Trust-Based Protocols For Secure Collaborative Routing in Wireless Mobile Networks

By

Aminu Bello Usman

SUBMITTED IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY
AT
AUCKLAND UNIVERSITY OF TECHNOLOGY
AUCKLAND, NEW ZEALAND
2018

To all those who helped me in my life.

Table of Contents

List of Tables

List of Figures

Table 1: Glossary and Notations

Notations	**Meaning**
$T_{coef(p)}$	Transitivity Coefficient of peer p
$av.Tra(N)$	Average Network Transitivity Coefficient
$Av.SPath(p->q)$	Average Shortest Path Between peer p and q
$CC(p)$	Closeness Centrality of peer p
$E(p->q)$	Energy Required for peer p to Communicate with peer q
$Dis(p,q)$	Distance Between peer p and peer q
$E_{loc}(N)$	Local Network Efficiency
Eg	Average Network Efficiency
$Av.D$	Average Distance Between peers in the Network
$Av.Acc.$	Average Accuracy of Trust and Reputation Model
$Av.En$	Average Energy of Trust Model Execution in the Network
A_p	Set of peers' attributes
$t_p^{(0)} = init(p)$	Initial trust of peer p
$t_{p,q}$	Local Trust Between peer p and peer q
$T_{p,q}$	Global Trust Between peer p and peer q
n_{preT}	Number of Pre-Trusted peers in the Network
$C_{p,q}$	Local Reputation Between peer p and q
$sat(p,q)$	Number of Satisfactory Transaction Between p and q
$unsat(p,q)$	Number of Unsatisfactory Transactions Between p and q
$\vec{t_p}$	Global Trust Vector of peer p
$\tau_{max}(a_q)$	Maximum Attributes Value of peer q
$\tau_{curr}(a_q)$	Peers' Current Attributes Value
$\hat{T}_{p,q}$	Global-Reliability Trust value of peer q computed by peer p
$d_{(a_p,a_q)}$	Difference Between peer ps' and peer qs' Attributes
$S_{(A_p,A_q)}$	Similarity Between peer p and peer q Attributes
$S_{p,q}$	Similarity Between peer p and peer q
$\dot{T}_{p,q}$	Global-Reliability Reputation value of peer q computed by peer p
N_{mf}	Number of Messages forwarded
M_{OH}	Total Messages' Overhead
N_{md}	Number of Messages Delivered
$deg(p)$	Degree of peer p
$T\dot{S}(q,d_{es})$	Transitive Coefficient Similarity of peer p with Messages' Destination
$T-Trust$	Transitive Trust Forwarding Strategy
$(dr_{q,Dist})$	Delivery Predictability of peer q with the Destination
Π_p^+	Packets Receiving Potential of peer p
Π_p^-	Packets' Forwarding Potential of peer p
$pr_{(p,q)}$	Probability of peer q Forwarding Record noted by peer p
$cov(\Pi^{*+},\Pi^{*-})_p$	Covariance of peer p Forwarding and Receiving Records
$\rho(\Pi^{*+}\Pi^{*-})_p$	Correlation of peer p Forwarding and Receiving Records

Attestation of Authorship

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

Aminu Bello Usman
AUT, New Zealand.

Abstract

In the context of Mobile Wireless Networks, researchers have proposed different collaborative routing schemes with fundamental objectives to maximise packet delivery, and minimise latency through improving peer routing decisions. One promising approach adopted by researchers to improve peers routing decisions is a trust-based routing mechanism. Trust-based routing protocols have several advantages including a better routing distribution strategy between wireless mobile peers and reliable forwarding decisions. The trust-based protocol enables peers in the network to dynamically forward data to a corresponding reliable and trustworthy peer for routing decisions and next peer selection strategy which can preserve the peers' routing resources. This reduces the queuing delay and prevents routing attacks in the network.

Along with several advantages of trust-based forwarding protocols, however, most of the current trust-based protocols of wireless mobile networks enable peers to make routing decisions based on trust relationships that manifest among peers but with less concern about the peers' attributes. This further makes the design of efficient, collaborative routing protocols a challenging task due to the high dynamics of peers' characteristics and mobility.

In this study, we developed an efficient routing decision strategy to provide efficient, secure and higher quality communication between wireless mobile devices.

Firstly, we explored the properties of complex networks and their impacts on trust and reputation propagation and evaluations, and presented the network performance analytical metrics for the design of an efficient trust-based forwarding protocol. Based on the theoretical, analytical and simulation studies observed in the study, we understand that the transitive contacts between the peers can be metrics elements of a trust-based routing protocol forwarding strategy.

Secondly, we designed a Dynamic Attributes Trust Model for Efficient Collaborative Routing (DATM): a trust-based scheme to enforce collaborative behaviour in wireless mobile networks taking into consideration the peers' attributes for an efficient routing scheme. DATM is a generic mechanism that can be integrated into any packet forwarding strategy or network management function to enable peers in the network to identify

reliable, trustworthy peers for routing handling.

Thirdly, based on the empirical evidence we exploited the existence of similar transitive contact patterns in the real data sets of Mobile Social Networks (MSNs). Therefore, we utilised the identified transitive connectivity properties to propose a new transitive data forwarding strategy which considers the similarity of transitive connectivity between peers for a data forwarding strategy. Our proposed transitive forwarding strategy gives preference to the peers with increasing transitive connectivity similarity to the messages' destination to improve the chances of message carriers delivering the message to the correct destination.

Finally, we proposed a model for evaluating the probability of the peers' forwarding and receiving potentials for local trust evaluations based on peers' forwarding and receiving potentials. In this regard, we introduced a correlation matrix for evaluating peers' global trust values to improve the routing performance and mitigate the malicious effect of attacking peers in the network. Then we leveraged our proposed attributes similarity analytical model and transitive contact model for the design of an efficient forwarding strategy between peers in the network. The advantage of the proposed Forward-Watcher approach is that through routing history created by the peers, it can statistically predict the future behaviour of their corresponding routing partners. The concept can also serve as an underpinning and cornerstone for developing self-cooperative protocols in wireless mobile networks using statistical analysis and correlation matrices.

Acknowledgments

I would like to express my sincere gratitude to my supervisor, Associate Professor Jairo Gutierrez, for his support and consistent feedback in my PhD studies. I enjoyed his mature and unreserved assistance to me during my difficult times as a PhD student, and I particularly appreciated his attitude, spirit and experience of research supervision. If I have the opportunity, I would love to work with him again.

I thank Dr Quan Bai for his assistance and contributions as my secondary supervisor, and it is my pleasure to thank Dr William Liu and Professor Ajit Narayanan. Without their support and understanding, this research could not have been brought to this stage.

I would like to thank all my academic colleagues in the Faculty of FCSIT, Bayero University, Kano, Nigeria and the entire Bayero University, Kano for all their support while conducting this study. I also express my appreciation to the members of Network Security Research Group, Auckland University of Technology, New Zealand and the members of WT404 Lab, with whom I shared very good times and valued their comments and feedback during my PhD studies.

My gratitude also extends to my late father, Alhaji Bello Usman, and his entire family. Special gratitude goes to my Mum, Hajiya Salamatu, who has been praying, assisting and helping me all my life; and above all, standing firm and strong to see that I am the person I am today.

I wish to express my gratitude to my wife, Nabeelah Naseer Ismaeel, for all the love, caring and understanding through this difficult time, and I thank her for wonderful support during my studies.

Finally, to my children, Muhammad Aminu Bello and Nasir Aminu Bello, for coming into my life and giving me beautiful joy and moral support to become a stronger and fully-fledged father.

Chapter 1

Introduction

This chapter presents the background of the studies, the motivation and the primary objectives of the research. The chapter also contains the problem statements, research questions, research hypotheses and research contributions.

1.1 Background

Emerging wireless embedded networks are equipped with unprecedented capabilities regarding communication, computation, storage and sensing. Today, human beings have experienced a development of worldwide communication networks that connect people to machines, and machines to machines. Further, recent developments in technology (e.g., environmental monitoring systems, intelligent transport systems and disaster monitoring and evaluation using embedded wireless sensor devices) are poised to reshape every aspect of the technology landscape: operational efficiency, quality of service, decision-making in routing process and efficient communications between peers. The generalisability of the communication mode of wireless mobile devices follows the peer-to-peer network paradigm; a communication mode that allows two or more devices to communicate with each other directly instead of through a central wireless access point. Thus, the models of mobile wireless communication and applications tend to give rise to spatially heterogeneous peer distributions and employ a distributed, multi-hop

network architecture in which peers are equally privileged participants in the networking and routing processes.

There are several application areas of wireless mobile networks for commercial, military and domestic purposes: for example, Delay Tolerant Networks (DTNs),Vehicle Ad-hoc Networks (VANETs), Mobile Adhoc Networks (MANETs), and SensorActuator Networks (SANETs). Some of the applications such as the deployment of low-cost Internet provision in remote or developing communities, underwater acoustic sensor networks and a network that operates in mobile or extreme terrestrial environments, will continue to emerge due to the tremendous growth in the use of mobile wireless communication. Given the different application domains, efficient routing in a wireless mobile network can be very challenging and exhibits different deployment, security and implementation considerations. Subsequently, the communication protocols in wireless mobile networks and routing strategies require different approaches and protocol engineering from those applied in various communication architectures [4],[5].

Debate continues on reliable and secure routing communication strategies of wireless mobile devices and applications in peer-to-peer (P2P) wireless architecture. One distinctive aspect of wireless mobile communication networks is the provision of a secure, resilient routing mechanism between wireless peers [6]. Routing is therefore, a fundamental mechanism in recent and future wireless P2P communication networks, and it is critical to ensure the availability of routing data and to prevent routing attacks.

Routing between wireless peers is a process by which information is passed from source to destination, via a series of intermediary wireless peers.

So far, however, there has been little discussion in the domain of secure and reliable data forwarding strategies in wireless mobile networks. What is not yet clear is how the

communication strategies between wireless devices can accommodate the rapid advancement and dynamic changes of wireless mobile architecture, protocols and applications? How can a peer in the network understand the status of its communication partners (genuine or malicious)? [7] Can a peer trust any encountered peer in the network for data handling? How can the peers in the network perform self-organization processes to provide a secure network paradigm with a high quality service? All these questions and many more are still in the archives of the literature waiting for an appropriate solution for the realisation of secure and efficient wireless mobile networks.

Moreover, one of the challenging aspects of protocol design in wireless mobile communication is the dynamic and distributed nature of wireless peers in the process of packet forwarding, network traffic control, selecting a good relaying peer or selecting the best possible path for data forwarding [8]. As a consequence, the need for collaborative routing between devices has emerged. The resultant collaborative routing task between peers empowers the peers to engage in greater routing tasks beyond those that can be accomplished by individual peers in the network [9] and it helps the peers in making collective routing decisions and judgements about the behaviour and actions of other peers in the network.

Collaborative routing between peers improves the peers' wireless communication efficiency [10]; resulting in efficient packet routing and data forwarding, jamming prevention and minimisation of end-to-end delay and latency [11], as well as improving data-centric behaviour of many wireless applications [12].

In a collaborative routing scheme, a peer may altruistically contribute its resources or serve as a good relay peer for the satisfaction of being an active contributor, or for the recognition (increase in popularity level) gained. Also, peers can collaborate and

cooperate in the processes of traffic relaying, outlier analysis and next neighbour selection to maximise total network throughput by using all the available peers for routing and data forwarding. This perception made it clear that the more the peers participate positively in the routing processes, the higher the network performance and the higher the chance for the network to be protected from denial of service attacks.

However, the collaborative routing mechanism, along with its advantages brings some challenges such as information error and losses caused by component failure of peers in the network, external interference, wireless transmission error and excessive packet drops [13] which can adversely affect the delivery performance of data communication in the network. Therefore, the success of collaborative routing mechanisms between wireless devices mainly depend on the extent to which the peers can make an efficient routing decision through identifying good relaying peers, non-selfish peers and reliable peers in the network.

To this end, several pieces of literature have proposed that the dynamic, autonomous nature of peers in collaborative routing mechanisms makes it difficult for the peers to have a predefined basis for the self-routing decision which can result in different non-uniform request distributions, and may lead to poor routing and unbalanced load distribution in the network [14, 15]. In addition, due to certain inherent peers' dynamic attributes (buffer, energy, connectivity, etc), dynamic routing behaviour (good or selfish routing behaviour) and limited resources, a peer can succeed in promoting different selfish behaviour in the network which can contribute to degrading the quality of communication between the peers involved in collaborative routing [16, 8].

Furthermore, the properties of self-cooperation, self-organization and self-control systems of wireless mobile networks in collaborative routing do not come into existence

automatically. They need to be enforced and managed so that the devices and the protocols of wireless P2P can be prepared to overcome different problems of variable conditions, faulty nodes and any strange or malicious behaviour in the network. Therefore, a distributed alternative mechanism is needed to achieve a high level of quality of service while minimising the resources used. In this line, the premise for self-cooperative, altruist behaviour monitoring is the trustworthiness of a peer, which needs to be established, observed and monitored for the peers' routing behaviour control and surveillance. Previous studies have shown that a cooperation and collaboration enforcement mechanism between the peers using the concept of trust and reputation, can increase the probability of network performance and quality of service [17] and provide peers with the best strategy for choosing a best relaying peer for routing collaboration.

Over the years, several scholars have resorted to going back to the drawing board in different fields of studies including social sciences to borrow the concept of trust and reputation as an alternative strategy for addressing the problem of peers' dynamic behaviour, trustworthiness, reliability evaluations and prediction. The basic idea behind trust and reputation in collaborative routing in wireless mobile networks is for the peers to rate each other and then use the aggregated trust rankinag and scoring to derive trust scores, which can assist peers in deciding whether to collaborate or not to collaborate in the future tasks.

