigma_{kj}$$

$$V_{ij}^{conf} = 1 - \sqrt{\frac{12\ \alpha_{kj}\beta_{kj}}{\left(\alpha_{kj} + \beta_{kj}\right)^2\left(\alpha_{kj} + \beta_{kj} + 1\right)}} \qquad (5\text{-}1)$$

where σ_{kj} is the beta distribution variance between k and j, α_{kj} and β_{kj} is the accumulated positive and negative interactions between k and j. $1 - \sqrt{12}$ is the normalisation constant to ensure that the value of confidence belongs to the interval between [0, 1], for more details, the reader is referred to [136].

Using this formula the value of confidence falls between the interval of [0, 1], where 0 means that no previous interactions are recorded between the recommending and evaluated node while 1 means complete confidence in trustworthiness of the evaluated node. The rational of using and computing the confidence value is shown in Figure 5-6. We compare the confidence value computed using the proposed method with that in [116] (we call it TMUC for short), which computes the confidence value using only the standard deviation. The proposed computation method of confidence value can effectively reflect the knowledge held by nodes based on the number of interactions better than the calculation in TMUC. For example, when $\alpha = \beta = 1$ which means there is no previous interaction between two nodes, the proposed method of computing confidence value is 0 while in TMUC, it is nearly 0.91 which is a high value close to 1. Starting with high confidence value in case of no interactions can confuse the trust mechanism and prevent it from making good judgment about behaviour of the evaluated node. Table 5-2 shows the values of positive and negative interactions and the confidence value for each level of interaction for both the proposed model and the work in TMUC. Figure 5-6 explains the relationship between interactions and the level of confidence when the trust levels are the same.

Table 5-2 Levels of confidence for the proposed model and TMUC model with the same trust levels

α	β	(successful interaction)	(failed interaction)	Trust value	Confidence value (proposed model)	Confidence value (TMUC model)
1	1	0	0	0.5	0	0.916666667
5	2	4	1	0.714285714	0.446716665	0.974489796
10	4	9	3	0.714285714	0.595938982	0.986394558
15	6	14	5	0.714285714	0.666357595	0.990723562
20	8	19	7	0.714285714	0.709401356	0.992962702
25	10	24	9	0.714285714	0.739179735	0.994331066
30	12	29	11	0.714285714	0.761351694	0.995253916
35	14	34	13	0.714285714	0.778686666	0.995918367
40	16	39	15	0.714285714	0.792721071	0.996419620
45	18	44	17	0.714285714	0.804384801	0.996811224
50	20	49	19	0.714285714	0.814277976	0.997125611

From Figure 5-6, it can be seen that the proposed method of computing confidence offers a better range for the confidence value as compared to that by TMUC. This variation reflects better accumulated interactions when the trust values (refer Table 5-2) are same. When there are no interactions, confidence value from the proposed model is 0 and it progresses with the increasing number of interactions. Whereas with TMUC, the confidence value is already at 0.91 in case of no interactions and thus is nearly at saturation level when number of interactions more than 19.

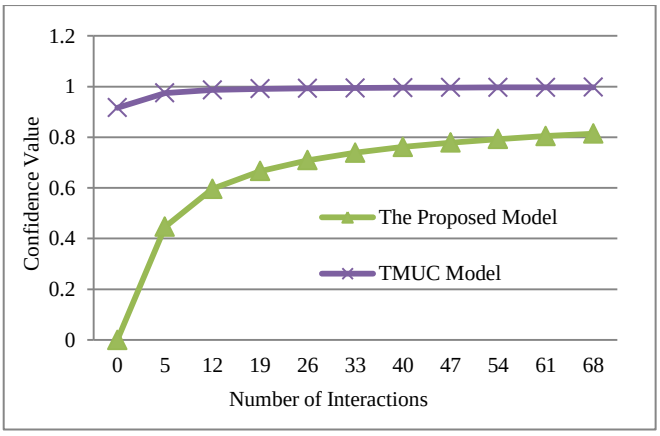


Figure 5-6 Relationships between Interactions and Confidence for the proposed model and TMUC model

B) Deviation Value V_{ij}^{dev}

Deviation value represents to what extent the received recommendation is compatible with the personal experience of evaluating node. This value has been used by the means of the deviation test in [18] to ensure the unity of view with the receiving node. Each node compares received recommendation with its own firsthand information and accepts only those not deviating too much from self-observations. In the proposed model the deviation value is used as an additional parameter in the clustering algorithm to filter out any recommendations deviating beyond a predefined deviation threshold. A problem that could arise here is when the evaluating node lacks historical information for interactions with the evaluated node, thus not providing a base value for comparison. In order to overcome this problem, the proposed method compares the confidence level of the evaluating node with that of the recommending node. The confidence value is calculated using Eq. (5-1). The deviation test is only applied if both nodes have similar level of confidence. Assume that there are three nodes (i, j and k), and node i attempts to calculate the trust value of its neighbour node j using recommendation provided by node k. In this scenario, node i first compares its confidence level which denoted as $Conf\_Level$ with the recommending node as in Eq. (5-2). If the confidence difference is less than a threshold value denoted as $Conf\_Threshold$, then node i calculates the deviation value as a difference between the receiving recommendation and direct observations of the evaluated node as held by the evaluating node as in Eq. (5-3). The resulting value is compared to a predefined deviation threshold d^{dev} and we exclude any recommendations that differ widely from the evaluating node's own information.

$$Conf\_Level = \left|CV_{ij} - CV_{kj}\right| \leq Conf\_Threshold \quad (5\text{-}2)$$

where CV_{ij} is the confidence value of i about j, and CV_{kj} is the confidence value of k about j. If the Eq. (5-2) is successful, deviation value V_{ij}^{dev} is calculated as follows:

$$V_{ij}^{dev} = \left|T_{ij}^{d} - T_{kj}^{r}\right| \leq d^{dev} \quad (5\text{-}3)$$

where T_{ij}^{d} is the direct trust value of i about j, and T_{kj}^{r} is the received trust value of k about j.

C) Closeness Centrality Value V_{ij}^{close}

Trust is a social concept and it is thus possible to apply the perceptions of social life in trust computation and recommendation propagation. An interesting direction of trust research in MANETs is to utilise social relationships in evaluating trust among nodes in a group setting by employing the concept of social structures [7]. The proposed model uses the concept of closeness centrality between the evaluating nodes and the recommending node from the social trust. Closeness centrality [137] measures the distance between the evaluated node and the recommending node in terms of physical distance, number of hops, or delays. In the proposed model closeness centrality is a measure of the distance between the evaluating node and the recommending node. The use of the closeness centrality enhances the filtering algorithm as close nodes are likely to possess same nature and counter nearly same environmental and operational conditions over a period of time in the network. Furthermore, close friends may have more interactions in the time of friendship. Consequently, trust values for the close neighbours converge to nearly same level. This may help in recognising the untrustworthy recommending node whose recommendation

is much different from the close recommending nodes. Closeness value V_{ij}^{close} refers to the degree of node i's closeness to a recommending node k at time t and is calculated by Eq. (5-4).

$$V_{ij}^{close} = \sqrt{(x_i^{loc} - x_k^{loc})^2 + (y_i^{loc} - y_k^{loc})^2} \leq d^{dis} \quad (5\text{-}4)$$

where (x_i^{loc}, y_i^{loc}), (x_k^{loc}, y_k^{loc}) are the positions of node i and node k at time t and d^{dis} is a predefined distance threshold between node i and node k which should be less than the transmission range.

D) Cluster Procedure

The cluster manager in the proposed model receives a list of recommendations from the recommendation manager and processes it using a clustering technique same as outlined in section 5.3. The clustering algorithm is run by the evaluating node on all the recommendations in the list $L = \{k_1, k_2, k_3, \dots, k_n\}$. A vector of three values $(V_{ij}^{conf}, V_{ij}^{dev}, V_{ij}^{close})$ is provided by a recommending node for the clustering operation. The clustering algorithm divides the vectors from the recommending nodes into a predefined number of clusters denoted as K. Initially each vector is considered as a cluster, and then two clusters with the shortest Euclidean distance are merged together to produce a new cluster. The clustering process is repeated by merging two clusters from the previous iteration until the predefined number of clusters K is reached. The first step of the clustering process aims to merge vectors with the closest similarity. In the second step, it selects the trustworthy clusters if all the recommending nodes in a specified cluster satisfy the following rules:

$$C^{Trustworthy} = \begin{cases} R_{ij}^{Trustwothy} \; if \; (V_{ij}^{conf} \geq d_{min}^{conf}) \; and \; (V_{ij}^{conf} \leq d_{max}^{conf}) \\ \qquad\qquad if \;\; (V_{ij}^{dev} \leq d^{dev}) \; and \; (V_{ij}^{close} \leq d^{dis}) \\ R_{ij}^{Untrustworthy} \qquad\qquad other \; wise \end{cases}$$

where $R_{ij}^{Trustwothy}$ is the trustworthy recommendation, $R_{ij}^{Untrustworthy}$ is the untrustworthy recommendation, d_{min}^{conf} is the minmum confidence threshold, d_{max}^{conf} is the maximum confidence threshold.

The next step is to apply majority rule to select the cluster with largest number of members. In the final step, trustworthy clusters are returned to the recommendation manager and to the evaluating node to update its indirect trust of the evaluated node. The proposed cluster process in the defence scheme works as shown in Algorithm 5-3.

Algorithm 5-3: Cluster Manager Algorithm for the Defence Scheme

1. ***For*** each recommendation list L ***Do***
2. ***For*** each rating vector in the list (α^r, β^r) ***Do***
3. ***Calculate*** confidence value V_{ij}^{conf} as in Equ. 7
4. ***Calculate*** deviation value V_{ij}^{dev} as in Equ. 8, 9
5. ***Calculate*** closeness value V_{ij}^{close} as in Equ. 10
6. ***Construct*** data vector as $(V_{ij}^{conf}, V_{ij}^{dev}, V_{ij}^{close})$
7. ***End*** For
8. ***Initialize*** each vector as a unique cluster
9. ***Repeat***
10. ***For*** each vector ***Do***
11. ***Merge*** two clusters with the shortest Euclidean distance
12. ***End*** For
13. ***Until*** number of clusters = K
14. ***For*** each cluster that appeared in the previous iteration ***Do***
15. ***If*** $(V_{ij}^{conf} \geq d_{min}^{conf})$ and $(V_{ij}^{conf} \leq d_{max}^{conf})$ ***Then***
16. ***If*** $(V_{ij}^{dev} \leq d^{dev})$ and $(V_{ij}^{close} \leq d^{dis})$ ***Then***
17. ***Select*** trustworthy cluster
18. ***End*** If
19. ***End*** If
20. ***End*** For
21. ***For*** each chosen trustworthy cluster ***Do***
22. ***Apply*** the majority rule
23. ***Return*** trustworthy cluster $C^{Trustworthy}$
24. ***End*** For
25. ***End*** For

5.5.2 Experimental Setting

The validity of the proposed defence scheme to mitigate the influence of dishonest recommendation is tested using an extensive experiment. A wireless MANET environment in the present of false rating information which is propagated in the network using bad-mouthing and ballot-stuffing attacks besides to the collusion attack is simulated. Further, a comparative study with the maturity model [76] proposed in the literature is conducted. As in subsection 5.4.2, the proposed trust model components are added to the simulator to conduct the experiment. A network with 50 mobile nodes is simulated and up to 80% misbehaving nodes are used to test the attacks. Table 5-3 shows the parameters used in configuring the network for the experiment. Bad-mouthing and ballot-stuffing attacks with additional permission to collude in both attacks are used in order to evaluate the defence scheme against dishonest recommendation. Number of dishonest nodes range from 0% to 80% and the dishonest recommendations provided deviate 50% from the honest recommendations. Badly behaving nodes (selfish nodes) counting to 20% always existed in the network and were responsible for collusion and jamming. Results from the experiment are based on multiple runs and a negligible variation is noticed.

Table 5-3 Network configuration

Parameter	**Value**	**Parameter**	**Value**
Nodes	50	**Packet size**	512 B
Area	700 m X 700 m	**Simulation time**	500 s
Speed	10 m/s	**Trust threshold**	0.4
Radio Range	250 m	**Publication timer**	30 s
Movement	Random waypoint model	**Fading timer μ**	10 s

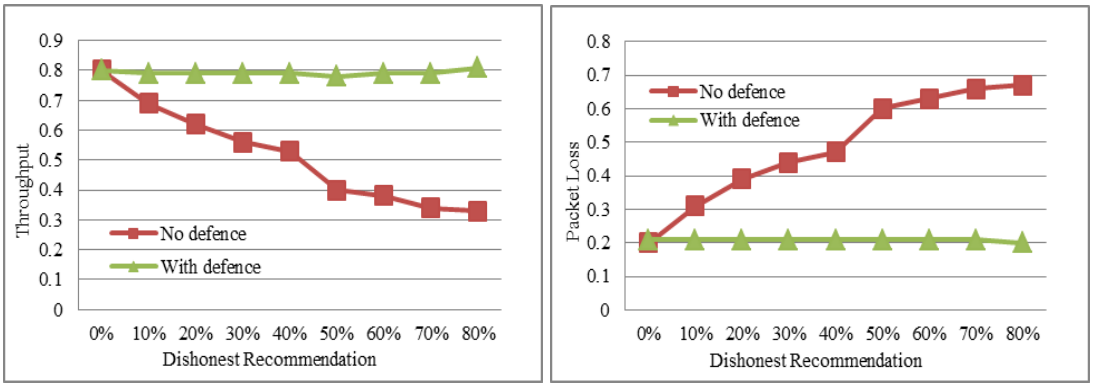
Parameter	Value	Parameter	Value
Routing Protocol	DSR	**Deviation threshold**	0.5
MAC	802.11	**Conf_Threshold**	0.4
Source-destination pairs	15	d_{min}^{conf}	0.5
Transmitting capacity	2 Kbps	d_{max}^{conf}	0.9
Application	CBR	d^{dis}	200 m

5.5.3 Performance Evaluation

The flow of the simulation is as follows. The performance of the entire network is represented by two parameters: Network throughput and packet loss in the presence of bad-mouthing, ballot-stuffing and selfish nodes. The trust value of a good node (not misbehaving) is evaluated against bad-mouthing attack to see the influence of such attack with and without incorporating the proposed defence scheme. The trust value of a bad node (misbehaving) is also evaluated against ballot-stuffing attack to see how such attackers can distort the trust value of this node. The performance of the proposed model in terms of recognised dishonest recommendations, false negative and false positive in the presence of bad-mouthing attacks with and without the defence scheme is examined. Similar experiment is conducted for ballot-stuffing attack. Finally, a comparative study is conducted with the maturity model [76] proposed in the literature.

Figure 5-7 demonstrates the effect of the dishonest recommendations on two performance metrics; throughput and packet loss for the whole network. The y-axis in Figure 5-7(a) shows the percentage of throughput, both with and without the defence scheme, in the presence of dishonest recommending nodes varying from 0% to 80% of the total population of nodes. It is observed that the network throughput without a defence falls from nearly 80% when the dishonest recommending nodes are not present to nearly 30% when population of the dishonest ones increases to 80%. Slight decrease and then

increase is noticed in the throughput (Figure 5-7(a)) for the network with defence when the percentage of dishonest recommendation nodes increases from 40% to 80%. This may be due to the fact that the throughput not only depends on the number of misbehaving nodes but also affected with the degree of connectivity (number of neighbours) and the ability of nodes to classify their neighbours as well as time required to achieve the classification which are different in each simulation due to network topology and mobility. However, the proposed defence mechanism was able to keep the value of throughput at nearly 80% even in case of higher population of the dishonest nodes. This is translated into that the defence scheme is able to mitigate the negative effect of dishonest recommendation on the throughput performance. The impact of dishonest nodes on packet loss is shown in the Figure 5-7(b). The percentage of packet loss rises with increasing the percentage of dishonest nodes from 20% to over 60% when no defence incorporated in the network. While only 20% packet loss can be maintained using the proposed defence scheme in the presence of dishonest recommending node that vary from 0% to 80% of the nodes in the network. Similarly, the percentage of packet loss decreases slightly when the percentage of dishonest recommendation nodes increases from 70% to 80% for the same reasons as discussed in the analysis of Figure 5-7(a). It can be seen from the above analysis that dishonest recommendations can significantly impact on the throughput and packet loss metrics by confusing the trust model. The proposed technique can keep those metrics at an acceptable level even when the population of dishonest nodes is high.