Trust is a relationship between trustee and trustors which can easily be interpreted from the actions of the peers involved. However, the nature and the process of trust and reputation management in collaborative routing networks requires a series of message transfers between the peers in the network; thus, the management of trust and reputation systems needs to take into consideration the applications' requirements, relationships between the peers (peers' connectivity and location of peers in the network),

peers' attributes and peers' specifications for efficient trust-based routing management.

A lot of efforts have been made to build trust mechanisms in different P2P technologies such as Distributed Ledger Technology (DLT). Distributed ledgers use independent computers (referred to as nodes) to record, share and synchronize transactions in their respective electronic ledgers (instead of keeping data centralized as in a traditional ledger)[18]. In a DLT Each node in a P2P network owns a full and up-to-date copy of the entire ledger. Every proposed local addition to the ledger by a network participant is communicated across the network to all nodes. Nodes collectively validate the change through an algorithmic consensus mechanism and exchange data [19]. However, it can be difficult to gather accurate, real-time data between nodes. With the advent of the Internet of Things (IoT), some of these difficulties are being addressed with low-cost commodity hardware, but this is potentially vulnerable to attack. Trust mechanism. Different studies in the literature have shown that the formation of effective cooperation, norms and trust in the IoT network largely depend on the type of the agents (their characteristics) and the relationship between interacting agents [20]. This equally goes in line with the concept of the elements of cooperative behaviour monitoring strategy in the wireless P2P networks proposed in [21] and the impact of connectivity between trustor and trustee for reliable trust evaluation [22].

The focus of this study is on trust-based forwarding decisions in wireless routing protocols of the mobile network. Since a message forwarding decision must be made for every message handled by a peer in the network, the reader should bear in mind that all the schemes proposed in this thesis are device-to-device forwarding schemes. It is beyond the scope of this thesis to explain the details of end-to-end routing mechanisms. Thus, the approach presented in this thesis is based on a trust and reputation scheme, which is widely used as a basis for the security mechanism to mitigate the problem of

peer misbehaviour in the networks [23, 24].

The principle of trust and reputation in our proposed concept is for the peers to rate each other and then use the aggregated trust ratings to derive trust scores, which can assist peers in deciding whether to collaborate or not to collaborate in their future tasks. Therefore, throughout this thesis, the peers' routing decisions are based on the established relationship between the peers in the network through credential exchanges and peers' attributes for peer reliability evaluation.

1.2 Motivation

Arising from the background statements, we here highlight some of the motivations of this research:

- The efficient forwarding decision between the peers is a fundamental property of a secure and reliable communication network. For example, in many mobile wireless networks, peers are expected to utilise their limited resources for routing functions (next peer selection, data forwarding, etc.) with the probability of higher packet delivery. Due to the distributed nature of the wireless mobile network, a peer may fail to appropriately identify a good forwarding peer in the network. This problem can be addressed when all the peers can perform self-routing decisions through the identification of a corresponding reliable, non-selfish (based on the peers' routing history) and capable peer (based on the peers' routing attributes) for data forwarding. Thus, it will be of great value to perform an in-depth analysis and to advance our understanding on how to develop a secure and self-cooperative routing scheme.

- Trust and reputation mechanisms are becoming the key instruments for designing a secure, reliable and efficient routing protocol in wireless mobile networks. One

of the most important features of trust and reputation mechanisms is that, contrary to many secure routing schemes, trust and reputation based systems provide means for adaptive and dynamic decision-making processes between peers at individual peer level behaviour. Such features are essential in networks that exhibit dynamicity in peer behaviour like that of wireless mobile networks [25]. However, there is an increasing concern [26, 27], that despite the efficacy of trust and reputation mechanisms' routing protocols, trust-based routing decisions suffer from several major drawbacks, taking into consideration peer reliability and peer routing attributes as additional trust evaluation elements for a reliable and proper trust-based protocol. Therefore, it will be of great value if a trust-based protocol that combines the metrics of peer trust behaviour and peer attributes can be realised.

- Many mobile wireless communication network operations are highly dependent on peer cooperation and coordination. This implies that, the performance and security interests of a peer are not limited to the peer itself but include the entire network and other peers' behaviour. Subsequently, peers' trust scoring behaviour is one type of information that contributes to peer routing decision making, and it affects other peer decisions as well. Thus, the security system should have the feature of a consulted and well-analyzed decision-making and behaviour mechanism, which is one of the characteristics of trust and reputation system routing models. Along with these advantages of a trust-based protocol, however, there is increasing concern over how to improve the efficacy of peer routing decisions in wireless mobile networks.

- During a disaster period, a candidate device for efficient and reliable communication is required for collaborative routing and node selection. At a point in time,

all the devices may be busy performing a routing task which can lead to many devices lacking adequate capacity to participate in a collaborative routing function. It is essential for the devices to be able to locate a corresponding reliable peer that is capable of handling data transmission. A question has been raised [28] "how can a peer in the network understand the resource level of its subject while making a correct routing decision?". Thus, it interests us to understand how to incorporate peer attributes into a trust-based routing process for peer reliability trust evaluations.

1.3 Problem Statements

Most existing routing schemes for Wireless P2P networks (e.g., WSN, MANETs, SANETs, etc.) make the assumption that the devices are usually cooperative in data forwarding and security control. In principle, this assumption might not always be correct. For example, in a Smart Power Monitoring System using Wireless Sensor Networks, a node may fail to participate in the collaborative task and data forwarding appropriately. As a result, the reading of the electrical parameters such as voltage, current and power of household appliances may not be accurately captured. This problem can lead to false meter readings, inaccurate load characterization and failure of outage detection or restoration, thus reducing smart grid stability and reliability. Therefore, making such assumptions may not reflect the real nature of collaborative routing in P2P wireless networks.

Also, some routing protocols pose that in a cooperative P2P wireless network environment, peers can interact with each other with no malicious behaviour. This, however, may not be a valid supposition in practice. For several reasons, e.g., peer malfunction, tampering by an adversary or peers' selfish behaviour, can cause the entire network

to cease to behave as anticipated. Another major challenge in collaborative routing is the unavailability of peer resources. For example, a peer may misbehave by refusing to forward a data packet because it is exhausted, overloaded, malicious or worn out [29]. Also, a peer may lack the CPU cycles for routing handling if it is overloaded, with limited buffer space or limited battery level. A malicious peer can launch a denial of service attack by dropping the data packet it received instead of forwarding it to the destination or the next near neighbour. In return, the network performance can be degraded with lots of packet drops and delays [30]. Therefore, for a routing scheme to achieve the anticipated collaborative routing, a proper trust evaluation needs to be in place so that the peers can dynamically evaluate the trustworthiness of their potential routing partners and determine the best possible corresponding peer for routing selection.

However, most of the existing trust and reputation models have focused on accurate reputations and peer trust value evalutions based on the successful transaction between the peers for stable routing systems, but they have not examined the influence of peer routing attributes, peer forwarding and receiving behaviour, peer preference and the influence of connectivity between peers concerning trust and reputation evaluation. As a result, prior research has shown that, the peer trust scoring behaviour of many trusts and reputation models is imperfect, noisy and prone to many security issues which limits their predictive power for efficient trust and reputation evaluation [31, 32].

In this line, several questions remain unanswered. For instance; can an arbitrary peer in a wireless mobile network be trusted for message handling? And to what degree? How can the decision trust value of a peer be captured to predict a peers' attributes and capabilities? Can the peers' routing (forwarding and receiving) behaviour be appropriately obtained and consistent to give a reliable basis for the prediction of the peers' trust

level in handling the routing task? How can the contextual peers' attribute correlation be captured and analysed for the peers' decision making? Obviously, to answer these questions, there is a need for numerous studies to bridge the gap between transactions based trust evaluation and attributes based trust evaluation. Thus, peer attributes can be a contributing factor for making efficient and correct trust evaluations. There is also a need for a conceptual trust model that can accurately learn the peers' routing behaviour to determine their forwarding and receiving accuracy for efficient trust evaluation.

1.4 Research Questions

This thesis will examine the four main research questions presented below:

- The first question this thesis asks is: "which category of the wireless peers' connectivity (contacts) can facilitate effective trust evaluation between peers, and by extension enhance collaborative routing decisions in wireless mobile networks?".
  - To attempt the above first question, another question needs to be asked: "Is there any correlation between the identified peers' connectivity category and network performance metrics which are essential considerations in the design of routing protocols?".
- The second question seeks to address how to build a dynamic trust model that takes into account the dynamic changes of peer routing attributes for efficient trust evaluations.
- The third question is: "how can the peers' contacts and connectivity in a wireless network be leveraged for the design of an efficient trust-based routing protocol?" To answer this question, we identify the following sub-questions:

  - Are the contacts between wireless mobile devices persistent enough to serve as an element for understanding peer connectivity patterns?
  - If the above question is yes, how can a peers' contacts be appropriately captured, summarised and represented adequately to understand the peers' connectivity pattern?
  - Can the peers' connectivity be used to serve as a basis for meaningful prediction of nodal mobility in a trust-based routing forwarding strategy?

- The fourth question of this research asks: "how can peers in wireless mobile networks learn the routing patterns of their potential routing partners to understand their forwarding and receiving ability for trust-based routing protocol design?" Along this line, we attempt to address the following sub-questions:
  - how can a peer learn the routing patterns of its subjects?
  - can a peers' behaviour be appropriately consistent to give an important basis for the prediction of the peers' reliability in handling the routing task?
  - how adequately can a peer understand the peer routing pattern for its subjects' trust evaluation?

1.5 Hypotheses

The hypotheses that will be tested in an attempt to answer the above questions in this study includes:

- In the design of a trust-based routing protocol, the exploration of the peers' routing attributes can significantly improve trust evaluation accuracy.
- In a trust-based routing protocol, the peers' trust evaluation can be extended to

the peers' routing attributes to incorporate the dynamic changes of their routing conditions for improving the quality of wireless peers' communications.

- The relative comparisons of the proliferation of peers' transitive connectivity can give a meaningful basis for determining a good relaying peer to forward packets toward the destination with less effort.

- Through properly distributed network observations, routing, listening and gathering statistics of routing history efficiently, peers' routing performance can be enhanced by making better routing decisions, and thus improve network performance.

1.6 Thesis Outline

The overall structure of the study takes the form of eight chapters. The first chapter introduces the research motivations, idea, aim and questions, and frames the theoretical contribution of the thesis in the context of related works.

Chapter two begins by laying out the theoretical dimension of the research, the major conceptual foundation and an overview of related approaches. The chapter also identifies the challenges and gaps that requires bridges in the design of trust-based routing protocols.

The third chapter is concerned with the methodology of the research. The chapter presents the details about the procedures and iterative processes executed in conducting this study.

The fourth chapter presents the preliminary investigations and findings of the research focusing on the influence of transitive connectivity and network performance metrics in the design of trust and reputation forwarding decisions in collaborative routing.

Chapter Five analyses the use of peer attributes as an element of trust and reputation

evaluation. The chapter presents a DATM protocol: a trust-based collaborative routing protocol which takes into consideration peer attributes (buffer occupancy as peer attributes) as an element of trust evaluation in the collaborative routing protocol.

Based on the foundation laid in Chapter Four, Chapter Six presents a Transitive Aware Trust-Based Protocol For Mobile Opportunistic Networks, which is an illustration of transitive connectivity as an element of trust-based routing decisions.

Chapter Seven draws upon the entire thesis, tying up the various analytical, theoretical and empirical strands in the presented Forward-Watcher Trust-based Model. The chapter also includes a discussion of a new way of interpreting peers' forwarding and receiving potentials using a statistical model.

Finally, Chapter Eight gives the thesis summary and a critique of the research findings. This chapter also gives a brief discussion of the research implications of the findings to future research in this area.

These chapters together form the iterative and design process presented in Chapter Three. Each of the Chapters Four to Eight, jointly presents segments, questions, contributions and answers to the questions raised as presented in the research questions (section 1.4).

1.7 Research Contributions and their Significance

The research works presented in this thesis addresses the issues discussed above. The key contributions of this work includes:

A Transitivity and Network Performance Metrics Analytical Model for efficient trust and reputation routing protocol. To the best of our knowledge, this is the first study reporting analytical relationships of the combined metrics of network performance and trust evaluations in a style that focuses on principles that are likely to be valuable in

trust-based routing protocol design. One possible implication of our analysis in the proposed transitivity model is that, a fast and efficient trust-based routing algorithm could be realised using the presented performance matrix-based model. While the presented study of the transitivity model in Chapter Four does not explicitly reveal how transitive connectivity can be integrated into the design of a trust-based routing protocol, it does partially substantiate that the transitive scaling factor can equally be applied in the design of an efficient trust-based forwarding strategy.

DATM: A Dynamic Attribute Trust Model for Efficient Collaborative Routing. DATM is a trust and reputation forwarding model in which each peer can dynamically detect a corresponding reliable and trustworthy peer for routing decisions and by extension can preserve the peers' routing resources and increase the collaborative routing performance. The proposed DATM has demonstrated for the first time how peers' routing attributes (buffer occupancy) can be integrated into their reliability evaluation in the design of a trust-based data forwarding strategy. The introduction of generalising peers' personalised similarity model for trust and reputation evaluation and a global trust evaluation model in DATM, has extended our knowledge of a trust-based routing protocol design through incorporating the peers' reliability in data forwarding decisions. The main implication of the proposed DATM protocol is that the protocol designers can focus their design on exploring different attributes and properties of the dynamic mobile network (e.g., peers' energy levels, spatial distribution and intermittent connectivity, etc.), and include these properties in the routing decision process.

A Transitive-Aware Trust-based Protocol for Mobile Opportunistic Networks. We analytically explore the existence of transitive connectivity patterns between peers in MSNs based on the derivation of connectivity traces. From the analytical studies and theoretical analysis, we realised that a similarity of transitive connectivity periodically

appears in the traces of MSNs. Based on the identified transitive connectivity patterns from the traces, we then proposed a new transitive data forwarding strategy which considers the similarity of transitive connectivity between peers. We further proposed a distributed transitive aware trust-based routing mechanism using modified agent trust algorithms in a mobile opportunistic network, where data is transmitted through a trustworthy transitive chain for better packet relaying strategy. The finding in the proposed transitive-aware trust-based protocol confirms previous findings that certain patterns of connectivity exist in the MSNs and contributes additional evidence that suggests the transitive connectivity/contacts can be elements of trust-based routing metrics.

Forward-Watcher Trust-based routing protocol. We introduce four important metrics for peer trustworthiness evaluation that are linked to learning peers' routing history based on messages (packets' beacons) overhearing for trust evaluation between peers. In this regard, we propose a model for evaluating the probability of the peers' forwarding and receiving potentials for local trust evaluations and a correlation matrix for evaluating peer global trust values. The proposed Forward-Watcher extends our knowledge on how to develop a simple statistics metric for learning peer routing processes for peer trust evaluations. The advantage of the proposed Forward-Watcher approach is that through routing history created by the peers, they can statistically predict the future behaviour of their corresponding routing partners. A Forward-Watcher Trust-based Model can also serve as an underpinning and cornerstone for developing self-cooperative protocols in wireless mobile networks using statistical analysis and correlation matrices.

1.8 Publications

- **Usman A. B.** and J. Gutierrez, "Datm: a dynamic attribute trust model for efficient collaborative routing," Journal of Annals Operations Research, Springer, Apr,2018. [Online]. Available:`https://doi.org/10.1007/s10479-018-2864-5` (accessed date 28/April/2018).

- **Usman A. B.** and J. Gutierrez, "Trust-based analytical models for secure wireless sensor networks," Security and Privacy Management, Techniques, and Protocols. IGI Global, 2018, pp. 47-65.

- **Usman A. B**., J. Gutierrez, and Bichi, A.B., "A Neighbourhood-Based Trust Protocol for Secure Collaborative Routing in Wireless Mobile D2D HetNets", In Press, 2018, Volume 16 No.4,International Journal of Computer Science and Information Security, IJCSIS ISSN 1947-5500, Pittsburgh, PA, USA. Available:`https://www.academia.edu/36564767/A_Neighbourhood-Based_Trust_Protocol_for_Secure_Collaborative_Routing_in_Wireless_Mobile_D2D_HetNets` (accessed date 28/April/2018).

- **Usman A. B.** and J. Gutierrez, "A reliability-based trust model for efficient collaborative routing in wireless networks," in Proceedings of the 11th International Conference on Queueing Theory and Network Applications, ser. QTNA '16. New York, NY, USA: ACM, 2016, pp. 15:1-15:7, [Online]. Available: `http://doi.acm.org/10.1145/3016032.3016057`,(accessed date 28/April/2018).

- **Usman, A. B.**, Liu, W., Bai, Q., Narayanan, A. (2015). Trust of the same: Rethinking trust and reputation management from a structural homophily perspective. International Journal of Information Security and Privacy, 9(2), 13-30.

doi:10.4018/IJISP.2015040102.

- **Usman, A**., Liu, W., Bai, Q., Narayanan, A. (2016). Exploring the Role of Structural Similarity in Securing Smart Metering Infrastructure. In 2015 IEEE IEEE International Conference on Data Science and Data Intensive Systems (pp. 343-349). Sydney, Australia: IEEE DSDIS Proceedings. doi:10.1109/DSDIS.2015.95.

- **Usman, A**., Liu, W., Bai, Q., Narayanan, A. (2015). Revealing the role of topological transitivity in efficient trust and reputation system in smart metering network. In 2015 IEEE International Conference on Data Science and Data Intensive Systems (pp. 337-342). Sydney, Australia: IEEE. doi:10.1109/DSDIS.2015.114.

- **Usman, A. B**, (2016) "Trust-Track: A New Paradigm for Mitigating Selfish Behaviour in Wireless Sensor Networks", abstract published in the proceeding of AUT research Symposium, 2016,

- **Usman, A.,** (2015), "Analysis of homophile effect for self- defensive and anomaly detection in WSN - based smart meters" abstract published in published in the proceeding of AUT research Symposium, 2015

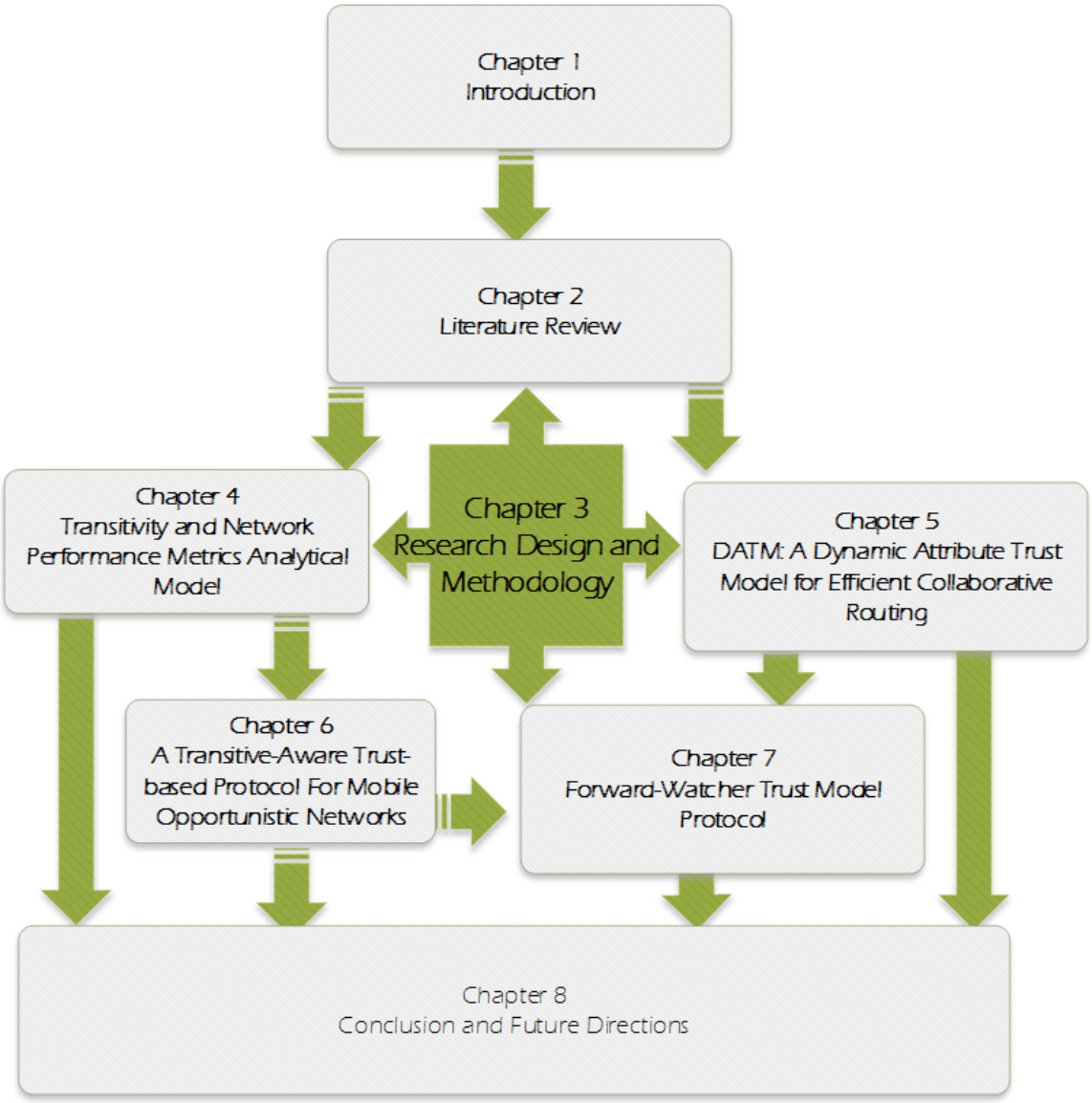


Figure 1.1: Study Structure

Chapter 2

Literature Review

A large and growing body of literature has investigated different topics on trust-based routing protocols in mobile wireless networks. This chapter systematically presents to the reader, the foundation of this research and what is already known about this research topic. The chapter outlines the key ideas, notions and theories that helps us understand the current status of the literature and the need for our proposed contribution.

Like many disciplines, the concept of trust and reputation models in computer science have developed its lexicon, partially inherited from the social sciences field of studies. Thus, this chapter presents some interesting theoretical foundations of trust and ground for our discussion about the original context of trust between agents in the networks. It presents different sociological concepts of trust management including the notion of a closed structure, which further leads our discussion to the concept of reciprocity and transitivity. Also presented are the features of self-cooperation, self-organization and self-control mechanisms for the design of an efficient trust-based collaborative routing strategy between mobile wireless networks.

2.1 Chapter Background

In the design of mobile wireless routing protocols, researchers make the assumption that the devices are usually cooperative in data forwarding and security control. Some of the

assumptions include collaboration between devices, guaranteed end-to-end connectivity, short and fixed delays, low error rates, etc. However, the current trend and future wireless communication networks may not necessarily possess characteristics that can support those assumptions.

Peer mobility, for example, in an intermittently connected network, can lead to spatially heterogeneous peer distributions, which by extension may cause network partitions; thus, the assumption of end-to-end connectivity cannot be valid in all cases. Another important technical challenge of some wireless mobile networks is managing dynamic network conditions such as the unreliability of peers and network links which result in frequent service outages. Further, current wireless mobile networks are no longer limited to the Internet. Nowadays, peers in the network can instantly communicate using different routing schemes and applications. Thus, the emerging mobile wireless communication networks keep on violating many basic design assumptions of the past. Arguably, the current and future routing protocols of a wireless device require an integrated collaborative approach for the different devices to communicate efficiently. This development has brought the need to convert peers to become self-cooperative and autonomous entities in the network. In this view, the probability that the wireless device has to interact or cooperate with each other will increase, and the need for attributing trustworthiness to the potential partners becomes a fundamental prerequisite [33].

Nonetheless, the properties of trust, self-cooperation, self-organization and self-control of wireless peers in the network do not come into existence automatically; they need to be enforced and incorporated into the routing protocol design. Through that, the devices and the protocols of wireless P2P networks can be prepared to overcome different problems of variable conditions, faulty nodes and any strange or malicious behaviour

in the networks. So far, the three most important mechanisms recognized in a decision support research, and of relevance to this research, are trust, reputation and cooperation management. This is due to the specific features or mechanisms of trust and reputation in dealing with the uncertainty concerning future actions of the participating peers in the network.

2.2 Trust and Reputation Foundation

Although trust is an underdeveloped concept in computer science and information technology, one can argue that the concept of trust is as old as the existence of human beings. There are also promising theoretical formulations and empirical studies in different related studies such as [34] and [35] that can support the formulation and modelling of trust and reputation. Further, the semi- and fully-distributed and autonomous systems, the seemingly imminent Internet of Things and artificial intelligence are providing further examples in which increasing complexity leads to obscure and unexplainable system behaviour [36]. In this regard, the concept of trust and reputation seems to be becoming an important consideration in the design of autonomous agents in the network.

In the first place, trust has to do with the belief, uncertainty, intention and willingness to cooperate or not to cooperate [37]. These attributes are mainly behavioural characteristics of human beings which cannot be accurately predicted with a high degree of accuracy. Although other areas of studies such as psychology, social economics and sociology adopted different methods of studying trust, the study of trust and reputation in computer science-related disciplines usually involves mathematical and computational modelling [38], the use of subjective and temporal logic specifications in trust assessment (which may not necessarily reflect various trust properties) [39] trust influence and cooperation between the peers in the network. Therefore, it interests us to understand

the original concept of trust from social science to lay a foundation for the concepts we will use eventually for our research contribution.

Further, the study of network structure, topology and the relationship between peers has been explored in different fields of studies such as communication networks [40] robustness of networks [41], structural monitoring, analysis and optimization [42], optimal routing decision [43], and information flow and dissemination in social networks [44] to mention but few.

Arguably, the modelling of trust in trust-based routing protocols needs to incorporate peers, network conditions and peer characteristics, and include a study of network science to carry out peer structural analysis in the network for trust evaluation [45].

While a substantial amount of literature has already detailed different areas of trust and reputation management in routing protocols, most of the existing approaches focus on developing a model and algorithm without taking into account any additional peer behaviour or attributes such as peer roles and position in the network, peer connectivity, peer attributes and the similarity between peers concerning peer resources and routing patterns for trust evaluation which are some of the construct elements for understanding peer routing behaviour for peer trust evaluation. As a result, prior studies have argued that peer trust ranking behaviour in trust models is imperfect and noisy [46, 47].

2.2.1 Trust

In a social context and human-centric viewpoint, trust is ascribed to relationships between people or social groups[37],[48]. In Information Security, trust is attributed to the behaviour of an entity expectedly for the intended purpose. Trust in collaborative routing for mobile networks is a mechanism for improving the efficacy of computing elements' decision making process for security and performance considerations [49].

Trust can also be characterised as the desire a device will do what it is expected to do regarding data forwarding without conveying damage to another device or the network. A device with a higher trust level is considered as a dependable routing element in the network, and it's implied that there is a high shot that the activities it is required to perform are finished in a way that is positive and trusted. Following the conduct and routing behaviour of devices, the trust value of devices can be estimated. So far, there is no comprehensible consensus on the definition of trust in a distributed computer networks; however, there are promising theoretical formulations and empirical studies such as [50] that can support the formulation and modelling of trust and reputation in a mobile environment.