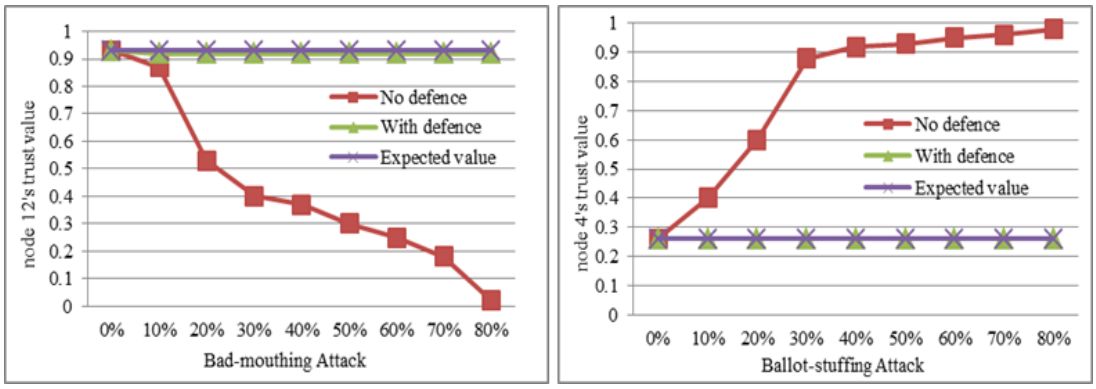
(a) Network throughput (b) Network Packet Loss

Figure 5-7 Network performance in the Presence of Dishonest Recommending nodes for a) Network Throughput; b) Network Packet Loss

Figure 5-8 demonstrates the average of the indirect trust held by other nodes in the network for a good node (node 12 in this case) and a bad node (node 4 in this case). The x-axis in Figure 5-8(a) displays the range for the population of bad-mouthing nodes from 0% to 80%.The y-axis shows the average of the indirect trust value for a good node (node 12 in this case) as held by all the nodes that have interacted with it in the past. A comparison has been made between three different parameters as follows. First, the indirect trust value when there are no dishonest nodes, called expected value. Second, the indirect trust value when dishonest nodes are present and the defence scheme is working, with defence. Third, the indirect trust value when the dishonest nodes are present and the defence technique is not working, no defence. It can be seen that with increasing population of badmouthing attackers, the average trust value of node 12 declines in case of no defence, whereas, the trust value remains the same as the expected value in case of with defence.

The effects of ballot-stuffing attack are shown in Figure 5-8(b). In the x-axis is the percentage of ballot-stuffing attack that varies between 0% to 80% and y-axis shows the values for the indirect trust compared against the same three

parameter i.e. expected value, with defence and no defence cases. From the figure, it can be seen that the attacking nodes have propagated unfairly positive rating for the dishonest node (node 4) thereby raising its trust value to above 0.9 while the attacker population was 80%. The results here show that the defence algorithm is capable of mitigating the influence of dishonest nodes by filtering out unfair ratings.

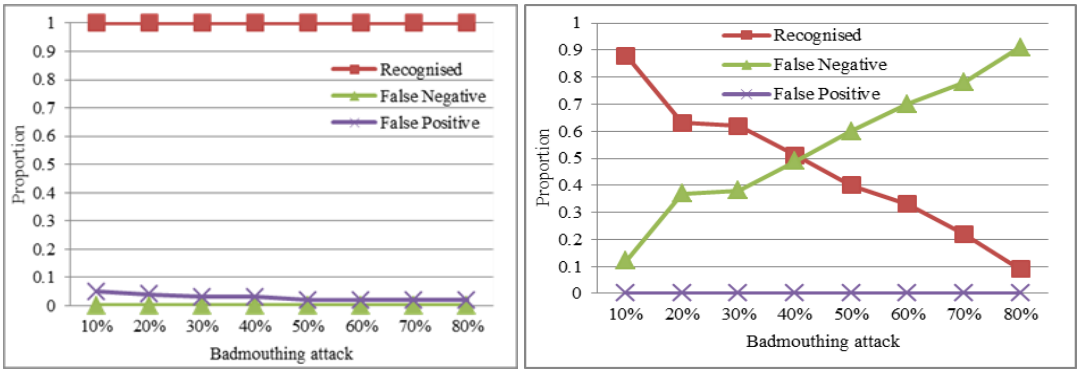


(a) Good-Node 12's Trust Value (b) Bad-Node 4's Trust Value

Figure 5-8 Trust evaluation for a) Good-node 12's trust value in the presence of bad-mouthing attack; b) Bad-node 4's trust value in the presence of ballot-stuffing attack

To test the proposed defence scheme further, we define three additional metrics: (a) recognised proportion, representing the number of dishonest recommendations identified by node i, (b) false negative proportion, indicating the number of dishonest recommendations identified as honest by node i, (c) false positive proportion, indicating the number of honest recommendations identified as dishonest by node i. Figure 5-9 and 6-6 show the results for these three metrics in the presence of bad-mouthing and ballot-stuffing attack. The x-axis in Figure 5-9(a) shows the percentage of bad-mouthing attack while y-axis shows the proportion of the recognised dishonest recommendation, false negative and false positive with the defence scheme in action. It can be observed that the defence algorithm can effectively mitigate the dishonest recommendation propagated by the bad-mouthing attackers regarding the recognition and false negative metrics.

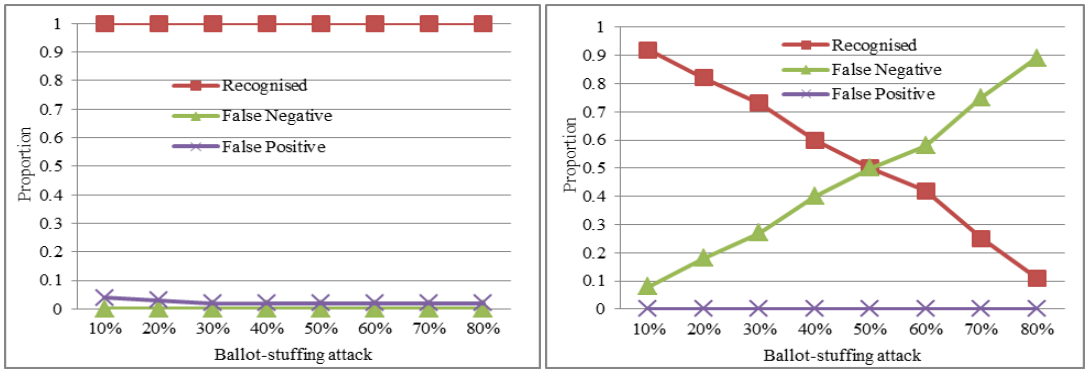
While it keeps the false positive proportion at a very low level (about 2%) when the attack percentage is more than 50%. Figure 5-9 (b) shows the case when the defence scheme is not in action. It can be seen that the proportion of recognised dishonest recommendation drops to less than 10% when the percentage of dishonest nodes increase to 80% and consequently the proportion of false negative increases with the increase in dishonest recommending nodes. As the defence scheme is not in action here, it accepts all the recommendations propagated in the network and updates the indirect trust value based on these recommendations. Therefore, the proportion of false positive remains at zero (Figure 5-9(b)).



(a) With Defence (b) Without Defence

Figure 5-9 Recognised, false Negative and false positive proportion in the presence of bad-mouthing attack for a) With defence; b) Without defence

Figure 5-10(a) shows results for ballot-stuffing attack. The proposed defence scheme is seen to be identifying dishonest recommendations and eliminating false negative effectively. The proportion of false positive is maintained at a reasonable level. The effect of dishonest recommendation in Figure 5-10(b) is obvious. When there is no defence incorporated the proportion of recognition drops from about 0.9 to nearly 0.1 with variation of the ballot-stuffing attackers from 0.1 to 0.8. The false negative proportion also increases to nearly 0.9 with the increasing percentage of the dishonest recommending nodes.



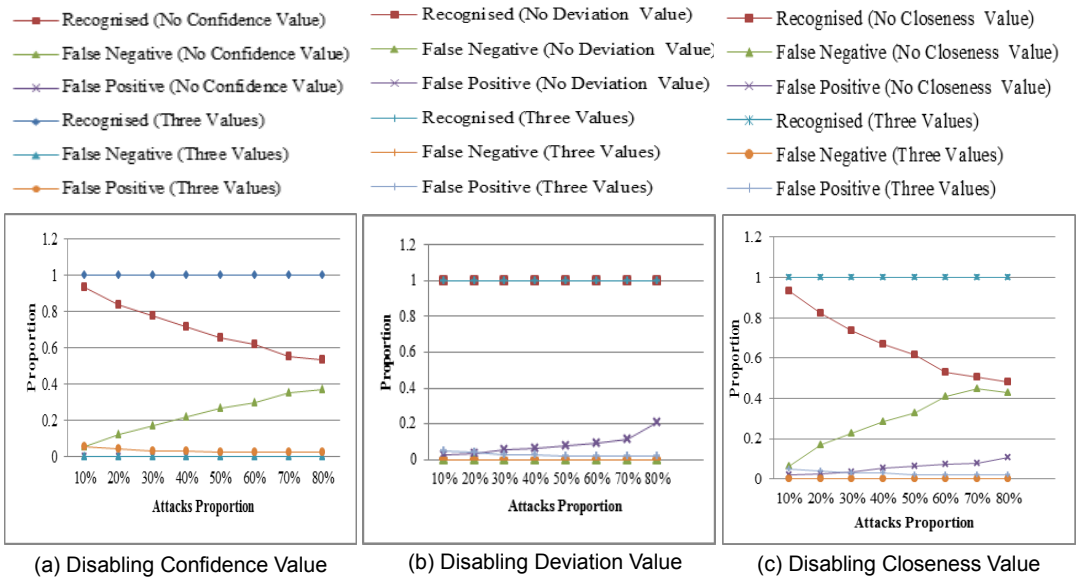
(a) With Defence (b) Without Defence

Figure 5-10 Recognised, false negative, and false positive proportion in the presence of ballot-stuffing attack for a) With defence; b) Without defence

Furthermore, the proposed defence scheme is examined to observe the effect of each criterion (recognised proportion, false negative proportion, and false positive proportion) in clustering recommendations. The experiments are conducted over a range of various attack percentage. The different attacks considered are bad-mouthing, ballot-stuffing, and collusion. The results are shown in Figure 5-11. First, the effect of the confidence value is tested by disabling it in the defence scheme and allowing the deviation and closeness value to work. It is obvious from Figure 5-11(a), that the defense scheme's performance is decreased in terms of recognised and false negative proportion of dishonest recommendation. The defense scheme is seen to be ineffective in recognising almost none of the dishonest recommendations propagated in the network by bad-mouthing, ballot-stuffing, and colluding attackers. On top, a number of false negative recommendations showed capable in penetrating the defense algorithm. The number of recognised proportion dropped with increase in the proportion of attack; from nearly 90% when just 10% of recommenders provide dishonest recommendations to nearly 50% when the dishonest recommenders reached 80%. On the other hand, false negative proportion increases with rise in the

number of dishonest recommenders from very small proportion nearly 5% to nearly 40% at 80% of attack percentage. Interestingly, the number of false positive proportion is stable at 0% which means no honest recommenders were treated as dishonest. The reason being that the confidence value doesn't allow nodes without enough experiences to provide recommendation and this can result in treating some honest recommenders as dishonest. It can thus be concluded that the confidence value factor enhances the performance of the defense scheme by eliminating dishonest recommendations (even though it could result in a small proportion of false positive). In second experiment, the deviation value is disabled in the clustering algorithm to understand its importance in the defense scheme. Figure 5-11(b) shows that the performance of the defense scheme is reduced due to introduction of some false positive proportion in the case of disabling the deviation value. The proportion of false positive, which treats good nodes as dishonest increased with rise in the number of dishonest recommendations propagated by attackers from nearly 2% at just 10% of attackers to more than 20% when almost the majority of propagated recommendations are dishonest. While disabling the deviation value has no effect on the performance of the recognised proportion of dishonest recommendations, as well as, the false negative proportion. It can be found that despite the small effect of the deviation value on the whole performance of the defense scheme, it is proposed to work with strong relation with the confidence value which is used to correct its values in the case of cold-start when insufficient experience exists to perform the deviation value. The third step in this experiment is to test the effect of the closeness value which is shown in Figure 5-11(c). It is obvious that disabling the closeness value has a strong impact on the three performance metrics of recognised, false

negative and false positive proportions. A great negative effect is on the proportion of recognised dishonest recommendations which fall to nearly more than 40% when most nodes provide dishonest recommendations. Similarly, the ability of the defense scheme in preventing the false negative decreases in which the number of false negative increases to more than 40% when 80% of attackers are existed. Besides, absence of the closeness value can introduce a number of false positive which increases to nearly 10% when dishonest recommendation providers are nearly 80%.

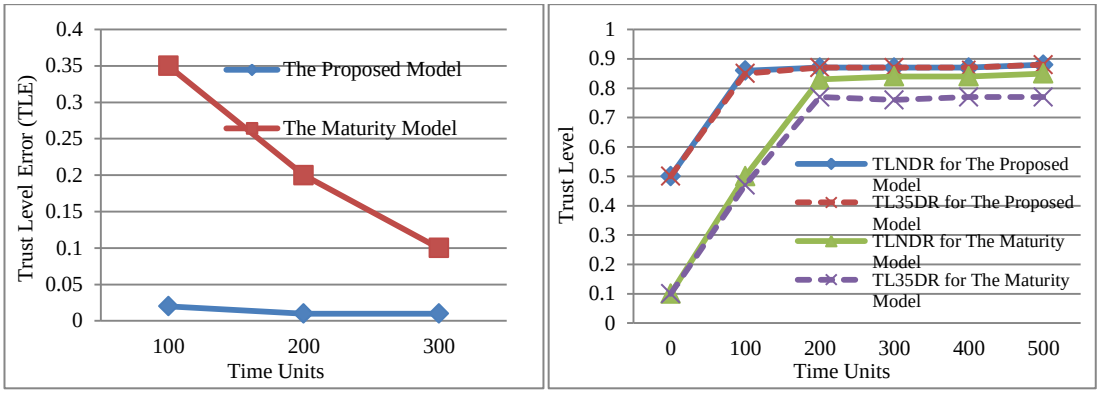


(a) Disabling Confidence Value (b) Disabling Deviation Value (c) Disabling Closeness Value

Figure 5-11 The effect of the three values in the clustering algorithm on the performance of defense scheme regarding recognised, false negative, and false positive proportion in the presence of bad-mouthing, ballot-stuffing, and collusion attacks for a) Disabling confidence value; b) Disabling deviation value; Disabling closeness value

A conclusion can be drawn is that the three proposed values have a great positive impact on the performance of the defence scheme despite the fact that one has more effect than another. Besides, the proposed values of the defense scheme are strongly correlated to work together in order to effectively prevent the influence of dishonest recommendations in the proposed trust models.

Finally, the performance of the proposed model is compared with the maturity model proposed in [76] in terms of two metrics: trust level error (TLE) which represents the proportion of error in evaluating the trust level of a node i (node 8 in this case); and trust level evaluation of a good node (node 1 in this case) by another node j in the network. We follow the same network configuration and node selection which is provided in the maturity model (see [76] for details) to conduct this experiment. In this configuration, a high speed network is presented with high node mobility, which is different from our first configuration. This configuration of the test network allows us to show the effectiveness of the proposed scheme. Figure 5-12 shows the results of this experiment. Figure 5-12(a) displays the trust level error over the simulation time. It can be seen that the proposed model can keep the TLE smaller than the error reported by the maturity model. The TLE in case of the proposed model is stable for the entire time of evaluation and converges to very small value nearly 0.01 towards the later phase. While for the maturity model, the TLE value is high initially (0.35) as compared to that of the proposed model and this only converged to 0.1 towards the end (time unit 3000). Figure 5-12(b) shows the effectiveness of the proposed defence scheme in evaluating the trust value of a good node (node 1) from the network. It considers the following scenarios: the expected trust value when there is no dishonest recommendation (TLNDR), and the same when there is 35% dishonest recommendation (TL35DR) both for the proposed model and the maturity model. The results show that the proposed model with the defence scheme can manage to avoid the dishonest recommendation and keep the trust value of node 1 near to the expected value and slightly higher than the results of the maturity model.



a) Trust Level Error with Time Units by other nodes to evaluate node 8' trust level

b) Good-Node 1' Trust Level with Time Units

Figure 5-12 Comparative study with maturity model for a) Trust level error; and b) Good-node 1' trust level

5.5.4 Cost of the Defence Scheme

Mobile ad-hoc networks are characterised by constrained resources in terms of communication, memory usage and computational complexity requirements. Any proposed model or defence scheme must reflect the trade-offs between accuracy of trustworthiness and network performance. As gathering and propagating trust information among distributed node can consume more resources of energy and time, it can enhance the decision making. Dynamic and highly mobile networks which suffer from several points of failure require techniques to enhance the decision making on nodes trustworthiness. However, the proposed defence scheme is lightweight in several aspects. In terms of communication, the proposed model is suitable for MANETs because only recommendation request and reply packets are used to send and receive a list of recommendations. The packets of recommendations are exchanged between a single source of information which is represented in the recommendation manager to and from the evaluating node and the recommending nodes. The data size and length is very small as every recommending node provides just three parameters of

accumulated positive and negative observations and its current position. The communication is also enhanced by an on-demand scheme in which a recommendation is requested whenever needed. Therefore, the defence scheme is conducted without network flooding and acquisition delay. The defence scheme is characterised with the advantage of a role-based management scheme for filtering dishonest recommendations in which three different components are interoperated to accomplish the task. The use of clustering in distributed networks can facilitate the data aggregation and reduce the computational power by each node to evaluate the trustworthiness of other nodes. One of the costs put on the proposed defence is the complexity that can be countered in maintaining the cluster and selecting the most trustworthy cluster. Another cost is the memory consumption in which the defence scheme consumes more memory to store recommendation for a period of time for conducting the filtering algorithm by the recommendation and clustering managers which is run by the evaluating node but no memory consumption on the side of the evaluated node. An additional cost is the time consumption which is more than the traditional defence which uses single recommender information to update the trustworthiness of the evaluated node. These costs can be reduced in the proposed defence scheme by using only the very last recommendations to be including in the clustering filtering computation. Dynamic selection of the number of recommendations based on a period of time can have many advantages, (1) reduce complexity and memory usage, (2) exclude any old recommendation from the calculation, (3) reduce the time that is used to select the trustworthy cluster.