Different fields of study usually define the term "trust" depending on their disciplines' discretion and views. For example, the work of [48] argued that the concept of trust must be considered as a multidimensional concept which develops (i) only under certain structural conditions and (ii) merges cognitive-affective and behavioural dimensions into a unified social experience. The study in [49] defines trust as the subjective belief of someone in the character, ability, strength, reliability, honesty or truth of someone or something.

From the computing and information technology view, Josang et al. [51] distinguish between two main categories of trust: reliability trust and decision trust. The concept of reliability trust is mainly based on the probability that an actor can perform a certain action either as a result of their capability, resources, location in the network, connectivity or attributes; while the concept of decision trust is based on the extent to which an actor is willing to depend on the action or the decisions of another actor with a feeling of relative security. Obviously, one can observe that the notion of combining reliability trust and decision trust can characterise the scenario of collaborative routing

where peer reliability for handling a routing task is a deciding element of successful routing between peers in the network. Therefore, throughout this thesis [and more precisely in Chapter Six], we will be referencing the definition of trust and reputation provided in [51]. This is to enable us to bridge the gap between the reliability trust and decision trust model in collaborative routing between wireless peers.

For example, let $t_{p,q}$ be the trust value that device p places in device q based on its prior experience with device q, where $t_{p,q} \in \langle 0, 1\rangle : p \neq q$. Each time device p encounters device q, it can assess the trust level of device q.The local trust value or initial ($t_{p,q}$) between p and q will increase or decrease depending on the rule of the game. Therefore, $sat(p, q)$ can represent the number of satisfactory encounters between device p and device q while $unsat(p, q)$ can represent the total number of unsatisfactory encounters between device p and device q. Thus, the resultant local trust value between the devices can be computed as in equation 2.1.

$$t_{p,q} = sat(p, q) - unsat(p, q). \tag{2.1}$$

From the initianl trust value in equation (2.1), the normalised trust value can be computed using equation 2.2.

$$t_{p,q} = \frac{max(C_{p,q}, 0)}{\sum_q max(C_{p,q}, 0)} : ||\vec{t_p}||i.e. \sum_{q=1}^{N} t_{p,q} = 1 \tag{2.2}$$

2.2.2 Reputation

A reputation system in routing protocol is a mechanism that allows devices to rate each other in the network in order to build trust. The role of reputation systems, is to gather a collective opinion of other devices to build trust that can enable trusted communications between devices in the network. The mechanism of reputation works well for trusted peer-to-peer transactions in P2P market places. For example, eBay

and Listia have a positive, negative, or neutral seller feedback reputation system, while others like Amazon, Etsy, and Yelp use a five-star reputation system for their businesses and service providers.

In the context of trust-based routing protocol, the definition of reputation proposed by Naseer et al. [52] suggests that a reputation can be viewed as a subjective expectation a device can have about another device's behaviour based on the previous history of their encounters. Conventionally, in a reputation model for routing protocols, each device can be a requestor (trustor); requesting the opinion of other devices, and a responder (trustee) who can provide its aggregated opinions (reputation). The reputation can be calculated based on various types of information including the rate of the devices' collaboration in the network [53].

For example, consider the normalised local trust value computed from equation (2.2), the calculated trust value of device q computed by other devices in the network can then be aggregated to build a reputation value of device q using the following equation (6.6).

$$T_{p,q} = \sum_{q} t_{p,q} t_{q,r} \tag{2.3}$$

From equation (2.3) and many other works in the literature including [54], it can be understood that the reputation management in a routing protocol is trust dependent and relies on the aggregated trust opinions of other peers to give a global trust or reputation value. Thus, the definition of routing protocol with respect to reputation systems is often difficult to determine without the inclusion of trust management system, and there is no common definition used by researchers . Reputation systems protocol are often named as Reputation System Based Trust-Enabled Routing Protocol [52], Reputation-and-trust-based systems [54], etc. To unify these concepts we have adopted

the term trust-based protocol to describe the trust and reputation protocol throughout this thesis.

Despite the diversity of different forms of trust and reputation models, the trust-based protocols in some way share common underlying phases as illustrated in Figure 2.1. Following is the brief description of the four generic phases of trust models for the trust-based protocol.

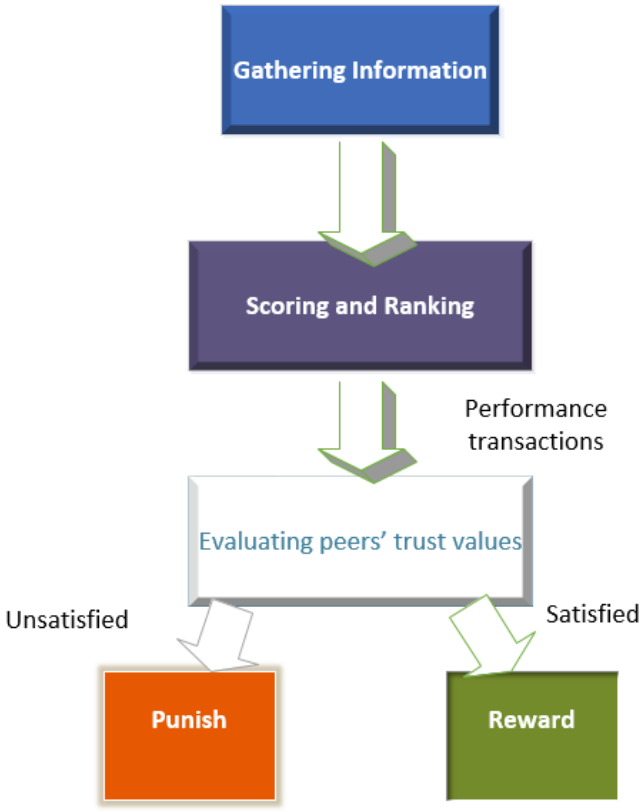


Figure 2.1: Generic Trust and Reputation Model Scheme

- **Monitoring or observation** This is the process of observing the activities of the peers in the network.
- **Scoring and Ranking** Based on the peer observations, a node can rank its neighbours or other nodes depending on their track records and previous encounters

for recommendation or trust decision purposes.

- **Evaluation** (Calculation): Based on the scoring evidence manifested as a result of peer observations, peers can calculate the resultant reputation value of a peer for further action or responses.

- **Response** This is a decision based on a peer's trust ranking value. The actions for the response include rewarding well behaving nodes and avoiding badly behaving nodes for the retribution or punishment of the misbehaving or malicious peers.

Though there are other aspects of reputation systems, trust ranking and reputation evaluation appear across all reputation mechanisms. Therefore, these standard components of trust and reputation schemes will be the basis of our analysis and contribution of this thesis.

Due to the nature of this research, it is important to review the concept of trust from its source (social science point of view). This is to enable us to lay a foundation for our contribution. In the next section, we will review different theoretical concepts of trust from the social science perspective that are related to the interests of this study.

2.3 Trust From Computational Social Sciences' View

Like many disciplines, trust and reputation have developed its lexicon, partially inherited from the social sciences field. For a complete introduction to trust, reputation and cooperation from social trust to digital trust we refer the reader to [55].However, some trust-theoretic notions are required for our discussion about the original context of trust between agents from the social science perspective.

One possible reason justifying the adoption of the network paradigm by researchers in

the study of trust and collective behaviour between peers may originate from the non-trivial dynamics of the relationship between interacting peers in the network. Indeed, different networks of wireless peers such as Mobile Adhoc Networks (MANETs), Vehicle Adhoc Networks (VANETs), Delay Tolerant Networks (DTNs) and Robot Networks, are not necessarily static networks. They can grow or decay, and their topologies evolve with the possibility of hubs emerging or declining, and communities or cliques forming [56]. It has, therefore, become apparent that it is important to consider the collective dynamic behaviour of the peers in the network for trust-based self-organization routing and for understanding the trust mechanism from the social sciences. We will provide in the next few sections some basic, possibly incomplete theoretic concepts and arguments about the essential features of trusts modelling from different views of the computational social sciences.

Worthy of notice is the idea of trust between agents in the network has to be understood regarding the agent relationship and organizational structure. Conventionally, there are three intrinsic characteristics of computational social science concerning trust and reputation: connectivity (the relationship between actors within a group and topological structure), collaboration (modelling the way actors interact), and community/neighbourhood (clustering or grouping through similarity and preference)[57].

- **Topological structure and connectivity** This represents the structure and the relationship (connectivity) between peers. Some related studies have pointed out that the connectivity between peers can be incorporated in developing effective strategies for establishing trust between peers in the network [58].

- **Collaboration** The recommendation process is constructed on collecting opinions based on peer collaboration with other peers in the form of trust ranking behaviour, and the quality of the recommendation. Also, many studies have

shown that having networks assessed on their functional similarities, interests and preference similarities can influence their trust and reputation habit and can play a significant role in predicting peer behaviour in the network [59].

- **Community/neighbourhood** Trust, collaboration and intimacy are some of the primary units of the analysis in the sense of community theory [60]. Having a community of actors based on their locations or spatial closeness can influence their trust and reputation habits and can play a significant role in predicting peer behaviour in the community [61].

2.3.1 Organisational Structure and Trust

One of the fundamental terms used in the study of organisation structure and actor behaviour is network. - A set of actors and the relationship between them it can be understood that network begins from the dyadic (two peers connected) perspective to the larger organisational structure. This concept of network has been adopted by various disciplines as a valuable way of studying organization and organizational behaviour, structural positions and the relation between peers.

In most social science research, the concept of social structure has long been agreed to be the source of social capital which plays a vital role in sustaining trust relationships between individuals and organizations to create values, trust and transfer of knowledge, and enhance creativity. In this line, there have been several attempts to address the trade-off between closed structure and open structure in which structure promotes trust, norms and cooperation among peers in the network. The analysis of these two social network group terms encompasses theories, models and assumptions that are based on the relational concept.

2.3.2 Open Structure

Figure 2.2 presents an example of open structure. From the figure, an actor q occupies a brokerage position and it can have three distinct benefits: Control Benefits (having access to control other peers in the network), Information and Referral Benefits (it can serve as a good recommender) and Uniting Benefit which are all significant factors that promote inter-organizational trust. There are some theories from the social science perspective including the work of Burt [62] who argued that having a central actor with a higher communicability index in the network can facilitate the transfer of information and provide reachability benefits in the network of peers. On this line, there are some non-distributed trust routing algorithms that follow this idea of centralised reputation systems such as those in [63, 64]. In a centralized trust and reputation system, the central peer (usually the most important peer in the network) will evaluate the peer trust behaviour, and perform all the tasks of trust aggregation and trust recommendation in the network. Although, the concept of a centralised reputation system works well in a simple network of peers or where a single central peer is needed for trust and reputation evaluation, it is less suitable in a distributed network of peers and it inherits a number of problems such as a single point failure (when a central peer fails or compromised). Therefore, we seek to observe a closed structure to lay the foundation of our contribution in this thesis. In the next sub-section, we study the closed structure and its related properties for efficient trust evaluation.

2.3.3 Closed Structure

The concept of closed structure was first introduced by [65] based on the observation that in a closed structure, there is a high degree for every peer in the network knowing every other peer directly or indirectly, and, as such, the peers are more likely to trust

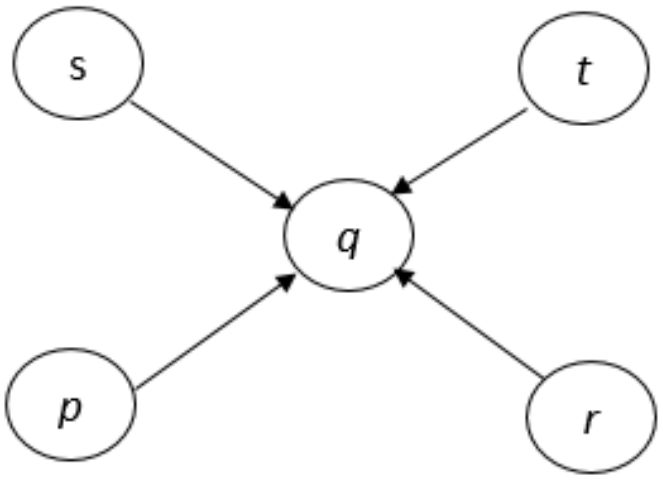


Figure 2.2: Simple Illustration of Open Structure

each other and predict other peer behaviour than in an open structure. Extending the theoretical work of [65] is the finding of Simmel [66], who argued that the triad is the fundamental unit of social analysis, and hypothesized that the strength or quality of relationships and trust are not based on the content of the relationship, but rather on the cohesive structure of the relationship. Simmel articulated several reasons and features of triad relationships and concluded that while a triad is the smallest form of group, increasing group size does not significantly alter its critical features. In a related development, the study in [67] presented Simmels work regarding Similien ties (closed structure) and structural holes (a form of open structure) and explored their roles in terms of task interdependence and effectiveness, the study showing that Simmelian ties promote development of group norms such as norms of cooperation and reciprocity, and also promote trust, cohesion and transitivity which are all positively correlated to interdependency and redundancy. Therefore, to lay the foundation of our concept of integrating peer routing attributes as trust evaluation factors, we seek to discuss the two important properties of closed structures: transitivity and reciprocity. Under

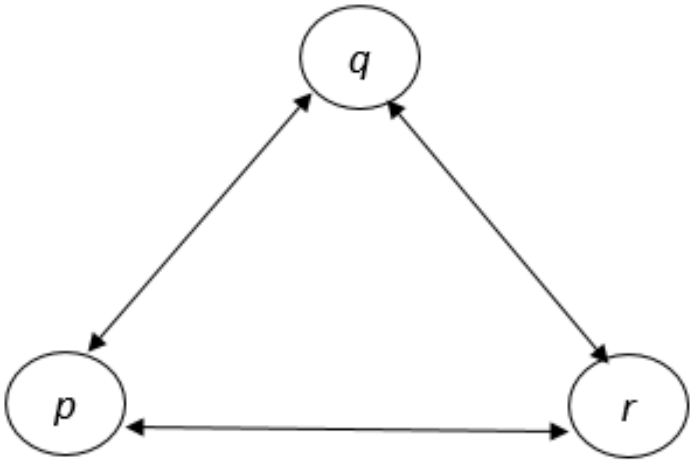


Figure 2.3: Simple Illustration of Closed Structure

the next headings, we discuss the properties of transitivity and reciprocity in detail. These two closed structure properties are the starting points of our proposed models in Chapters Four, Six and Seven.

2.3.4 Transitivity

In this subsection, we seek to review some related studies on transitivity in trust. Transitivity in trust is very often considered a trivial and simple property from the classical social and cognitive models, mathematics, logic and grammar. In fact, the complexity of the trust notion suggests evaluating relationships with transitivity in a more adequate way. Transitivity is one of the oldest existing concepts used to implement a popular community finding method and the creation of links in a social network based on the concept of sharing common nodes. It also tallies with the dynamic balance theory [68] and the Simmelian triangle theory as explained earlier which states that the localized cohesion between transitive actors is optimal for sharing information, encouraging cooperation and minimising conflict between the actors [69]. However, it is important to

clarify that trust is not transitivity perfect due to the subjectivity and context-specific nature of trust [70], but an important property that can be integrated into the design of trust-based routing for efficient trust propagation and evaluation between peers in the network. Transitivity can, therefore, be characterised as a property of the relationship between actors of a similar nature and friends who may stand for each other. For instance, [71] characterises transitivity as a very important driven factor of trust and reputation evaluation within a network of peers.

In principle, trust and reputation can be aggregated based on the direct interaction between peers or through trust-chains (trust anchors). These features of trust made it feasible to be implemented in a distributed network of different topological order and arrangement. The ability of a peer to aggregate trust value of the corresponding neighbouring peers and establish communication is limited to the distance and interaction between the peers in the network. In a situation where all the peers are not directly connected or interfaced with each other, the trust and reputation aggregation and evaluation will be based on a chain of referrals (number of possible hop counts between the peers). In this situation, exploring the suitable connectivity or trust chain is essential.

2.3.5 Reciprocity

In this section, we seek to review the concept of reciprocity in the context of the social sciences and trust-based modelling. The concept of reciprocity has been widely studied in various fields of study. For example, from a social psychology point of view, reciprocity can be simplified as a social rule that actors tend to repay, in a similar way, what another actor has provided for them [72]. In other words, actors give back (reciprocate) the kind of treatment they have received from others. Reciprocity has been identified amongst the most well-known mechanisms that may sustain trust and cooperation

evolution among peers for behaviour-oriented modelling [73], and it is considered as one of the promoting factors of mutual interactions between actors by returning similar acts. This property plays important roles in the process of spreading information and ideas, and provides good features for ranking and classification-based methods for trust prediction [74].

The simple model presented in Figure 2.4 shows the reinforcing relationships among trust, reputation and reciprocity. The direction of the arrow indicates the direction of influence among the variables, while the dashed line indicates a mechanism of net benefit [outside the scope of this thesis].

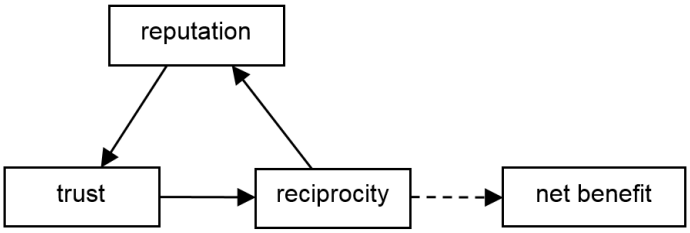


Figure 2.4: Illustration of Reciprocity Model

Trust and reciprocity are interrelated and can be applied in quantifying the trustworthiness of agents regarding the exchange of mutual deeds. For example, the work of [75] developed quantitative models for measuring reciprocity and exploring the extent to which reciprocity exists in the trust network and the measures for predicting trust behaviour. The author measured trust reciprocity using link reciprocity in the network which has also been studied in the context of Web networks and email networks, and was referred to as the global measure of reciprocity in [76]. Further, the work of [77] presents two types of reciprocity, namely: direct reciprocity and indirect reciprocity.

- **Direct reciprocity:** The notion of direct reciprocity was initially proposed by Robert Trivers [78], as a mechanism for the evolution of cooperation between a

pair of actors. Direct reciprocity can lead to the evolution of cooperation between a pair of actors if the probability of their encounter exceeds the cost-to-benefit ratio of the altruistic act. For example, considering Figure 2.5, the action or help of p to q is dependent on the outcome it receive from q. i.e if p help q, then q can reciprocate to help p.

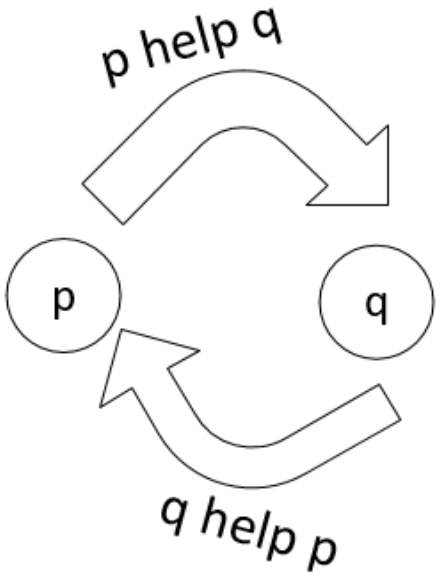


Figure 2.5: Illustration of Direct Reciprocity [1]

- **Indirect Reciprocity:** In an indirect reciprocity model, when there are randomly chosen pairwise encounters between the actors of a population, one actor behaves as a donor and the other as a recipient. The donor can decide whether or not to cooperate. The interaction can be observed by the members in the network who might act as watchers and inform other actors in the network. Usually, indirect reciprocity comes in two different flavours as presented in Figure 2.6 [79]. The upstream reciprocity (left) is based on the recent positive experience. An actor who is receiving a donation may feel encouraged to donate in turn. Downstream reciprocity (right) is built on the reputation of peers in the network. As

illustrated in Figure 2.6, because of p has helped q, therefore receives help from r

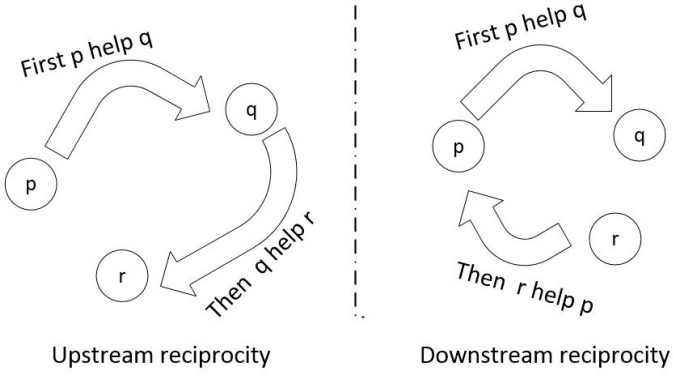


Figure 2.6: Illustration of Indirect Reciprocity [1]

Furthermore, both trust and reciprocity are the types of social capital embedded within personal relations. It is, therefore, common knowledge that the level and the degree of the peer reciprocity among the peers can serve as an instrument for trust estimation, trust prediction and peer trust evaluation.

So far, there are many reciprocity strategies for predicting peer trust behaviour proposed by psychologists [80], social science economists [81], game-theoreticians [82] and topology modelling authors [83]. To join the line, we propose that predicting the reciprocity or the peer altruist forwarding pattern for trust-based routing protocol design can be achieved through developing a model of the peer forwarding and receiving correlation. In chapter seven of this study, we propose a Forward-Watcher trust routing protocol based on the concept of direct and indirect reciprocity.

2.4 Review of Trust and Reputation Algorithms

There are many well-known trusts and reputation systems in the literature. In this section, we provide a summary of a few that are related to the interests of this research.

We choose each trust and reputation scheme to provide a glimpse of how the systems work, as well as to provide insights into the different components of trust and reputation schemes.

The EigenTrust is a reputation scheme proposed by Kambar et al [84] that uses transitive trust chains for computing a global trust value for each peer in the network of peers. The scheme populates a matrix of the number of positive experiences minus the number of negative experiences between the peers (the negative experience value is replaced with a 0). The resultant matrix is then normalised to convert the sum of each row to 1. The eigenvector of the resultant matrix which contains the elements of the eigenvalues is then computed to produce a column vector that contents the global reputation values. Each peer performs this computation in a distributed Eigen Trust scheme by exchanging reputation information with other peers in the network that have interacted. The resulting reputation values are then stored in a distributed hash table to reduce the likelihood of successful manipulation of reputation values.

Additionally, the beta distribution function has a strong foundation on statistical theory and less computational complexity compared to related approaches which makes it more applicable to Wireless Sensor Networks. For example, recently, the work of [85] proposed a Beta-based Trust and Reputation Evaluation System (BTRES) for WSNs node trust and reputation evaluation. The BTRES uses the concepts of monitoring nodes behaviour, and the beta distribution is used to describe the distribution of node credibility. The selection of relay and benevolent nodes is based on the node trust value.

Several studies continue to propose different trust and reputation models based on recommendation systems that can be compatible and implemented in many application domains. The work of [86] analysed the basic types of trust models: experience

based trust models and reputation-based trust models for determining whom to trust over the various system with different transaction frequencies, reputation accuracy and trustee trustworthiness. The framework introduced the learning parameter to perform a weighting between reputation-based trust modelling and experience-based trust modelling. The author reported that, for effective trust modelling, the trustor should use the learning parameter for each potential trustee since the transaction frequency, accuracy of reputation and trustworthiness characteristics may vary. The result of the work also demonstrated that a combination of experience- and reputation-based models are better over a broad range of system characteristics.

Currently, there are many trust and reputation models proposed in the literature; the focus of most of them is to model trust based on the satisfactory and unsatisfactory behavior of the peers (Eigentrust)[87]; the use of community-based reputations to help estimate the trustworthiness of peers (peer-to- peer trust model) [96]; peer feedbacks and global reputation scores (Power trust models) [88]; and the selection of the most trustworthy node through the most reputable path in the network (BTRM-WSN Trust model) [89]. Also, the work of [90] proposed statistical trust and reputation evaluation techniques and investigated the result of the scheme for the design of trust evaluation rules. For example, the intense study of [91, 51] explored the roles of reputation systems for encouraging good behaviour and promoting adherence between actors. On the other hand, the work of [92] proposed a novel reputation framework (RFSN) that includes five different sections: direct reputation evaluation, indirect reputation evaluation, reputation synthesis, behaviour, and conversation. The model captures the details of the evaluation processes of trust in wireless sensor network.

Likewise [93] proposed Gaussian trust and reputation computation in multiple-input-multiple-output (MIMO) wireless sensor networks. The study proposed an analytical

framework to characterise the direct based reputation for fading MIMO scenarios based on multivariate Gaussian distribution and Bayesian theorems. Recently, [94] proposed an Efficient Distributed Trust Model (EDTM) for WSNs, the author arguing that most of the current trust and reputation models take communication behaviour between the nodes into account to calculate the sensor node trust value. The EDTM considers the number of packets received by sensor nodes, and direct trust and recommendation trust are selectively derived. However, the framework did not consider familiarity and reliability to improve the accuracy of the recommendation trust.

2.4.1 Trust and Reputation Based on Direct Neighbours' Feedback: Direct Trust

Many of the ad-hoc network trust models are naively based on a trust-your-neighbour relation. In this type of trust model, the entire trust management system (origination, managing and expiration) usually has a short lifespan, and the peers may lack a comprehensive knowledge of the overall neighbour trust level. As a result, most of the direct trust models only work in an environment where all the nodes are self-organized and mobile (e.g., military and law enforcement applications) which limits their functionalities to some specific areas. Recently, several attempts were made by many authors to propose a different improvement in the various aspects of direct trust and reputation algorithms. For example, the study in [95] introduced a zone-based trust management agreement scheme in wireless sensor networks. The scheme was designed to detect and revoke groups of compromised nodes within the trust formation and forwarding phase. Each node directly interacts with the neighbouring nodes for the trust report event and stores the report in a knowledge cache. The proposed protocol comprises of a zone discovery phase, trust formation and forwarding phases. Before making a final judgement, a trustor will always compute the difference between the probability distribution

function of the neighbourhood trust and the probability distribution function of the information received from its neighbours at every slot of time (say, T). The total trust factor can be determined based on the deviation between the reports of the observation using the information theoretic metric KL-divergence.

Also, the work in [96] proposed a novel, Connected Dominating Set (CDS)-based reputation monitoring system. Which employs a CDS-based monitoring backbone to securely aggregate the reputation of sensors without subjecting them to energy depletion or reputation pollution attacks.

In addition, apart from constraints that are application-specific, the concept of direct trust suffers from the following setbacks that may limit its application in a distributed and autonomous wireless network: a) Notion of prediction: peer p can either trust peer q or distrust peer q [97], since it has no other means of trusting peer q; b) peer p can only compute peer qs' trust value under the condition that peer p trusts peer q; C) Energy depletion problem; the amount of energy needed for a wireless node to accomplish trust management processes (trust aggregation and trust evaluation) with all other neighboring peers in a distributed network will be high, since the trust between peers can only be derived based on their direct contacts and the energy needed for the node to communicate with other peers is proportional to its distance with other peers in the network [98, 99], and as we have shown in section in section 4.3.2.