5.6 Summary

A recommendation based trust model for MANETs is built to investigate the influence of attacks related to recommendations using two filtering algorithms. The use of recommendation can efficiently allow nodes to acquaint with each other without previous interactions but it exposes nodes to dishonest and unfair recommendation. Therefore, a dynamic recommender selection algorithm based on three rules is used to filter out dishonest recommendations. The algorithm utilises the clustering technique accompanied with a deviation detection to filter out unfair recommendations exchanged by nodes in the network. The proposed algorithm has been tested by simulation against both bad-mouthing and ballot-stuffing attacks. The results of the simulation indicate that the model can safely incorporate honest recommendations received by recommenders and eliminate untrustworthy ones at a small number of dishonest recommenders which do not exceed 50%.

The recommendation based trust model is further enhanced with an effective defence scheme which is developed and analysed to filter attacks related to dishonest recommendation and consider characteristics of MANET. The proposed defence scheme also utilised the clustering technique to filter out unfair recommendations exchanged by nodes in the network based on three values: (a) the level of confidence held by a node about others, (b) deviation threshold which ensures the unity of views between evaluating node and the evaluated node, and (c) closeness centrality value to ensure that recommending node is a close friend to the evaluating node for a period of time. The proposed defence scheme is tested by extensive simulation in terms of throughput and packet loss, against both bad-mouthing and ballot-stuffing attacks, and also compared with other proposal. The simulation

results indicated that the proposed defence scheme can safely incorporate correct indirect trust evidences received by recommendations and eliminate untrustworthy ones. Moreover, it reduced the effect of false negative and false positive problems in selecting recommending nodes. The use of social property of trust to ensure that nodes are close friends in MANET, as well as, a quality of service property to select recommender which is proposed in this chapter are promising. Therefore, in the next chapter, a proposal to utilising more important social and QoS properties of trust is developed and designed to enhance the trustworthiness evaluation of nodes in the network.

Chapter 6 A Recommendation Based Model Using Multidimensional Trust Metric: Social Trust and QoS Trust

In this Chapter, social feature of a friendship based trust management model for MANETs is introduced, to secure the routing protocol between source and destination nodes based on the degree of friendship of each node in the path. Further, this chapter proposes a cognitive trust model with a composite multidimensional trust metric by combining the social properties of trust with quality of service (QoS) trust properties. It considers the wider use of social trust properties to represent the complexity of human behaviour in MANETs. It investigates the impact of embedding social properties of trust on network performance measures. Peer to peer evaluation and path evaluation are considered to allow nodes evaluate another nodes' behaviour and optimise their decisions regarding the trustworthiness of path selection.

6.1 Introduction

Trust is a social concept which can be used by nodes to evaluate the behaviour of other neighbours to decide on whether to assign them network activities or not based upon observations from past behaviour and recommendations from other nodes in the network. Very much as in the case of the human observation process, trust here is based on the accumulation of observations from various similar or dissimilar sources, to collect and combine the required information to decide on the trustworthiness of a perceived entity. MANETs show close similarities to the human behaviour model in the case of a number of nodes which have never interacted before are able to acquaint themselves and communicate with each other. Besides, nodes' perceptions, motivations, and goals for interactions are different,

besides, the presence of a selfishness concept, bad mouthing and ballot stuffing are other aspects showing similarity to human behaviour. Consequently, it is vital for a useful trust model to be related to human patterns of behaviour, because these patterns can be used to increase the model's quality in terms of deducing the degree of friendship, level of honesty, privacy, and the correctness of information derived from direct interactions or by recommendations. Moreover, combining all these metrics to produce multidimensional trust evaluation metric can enhance the performance of the evaluation and consequently enhance the performance of the network.

The main contributions of this chapter are in overcoming the limitations of existing trust models in two ways. Firstly, it introduces the social feature of a friendship based trust management model for securing MANETs. The model defines two distinguished metrics to measure friendship behaviour, namely honesty and confidence. Honesty is used to measure the negative and positive behaviour of nodes and whether to cooperate or defect, while confidence measures the ability of nodes to provide correct information in estimating other nodes' trustworthiness. These two metrics are used to measure behaviours and how these behaviours can change over time to affect the type of friendship degree dynamically.

Secondly, it proposes a model with a multidimensional composition for its trust metric. In MANETs, trustworthiness evaluation demands multidimensional properties which show human behaviour as well as QoS. Therefore, a multidimensional trust model that is based on representing trust relationships between nodes as human behaviour by considering social properties and QoS is proposed. This model can be used to enhance the efficiency of the system and improve the trust evaluation metric accuracy.

Further, the model uses two different stages of evaluation; peer to peer evaluation and path evaluation. A node in MANETs can evaluate the trustworthiness of its neighbour to decide whether to interact with it or not. However, the ability of the node not only to evaluate the whole path from source to destination, but also to evaluate the entirety of available paths, is very important to optimise routing and select the best path among those available. At the peer to peer level, social and QoS properties are considered, while at the path level, a minimum trust combination is used to choose a path with a small number of hubs and where each intermediate node on the path has a minimum acceptable trust value. This two-stage evaluation should enhance the accuracy of the model and have a positive impact on improving network performance.

6.2 A Friendship-Based Trust Management Model

A friendship-based trust management model to secure the routing protocol between source and destination nodes based on the degree of friendship of each node in the path is proposed. The model considers the issue of using social properties of trust to reflect the nodes' behaviour and study their dynamic properties of the friendship degrees in MANETs.

6.2.1 Friendship Degree Relationships

Relationships between nodes can be differentiated based on the degrees of friendships evaluated by the evaluating node. The proposed model uses the concept of dividing the relationships between nodes into different categories and permits the relationships to develop or change dynamically over time based on the confidence (level of experience) and honesty (positive and negative behaviour) of nodes in the previous interactions between the evaluating and the evaluated node. The categories of the friendship degrees $T_{ij}^{Friendship}$ are divided as follows:

- *Stranger* STRANGER: a stranger node has no previous interaction with the evaluating node.
- *Acquaintance* ACQUAIN: a node that has few interactions with the evaluating node and it is difficult to decide whether this node is a friend or a misbehaving node.
- *Friend* FRIEND: a friend node has enough interactions with the evaluating node and the honesty value of this node is high.
- *Misbehave* MISBEHAVE: a node which has enough interactions with the evaluating node and its honesty value is low.
- *Redeemed* REDEMP: a node that changes its behaviour from non-cooperative to become fully cooperative in network activities.

A node in MANETs may adjust its behaviour dynamically according to its own operational state and environmental conditions. Malicious nodes can be redeemed as good nodes based on trust evaluation performed in every trust update interval t. We model these behaviours by allowing the evaluating node to dynamically investigate the relationship with the node under evaluation and update it according to a new observation. For example, *MISBEHAVE* indicates that the node is misbehaving by being bad at providing services in terms of packet forwarding or as a recommender. When the behaviour of the node changes, the relationship between it and other nodes can be updated as *REDEMP, which* means that the evaluated node may behave well in the next interaction. This degree of friendship is used as a constraint to help nodes decide whether to interact with other nodes or not. For example, in the case of redemption, when a node put as REDEMP cannot be trusted as a node which behaves well all the time in the network.

Friendship degree is based on two metrics: *Honesty* and *Confidence*, and computed as follows.

6.2.2 Friendship Degree Components

A) Honesty $T_{ij}^{Honesty}$

Honesty is a social property that is used to evaluate the behaviour of nodes to act as a favour for themselves or the communities they are parts of [138]. It is considered by a number of researchers as an indicator of positive or negative behaviour [78 , 79 , 139]. In the proposed model, the honesty metric is utilised differently by combining it with confidence to construct friendship relationships between nodes. It evaluates the degree of honesty of the evaluating node i about the evaluated node j based on the direct observation or recommendation collected by other nodes in the network. It is the measure of positive and negative interactions (i.e. forwarding and dropping packets). The value of $T_{ij}^{Honesty}$ is computed by using the number of positive interactions α_{ij} between node i and j over the maximum number of positive and negative interactions $\alpha_{ij} + \beta_{ij}$. The initial value of $T_{ij}^{Honesty}$ is 0.5 at time t = 0, which means that node j is a stranger to node i and no previous interaction has been observed. The $T_{ij}^{Honesty}$ value develops over time and its value belongs to the interval [0, 1]. Positive interactions increase the value of $T_{ij}^{Honesty}$ while the negative interactions can lead to a decrease in its value. The value of α_{ij} and β_{ij} would be updated when observing new positive or negative interactions. The previous interactions are decreased to reduce the influence of old values using the decay factor as in subsection 4.2. In this model, $T_{ij}^{Honesty}$ is computed by using the expectation of beta function as in Eq. (6-1).

$$T_{ij}^{Honesty} = \frac{\alpha_{ij}}{\alpha_{ij} + \beta_{ij}} \quad (6\text{-}1)$$

B) Confidence $T_{ij}^{Confidence}$

Confidence is a social property that is used to indicate how strong a tie is between two interacting nodes. It is utilised as a measure that indicates how frequently nodes interact with one another and to evaluate how strong the relationships are between interacting nodes. In the proposed model, confidence is used to measure the level of experience one node can gain about another as a result of a sequence of interactions. It evaluates the number of interactions between two nodes. A high number of interactions can be translated into the idea that the evaluating node has a strong relationship with the evaluated node. Consequently, it improves the ability of the evaluating node to judge the trustworthiness of the node under evaluation. In the model presented here, the value of $T_{ij}^{Confidence}$ is a variance value of all past experiences between two interacting nodes. Assume that node i has observed a sequence of positive and negative interactions at time t; the $T_{ij}^{Confidence}$ value is measured by using the beta standard deviation σ as in Eq. (6-2). Beta standard deviation equation is redefined to normalise its values on the interval [0, 1] using the constant $1 - \sqrt{12}$.

$$T_{ij}^{Confidence} = 1 - \sqrt{12}\sigma_{ij}$$

$$T_{ij}^{Confidence} = 1 - \sqrt{\frac{12\ \alpha_{ij}\beta_{ij}}{(\alpha_{ij} + \beta_{ij})^2(\alpha_{ij} + \beta_{ij} + 1)}} \quad (6\text{-}2)$$

where α_{ij} and β_{ij} represent the positive and negative interactions observed by node i about node j. The value of $T_{ij}^{Confidence}$ belongs to the interval [0, 1]. At time $t = 0$, when there is no observation or evidence between evaluating and evaluated node, the value of $T_{ij}^{Confidence}$ is 0. This means that node i is

not able to judge the honesty of node j even if its honesty value is more than a trust threshold. The value of $T_{ij}^{Confidence}$ develops over time by increasing the number of positive or negative interactions. The updated value of α_{ij} and β_{ij} would be calculated when observing positive or negative interactions and decreased by time to reduce the effect of old experience.

Friendship degrees $T_{ij}^{Friendship}$ between evaluating and evaluated nodes are used to compute the overall trust of nodes. The predefined thresholds used in this model to classify nodes which are shown in Table 6-1 are identified by practice as the best values to increase the ability of nodes to assess trustworthiness of other neighbours in the network. For example, the MISBEHAVE threshold of 0.4 ensures that nodes are quickly detected as misbehaving nodes after performing a reasonable number of bad interactions. Table 6-1 shows the degrees of friendships based on the values of honesty and confidence.

Table 6-1 Friendship degree values between the evaluating and the evaluated node

Friendship degree $\boldsymbol{T_{ij}^{Friendship}}$	**Honesty** $\boldsymbol{T_{ij}^{Honesty}}$	**Confidence** $\boldsymbol{T_{ij}^{Confidence}}$
STRANGER	$T_{ij}^{Honesty} = 0.5$	$T_{ij}^{Confidence} = 0$
ACQUAIN	$T_{ij}^{Honesty} \geq 0.5$	$0 < T_{ij}^{Confidence} < 0.5$
FRIEND	$T_{ij}^{Honesty} \geq 0.5$	$0.5 \leq T_{ij}^{Confidence} \leq 1$
MISBEHAVE	$T_{ij}^{Honesty} < 0.4$	$0.5 \leq T_{ij}^{Confidence} \leq 1$
REDEMP	$T_{ij}^{Honesty} \geq 0.4$	$0.5 \leq T_{ij}^{Confidence} \leq 1$

Table 6-2 shows the decision making by the evaluating node about whether to interact with the evaluated node or not. The decision depends on the aggregated direct and indirect friendship degree of the evaluated node.

Table 6-2 Friendship degree values and decision of interaction

Friendship degree $T_{ij}^{Friendship}$	**Decision of interaction**
STRANGER	1. Evaluating node cannot directly interact. 2. Evaluating node gives more weight to indirect information. 3. If the overall trust is still stranger, evaluating node should look for another neighbour.
ACQUAIN	1. Evaluating node cannot directly interact. 2. Evaluating node gives more weight to indirect information. 3. Based on the overall trust value, the evaluating node can choose to interact with it or decide to look for another neighbour.
FRIEND	1. Evaluating node can directly interact. 2. Evaluating node gives more weight to direct information. 3. Consequently, it avoids any dishonest recommendation from other nodes.
MISBEHAVE	1. Evaluating node cannot directly interact. 2. Evaluating node gives more weight to direct information. 3. Consequently, it avoids any dishonest recommendation from other nodes.
REDEMP	1. Evaluating node can directly interact or choose to look for another neighbour. 2. Evaluating node gives more weight to direct information. 3. Consequently, avoid any dishonest recommendation from other nodes.

For each node in the network, trust value T_{ij} is calculated by combining both direct and indirect friendship degree values with different weights denoted by w_D and w_I respectively. T_{ij} is computed according to Eq. (6-3).

$$T_{ij} = w_D * TD_{ij}^{Friendship} + w_I * TI_{ij}^{Friendship} \quad (6\text{-}3)$$

where $TD_{ij}^{Friendship}$ is the direct evaluation of friendship degree by the node itself, and $TI_{ij}^{Friendship}$ is the indirect information collected by recommendations by other nodes in the network. Meanwhile, w_D and w_I are different weights for direct and indirect information and adjusted dynamically according to Table 6-2.

6.2.3 Experimental Setting

The friendship degree components are added to the simulator to test the validity of the model. A network with 50 randomly placed nodes in an area of 700×1000 square meters is simulated. Several nodes were randomly selected to be misbehaving by dropping packets by two rates: 50% and 80% of the packets transmitted in the network. Table 6-3 shows the parameters used in configuring the network for the experiment. Selfish attack with different percentages of dropping rates and additional permission to collude were used in order to evaluate the proposed model. Badly behaving nodes (selfish nodes) amounting to up to 50% always existed in the network and were responsible for collusion and jamming. Bad-mouthing and ballot-stuffing attacks which relate to dishonest recommendation problem by falsely degrade or promote trust value for a particular node also existed at 20% for each type. Results from the experiment are based on multiple runs, and negligible variation is noticed.

Table 6-3 Network configuration

Parameter	**Value**
Nodes	50
Area	700 m X 1000 m
Speed	10 m/s
Radio Range	250 m
Movement	Random waypoint model
Routing Protocol	DSR
MAC	802.11

Parameter	Value
Source-destination pairs	15
Transmitting capacity	2 Kbps
Application	CBR
Packet size	512 B
Simulation time	500 s
Trust threshold	0.4
Fading timer μ	10 s
Deviation threshold	0.5

6.2.4 Experimental Evaluation

The model first investigates the metrics of friendship degrees: honesty and confidence based on the number of interactions and how these values develop over time. Figure 6-1 shows the value of honesty and confidence and their values at different numbers of interactions. It is obvious that these two values develop by increasing the number of interactions. These two values are combined together to produce the friendship degree between two nodes. From the figure it can be seen that in the early stages of the simulation when there are not sufficient interactions, the difference between the values for honesty and confidence is large and this is interpreted as showing that nodes are strangers or just becoming acquainted. Later, by increasing the number of interactions, the values of both metrics become closer and this can be translated as showing that nodes friendship degrees change to become either friends or malicious. Consequently, nodes are now able to make correct decisions about whether to interact with other nodes or not.