2.4.2 Recommendation/Referral in Trust and Reputation

As mentioned in the above section, trust evaluation based on direct experience is not often obtainable to the assessors and sometimes having a direct experience between all peers in a large-scale network is non-trivial. Therefore, aggregating trust opinions of other peers on a particular agent remains a fundamental building block of successful

trust and reputation systems. One common issue in trust aggregation based on the recommendation is the reliance on peer interactions to evolve the global trust value of an agent. Inherently, this creates an undesirable dependency, where the peer interaction and connectivity plays a significant role in the accuracy of the resultant trust score. Further, because the process of reputation and recommendation aggregation involves a series of message transfers across the chain of peers, the management of the recommendation may prompt many challenges. Also, in the recommendation processes, knowing who made the recommendation and the time at which recommenders make a recommendation is essential for determining the accuracy of the recommendations value and to minimise the problem of trust decay respectively. Thus, modelling the recommendation or referral between peers in the network might not complete without visiting some related concepts of peer interactions and connectivity for proper trust evaluation. In the next subsections, we present some related surveys that specifically focus on trust and reputation models that are of great interest to this study.

2.4.3 Summary of the Related Surveys in Trust and Reputation Models

There are various comprehensive survey articles on trust and reputation management that focuses on P2P networks. Here, we highlight some of the surveys that are related to our work. For example, the survey in [100] reported a systematic review of various trust and reputation systems for P2P-based web services and the survey classified different trust and reputation systems into three categories: 1) centralised vs. decentralised reputation systems, 2) agent vs. resources and 3) global vs. personalised trust and reputation systems. The report of the survey concluded that collaborative filtering would be better for the implementation of reputation in recommender systems technology.

Also, the work of [101] provides a survey on the different frameworks for general decomposition of existing reputation systems. The survey classifies different attacks by identifying which reputation system components and design choices are vulnerable to attacks. The survey also explored different defence mechanisms against those attacks for the future reputation system.

Subsequently, the survey in [102] focuses on computational trust models for wireless communication networks (WSNs) and cognitive radio networks (CRNs). The survey reported two major categories of trust and reputation: individual-level trust and system-level trust. Based on the report of the survey, the majority of trust and reputation models focus mostly on the detailed aspects of individual-level trust due to the following reasons: i) the individual trust mechanism facilitates first-hand interaction and experiences between the peers, ii) aggregates testimonies from witness nodes about potential interaction partners and evaluates trustworthiness of potential interaction partners based on the available past experience, while some trust models consider system interaction protocols to enforce cooperation among the nodes in a network.

[103] presented a survey of trust management for mobile ad hoc networks in distributed environments. The survey reported different potential attacks and performance metrics of trust and reputation models based on composite cognitive, social information and communication taking into account severe resource constraints of mobile ad hoc networks such as, computing power, bandwidth, quality of service, node mobility, topology changes and propagation channel conditions. Furthermore, the author concluded that, exploring the social relationship in evaluating trust and collaboration through employing the concept of a social network is a potential fruitful research in trust and reputation for mobile ad hoc networks.

Also, the work in [104] presented a survey on trust management in mobile ad hoc networks based on the subjective nature of belief for behaviour prediction. The survey explored different techniques for trust value calculation and trust propagation, and the concept of trust value can be used to promote confidence between the peers in the network. The survey also presents a summary of different related work on trust metrics, trust dynamics and how trust can change with time in the processes of trust propagation, trust aggregation and trust prediction. The study further reports different methods for trust measurements including fuzzy probability and trust scales.

In the same line, the work of [105] provided a comprehensive survey on the security issues against trust and reputation models in a peer-to-peer network. The survey explored many different attacks such as Sybil attacks, bad mouthing attacks, on-off attacks, conflicting behaviour attacks, newcomer attacks, ballot-stuffing and their corresponding measures such as weighted transaction influence, identity verification and opinion discounting. However, the survey did not report how all the stated solutions can address the security challenges in fully decentralised systems.

Also, the work of [106] presented a general survey on the relationship between interest similarity and trust based on collecting information about the users view regarding the relationship between trust and interest similarity. The survey reported that, there is a positive relationship between trust and interest similarity which means that, the more two people are similar, the greater the trust relationship between them. [107] presented a survey on a web-based social network. The work in [108] presented the survey on the study and analysis of exiting trust systems in participatory sensing applications. The survey explored common features of participatory sensing and analysed their vulnerabilities and attacks based on two types of participatory sensing. The work also identified many trust problems and attacks that have not been addressed in the literature. The

survey in [109] explored the concept of security and in management in opportunistic networks.

2.5 Trust-Based Routing Protocol

Before the trust-based routing protocols, the job of the peers routing forwarding was only to forward packets from the sources to the destinations. Trust-based routing ideology encourages that, in addition to forwarding the packets from the sources to the destination, intelligent forwarding decisions can be incorporated to increase routing performance and security considerations. A trust-based routing protocol is, therefore, a routing scheme in which the peers in the network can integrate their opinion about the behaviour, reliability and the trustworthiness of their neighbours or any peer in the network. The peers' opinion is aggregated and quantified as a trust metric or aggregated trust value. For example, when two peers p and q interact, they can establish a local trust between themselves. Let $t_{p,q}$ be the trust value that peer p places in peer q based on its prior experience with peer q, where $t_{p,q} \in \langle 0, 1\rangle : p \neq q$. The local trust value $t_{p,q}$ from different peers who once had an experience with peer q can then be aggregated to build a global trust value of peer q. The global trust value of a peer is a peers credentials that a peer can use to interact with other peers who have never interacted with it before. The peers can also use the global trust value of a peer to rate and predict its behaviour.

Trust-based data forwarding has been extensively studied in wireless routing for fault-tolerant networks [110], opportunistic environment [111], mobile ad-hoc networks [112]. Traditionally, the forwarding strategy between wireless peers can be either end-to-end or hop-by-hop. In the end-to-end trust-based routing forwarding, the set of forwarding peers can be determined on the fly on a packet basis using certain criteria [113].With

hop-by-hop forwarding strategy, each forwarding peer (including the packet sources) determine its own forwarder set based on the trust level of the peers. A selected forwarding peer will again do this process until the messages reach the destination.

2.5.1 Summary of Related Forwarding Strategies for Dynamic Routing Protocol

Recent attention has focused on the issue of packet forwarding in non-cooperative configurations. Different trust-based routing protocols designed to address the quality of service degradation, selfish and non-cooperative routing behaviour, and end-to-end delay aspects have been proposed in the literature.

Some of the serious discussions and analysis about trust-based routing protocols are based on game theory [114], fuzzy logic [115] or Bayesian network [116]. Some of the possible reasons why the above-mentioned techniques are commonly used in trust-based modelling include; (i) both game theory and fuzzy logic can be used for modelling cooperative behaviour in complex networks (ii) they can be used for learning the dynamic pattern of peers' states and interactions for proper predictions [117].

For example, [118] employed the uses of fuzzy inference rules to improve the routing protocols with fuzzy dynamic programming in MANETs. Though the concept was highly referenced in the literature, the model did not take into account the dynamic nature and behaviour of P2P due to the problem of multiparameter optimisation limitations and computational complexity of fuzzy systems.

Additionally, there have been some longitudinal studies that proposed a trust-based routing for different reasons. For example, the study in [119] proposed a Trust-Aware Routing Framework for WSNs (TARF). TARF provides a trustworthy and energy-efficient route between a sender and a receiving node. Also, the work of [120] proposed a trust-based protocol for the energy-efficient routing decision, the proposed protocol

reducing delay and routing overheads; however, the routing decision in the model only considered the selection of the shortest link to avoid the depletion of energy.

Furthermore, in the proposed trust model of [121], when a misbehaving peer is detected, the neighbouring peers can isolate the misbehaving peer for data forwarding or any other cooperative function. Nevertheless, the model only considers counting the systematic failure of a peer as a method of learning the capability of the peer, not the attributes. In this type of model, the learning parameters can be faulty due to the dynamic change of peer behaviour (good or bad). The work of [122] proposed a reputation system-based solution for trust-aware routing, which implements a new monitoring strategy called an efficient monitoring procedure. The model considers the reputation value as a factor in the routing decision that may not explicitly reveal the peers capacity for handling the routing decision.

Recently, due to the rapid development of complex and autonomous P2P networks, the concepts of trust, reputation and cooperation continue to receive an enormous attention in the field of P2P networking. Also, the study in [123]proposed a trust-aware routing protocol for SANETs. Nonetheless, the model cannot escape criticism since it only exploits past node routing behaviour and link quality for determining the efficient paths with no more or less concern about the peer reliability for routing handling.

Opportunistic Data Forwarding

There are a large number of packet forwarding protocols in opportunistic networks. One of the categories of the protocol addresses the problem of packet forwarding to a pre-known single destination peer or group of peers in the network [124].In this type of protocol, it is expected that a qualified forwarder is supposed to have a higher chance of delivering the packets (delivery predictability) either to the destination or another peer that can successfully deliver the packet to the destination. To some extent,

such competency of delivering the data packets is substituted with the probability of meeting the destination [125], based on the peers' behavioural profiles [126] which are generally approximately predicted regarding the peers' encounter. However, most of the routing schemes that are based on this concept ignore the fact that a malicious peer can arbitrarily claim its probability of meeting the destinations based on the rules of the routing strategy. The study in [127]presented a unicast routing technique for multi-hop wireless for opportunistic forwarding titled ExOR. ExOR has a good routing performance. However, it enforces global coordination of among forwarding nodes, which is difficult in large networks. Another drawback of ExOR is there is less possibility of forwarding peers that are connected via fewer quality links to overhear the message acknowledgement, therefore, the forwarding peers can make inconsistent forwarding decisions.

Network Coding

Before exploring the implication of our proposed model in a wireless network, we provide a concise description of network coding. Due to the different constraints of wireless transmission media such as delay, signal attenuation, latency and network channel conditions, the wireless network suffers from low throughputs and frequents unexpected disruptions. Network Coding (NC) is a multicast networking technique in which the packets are encoded and decoded to increase network performance, minimise delays and improve the system robustness. Different NC routing protocols explore the broadcast nature of multihop wireless channels [128] for packets' forwarding decisions. The notion of network coding was initially proposed by Ahlswede *et al.*[129] for achieving the *min-cut* (the maximum amount of flow passing from the source to the sink) in multicast wireless communications. Since then, several other NC routing decisions were proposed in the literature. For example, the opportunistic network coding scheme such as COPE

[130] which uses XOR operation to perform coding.CORE exploits the broadcast nature of the wireless medium through setting each node into a promiscuous mode to snoop packets communicated by its neighbours. The snooped packets are used in coding decisions.

To sum it all up, several trust-aware models based on energy aware, location aware, and delay tolerance will continue to emerge. Considerably more work is needed for further in-depth analysis to advance this research area (trust-based routing proto- cols).

2.5.2 Importance of Trust-Based Routing Protocols

Trust-aware routing is an important routing scheme for efficient collaborative routing between peers in the network [131, 132]. Thus, it is possible to hypothesise that many collaborative wireless routing schemes may not efficiently work if the peers are not able to determine the corresponding trustworthy routing partners for data forwarding and collaborative tasks. Therefore, ascribable to the considerable damages and adverse effects of the untrustworthy or unreliable peer in the routing function, which by extension can affect the quality and reliability of data and routing protocols, analyzing the trust level of a peer has a positive influence on the confidence with which a peer conducts transactions in the networks [133]. A considerable amount of literature has been published on the importance and motivations of a trust-based routing protocol in collaborative routing schemes, see for example [134][135]. The following, is a summary of the importance of trust-based routing protocols.

1. **Detecting selfish and dynamic behaviour analysis -** Conventional security mechanisms cannot address the problem of selfish and dynamic changes of peer behaviour from honest to malicious and vice-versa. However, the concept of trust and reputation have proved to be useful for different dynamic behaviour analyses,

and providing a mechanism for detecting selfish behaviour and adaptive dynamic decision processes [136, 137].

2. **Cooperation, altruist observance -** In contrast to many conventional security solutions, trust and reputation influence self-cooperative behavior through enforcing cooperation and fairness between peers which can help them in detecting and avoiding the effect of a mis-behaving peer on the basis of monitoring, assigning reputation measures to every peer and isolation of the detected misbehaving peer [136, 138].

3. **Generalize and modular solution approach -** In addition to cooperative behaviour, the trust and reputation system provides a mechanism to the peers to fight against any attacks collectively in making a decision about peer behaviour in the processes of trust ranking and scoring a peer, punishing a misbehaving peer or rewarding a behaving peer.

4. **Less complexity-** It is obvious that conventional security solutions requires lots of energy and processing ability for the processes of key generation, key distribution, key management and both encryption and decryption tasks, which are usually complex and computationally expensive, and require significant memory and processing overheads. However, the use of trust and reputation do not necessarily involve such computational techniques as in the case of public key infrastructure [138, 139].

2.5.3 Properties of Trust-Based Routing Protocols

As presented in the above section, the trust and reputation mechanism is a promising solution to the problem of collaborative routing. It is worth mentioning that an effective decision mechanism needed at a routing layer for the peer collaboration and a dynamic

decision can be achieved using the concepts of trust and reputation. Difficulties arise however when an attempt is made to propose a trust-based routing scheme that can satisfy the desired properties of trust-based routing protocols. Summarised below are some of the desired properties of trust-based routing schemes suggested by related studies [140, 141, 142, 143].

- Scalability: The process of trust management should be able to suit a large range of networks with a high level of accuracy and security.
- Portability: The peers should be able to join and leave the network securely at any time.
- Self-Organization: The peers should be able to organize themselves for trust and reputation management. i.e. the trust management processes should not rely on a centralised authority.
- Anonymity:The trust management process between the peers should be anonymous such that it cannot be revealed or known to avoid problems of spoofing, forgery or replay attacks.
- Decentralisation of the trust establishment processes: The trust establishment processes should be highly decentralised, so they can be adapted to the highly dynamic and distributed nature of wireless sensor networks.
- Coping with sparse information: Peers should have enough scoring and ranking information for efficient trust evaluation.
- Location, Context and time specific: Dynamic trust metrics that will take into consideration the dynamic, context-aware and complex nature of distributed networks.

- Integrated confidence measure and credibility: The inaccuracy and uncertainty of many trust models increase with incomplete scoring and ranking and recommendation information available in the network, thus adding a confidence measure that will minimize the trust scoring and ranking sparsity problem is essential.

- Robustness and attack resistance: A good trust and reputation system should be resistant to attacks.

- Behaviour prediction: A good trust and reputation model should incorporate the learning methods of peer previous behaviour patterns for the prediction of peers' future behaviour.

2.5.4 Peers' Routing Attributes in Trust-Based Routing Protocols

One of the critical issues associated with achieving some of the desired properties of a trust-based routing scheme is the integration of peers' trustworthiness concerning routing history and the peers' attributes for understanding peer reliability. It is, therefore, apparent that studying the peers' routing attributes can lead to a greater understanding of developing efficient trust-based routing protocols. Here we highlight some of the reasons why the incorporation of peers' routing attributes is vital for trust-based routing protocols.

- Peers routing context attributes - As with any end-user supported infra- structure, device profile and status (location, buffer size estimation, battery level, and mobility) are useful information for the peers in route selection, quality-of-service verification, and traffic engineering in addition to the trustworthiness of the peers in the network.

- Network context/ Structure or network topology - The network context or topology attributes show network conditions and measurements (link quality, congestion, bandwidth, communication distance, communicability and the geodic distance between the peers) which are all important factors for the exploration of the peer attributes and behaviour in the network. For example, in the case of a Sybil attack or a spoofing attack (a form of stealing peer identities), it would be very unfeasible for the attacker to have a holistic understanding of the network context and topology structure; therefore, the structural information between the peers would not be easy to steal and forge for malicious activities.

- Non-predictable nature of the peer attributes and context - While it is possible to predict trust scoring and ranking behaviour using the current trust and reputation models, it will be difficult to predict and learn the dynamic change of peer attributes and resources. The change of peer energy levels, location and connectivity, which by extension will equally affect the change of peer clustering coefficient, geodic distance and communicability distance, are all non-predictable.

- Powerful representation - Both the peer attributes, and the network topology attributes represents the detailed relationship between the peers, both shortest and longest path, communicability and reachability between the peers, centrality, geodic distance, density, closeness measure which can all be used to model the peers behavior and attributes in the network.

- Spanner property of topology structure - One of the challenges of wireless sensor network solutions is energy inefficiency. Implementing trust and reputation in WSN should take into account the energy needed for communication between peers, link and interface maintenance etc. As a result of dynamic properties

of topology and different cooperative energy spanners, algorithms can be incorporated to optimize the energy needed for trust management while taking into consideration the efficiency of the trust and model implementation.

- Relational nature of problem domain - The nature of trust and reputation can be observed as a relational phenomenon between peers. One can argue that the nature of topology or organisational structure is also relational just as in the case of a trust relationship where the trust and distrust can equally be represented by the weight of the links between the trustee and the trustor. Also, the network science and structure are being used to support the aspect of how information is represented, processed and transformed into the network.

2.5.5 Some Challenges Identified in Trust-Based Routing Protocols

Different proposed trust-based routing schemes in the literature have been vigorously challenged and contested by related studies. Critics question the routing protocol which does not consider the peer attributes and resources for reliable routing decisions. Therefore, we briefly discuss some issues that we believe are open problems in the field of trust-based routing schemes.

While being complimentary to the previous works in the literature, to our knowledge most of the existing approaches focus on developing a model and algorithm without taking into account peer attributes, connectivity and location in the network for trust and reputation evaluations. As a result, prior research has shown that in most of the trust and reputation evaluation protocols, the peer scoring and ranking behaviour is imperfect, noisy and prone to many security issues which limit their predictive power for making routing decisions [144, 145]. This indicates the need to understand and explore the peers' routing attributes that can improve the efficacy of trust-based routing

protocols.

Also, without loss of generality, none of the previous work has explored the roles of the peer attributes such as memory sizes, link capacity, connectivity and the influence of peer similarity in terms of peer routing attributes in trust and reputation evaluation. Consequently, there is a lack of standard orientation for the prediction of the peer attributes in the process of designing trust and reputation models during the following operations: trust evaluation processes, trust propagation and the processes of detecting non-capable peers for routing handling in the network [25].

Additionally, in many distributed implementations of trust and reputation models (for example, Eigen Trust), there are some peers in the network that are known to be trustworthy (pre-trusted peers) in the initial stage of trust and reputation implementation. The free, trusted peers (peers that are given initial trust values) are randomly selected with no prior experience of their reliability for data forwarding and collaborative routing tasks. In the event where the selected pre-trusted peers are non-capable peers, or they have limited resources, the network performance can be affected.

Additionally, while the distributed trust-based routing algorithms were purposely proposed to overcome the challenges of a) the computing and storing of the global trust vector, and b) the problem of central computation storage and message overhead, many trust and reputation models still face some challenges concerning exploring peer reliability and capability for routing decisions. Also, queries in many trust-based routing schemes are flooded throughout the network, with each peer responding to a query if it possesses the file. The peers can then choose a corresponding peer to communicate based on their reputation value alone; however, the peers cannot instantaneously take into account the dynamic changes and intermittent connectivity between the peers and

peer resources which are all important factors for improving the quality of communication between the peers in the network.

Trust matrix sparsity arises from the phenomenon that the peers have no sufficient information of scoring and ranking other peer trust behaviour or when the peers only rate or give a recommendation for the few peers in the network. This is very common in the implementation of trust and reputation algorithms in a sparse P2P network. This problem can affect the recommendation and reputation integrity due to the limited information to judge and predict peer trust behaviour.

As mentioned earlier, the trust of a peer includes both its decision trust and reliability trust. Therefore, the reliability of a peer is a significant factor for trust decision evaluation. However, the goal of many trust models is to identify the sources of inauthentic files and biased peers. In this case, the resultant trust value does not distinguish between a reliable peer with available resources and a non-reliable peer with fewer resources for handling routing tasks. Therefore, such trust-based protocols are limited to a decision trust with no more or less concern about the reliability of the peers in dealing with the routing task.

Notion of prediction and repudiation: In most of the existing trust-based routing models, the peer scoring and ranking habits and behaviour can be learned, forged or mimicked. Likewise, a peer may deny their ratings and refuse to accept the ramification of their actions. This is possible when the trust evaluation of the peers is only based on successful or unsuccessful transactions [97].

Selfish behaviour and bad recommendation problems: Most currently existing trust and reputation models have a principal drawback of not being able to detect noncooperative (selfish) behaviour. As a result, many attacks such as Sybil attack, DoS or colluding attacks, bad recommendation attacks, bad mouthing attacks, ballot stuffing attack and

on-off attack are possible to succeed when using trust and reputation models. For example; slandering, self-promotion by a peer and collusion where participants might give recommendations deviating from their real experience. All these are very common attacks when employing trust and reputation metrics in routing protocols [97, 146].

Self-organization problem: The ability of an agent to predict other agent future behaviour and expectancy of the agent cooperation is essential in trust and reputation models. However, this is difficult to be achieved without formulating an expectancy of the behaviour and the environment. Most of the existing trust and reputation models do not take such aspects into consideration which limits their ability to promote self-organization principles in decision-making processes [147].

Inaccurate peer information such as scoring and ranking behaviour, location in the network, peer rank and roles in the network can affect the integrity and the credibility of the peer reputation evaluation and recommendations decisions. It worth mentioning that most of the trust and reputation models do not take into consideration the details of the peers.

Further, no research has been found that surveyed extensively the concept of trust and reputation in P2P networks about a peer being reliable and the extent to which a peer can handle a routing task, thereby improving the quality of communication between the peers. Previous studies have shown that exploring the peer attributes, and routing ability are some of the essential considerations for quantifying the peer trustworthiness in the network, which was not extensively addressed in the previous studies and literature on trust and reputation management [148].

To sum it all up, as presented in [149], the concept of trust and reputation in collaborative routing between wireless peers encompasses the quality state of a peer being reliable and the extent to which a peer can handle a routing task, thereby improving

the quality of communication between the peers. Consequently, exploring the peer attributes and routing ability are some of the essential considerations for quantifying the peer trust behaviour and reliability in the network. As mentioned in the previous chapter, our notion is that in making a routing decision, the processes of quantifying the trustworthiness between peers can be extended to the exploration of the peer attributes for improving the quality and the state of the peer communication ability.

2.6 Chapter Summary

In this chapter, we presented the systematic foundation of this research and what is already known on this research topic. Chapter Two provided an exciting opportunity to advance our knowledge on the topic of this research. The chapter outlined the key ideas and theories that help us understand the current status of the literature and the need of our proposed contributions. The concept of transitivity, reciprocity and similarity between agents were presented in the chapter as the foundation of our proposed forwarding schemes and contributions in this study. The chapter also gives a concise review of trust and reputation algorithms, a summary of different trust-based forwarding strategies and some challenges identified in trust-based routing protocols.

Chapter 3

Research Design

This chapter introduces and contains a discussion of, the research design and methodology approach best suited to examine the research questions set out in chapter one. The chapter begins with an overview of the adopted research method then it follows with an outlined series of activities of the processes and approaches planned for the experiments and evaluation methods. Given the importance of the research design in the choice of research instruments, a justification of each step, methods, and tools used in conducting this study are provided in this chapter. We present high-level diagrams and the iterative processes involved in conducting this research, the justification of the research methodology and the summary of how each process of the research design was conducted.

3.1 Background: Design of the Study

In recent years, several studies in the field of information systems [150] [151][152], computing studies [153] [154], and engineering [155] have succeeded in integrating design science (DS) research methodology as one of the major components of research in information systems and related disciplines. One of the reasons why the design science research methodology was accepted in computer and information-related disciplines was it incorporates principles, practices and procedures required to carry out scientific

research [156]. Furthermore, the objectives of the DS methodology, which involve consistency between research and the prior literature, a process model for conducting the research and a model for evaluating and presenting the research outcomes, made it feasible to be applied in areas of information science, and computer science related disciplines [156]. To our knowledge, DS is one of the best-suited research methodologies to examine the research questions set out in this thesis.

Moreover, some of the key issues associated with addressing the challenges of a trust model as desired in this study include the integration of different concepts, theories and models from the social sciences (trust, cooperation, dependency and relationships), and peers attributes. Therefore, solving the problems and challenges associated with trust-based routing protocols in P2P networks in a holistic way might not be feasible within the limits and the scope of this study. In this regard, this study will focus more on an objectives-centred solution approach. Throughout this research, the study will focus on a qualitative approach which requires an extensive knowledge of the state of the desired objectives and the series of activities on how to achieve those objectives. Figure 3.1 presents the design study and the process flow of conducting this research. A description of each process is presented in the following sub-sections.

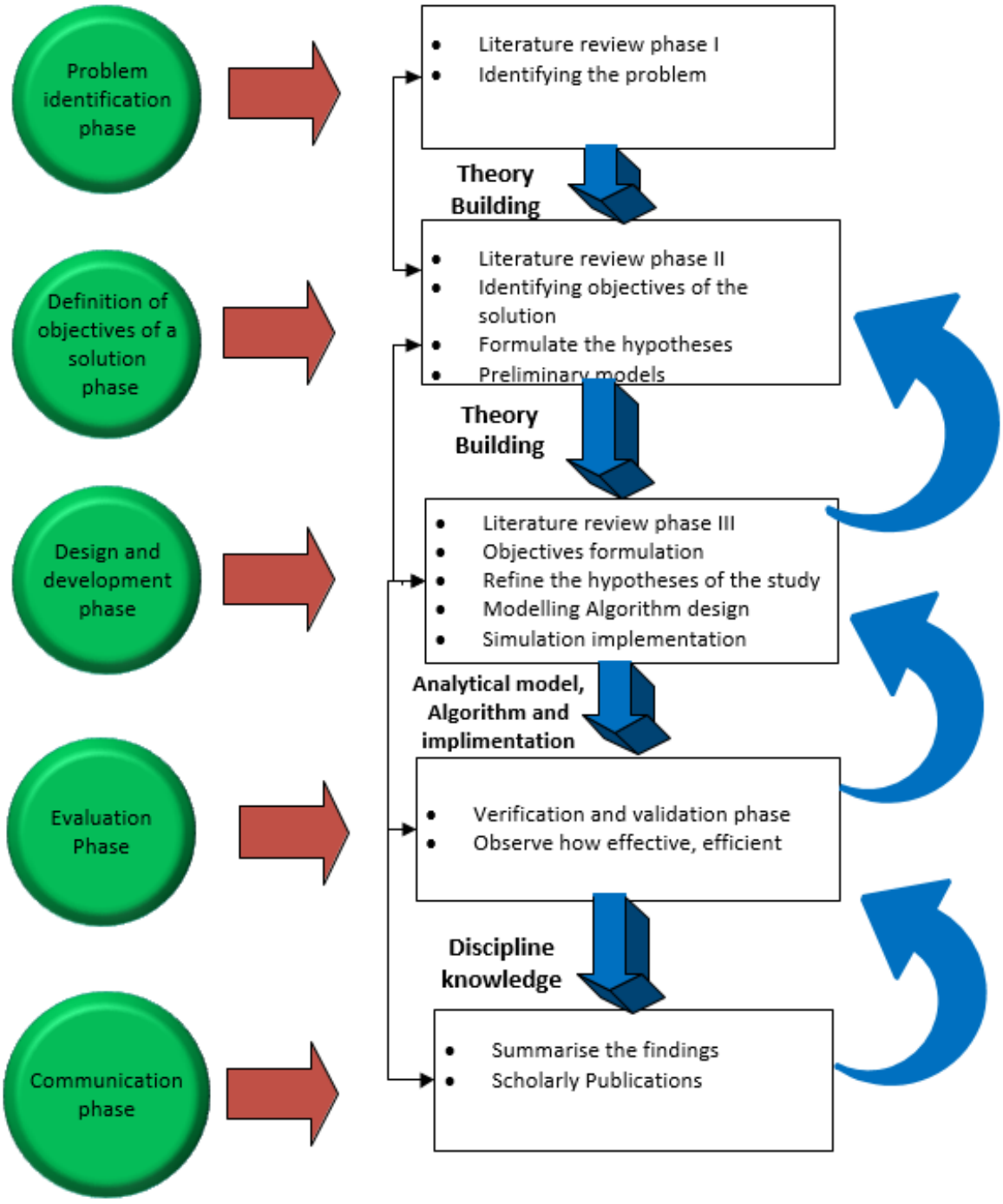


Figure 3.1: Design of the Study

3.1.1 Problem Identification and Definition of the Objectives for a Solution:

The research life cycle of this thesis is depicted in Figure 3.1. The figure shows an integrated approach which we believe is necessary to enable us to answer the questions of this study and to keep pace with technological innovation and organisational acceptance[150]. The methodological approach we adopted consists of five research phases: problem identification, the definition of the objective of a solution, design development, evaluation, and communication.