Another evaluation metric is the testing of the dynamic development of friendship degrees over the time of the simulation, and this is shown in Figure 6-2. The figure shows the percentage of friendship degrees of node 7 for all the nodes interacted with during the time of simulation. From the figure, it can be seen that in the early stages of the simulation, most friendship degrees are either stranger or acquaintance, with percentages of more than 80% after 100

seconds, while friend and malicious degrees are very small, at less than 10% of the relationships. However, by increasing the time of simulation, the nodes are able to define the friendship degrees of most the nodes with as friends or malicious and this increases to nearly 60% of all the relationships between node 7 and other nodes with which it has interacted by the end of simulation. Meanwhile, the percentage of strangers and acquaintances are decreased over time to less than 40% of the relationships at the end of the simulation.

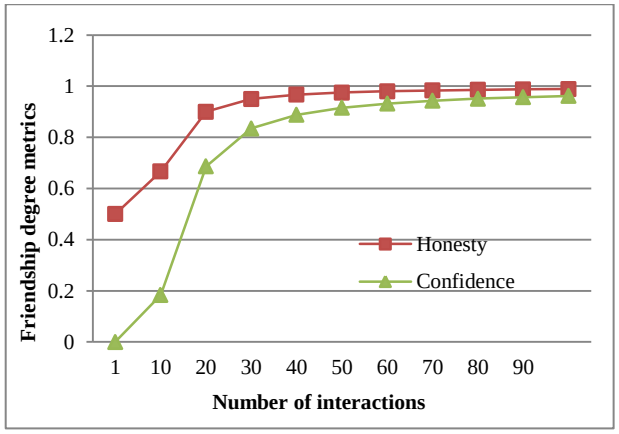


Figure 6-1 Friendship-based trust model metrics and their values at different numbers of interactions

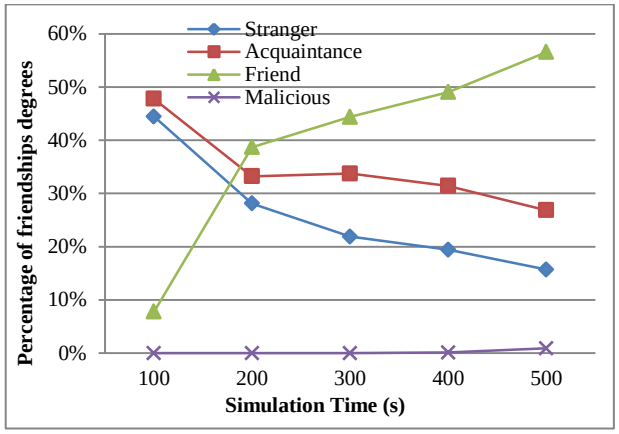


Figure 6-2 The developments of friendship degrees over time in the presence of 20% misbehaving nodes

Another evaluation metric is based on considering the adaptation of the proposed model in routing protocols such as DSR or AODV and checking its applicability and impact on the network performance, as shown in Figure 6-3

and 6-4. Figure 6-3 displays on the x-axis the number of misbehaving nodes, ranging from 10%, which means majority of nodes are behaving normally, to 50% misbehaving nodes, which means that half of the nodes conduct attacks. The y-axis shows the percentage of the network throughput of both standard DSR and friendship-based DSR that adopts the trust model to reflect the behaviour of nodes. The figure shows that the throughput for the proposed trust model gradually drops as the number of misbehaving nodes increases, but it remains at an acceptable level, at nearly 12,000, when the percentage of misbehaving nodes increases to 50%. Meanwhile, standard DSR throughput is less than the proposed model and falls to just under 7,000 when the percentage of misbehaving nodes reaches the maximum level of attacks.

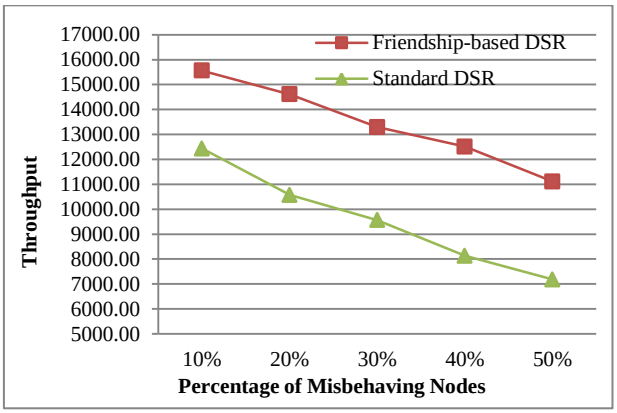


Figure 6-3 Network performance in the presence of misbehaving nodes for network throughput metric

Figure 6-4 displays the percentage of packet loss of both standard and friendship-based DSR with the same percentage of misbehaving nodes, which ranges from 10% to 50% misbehaving nodes. It shows an improvement in the ratio of packet loss for friendship-based DSR over the standard DSR in all the considered cases. The percentage of packet loss of the friendship-based DSR is increased to just fewer than 40% when half of the nodes try to reduce the efficiency of the network and the trust model. In comparison, the

standard DSR without the adaptation of the proposed model increases to 60% loss of the forwarded packets.

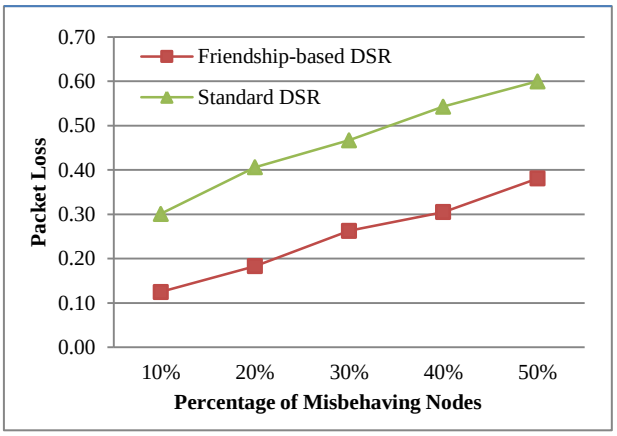


Figure 6-4 Network performance in the presence of misbehaving nodes for network packet loss metric

6.3 A Trust Model Based Composite Metric

As in previous chapters, the proposed model categorises nodes into three types: evaluating node, evaluated node, and recommending node. As the name suggests, any node i assessing the trustworthiness of another neighbouring node j is an evaluating node. Node j in this case is the evaluated node. The evaluating node assesses the trustworthiness of another neighbouring node by considering its own experience or recommendations for the evaluated node from a set of other nodes $\{k_1, k_2, k_3, \dots, k_N\}$ in the network. These nodes, in this case, are the recommending nodes. The basic architecture of the proposed trust evaluation model is given in Figure 6-5. Mainly, the model is used to secure the routing protocol between the source and destination nodes based on peer evaluation and path evaluation.

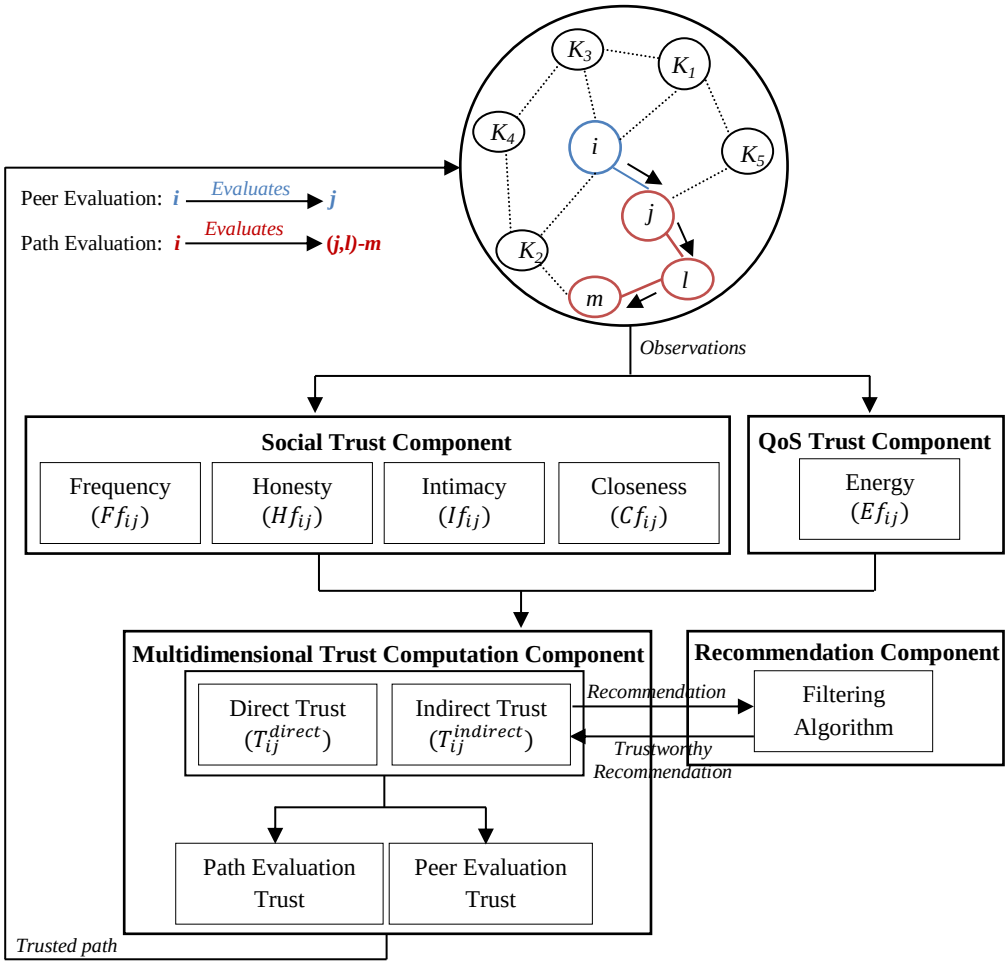


Figure 6-5 The proposed model components

In peer evaluation, nodes in the network observe each other's behaviour in order to build a trust relationship which reflects the trust that one node can place in another. The trust relationship is valuable in helping nodes decide whether or not to forward packets to their neighbour. On the other hand, path evaluation evaluates all the available paths to the destination in terms of number of hubs (closeness centrality) and trustworthiness of each node in between. Peer evaluation in terms of both direct and indirect trust is computed by aggregating multidimensional factors; social trust and QoS trust. Three factors of the social trust component include; frequency, honesty and intimacy. The energy factor of the QoS trust component is used to

compute the peer evaluation. Meanwhile, minimum and closeness factors are used to compute path evaluation by allowing source nodes to evaluate the available paths based on the minimum trust value of intermediate nodes above a trust threshold, and smallest hop count in those paths which meet the trust requirement.

Assuming that i is an evaluating node and j the evaluated node, the trustworthiness of node j to node i is calculated by combining four factors, including: a) the frequency factor Ff_{ij} which is used to measure the level of experience between node i and j. This reflects the problem of misinformation based on short and long term observations. b) The honesty factor Hf_{ij} which is utilised to measure whether a node is selfish/malicious or not. c) The intimacy factor If_{ij} which is used to measure the level of experience in terms of time. This reflects the level of experience of node j with node i in comparison with other nodes have previously interacted with node i. d) The energy factor Ef_{ij} which is used to measure whether a node is capable of performing the intended task or not. The energy factor is considered because of its scarcity and importance in MANETs. Therefore, the trustworthiness between node i and j can be determined by Eq. (6-4).

$$T_{ij}^{direct} = Ff_{ij}^{direct} + Hf_{ij}^{direct} + If_{ij}^{direct} + Ef_{ij}^{direct} \quad , \qquad (6\text{-}4)$$

$$T_{ij}^{indirect} = Ff_{ij}^{indirect} + Hf_{ij}^{indirect} + If_{ij}^{indirect} + Ef_{ij}^{indirect}$$

For each node in the network, trust value T_{ij} is calculated by combining both direct and indirect trust values with different weights denoted by w_{direct} and $w_{indirect}$ respectively and $w_{direct} + w_{indirect} = 1$. T_{ij} is computed according to Eq. (6-5).

$$T_{ij} = w_{direct} * T_{ij}^{direct} + w_{indirect} * T_{ij}^{indirect} \quad (6\text{-}5)$$

6.4 Multidimensional Trust Factors and Evaluation

6.4.1 Peer to Peer Trust Evaluation

This subsection describes how peer-to-peer trust evaluation is conducted between the evaluating node and the evaluated node. If the evaluating node i intends to evaluate the trustworthiness of the evaluated node j, node i will consider four components of trust as follows:

A) Frequency-based social trust factor Ff_{ij}

Frequency is a social property which is used to indicate to how strong a tie is between two interacting nodes. It is defined as follows: the more frequently nodes interact with one another, the stronger their opinions of friendship [137]. The frequency factor has been used by several research studies to indicate the tie strength in routing protocols in distributed networks such as mobile ad hoc networks (MANETs) and mobile social networks (MSNs) [140 , 141 , 142]. In the proposed model, the frequency social trust factor measures the level of experience which one node can gain about another as a result of a sequence of interactions. This is done by evaluating the number of interactions between two nodes. A high number of interactions can be translated as meaning that the evaluating node has a strong relationship with the evaluated node. Consequently, it improves the ability of the evaluating node to judge the trustworthiness of the node under evaluation. In the model presented here, the value of Ff_{ij} is a variance value of all past experiences between two interacting nodes. Assuming that node i has observed a sequence of positive and negative interactions at time t; the Ff_{ij} value is measured by using the beta standard deviation σ as in Eq. (6-6).

$$Ff_{ij} = 1 - \sqrt{12}\sigma_{ij}$$

$$Ff_{ij} = 1 - \sqrt{\frac{12\ \alpha_{ij}\beta_{ij}}{(\alpha_{ij} + \beta_{ij})^2(\alpha_{ij} + \beta_{ij} + 1)}} \quad (6\text{-}6)$$

where α_{ij} and β_{ij} represent the positive and negative interactions observed by node i about node j. The value of Ff_{ij} belongs to the interval between [0,1]. At time $t = 0$, the value of α_{ij} and β_{ij} is 1, which means that no observation or evidence has been collected. Thus, the value of Ff_{ij} is 0 and develops over time by increasing the number of interactions. The updated value of α_{ij} and β_{ij} would be calculated as $\alpha_{ij} = \rho + 1$ and $\beta_{ij} = n + 1$, where ρ and n represent the positive and negative collected observations respectively, and ρ and $n \geq 0$. The previous interactions are decreased to reduce the influence of their old values as in subsection 3.2. As an example, assuming that node i has interacted with node j at different time stamps $\{t_0, t_{12}, t_2, \ldots, t_{10}\}$ and that the number of interactions is between 0 and 68, the value of Ff_{ij} is shown in Table 6-4.

Table 6-4 Frequency-based social trust factor and its possible values at different interactions

Time stamp t	Number of interactions	Frequency factor Ff_{ij}
t_0	0	0
t_1	5	0.446716665
t_2	12	0.595938982
t_3	19	0.666357595
t_4	26	0.709401356
t_5	33	0.739179735
t_6	40	0.761351694
t_7	47	0.778686666
t_8	54	0.792721071
t_9	61	0.804384801
t_{10}	68	0.814277976

B) Honesty-based social trust factor Hf_{ij}

Negative and positive behaviours of nodes are indicators of the honesty of nodes in detecting irregular behaviour such as selfishness or malicious attacks. Honesty is a social property which is defined as the way in which nodes behave in terms of acting to favour themselves or the communities of which they are a part[138]. This is considered by a number of researcher as an indicator of positive or negative behaviour (as in [78 , 79 , 139]. Honesty is an important social trust factor in the proposed model and refers to the degree of honesty of the evaluating node i about the evaluated node j based on the direct observation or recommendation collected by other nodes in the network. It is a measure of successful or failed interactions (i.e. forwarding and dropping packets). The value of Hf_{ij} is computed by using the number of successful interactions α_{ij} between node i and j over the maximum number of successful and failed interactions $\alpha_{ij} + \beta_{ij}$. The initial value of Hf_{ij} is 0.5 at time t = 0, which means that node j is a stranger to node i and no previous interaction has been observed. The Hf_{ij} value develops over time also, and its value is between 0 and 1. Positive interactions increase the value of Hf_{ij}, while negative interactions can lead to a decrease in its value. The value of α_{ij} and β_{ij} would be updated when observing new positive or negative interactions. The previous interactions are decreased to reduce the influence of their old values as in subsection 3.2. In this model, Hf_{ij} is computed by using the expectation of beta function as in Eq. (6-7).

$$Hf_{ij} = \frac{\alpha_{ij}}{\alpha_{ij} + \beta_{ij}} \tag{6-7}$$

Table 6-5 gives an example to show the influence of positive and negative observations on the value of Hf_{ij}. Assume that node i has observed a sequence of interactions with node j and is now in a position to judge the

honesty factor of node j. From the table, it can be seen that honesty is a very important factor in evaluating the trustworthiness of nodes because of its ability to reflect the behaviours of nodes, whether intending to behave badly or well.

Table 6-5 Honesty-based social trust factor and its possible values at different positive and negative interactions

Positive interaction α_{ij}	**Negative interaction β_{ij}**	**Honesty factor Hf_{ij}**
1	1	0.5
5	1	0.833333333
5	3	0.625
8	3	0.727272727
15	3	0.833333333
15	10	0.6
20	10	0.666666667
25	20	0.555555556
40	20	0.666666667
80	20	0.8

C) Intimacy-based social trust factor If_{ij}

In a social network, a node for whom a great deal of time has been spent connected to another node can refer to a strong relationship between the two. This factor is involved in several models, such as those of [78 , 137 , 142]. However, this factor is not always clearly defined, and its computation differs from model to another. In the proposed model, the If_{ij} factor is a measure of the level of interaction experiences in terms of time. It indicates the duration of time which the evaluating node has spent connected to an evaluated node compared to other connected neighbours in the network. If_{ij} is therefore defined as a measure of how much time node i has been connected to node j compared with others. It is computed by the number of interactions between nodes i and j over the maximum number of interactions between node i and any neighbouring node over the time period, according to Eq. (6-8).

$$If_{ij} = \begin{cases} 0.5, & d = D \\ \dfrac{d}{D}, & otherwise \end{cases} \quad (6\text{-}8)$$

where $d = \alpha_{ij} + \beta_{ij}$, which is the accumulated positive and negative interactions between node i and j and $D = \sum_{k=1}^{n} \alpha_{ik} + \beta_{ik}$, which represents the accumulation of interactions between node i and any other node which has been interacted with across all encountered nodes. The value of the intimacy factor is between the interval [0,1] and it is 0.5 when node j is the only node which has interacted with node i at time t, and increases or decreases according to the number of interactions between node i and j and other encountered nodes. Table 6-6 gives an example of the intimacy factor and how its value changes according to the number of interactions between the evaluating node and other encountered nodes.

Table 6-6 Intimacy-based social trust factor and its possible values at different interactions between $\boldsymbol{i}$ and $\boldsymbol{j}$ and other encountered nodes

Number of interactions between i and j	**Number of interactions between i and other encountered nodes**	**Intimacy factor If_{ij}**
2	2	0.5
5	7	0.714285714
10	17	0.588235294
20	44	0.454545455
38	60	0.633333333
50	100	0.5
50	280	0.178571429
51	400	0.1275
80	550	0.145454545
90	720	0.125

D) Energy-based QoS trust factor Ef_{ij}

Energy is a critical QoS factor of trust. It is considered in this model because of its scarcity in the MANETs environment. All nodes are energy-constrained and the lifetime of each node depends on its energy consumption. In

conventional trust models, nodes tend to choose neighbours with the highest trustworthiness without giving concern to the energy factor, and this can lead to causing trustworthy nodes to die quickly and consequently be lost from the network. Therefore, considering the energy factor can help trustworthiness evaluation in two ways. Firstly, it can keep good nodes alive for more time as the evaluation depends not only on the trust value. Secondly, watching nodes' level of energy can help in detecting selfish and malicious behaviour in which selfish nodes will continue to have high levels of energy, while malicious nodes will spend more energy in performing attacks. In the proposed model, the Ef_{ij} factor indicates the remaining energy level of the node after each trust update interval t performed by the evaluating node i about the evaluated node j. The energy factor is calculated as in Eq. (6-9).

$$E_{ij}^{Remain} = E_{ij}^{Current} - E_{ij}^{Consumed}$$

$$Ef_{ij} = \frac{E_{ij}^{Remain}}{E_{ij}^{Initial}} \quad (6\text{-}9)$$

where $E_{ij}^{Consumed}$ is the level of energy consumed by node j in performing interactions, $E_{ij}^{Current}$ is the previous current energy of node j, E_{ij}^{Remain} is the remaining level of energy of node j, and $E_{ij}^{Initial}$ is the initial level of energy of node j to start with. Energy is initially at the same level for all nodes in the network. Receiving and transmitting packets are the only types of communications which are considered for energy consumption. Over time, the level of energy is adjusted based on each node's interactions. The value of the energy factor is defined in the interval [0, 1]. It starts at 1, which refers to a situation where nodes have a full battery, and gradually decreases over time as nodes involve themselves in more communications. Nodes continue to be effective in performing interactions so long as the energy factor is not

reduced to a particular threshold $E_{ij}^{Threshold}$. However, the relationship between energy factor and level of energy consumed is governed by linear relationships, as shown in Figure 6-6.

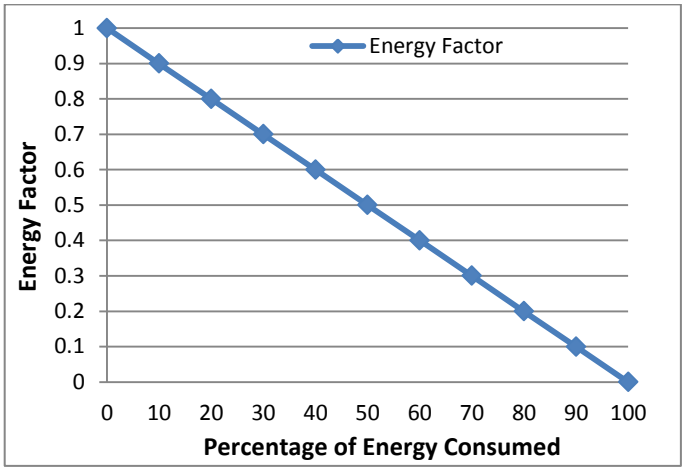


Figure 6-6 The relationship between energy factor and consumed energy

6.4.2 Path Trust Evaluation

The path evaluation process is achieved by the source node based on a selection technique to guarantee choice of the shortest path which meets the security requirements of QoS and social trust. The path selection technique must determine paths that fulfil specified requirements and constraints. Employed metrics for the path selection technique are based on the values of these metrics for the intermediate nodes on the whole path. The value of path trust evaluated by the source node should not exceed the trust value of the intermediate nodes. Therefore, this model proposes the use of two composite metrics as a path selection method to evaluate the path between source and destination, as follows.

A) Minimum-based trust factor Mf_{sd}

In MANETs, if there are a number of available paths from source to destination, a source node s evaluates those paths which meet the required trust value by considering the minimum trust value of intermediate nodes that

is above a trust threshold as an overall evaluation value. At time t, the minimum trust factor Mf_{sd} of a path P is computed by taking the minimum trust value of the intermediate nodes as an overall trust value of the path as in Eq. (6-10).

$$Mf_{sd} = Min\big(T_{ij}(t)\big|i,j \in P \text{ and } j \text{ is next hop neighbour of } i\big) \quad (6\text{-}10)$$

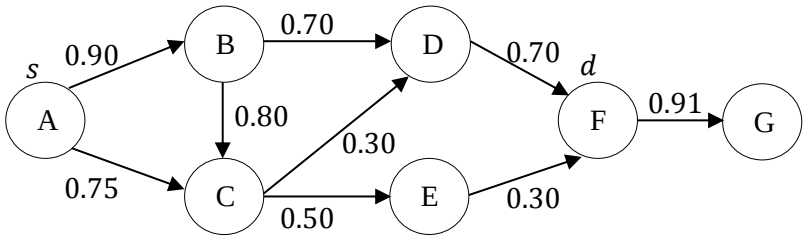


Figure 6-7 Minimum-based trust factor computation

As shown in Figure 6-7, at time t, node A is the source node that evaluates the possible paths to the destination F. Although there are five possible paths to the destination, Mf_{sd} of the path $(A \to B \to D \to F)$ with trust value of intermediate nodes $B, D = (0.90, 0.70)$ is 0.90, which is the most trustworthy path from source to destination. The minimum based trust factor has an advantage in computing path trust because of its ability not to increase the trust path more than the smallest acceptable trust value of the intermediate node. Some research papers use the continued product of node trust values in the path, as in [143]. However, while this method does not increase trust more than the trust values of intermediate nodes, it is unable to give the correct path trust that reflects the actual trustworthiness of the intermediate nodes. For example, Table 6-7 shows the available paths from node A to F and their trust values and path trust using two methods; the minimum method and the product method. The path trust using the product in path numbers 2 and 5 is 0.38 and 0.36 respectively. These values are less than the trust

threshold and these two paths are considered untrustworthy. However, this does not reflect the truth, in which intermediate nodes on both paths are considered to be trustworthy and should not be excluded from the selection. Meanwhile, our method gives a minimum value to consider path trust of 0.5, which is considered a trustworthy path because this value is more than the trust threshold.

Table 6-7 Comparison of the minimum-based trust factor and product method in calculating path trust for all available paths from source to destination

Path number	Path from s to d Node $A \rightarrow F$	Trust value	Minimum method	Product method
1	A → B → D → F	(0.90,0.70)	0.70	0.63
2	A → C → E → F	(0.75,0.50)	0.50	0.38
3	A → C → D → F	(0.75,0.30)	0.30	0.23
4	A → B → C → D → F	(0.90,0.80,0.30)	0.30	0.22
5	A → B → C → E → F	(0.90,0.80,0.50)	0.50	0.36

B) Closeness centrality-based social trust factor Cf_{sd}

Closeness centrality is the metric used by social networks [137 , 138] to describe the efficiency of information propagation from source node s to the destination d. Cf_{sd} can be defined as a measure of the distance between s and d in terms of physical distance, number of hops, or delays. In the proposed model, closeness centrality is considered as a measure of number of hops between node s and node d. Cf_{sd} is calculated as the inverse of the sum of the distances between node s and node d in the network. The distance is measured by the number of hops between the source and destination node and this can be calculated as in Eq. (6-11).

$$C_{ij} = \frac{1}{\sum_{d \neq 1} distance(s,d)} \tag{6-11}$$

Source node s selects the route with the largest C_{ij} which indicates the smallest hop count in the paths that meet the trust requirement. If paths that

meet the required minimum trust value have an equal hop count, the source node s chooses the path with the maximum path trust as the most trustworthy path. Considering the previous example presented in Table 6-7, node s will consider only paths 1, 2, and 5, as their path trust is more than the trust threshold in the first evaluation. In the second evaluation, node s will consider paths 1 and 2 because they are two hops' distance from the destination d and then node s will select path 1, as its minimum trust factor is 0.7 which is more than the trust of path 2, as the most trustworthy path.

6.5 Simulation and Analysis

The proposed trust model based composite metric is tested through extensive simulation in terms of throughput, packet loss, and energy consumption against badly-behaving nodes (selfish, blackhole and greyhole attacks). It is compared with another proposal available in the literature to show its capability in evaluating trustworthiness. The relation of social and QoS trust values to the number of successful interactions between evaluating nodes and evaluated nodes is also considered.

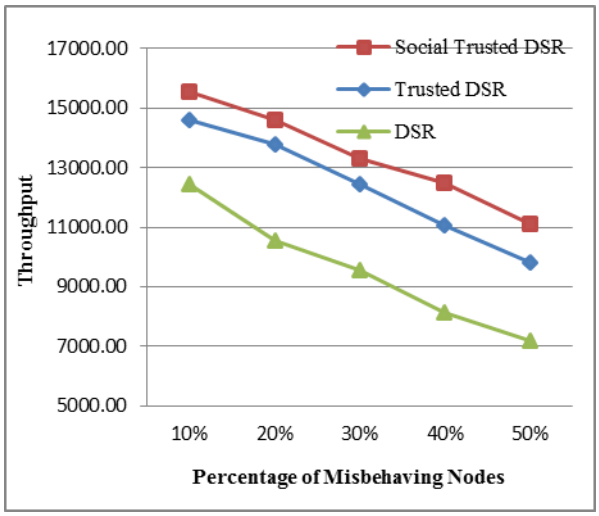
6.5.1 Experimental Setting

The setting used for this experiment is the same as in Table 6-3 in section 6.2.3. The social and QoS trust model components are added to the simulator to test the validity of the model. Several nodes were randomly selected to be misbehaving by dropping packets by two rates: 50% and 80% of the packets transmitted in the network. Selfish attack with different percentages of dropping rates and additional permission to collude were used in order to evaluate the proposed composite trust evaluation metric. Badly behaving nodes (selfish nodes) amounting to up to 50% always existed in the network and were responsible for collusion and jamming. Bad-mouthing and ballot-stuffing attacks which relate to dishonest recommendation problem by falsely

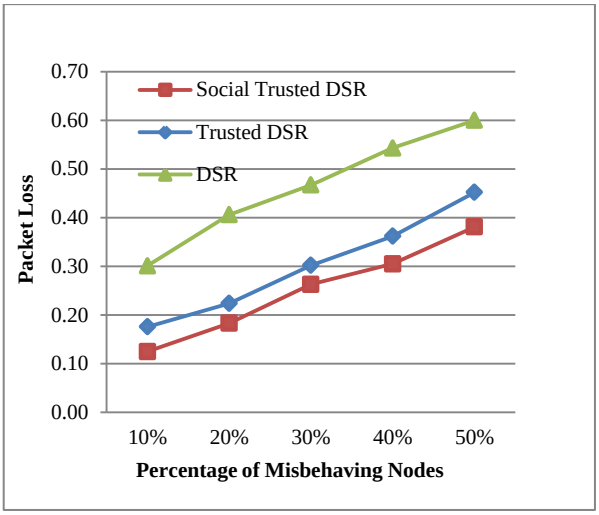
degrade or promote trust value for a particular node also existed at 20% for each type. Results from the experiment are based on multiple runs, and negligible variation is noticed.

6.5.2 Performance Evaluation

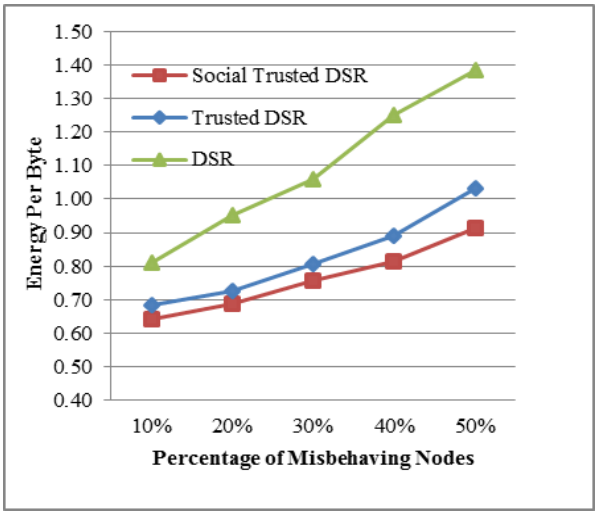
The flow of the simulation is as follows. The performance of the entire network is represented by three parameters; *Network throughput*, *Packet loss*, and *Energy consumption* in the presence of misbehaving nodes (selfish, bad-mouthing, and ballot-stuffing nodes in this case). In order to check the effectiveness of the proposed model, the performance of the network is tested in three cases: first, for the standard DSR routing protocol which does not consider trust relationships between participating nodes; second, for the trusted DSR routing protocol which only considers trust relationships between nodes in terms of forwarding packets; and finally, for the proposed trust model which combines both social trust and QoS trust to evaluate nodes' trustworthiness. Trust level evaluation of good, moderate, and bad nodes by other nodes in the network for both trusted DSR and social Trusted DSR in the presence of attacks is tested. A comparative study with service-based multidimensional trust model proposed in [79] was conducted.



(a) Network throughput



(b) Packet Loss



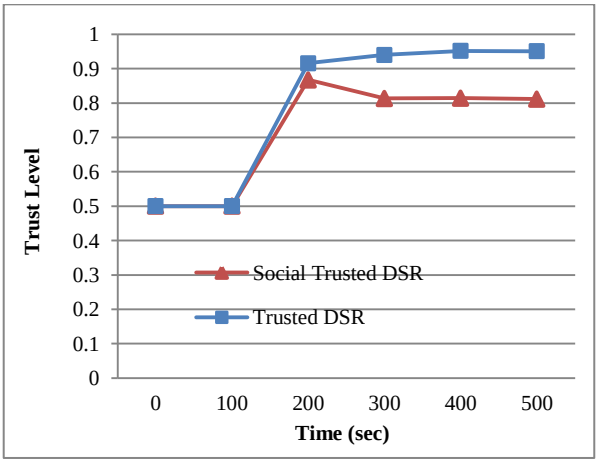
(c) Energy Consumption

Figure 6-8 Network performance in the presence of misbehaving nodes for the social trusted DSR, trusted DSR, and standard DSR routing protocol for (a) Network throughput, (b) Packet loss, (c) Energy consumption

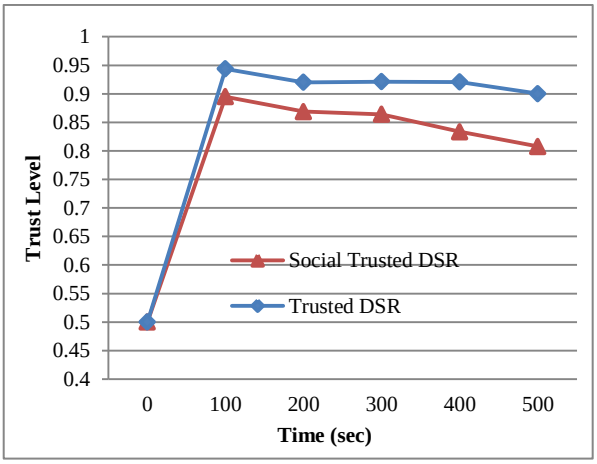
Figure 6-8 demonstrates the effect of misbehaving nodes on network performance metrics in terms of throughput, packet loss and energy. Figure 6-8(a) shows the performance of the throughput in the presence of misbehaving nodes. The y-axis shows the percentage of throughput for the standard DSR, trusted DSR and social trusted DSR, in the presence of misbehaving nodes varying from 10% to 50% of the population. It is observed

that the network throughput for the social trusted DSR routing protocol outperforms both the trusted DSR and the standard DSR. In the trusted DSR, the network throughput is higher than the standard DSR but is still less than the proposed model with social and QoS capability. However, the proposed model was able to maintain the value of throughput as higher than the other protocols in all cases of higher population of the misbehaving nodes because of its ability to enhance the trustworthiness evaluation of nodes in selecting honest neighbours, and consequently, enhance the network throughput. The impact of misbehaving nodes on packet loss is shown in Figure 6-8(b). The percentage of packet loss rises with an increase in the percentage of misbehaving nodes, from nearly 10% when there are only 10% misbehaving nodes in the network, to less than 40% when the percentage of misbehaving nodes increases to half of the total population. Meanwhile, for the trusted DSR, the packet loss percentage increases to nearly 50% and for the standard DSR it increases to nearly 60% when there are 50% misbehaving nodes present in the network. It can be seen from the above analysis that the social trusted DSR can outperform the other two protocols in terms of the packet loss metric by considering more social attributes of trust and QoS trust. Figure 6-8(c) shows the impact of misbehaving nodes on energy consumption. The energy consumed per byte is shown on the y-axis in the presence of misbehaving nodes. From the figure, it is obvious that the energy consumption percentage in the Social Trusted DSR is less than both the Trusted DSR and the Standard DSR routing protocol as it is able to reduce the number of dropped packets than both protocols. It is also observable that the energy level in the Trusted DSR is slightly different from the proposed protocol: especially when the percentage of misbehaving nodes is less than 30%. Moreover, the energy performance of the proposed model is far better

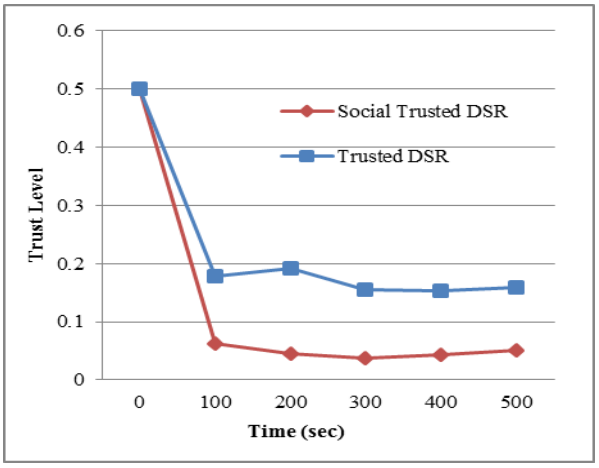
than the pure DSR when there are no trust relationships adopted between nodes. Therefore, from the network performance analysis above, it can be concluded that the proposed model can keep the network performance metrics of throughput, packet loss, and energy consumption at an acceptable level even when the percentage of misbehaving nodes is half of the total population.



(a) Good Node (node 30)



(b) Moderate Node (node 17)

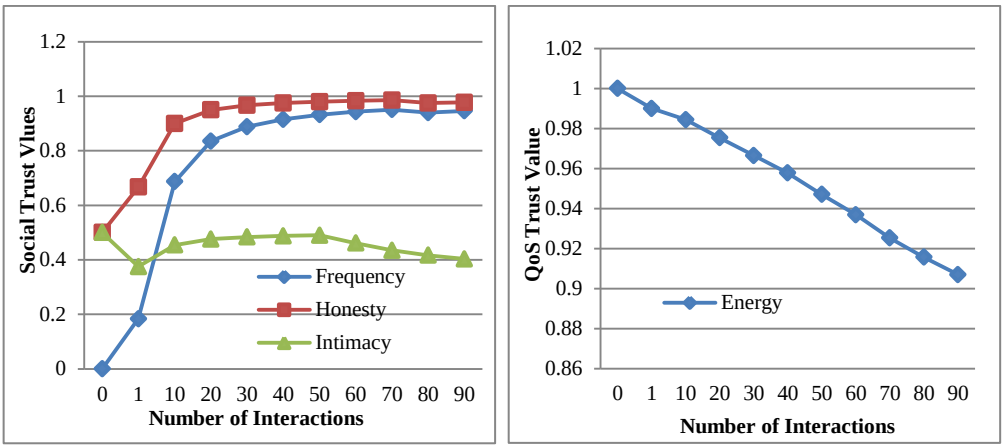


(c) Bad Node (node 13)

Figure 6-9 Trust evaluation of a node by all nodes in the presence of 20% black hole attack, 20% bad-mouthing attack, 20% ballot-stuffing attack for (a) Good Node, (b) Moderate Node, (c) Bad Node

Figure 6-9 demonstrates the trustworthiness evaluation of good, moderate, and bad nodes by other nodes in the existence of selfish, bad-mouthing, and ballot stuffing attacks. Figure 6-9(a) shows the trust level of a good node which has a high trust value after a sufficient number of successful interactions with nodes in the network. It is obvious that in the trusted DSR, which only uses packet forwarding for evaluation, the trust value of node 30 is higher than its trust value as given by the social trusted DSR, because STDSR evaluates the node's trustworthiness based on energy, duration of interactions, and number of interactions. The proposed model could be used to reflect the dynamic characteristic of MANETs and solve the problem of being able to conduct the assigned service in terms of both high reputation and resources available. Figure 6-9(b) shows the same behaviour as in Figure 6-9(a) for both models in evaluating a moderate node whose trust value is moderate after sufficient interactions with other nodes. As can be seen, the trust value of the STDSR is less than the TDSR in all cases. Figure 6-9(c) shows the trust evaluation of a bad node (node 13 in this case). It is

clear that the trust value of the node is very low because of its bad behaviour as a packet forwarder and as a recommender. However, STDSR maintains this value at a lower level than the evaluation of the TDSR because this kind of node needs to use its energy resources to conduct such attacks, and also intimacy could be very small as a result of avoiding interactions with such nodes by other nodes in the network. Consequently, nodes can circumvent bad experience before interacting with bad nodes.

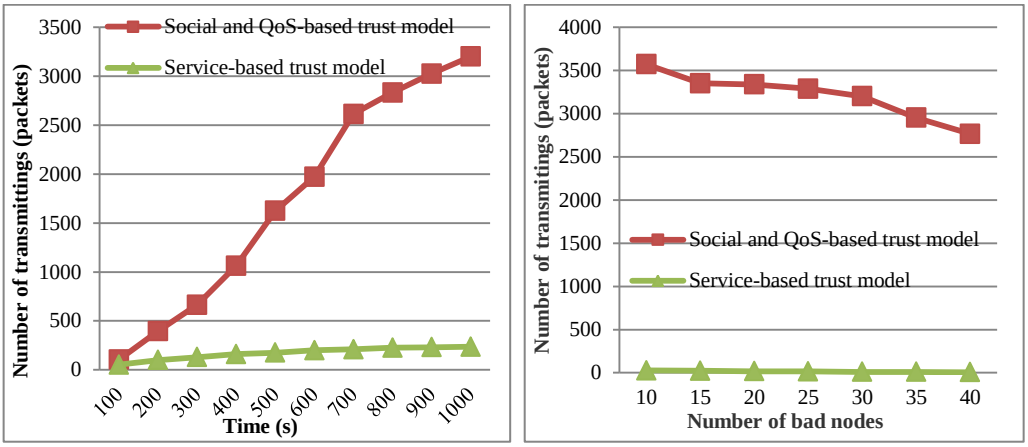


(a) Social Trust Values (b) QoS Trust value

Figure 6-10 Social and QoS trust values in relation to the number of successful interaction between evaluating node and evaluated node for (a) Social trust values; (b) QoS trust value

Figure 6-10 shows the value of the social trust and QoS trust components used to produce the composite trust metric in relation to the number of interactions. Figure 6-10(a) demonstrates the value of social components; frequency, honesty and intimacy. It is seen that these values are changed by increasing the number of interactions, in which frequency starts with the value 0 when there is no interaction between the two nodes, and rises by increasing the number of interactions. Honesty increases as the number of successful interactions increases. Intimacy fluctuates according to the number of interactions between the evaluated node and with the other nodes which have had interactions with the evaluating node. In contrast, Figure 6-

10(b) shows that the estimated energy value of the evaluated node decreases as it becomes involved in more interactions with other nodes in the network. Consequently, the evaluation of the components used to calculate trust shows that the proposed model is able to effectively consider the dynamic characteristics of MANETs by using social and QoS trust.



(a) Nodes' performance with increasing time of simulation in the presence of 30% bad nodes

(b) Nodes' performance with increasing number of bad nodes

Figure 6-11 Comparative study with service-based multidimensional trust for (a) Nodes' performance with increasing time of simulation; and (b) Nodes' performance with increasing number of bad nodes

Finally, the performance of the proposed model is compared with a multidimensional model which uses multiple decision factors of security trust and quality trust as proposed in [79], and which considers no social network properties of trust. The comparison is conducted in terms of a perfect transmitted packets metric, which represents the proportion of successfully transmitted packets via trustworthy paths in which all intermediate nodes in the selected paths meet the minimum requirements for all the composite factors. We follow the same network configuration and node selection which is provided in the service-based multidimensional trust model (see [79] for details) to conduct this experiment. Figure 6-11 shows the results of the

experiment. Figure 6-11(a) displays the packets transmitted successfully over the simulation time in the presence of 30% bad nodes. It can be seen that the proposed model can achieve a number of transmitted packets which is greater than the number reported by the service-based model. The number of transmitted packets in case of the proposed model is increased dramatically for the entire time of evaluation and converges to nearly more than 3000 packets towards the later phase. In comparison, for the service-based model, the number of transmitted packets value is low initially, at half of the packets transmitted by the proposed model and this only converges to nearly 300 packets towards the end of the simulation. Figure 6-11(b) shows the effectiveness of the proposed social and QoS model in transmitting packets successfully with the existence of bad nodes which drop packets intentionally. In the case of the proposed model, the number of transmitted packets decreases when the number of bad nodes increases in the network, and decreases to just over 2500 packets towards 40% bad nodes. Meanwhile, for the service-based model, the number of transmitted packets is very low over all percentages of bad nodes and stands at less than 10 packets at 40% of bad nodes. The results show that the proposed model with social and QoS capability can enhance the performance of the network over both the traditional models and multidimensional models which give no consideration to the social properties of nodes in MANETs.

6.6 Summary

A friendship-based trust management model for MANETs is proposed to reflect nodes' behaviour and cope with multiple misbehaving attacks. The model utilises the social property of friendship degrees that is based on combining two social metrics: honesty and confidence. Dynamic developments of friendships over time are considered to represent the

behaviour of nodes in a human manner. The proposed model has been tested by simulation against different types of attacks such as blackhole, greyhole, bad-mouthing, and ballot-stuffing attacks. The results of the simulation indicate that the proposed model can accurately evaluate the behaviour of nodes as in human patterns. Further, a composite metric based on social properties and QoS factors is developed and analysed to secure routing protocols in the MANET. The use of single trust metric based approaches cannot reflect the behaviour of nodes, and exposes them to inaccurate evaluation of other nodes' trustworthiness. Therefore, the proposed multidimensional trust model utilises multiple factors which depend on more social and QoS properties to represent the behaviour of nodes in a human manner and reflect the complexity of trust. The model evaluates nodes' trustworthiness at two levels to provide more accurate decisions, including both peer to peer evaluation and path evaluation techniques. The proposed model has been tested through extensive simulation and also compared with another. The simulation results indicate that the proposed model can enhance the evaluation of nodes' trustworthiness by considering multiple factors instead of depending on a single factor. Moreover, the model enhances the performance of the network and reduces the effect of bad nodes.

Chapter 7 Conclusion and Future Work

Conclusions of the thesis are provided in this chapter by illustrating a summary of the accomplishments. Some suggestions of future work in this area are also presented.

7.1 Conclusions

This thesis proposes to use the concept of trust and reputation as a security mechanism to secure routing protocols in MANET. It explored the definitions of these concepts available in the literature, and defines trust based on the combination of multiple definitions suit the thesis context. An overview of the state of the art of trust and reputation management in four important applications; E-Commerce and E-Market, Peer-to-Peer Networks, Social Networks, and Mobile Ad Hoc Networks were presented. Besides this, three well known techniques to compute trustworthiness in distributed systems, namely Game Theory, Fuzzy Theory and Probability Theory, were investigated in the four mentioned applications. Through the review of the literature, the problem of evaluating and computing trustworthiness in MANET application was identified in Chapter 3, which presented the problem definition and the important components that should be combined to work together in the proposed trust model.

A trust metric model was developed to monitor misbehaving nodes in ad hoc routing protocol, their harmful influence was mitigated and they were avoided by nodes in selecting a reliable routing path. This model presented in Chapter 4 and uses multiple trust evidence, including direct trust, indirect trust and opinion trust to evaluate nodes' trustworthiness. The model is believed to be simple and comprehensive in the way all the available information needed for calculating trustworthiness is gathered and used as appropriate. The model is totally decentralised and depends on the nodes'

experience gained in previous interactions, giving greater importance to recent experiences. Further, it has the ability to give another chance to misbehaving nodes to recover their trustworthiness values and come again to the network. The node can use its own evidence (direct trust) or can use external evidence or recommendations by other nodes (indirect trust). A simple method was used to deal with dishonest recommending nodes and this was sufficient, as no attacks related to providing dishonest recommendations are considered.

To enhance the proposed model, there was a need to extensively investigate the problem of dishonest recommendations. Chapter 5 presented a design of effective solutions to this problem. It provided security analysis on the countermeasures relevant to five attacks which aim to distort the correctness of the received recommendations. A recommendation based trust model with an enhanced dynamic recommender selection is developed and analysed to filter attacks related to dishonest recommendations exchanged by nodes in the MANET. The model is strengthened by incorporating a combination of three rules used to filter out recommendations. These are the majority opinion, personal experience, and quality of service approaches. Each of these rules inherent drawbacks when singly been applied in filtering recommendations in MANETs. The combination of them is believed to enhance the selection procedure and keep the trustworthiness evaluation near to ground truth value. The filtering algorithm is advantageous in enhancing the selection of recommending nodes in the way it considers multiple MANETs' characteristics including level of experience, scarcity of knowledge (i.e. data sparsity problem), and how close the recommender to the evaluating node.

As the research continues, some other characteristics of MANETs need to be investigated such as time and location of recommending nodes. Therefore, chapter 5 presented another filtering algorithm, namely, an effective defence scheme, which utilises the clustering technique to filter out unfair recommendations exchanged by nodes in the network based on three values: (a) the level of confidence held by a node about others, (b) deviation threshold which ensures the unity of views between evaluating node and the evaluated node, and (c) closeness centrality value to ensure that recommending node is a close friend to the evaluating node for a period of time. The proposed defence scheme is proven to be capable to safely incorporate correct indirect trust evidences received by recommendations and eliminate untrustworthy ones. It reduces the effect of false negative and false positive problems in selecting recommending nodes. Moreover, the accompanied costs with the proposed defence scheme were investigated. These costs can be reduced by using only the very last recommendations to be including in the clustering filtering computation. Dynamic selection of the number of recommendations based on a period of time can have many advantages, (1) reduce complexity and memory usage, (2) exclude any old recommendation from the calculation, (3) reduce the time that is used to select the trustworthy cluster.

In chapter 6, a friendship-based trust management model for MANETs was proposed to reflect nodes' behaviour and cope with multiple misbehaving attacks. The model utilised the social property of friendship degrees that is based on combining two social metrics: honesty and confidence. The model is effective in the way dynamic developments of friendships over time were considered to represent the behaviour of nodes in a human manner. Moreover, direct and indirect relationships and the effect of dishonest

information were also considered to help nodes make accurate decisions about the trust relationships with other nodes. The results of the simulation indicated that the proposed model accurately evaluated the behaviour of nodes as in human patterns, and made correct decisions whether to interact with others or not. Chapter 6 further enhanced the trustworthiness evaluation of nodes by proposing a composite multidimensional trust model with more social properties and QoS factors to secure routing protocols in the MANET than the friendship based model. The proposed model is recognised as an applicable model for future MANETs, in which it utilises multiple factors that depends on social and QoS properties of trust to represent the behaviour of nodes in a human manner and reflect the trust complexity. The use of two levels of evaluation includes peer to peer evaluation and path evaluation techniques provided more accurate decisions than the single evaluation metrics. Considering multiple factors instead of depending on a single factor enhanced the evaluation of nodes trustworthiness and this was believed in the way the model enhanced the performance of the network and reduced the effect of bad nodes.

A general conclusion that can be drawn from the results of this research is that the behaviour of nodes can be reflected using appropriate recommendation based trust and reputation models in MANETs. Such models can enhance the cooperation of nodes and cope with multiple misbehaving attacks. Nodes can learn to be able to select their honest neighbours and avoid dishonest nodes based on multidimensional parameters that can be derived from the social and QoS trust during the period of interactions. Social properties of trust can be applied to MANETs to enhance the security level of nodes and help them improve the capability of evaluating others' trustworthiness similarity to human behaviour. The use of

proof of time and location is a promising technique that can be utilised in MANETs' applications which are increasing in future network paradigms including vehicular and robotic ad hoc networks. The proposed techniques enhanced the performance of the network throughput, packet loss, and energy to nearly more than 10% in most the proposed models than the standard settings. False negative and false positive problems in evaluating trustworthiness of nodes are significantly improved. The capability of nodes to survive from being vulnerable to intentionally generated dishonest trust information is also enhanced.

7.2 Future work

In this section, a number of suggestions for the future work are given for the continuation of the work presented in this thesis.

1. In the proposed models, a set of social and QoS properties of trust used to model the behaviour of nodes in MANETs. These models can be extended by using more social and QoS properties to detect any malicious or bad behaving like newly joined nodes or changing identities. Dealing with such attacks is still an open and challenging problem of trust models. A comprehensive study of the effect of social and QoS trust on the trustworthiness evaluation process, and which properties has more importance on the nodes decision is also missing in the trust research. In addition, dynamic weightings and giving different importance to the different factors at different times of nodes' neighborhoods is still an open problem needs to be considered in future.
2. Mobile ad-hoc networks are characterised by constrained resources in terms of communication, memory usage and computational complexity requirements. Besides, such environments suffer from several points of failure which require techniques to enhance the decision making on nodes

trustworthiness. A research to extensively investigate the trade-offs between accuracy of trustworthiness and network performance is desired. Lightweight techniques in gathering and aggregating trust information from different sources can be considered as an important future direction of trust management in MANET.

3. In regard to the recommendation filtering scheme, the proposed filtering technique takes into consideration the dynamic characteristics of MANETs that change over time in which the honesty of recommending nodes is evaluated over a period of time to mitigate the influence of bad behaviour of the same node over time. Due to mobility, the location and number of recommending nodes change over time. Therefore, the proposed defence scheme can be extended by weighting recommendations based on time and location to mitigate the influence of location and time dependent attacks.
4. Marti et al. [19] first introduce the redemption of nodes in case of a node is wrongly identified as a misbehaving node by the trust system. Offering a second chance service for such nodes or even nodes that misbehave intentionally or by forcing the conditional environment can be considered as one future direction to study the redemption friendship of nodes. Incorporating suitable rules to study the self-redemption property of nodes can be used to allow nodes to change their malicious intensions and show good behaviours. Further, identifying and dealing with nodes that may exploit the redemption service to make the system unstable.
5. Although, several trust models to secure routing algorithms in MANETs have been proposed to evaluate node's trustworthiness by monitoring the transmission behavior in case of malicious intentions or node capability, a comprehensive dynamic route optimisation selection algorithm is still open

and challenging problem in trust evaluation. Finding dynamic optimisation rules to efficiently select routes in MANETs is difficult because of MANETs' unique characteristics of mobility and scarcity of resources. Suitable methods like fuzzy logic or ant colony can be used to allow nodes choose the most trustworthy routes (i.e. optimised path) between source and destination.

References

[1] H. Deng, W. Li, and D. P. Agrawal, "Routing security in wireless ad hoc networks," *Communications Magazine, IEEE*, vol. 40, pp. 70-75, 2002.

[2] I. Chlamtac, M. Conti, and J. J.-N. Liu, "Mobile ad hoc networking: imperatives and challenges," *Ad Hoc Networks*, vol. 1, pp. 13-64, 2003.

[3] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," *Wireless Communications, IEEE*, vol. 11, pp. 38-47, 2004.

[4] R. Shankaran, V. Varadharajan, M. A. Orgun, and M. Hitchens, "Context-aware trust management for peer-to-peer mobile ad-hoc networks," in *Computer Software and Applications Conference, 2009. COMPSAC'09. 33rd Annual IEEE International*, 2009, vol. 2, pp. 188-193.

[5] D. Katsaros, N. Dimokas, and L. Tassiulas, "Social network analysis concepts in the design of wireless ad hoc network protocols," *Network, IEEE*, vol. 24, pp. 23-29, 2010.

[6] W. Li, J. Parker, and A. Joshi, "Security through collaboration and trust in manets," *Mobile Networks and Applications*, vol. 17, pp. 342-352, 2012.

[7] J.-H. Cho, A. Swami, and R. Chen, "A survey on trust management for mobile ad hoc networks," *Communications Surveys & Tutorials, IEEE*, vol. 13, pp. 562-583, 2011.

[8] A. A. Pirzada and C. McDonald, "Trust establishment in pure ad-hoc networks," *Wireless Personal Communications*, vol. 37, pp. 139-168, 2006.

[9] W. J. Adams and N. J. Davis IV, "Toward a decentralized trust-based access control system for dynamic collaboration," in *Information Assurance Workshop, 2005. IAW'05. Proceedings from the Sixth Annual IEEE SMC*, 2005, pp. 317-324.

[10] H. Yu, S. Liu, A. C. Kot, C. Miao, and C. Leung, "Dynamic witness selection for trustworthy distributed cooperative sensing in cognitive radio networks," in *Communication Technology (ICCT), 2011 IEEE 13th International Conference on*, 2011, pp. 1-6.

[11] X. Li, F. Zhou, and X. Yang, "A multi-dimensional trust evaluation model for large-scale P2P computing," *Journal of Parallel and Distributed Computing*, vol. 71, pp. 837-847, 2011.

[12] Z. Yan, P. Zhang, and T. Virtanen, "Trust evaluation based security solution in ad hoc networks," in *Proceedings of the Seventh Nordic Workshop on Secure IT Systems*, 2003, vol. 14.

[13] A. A. Pirzada and C. McDonald, "Establishing trust in pure ad-hoc networks," *Proceedings of the 27th Australasian conference on Computer science-Volume 26*, pp. 47-54, 2004.

[14] N. Pissinou, T. Ghosh, and K. Makki, "Collaborative trust-based secure routing in multihop ad hoc networks," in *NETWORKING 2004. Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications*, vol.: Springer, 2004, pp. 1446-1451.

[15] S. Buchegger and J. Y. Le Boudee, "Self-policing mobile ad hoc networks by reputation systems," *Communications Magazine, IEEE*, vol. 43, pp. 101-107, 2005.

[16] R. Li, J. Li, P. Liu, and J. Kato, "A Novel Hybrid Trust Management Framework for MANETs," *Distributed Computing Systems Workshops, 2009. ICDCS Workshops' 09. 29th IEEE International Conference on*, pp. 251-256, 2009.

[17] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," *ACM Transactions on Sensor Networks (TOSN)*, vol. 4, p. 15, 2008.

[18] S. Buchegger and J. Y. Le Boudec, "A Robust Reputation System for P2P and M bile Ad hc Netw rks P2P and Mobile Ad-hoc Networks," 2004.

[19] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proceedings of the 6th annual international conference on Mobile computing and networking*, 2000, pp. 255-265.

[20] P. Michiardi and R. Molva, "Core: A COllaborative REputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks," Presented at Communications and Multimedia Security Conference. Available: [Accessed:

[21] G. Thanigaivel, N. A. Kumar, and P. Yogesh, "TRUNCMAN: Trust based routing mechanism using non-cooperative movement in mobile ad-hoc network," in *Digital Information and Communication Technology and it's Applications (DICTAP), 2012 Second International Conference on*, 2012, pp. 261-266.

[22] B. Wu, J. Chen, J. Wu, and M. Cardei, "A survey of attacks and countermeasures in mobile ad hoc networks," in *Wireless Network Security*, vol.: Springer, 2007, pp. 103-135.

[23] P. Michiardi and R. Molva, "Core: A COllaborative REputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks," *Communications and Multimedia Security Conference*, pp. 107–121, 2002.

[24] K. Paul and D. Westhoff, "Context aware detection of selfish nodes in dsr based ad-hoc networks," in *Global Telecommunications Conference, 2002. GLOBECOM'02. IEEE*, 2002, vol. 1, pp. 178-182.

[25] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decision support systems*, vol. 43, pp. 618-644, 2007.

[26] M. Daignault, M. Shepherd, S. Marche, and C. Watters, "Enabling trust online," in *Electronic Commerce, 2002. Proceedings. Third International Symposium on*, 2002, pp. 3-12.

[27] S. Grabner-Kräuter and E. A. Kaluscha, "Empirical research in on-line trust: a review and critical assessment," *International Journal of Human-Computer Studies*, vol. 58, pp. 783-812, 2003.

[28] A. Abdul-Rahman and S. Hailes, "Supporting trust in virtual communities," in *System Sciences, 2000. Proceedings of the 33rd Annual Hawaii International Conference on*, 2000, p. 9 pp. vol. 1.

[29] J. Sabater and C. Sierra, "Review on computational trust and reputation models," *Artificial intelligence review*, vol. 24, pp. 33-60, 2005.

[30] Z. Yan, V. Niemi, Y. Dong, and G. Yu, "A user behavior based trust model for mobile applications," in *Autonomic and Trusted Computing*, vol.: Springer, 2008, pp. 455-469.

[31] Y. D. Wang and H. H. Emurian, "An overview of online trust: Concepts, elements, and implications," *Computers in human behavior*, vol. 21, pp. 105-125, 2005.

[32] J. Golbeck, "Computing with trust: Definition, properties, and algorithms," in *Securecomm and Workshops, 2006*, 2006, pp. 1-7.

[33] J. Golbeck and J. Hendler, "Inferring binary trust relationships in web-based social networks," *ACM Transactions on Internet Technology (TOIT)*, vol. 6, pp. 497-529, 2006.

[34] J. Liu and V. Issarny, "Enhanced reputation mechanism for mobile ad hoc networks," in *Trust management*, vol.: Springer, 2004, pp. 48-62.
[35] S. Ruohomaa and L. Kutvonen, "Trust management survey," in *Trust Management*, vol.: Springer, 2005, pp. 77-92.
[36] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The eigentrust algorithm for reputation management in p2p networks," in *Proceedings of the 12th international conference on World Wide Web*, 2003, pp. 640-651.
[37] H. Li and M. Singhal, "Trust management in distributed systems," *IEEE Computer*, vol. 40, pp. 45-53, 2007.
[38] H. Yu, Z. Shen, C. Miao, C. Leung, and D. Niyato, "A survey of trust and reputation management systems in wireless communications," *Proceedings of the IEEE*, vol. 98, pp. 1755-1772, 2010.
[39] A. Jøsang and S. L. Presti, "Analysing the relationship between risk and trust," in *Trust Management*, vol.: Springer, 2004, pp. 135-145.
[40] K. Govindan and P. Mohapatra, "Trust computations and trust dynamics in mobile adhoc networks: a survey," *Communications Surveys & Tutorials, IEEE*, vol. 14, pp. 279-298, 2012.
[41] C. H. Soanes, S., *Compact Oxford English Dictionary of Current English*. Oxford: Oxford University Press, 2005.
[42] M. Deutsch, "Cooperation and trust: Some theoretical notes," 1962.
[43] C. Castelfranchi and R. Falcone, "Trust is much more than subjective probability: Mental components and sources of trust," in *System Sciences, 2000. Proceedings of the 33rd Annual Hawaii International Conference on*, 2000, p. 10 pp. vol. 1.
[44] D. Gambetta, "Trust: Making and breaking cooperative relations," 1988.
[45] A. Jøsang, R. Hayward, and S. Pope, "Trust network analysis with subjective logic," in *Proceedings of the 29th Australasian Computer Science Conference-Volume 48*, 2006, pp. 85-94.
[46] T. Grandison and M. Sloman, "Trust management tools for internet applications," in *Trust Management*, vol.: Springer, 2003, pp. 91-107.
[47] E. Chang, T. S. Dillon, and F. K. Hussain, "Trust and reputation relationships in service-oriented environments," in *Information Technology and Applications, 2005. ICITA 2005. Third International Conference on*, 2005, vol. 1, pp. 4-14.
[48] F. G. Mármol and G. M. Pérez, "Security threats scenarios in trust and reputation models for distributed systems," *computers & security*, vol. 28, pp. 545-556, 2009.
[49] P. R. Varadarajan and M. S. Yadav, "Marketing strategy and the internet: an organizing framework," *Journal of the Academy of Marketing Science*, vol. 30, pp. 296-312, 2002.
[50] D.-Q. Li, Y.-Q. Liang, H. Yang, and L.-L. Li, "Study of E-commerce Trust Management Formal Model Based on Reputation," in *ICEE*, 2010, pp. 2253-2256.
[51] R. Maranzato, M. Neubert, A. M. Pereira, and A. P. do Lago, "Feature extraction for fraud detection in electronic marketplaces," in *Web Congress, 2009. LA-WEB'09. Latin American*, 2009, pp. 185-192.
[52] H. Li and M. Singhal, "Trust management in distributed systems," *Computer*, vol. 40, pp. 45-53, 2007.
[53] G. Zacharia and P. Maes, "Trust management through reputation mechanisms," *Applied Artificial Intelligence*, vol. 14, pp. 881-907, 2000.

[54] S. Ba and P. A. Pavlou, "Evidence of the effect of trust building technology in electronic markets: Price premiums and buyer behavior," *MIS quarterly*, pp. 243-268, 2002.

[55] Y. Zhang, K.-J. Lin, and R. Klefstad, "DIRECT: A robust distributed broker framework for trust and reputation management," in *E-Commerce Technology, 2006. The 8th IEEE International Conference on and Enterprise Computing, E-Commerce, and E-Services, The 3rd IEEE International Conference on*, 2006, pp. 21-21.

[56] R. Kerr and R. Cohen, "Towards provably secure trust and reputation systems in e-marketplaces," in *Proceedings of the 6th international joint conference on Autonomous agents and multiagent systems*, 2007, p. 172.

[57] R. Li and J. Li, "Requirements and design for neutral trust management framework in unstructured networks," *The Journal of Supercomputing*, vol. 64, pp. 702-716, 2013.

[58] Y.-F. Wang, Y. Hori, and K. Sakurai, "Characterizing economic and social properties of trust and reputation systems in P2P environment," *Journal of Computer Science and Technology*, vol. 23, pp. 129-140, 2008.

[59] K. Aberer and Z. Despotovic, "Managing trust in a peer-2-peer information system," in *Proceedings of the tenth international conference on Information and knowledge management*, 2001, pp. 310-317.

[60] A. Singh and L. Liu, "TrustMe: anonymous management of trust relationships in decentralized P2P systems," in *Peer-to-Peer Computing, 2003.(P2P 2003). Proceedings. Third International Conference on*, 2003, pp. 142-149.

[61] L. Xiong and L. Liu, "Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities," *Knowledge and Data Engineering, IEEE Transactions on*, vol. 16, pp. 843-857, 2004.

[62] R. Zhou and K. Hwang, "Powertrust: A robust and scalable reputation system for trusted peer-to-peer computing," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 18, pp. 460-473, 2007.

[63] S. Song, K. Hwang, R. Zhou, and Y.-K. Kwok, "Trusted P2P transactions with fuzzy reputation aggregation," *Internet Computing, IEEE*, vol. 9, pp. 24-34, 2005.

[64] R. Cascella and R. Battiti, "Social networking and game theory to foster cooperation," in *2nd ENISA Workshop on Authentication Interoperability Languages, Paris, France*, 2007.

[65] J. Caverlee, L. Liu, and S. Webb, "Socialtrust: tamper-resilient trust establishment in online communities," in *Proceedings of the 8th ACM/IEEE-CS joint conference on Digital libraries*, 2008, pp. 104-114.

[66] J. Sabater and C. Sierra, "Reputation and social network analysis in multi-agent systems," in *Proceedings of the first international joint conference on Autonomous agents and multiagent systems: part 1*, 2002, pp. 475-482.

[67] J. Golbeck, "The dynamics of web-based social networks: Membership, relationships, and change," *First Monday*, vol. 12, 2007.

[68] J. Golbeck, *Computing with social trust*: Springer, 2009.

[69] M. Maheswaran, H. C. Tang, and A. Ghunaim, "Towards a gravity-based trust model for social networking systems," in *Distributed Computing Systems Workshops, 2007. ICDCSW'07. 27th International Conference on*, 2007, pp. 24-24.

[70] S. Nepal, W. Sherchan, and C. Paris, "Strust: A trust model for social networks," in *Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on*, 2011, pp. 841-846.

[71] B. Ali, W. Villegas, and M. Maheswaran, "A trust based approach for protecting user data in social networks," in *Proceedings of the 2007 conference of the center for advanced studies on Collaborative research*, 2007, pp. 288-293.

[72] J. Luo, X. Liu, and M. Fan, "A trust model based on fuzzy recommendation for mobile ad-hoc networks," *Computer Networks*, vol. 53, pp. 2396-2407, 2009.

[73] S. Soltanali, S. Pirahesh, S. Niksefat, and M. Sabaei, "An efficient scheme to motivate cooperation in mobile ad hoc networks," *Networking and Services, 2007. ICNS. Third International Conference on*, pp. 98-98, 2007.

[74] S. Chen, Y. Zhang, Q. Liu, and J. Feng, "Dealing with dishonest recommendation: The trials in reputation management court," *Ad Hoc Networks*, vol. 10, pp. 1603-1618, 2012.

[75] C. Zouridaki, B. L. Mark, M. Hejmo, and R. K. Thomas, "E-Hermes: A robust cooperative trust establishment scheme for mobile ad hoc networks," *Ad Hoc Networks*, vol. 7, pp. 1156-1168, 2009.

[76] P. B. Velloso, R. P. Laufer, D. de O Cunha, O. C. M. Duarte, and G. Pujolle, "Trust management in mobile ad hoc networks using a scalable maturity-based model," *Network and Service Management, IEEE Transactions on*, vol. 7, pp. 172-185, 2010.

[77] H. Yu, S. Liu, A. C. Kot, C. Miao, and C. Leung, "Dynamic witness selection for trustworthy distributed cooperative sensing in cognitive radio networks," *Communication Technology (ICCT), 2011 IEEE 13th International Conference on*, pp. 1-6, 2011.

[78] J.-H. Cho, A. Swami, and R. Chen, "Modeling and analysis of trust management for cognitive mission-driven group communication systems in mobile ad hoc networks," in *Computational Science and Engineering, 2009. CSE'09. International Conference on*, 2009, vol. 2, pp. 641-650.

[79] L. Yu, C. Qian, Z. Liu, K. Wang, and B. Dai, "Ad-hoc multi-dimensional trust evaluation model based on classification of service," in *Communications and Networking in China (CHINACOM), 2010 5th International ICST Conference on*, 2010, pp. 1-5.

[80] C. Dellarocas, "Reputation mechanisms," *Handbook on Economics and Information Systems*, pp. 629-660, 2006.

[81] S. Phelps, P. McBurney, and S. Parsons, "Evolutionary mechanism design: a review," *Autonomous Agents and Multi-Agent Systems*, vol. 21, pp. 237-264, 2010.

[82] S. Ba, A. B. Whinston, and H. Zhang, "Building trust in online auction markets through an economic incentive mechanism," *Decision support systems*, vol. 35, pp. 273-286, 2003.

[83] L. I. Li, "Reputation, trust, and rebates: How online auction markets can improve their feedback mechanisms," *Journal of Economics & Management Strategy*, vol. 19, pp. 303-331, 2010.

[84] C. Buragohain, D. Agrawal, and S. Suri, "A game theoretic framework for incentives in P2P systems," *arXiv preprint cs/0310039*, 2003.

[85] R. Gupta and A. K. Somani, "Game theory as a tool to strategize as well as predict nodes' behavior in peer-to-peer networks," in *Parallel and Distributed Systems, 2005. Proceedings. 11th International Conference on*, 2005, vol. 1, pp. 244-249.

[86] S. M. Allen, M. J. Chorley, G. Colombo, and R. M. Whitaker, "Incentivising cooperation between agents for content sharing," in *Web Intelligence and Intelligent Agent Technology (WI-IAT), 2010 IEEE/WIC/ACM International Conference on*, 2010, vol. 2, pp. 79-84.

[87] G. Colombo, R. M. Whitaker, and S. M. Allen, "Cooperation in Social Networks of Trust," in *Self-Adaptive and Self-Organizing Systems Workshops, 2008. SASOW 2008. Second IEEE International Conference on*, 2008, pp. 78-83.

[88] V. Srinivasan, P. Nuggehalli, C.-F. Chiasserini, and R. R. Rao, "Cooperation in wireless ad hoc networks," in *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, 2003, vol. 2, pp. 808-817.

[89] M. Felegyhazi, J.-P. Hubaux, and L. Buttyan, "Nash equilibria of packet forwarding strategies in wireless ad hoc networks," *Mobile Computing, IEEE Transactions on*, vol. 5, pp. 463-476, 2006.

[90] S. K. Bista, K. Dahal, P. Cowling, and B. M. Tuladhar, "Evolution of Cooperativeness in a Business Game Relying on Acquaintance Based Trustworthiness Assessment," in *Commerce and Enterprise Computing, 2009. CEC'09. IEEE Conference on*, 2009, pp. 16-23.

[91] W. Yu and K. R. Liu, "Game theoretic analysis of cooperation stimulation and security in autonomous mobile ad hoc networks," *Mobile Computing, IEEE Transactions on*, vol. 6, pp. 507-521, 2007.

[92] S. K. Bista, K. Dahal, P. Cowling, and A. Bouras, "Assessing trustworthiness of nodes to enhance performance in mobile ad hoc networks," in *Privacy Security and Trust (PST), 2010 Eighth Annual International Conference on*, 2010, pp. 80-87.

[93] L. A. Zadeh, "Fuzzy sets," *Information and control*, vol. 8, pp. 338-353, 1965.

[94] S. Nefti, F. Meziane, and K. Kasiran, "A fuzzy trust model for e-commerce," in *E-Commerce Technology, 2005. CEC 2005. Seventh IEEE International Conference on*, 2005, pp. 401-404.

[95] Z. Wei, L. Lu, and Z. Yanchun, "Using fuzzy cognitive time maps for modeling and evaluating trust dynamics in the virtual enterprises," *Expert Systems with Applications*, vol. 35, pp. 1583-1592, 2008.

[96] H. Chen and Z. Ye, "Research of P2P Trust based on Fuzzy Decision-making," in *Computer Supported Cooperative Work in Design, 2008. CSCWD 2008. 12th International Conference on*, 2008, pp. 793-796.

[97] M. Lesani and S. Bagheri, "Applying and inferring fuzzy trust in semantic web social networks," in *Canadian Semantic Web*, vol.: Springer, 2006, pp. 23-43.

[98] Y.-M. Li and C.-P. Kao, "TREPPS: A trust-based recommender system for peer production services," *Expert Systems with Applications*, vol. 36, pp. 3263-3277, 2009.

[99] H. Xia, Z. Jia, L. Ju, and Y. Zhu, "Trust management model for mobile ad hoc network based on analytic hierarchy process and fuzzy theory," *IET wireless sensor systems*, vol. 1, pp. 248-266, 2011.

[100] A. Jøsang, "Trust and reputation systems," in *Foundations of security analysis and design IV*, vol.: Springer, 2007, pp. 209-245.

[101] M. K. Deno and T. Sun, "Probabilistic trust management in pervasive computing," in *Embedded and Ubiquitous Computing, 2008. EUC'08. IEEE/IFIP International Conference on*, 2008, vol. 2, pp. 610-615.

[102] A. Jsang and R. Ismail, "The beta reputation system," in *Proceedings of the 15th bled electronic commerce conference*, 2002, pp. 41-55.
[103] P. Dong, H. Wang, and H. Zhang, "Probability-based trust management model for distributed e-commerce," in *Network Infrastructure and Digital Content, 2009. IC-NIDC 2009. IEEE International Conference on*, 2009, pp. 419-423.
[104] Y. Wang and J. Vassileva, "Trust and reputation model in peer-to-peer networks," in *Peer-to-Peer Computing, 2003.(P2P 2003). Proceedings. Third International Conference on*, 2003, pp. 150-157.
[105] B. Yu, M. P. Singh, and K. Sycara, "Developing trust in large-scale peer-to-peer systems," in *Multi-Agent Security and Survivability, 2004 IEEE First Symposium on*, 2004, pp. 1-10.
[106] U. Kuter and J. Golbeck, "Sunny: A new algorithm for trust inference in social networks using probabilistic confidence models," in *AAAI*, 2007, vol. 7, pp. 1377-1382.
[107] G. Liu, Y. Wang, and M. Orgun, "Trust inference in complex trust-oriented social networks," in *Computational Science and Engineering, 2009. CSE'09. International Conference on*, 2009, vol. 4, pp. 996-1001.
[108] J. Li, R. Li, and J. Kato, "Future trust management framework for mobile ad hoc networks," *Communications Magazine, IEEE*, vol. 46, pp. 108-114, 2008.
[109] F. Li and J. Wu, "Uncertainty modeling and reduction in MANETs," *Mobile Computing, IEEE Transactions on*, vol. 9, pp. 1035-1048, 2010.
[110] Z. Wei, H. Tang, F. R. Yu, M. Wang, and P. Mason, "Security Enhancements for Mobile Ad Hoc Networks with Trust Management Using Uncertain Reasoning," 2014.
[111] F. Bao, R. Chen, M. Chang, and J.-H. Cho, "Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection," *Network and Service Management, IEEE Transactions on*, vol. 9, pp. 169-183, 2012.
[112] J. Liu and V. Issarny, "An incentive compatible reputation mechanism for ubiquitous computing environments," *International Journal of Information Security*, vol. 6, pp. 297-311, 2007.
[113] E. Weisstein, W., "Gamma Function." http://mathworld.wolfram.com/: MathWorld--A Wolfram Web Resource, 2010.
[114] C. Zouridaki, B. L. Mark, M. Hejmo, and R. K. Thomas, "A quantitative trust establishment framework for reliable data packet delivery in MANETs," in *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*, 2005, pp. 1-10.
[115] Y. L. Sun, Z. Han, and K. R. Liu, "Defense of trust management vulnerabilities in distributed networks," *Communications Magazine, IEEE*, vol. 46, pp. 112-119, 2008.
[116] M. K. Denko, T. Sun, and I. Woungang, "Trust management in ubiquitous computing: A Bayesian approach," *Computer Communications*, vol. 34, pp. 398-406, 2011.
[117] T. Issariyakul and E. Hossain, *Introduction to network simulator NS2*: Springer, 2011.
[118] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," in *Mobile computing*, vol.: Springer, 1996, pp. 153-181.

[119] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA'99. Second IEEE Workshop on*, 1999, pp. 90-100.

[120] C. Bettstetter, G. Resta, and P. Santi, "The node distribution of the random waypoint mobility model for wireless ad hoc networks," *Mobile Computing, IEEE Transactions on*, vol. 2, pp. 257-269, 2003.

[121] H. Simaremare, A. Syarif, A. Abouaissa, R. F. Sari, and P. Lorenz, "Performance comparison of modified AODV in reference point group mobility and random waypoint mobility models," Presented at Communications (ICC), 2013 IEEE International Conference on. Available: [Accessed:

[122] J.-L. Huang and M.-S. Chen, "On the effect of group mobility to data replication in ad hoc networks," *Mobile Computing, IEEE Transactions on*, vol. 5, pp. 492-507, 2006.

[123] Y. Yu, K. Li, W. Zhou, and P. Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures," *Journal of network and computer applications*, vol. 35, pp. 867-880, 2012.

[124] F.-H. Tseng, L.-D. Chou, and H.-C. Chao, "A survey of black hole attacks in wireless mobile ad hoc networks," *Human-centric Computing and Information Sciences*, vol. 1, pp. 1-16, 2011.

[125] G. F. Lucio, M. Paredes-Farrera, E. Jammeh, M. Fleury, and M. J. Reed, "Opnet modeler and ns-2: Comparing the accuracy of network simulators for packet-level analysis using a network testbed," *WSEAS Transactions on Computers*, vol. 2, pp. 700-707, 2003.

[126] C. Cicconetti, E. Mingozzi, and G. Stea, "An integrated framework for enabling effective data collection and statistical analysis with ns-2," in *Proceeding from the 2006 workshop on ns-2: the IP network simulator*, 2006, p. 11.

[127] A. Robbins, *Effective AWK Programming: Text Processing and Pattern Matching*: " O'Reilly Media, Inc.", 2001.

[128] Z. Liu, S. Lu, and J. Yan, "Secure routing protocol based trust for ad hoc networks," in *Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2007. SNPD 2007. Eighth ACIS International Conference on*, 2007, vol. 1, pp. 279-283.

[129] R. Li, J. Li, P. Liu, and J. Kato, "A Novel Hybrid Trust Management Framework for MANETs," in *Distributed Computing Systems Workshops, 2009. ICDCS Workshops' 09. 29th IEEE International Conference on*, 2009, pp. 251-256.

[130] J. Cai, P. Yi, J. Chen, Z. Wang, and N. Liu, "An adaptive approach to detecting black and gray hole attacks in ad hoc network," *Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on*, pp. 775-780, 2010.

[131] K. Hoffman, D. Zage, and C. Nita-Rotaru, "A survey of attack and defense techniques for reputation systems," *ACM Computing Surveys (CSUR)*, vol. 42, p. 1, 2009.

[132] Y. Ma, H. Lu, and Z. Gan, "An Improved Direct Trust Evaluation Algorithm for the Context-Aware Trust Model," in *Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2013 Seventh International Conference on*, 2013, pp. 196-201.

[133] N. Lathia, S. Hailes, and L. Capra, "Trust-based collaborative filtering," in *Trust Management II*, vol.: Springer, 2008, pp. 119-134.

[134] G. Theodorakopoulos and J. S. Baras, "Trust evaluation in ad-hoc networks," *Proceedings of the 3rd ACM workshop on Wireless security*, pp. 1-10, 2004.

[135] G. V. Crosby, L. Hester, and N. Pissinou, "Location-aware, Trust-based Detection and Isolation of Compromised Nodes in Wireless Sensor Networks," *International Journal of Network Security*, vol. 12, pp. 107-117, 2011.

[136] C. Zouridaki, B. L. Mark, M. Hejmo, and R. K. Thomas, "Hermes: A quantitative trust establishment framework for reliable data packet delivery in MANETs," *Journal of Computer Security*, vol. 15, pp. 3-38, 2007.

[137] E. M. Daly and M. Haahr, "Social network analysis for information flow in disconnected delay-tolerant MANETs," *Mobile Computing, IEEE Transactions on*, vol. 8, pp. 606-621, 2009.

[138] N. Vastardis and K. Yang, "Mobile Social Networks: Architectures, Social Properties, and Key Research Challenges," *Communications Surveys & Tutorials, IEEE*, vol. 15, pp. 1355-1371, 2013.

[139] F. Bao, I.-R. Chen, M. Chang, and J.-H. Cho, "Hierarchical trust management for wireless sensor networks and its application to trust-based routing," in *Proceedings of the 2011 ACM Symposium on Applied Computing*, 2011, pp. 1732-1738.

[140] F. Nazir, J. Ma, and A. Seneviratne, "Time critical content delivery using predictable patterns in mobile social networks," in *Computational Science and Engineering, 2009. CSE'09. International Conference on*, 2009, vol. 4, pp. 1066-1073.

[141] E. Bulut and B. K. Szymanski, "Friendship based routing in delay tolerant mobile social networks," in *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*, 2010, pp. 1-5.

[142] E. M. Daly and M. Haahr, "Social network analysis for routing in disconnected delay-tolerant manets," in *Proceedings of the 8th ACM international symposium on Mobile ad hoc networking and computing*, 2007, pp. 32-40.

[143] H. Xia, Z. Jia, X. Li, L. Ju, and E. H.-M. Sha, "Trust prediction and trust-based source routing in mobile ad hoc networks," *Ad Hoc Networks*, vol. 11, pp. 2096-2114, 2013.