In problem identification, we identified the research problems from the related literature and findings by other scholars, and we aspire to deduce the objectives in the process of delivering the proposed solution of the study. The outcome of the problem identification helps us to understand the potential insights and impacts on practical applications of our proposed solutions and to build theories. The findings of the theory building help us to understand the research hypotheses, guide the design of the preliminary models, develop new ideas and concepts and construct a definition of objectives of a solution we are proposing. It also helps us in building conceptual frameworks and new models (such as mathematical models, simulation models and analysis)[157].

Since this is a rather long list of difficulties, we, therefore, itemised the objectives of the study as presented in Chapter One. ii) Formulation of hypotheses: based on the itemised list of the objectives, we formulated the testable explanations of the problems and objectives that can be tested by further observations or experimentation. iii) Preliminary models: looking at the outlined objectives and hypotheses, we propose the initial models in chapter Four to test the hypotheses of the study.

3.1.2 Design and Development of the Study

Figure 3.2 and 3.3 presents the systems' design and systems' development processes of this research. In the systems' design process, the objectives of the study were derived from the literature based on the three related areas: (i) Trust, (ii) characteristics and attributes of wireless mobile networks (iii) secure wireless mobile networks. The next stage in the development phase is the modelling and algorithm design. The system design process presented in Figure 3.2, presents essential ingredients of the research design of this study. The figure indicates "an integrated multi-dimensional and multi-methodological approach that generates research results [150]. The figure incorporates four complementary forms phases of this study: theory building, observations, system development and implementation. In the theory building phase, we used different conceptual frameworks, mathematical models method to develop prototype models and algorithms. The theory building phase of the study provides inputs to system development phase and implementation phase in an iterative process. Further, the theory building phase suggests new research hypotheses and guides in the implementation phase and helps in addressing the difficulties encountered in system development activities, which lead to modification of the concepts. The design theory phases of the study include a continuous knowledge refinement an introduction of new ideas/constructs [158].

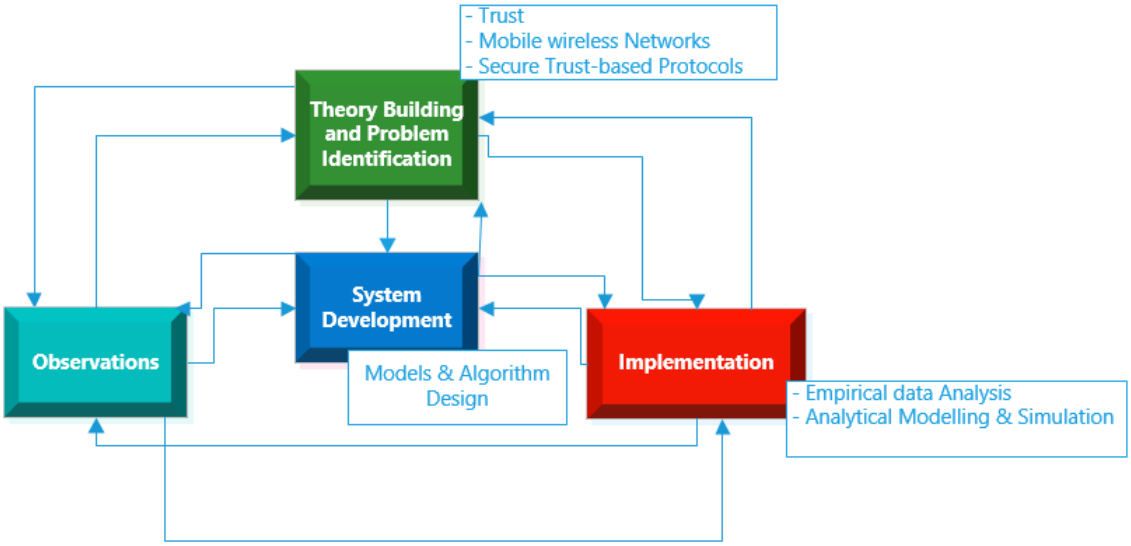


Figure 3.2: Systems Design Process

The initial phase of development processes was a conceptual framework; a footing of new approaches and ideas of the study. The functional entities of the proposed systems components and interrelationships among them were identified in the system development architecture before building the systems' prototype. On the other hand, it was a challenge to find a convenient simulation tool for trust-based routing protocols. This is due to some peculiar characteristics and differences between trust-based routing protocols and the traditional P2P routing protocols. For example, a trust-based routing protocol design involves the process of identification and analysis of trust relationships between peers (*trustworthy peers, non-trustworthy peers*); trust-based routing protocols also include the process of trust management (trust establishment, trust evaluation and trust propagation). These characteristics, however, might not be fully available in the traditional P2P routing protocol validation tools.

Normally, in the design of a trust-based routing protocol, a peers' ultimate goal may depend on its ability to accurately choose a trustworthy peer (not a routing path as in the case of traditional routing protocols) based on certain elements which include

a peers' dynamic routing behaviour in a large range of peer settings. In other words, it involves taking into consideration frequent changes of peers routing attitudes, etc. One can observe that these trust properties might be not be supported by traditional routing protocol design tools for validations. It is therefore important to appropriately understand the validation method and explore the possibility of whether the adopted tools can produce meaningful results.

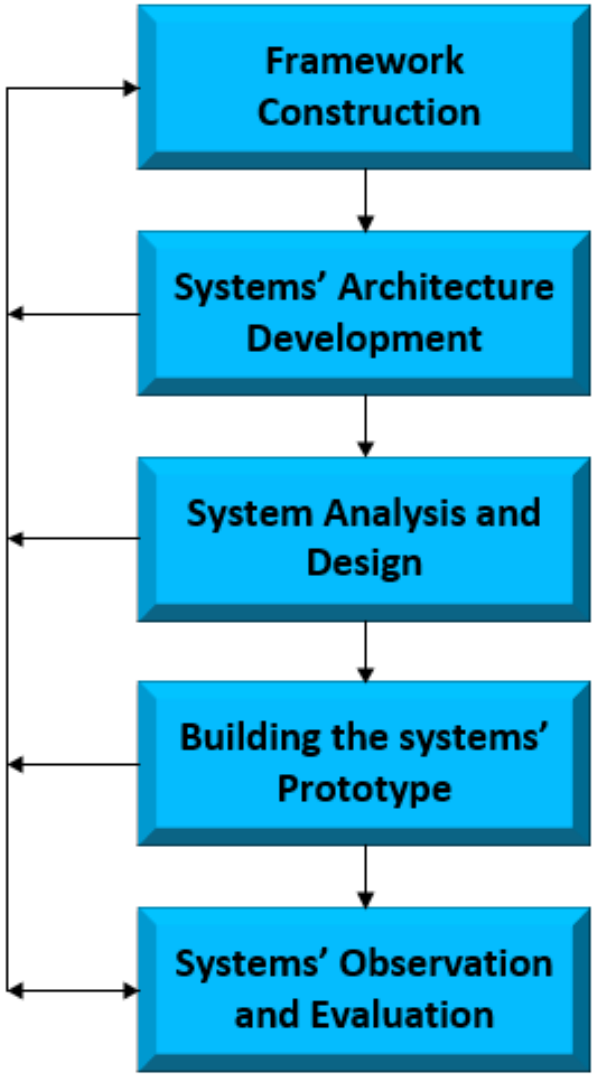


Figure 3.3: Systems Development Process

On the other hand, the use of a testbed for laboratory experiments is an important approach to validate a routing protocol. Especially, since a testbed can be used for real data experiments, it can also capture important details that might not be well addressed in simulation studies. Nonetheless, as the complexity of the analysis increases, so does the need to employ a scalable mechanism to handle the complex scenario. The scalability of the testbed is limited due to the following challenges: limited flexibility, cost, and it might be difficult to reconfigure. Similarly, a testbed does not allow the researchers to accurately reflect the randomness and interdependence present in the real interaction with resources and other system elements [159]. Simulation experiments, however, do take into account the randomness and interdependence which characterize the nature of the real-life applications of trust-based routing protocols.

Furthermore, to some extent, a trust-based routing protocol requires the aggregation of many data flows, interactions and information from peers [47]; therefore, it requires a high level of abstraction for the validation process. The simulator can allow the researchers to examine the general network activities and interactions between peers. It is however, difficult to achieve this abstraction mechanism under which a protocol can be evaluated using a testbed. To summarize, while the testbed can be used to determine the operational status of a simple system and the exact accuracy of the model in a real-life environment, it is however, less suited to general experimentation and evaluation [160]. Therefore, we adopted the analytical modelling and simulation methods for evaluating the research outcomes of this study.

3.1.3 Models' Impimentation

The use of computer simulation for scientific experiments can be traced back to the period directly following World War II, and since then many science-related fields such as nuclear physics, astrophysics, particle physics, materials science, engineering, fluid

mechanics, climate science, evolutionary biology, ecology, economics, decision theory and many more have used simulation techniques. In its broadest sense, a computer simulation can be regarded as a comprehensive method for studying systems [161]. This method includes the activities of choosing the desired model to be tested, developing a strategy of implementing the desired model in a form that can be run and carried out in a computer, calculating the output of the algorithm, and visualizing and analyzing the result of the data [162]. Unlike simple computation, computer simulation studies involves the use of calculation techniques that can be derived from extra theoretical and mathematical concepts.

As summarised in [161], generally, computer simulations can be classified under three different categories. The first category is for heuristic purposes. Under this category, computer simulation can be used to communicate knowledge to others or to explore features of possible representational structures. The second category is when the purpose of the computer simulation is to bring information about how some systems in the real world are expected to behave under a particular set of circumstances, for example, when using computer simulation for prediction. Under the third category, simulation can be utilized for understanding systems and their behaviour. In this category, which is more related to our interest, a computer simulation can be used to answer questions about how events could have occurred, or are about to occur. Often, but certainly not always, the method of implementing a trust-based system is by means of a computer simulation; a few examples include [163, 164, 165].

However, it is worth acknowledging that the choice of simulator that supports the properties of a trust-based routing protocol is challenging. Therefore, instead of adopting a single simulator that may not cover the wide scope of this research, and may give us a monolithic simulation result, we chose two main simulation tools. The simulation

experiment adopted in conducting this research is a mixture of two simulation environments. This became necessary due to the nature of the research objectives outlined in this study.

Trust and Reputation Simulator for Wireless Sensor Network (TRMSim-WSN)

The Trust and Reputation Simulator for Wireless Sensor Networks (TRMSim-WSN) [2] is a Java-based trust and reputation model simulator aimed to provide a convenient and feasible way to test a trust and reputation model over WSNs settings and to compare it with other existing models. It is widely used for the implementation, testing and validation of trust models in different network systems such as distributed WSNs, P2P Networks, Multi-agent systems, etc. It provides several Trust and Reputation models such as Eigen Trust [84], Peer Trust [166], Power trust [88], Trip Trust [165] etc. It also allows researchers to implement and test their developed trust and reputation protocols using either static or dynamic topologies. TRMSim-WSN also allows researchers to model peers message forwarding behaviour such as fraudulent behaviour and benevolent behaviour of peers in the design of message routing protocol.

Some of the useful features of TRMSim-WSN include flexibility for changing network topologies in which communication links are created/destroyed, varied implementation of trust models and algorithms, and it allows adjustment of simulation parameters to test a wide range of network design and trust evaluation rule changes. We therefore employed TRMSim-WSN to test the preliminary concepts for peer trust evaluation. We used TRMSim-WSN to study the influence of structural transitivity for trust propagation and evaluation between peers in a distributed network setting as presented in Chapter Four.

Figure 3.4 shows a screenshot of the main window of TRMSim-WSN. To perform a

simulation using TRMSim-WSN, one can create a network of WSN using a minimum and a maximum number of peers or by importing the desired network topology to be simulated from an XML file. The wireless range parameter of the peers can be increased or decreased by adjusting a range radio button. The percentage of benevolent, malicious, relay and idle peers can be set. Depending on the default trust algorithm parameters, the models' parameters can be adjusted from the setting frame.

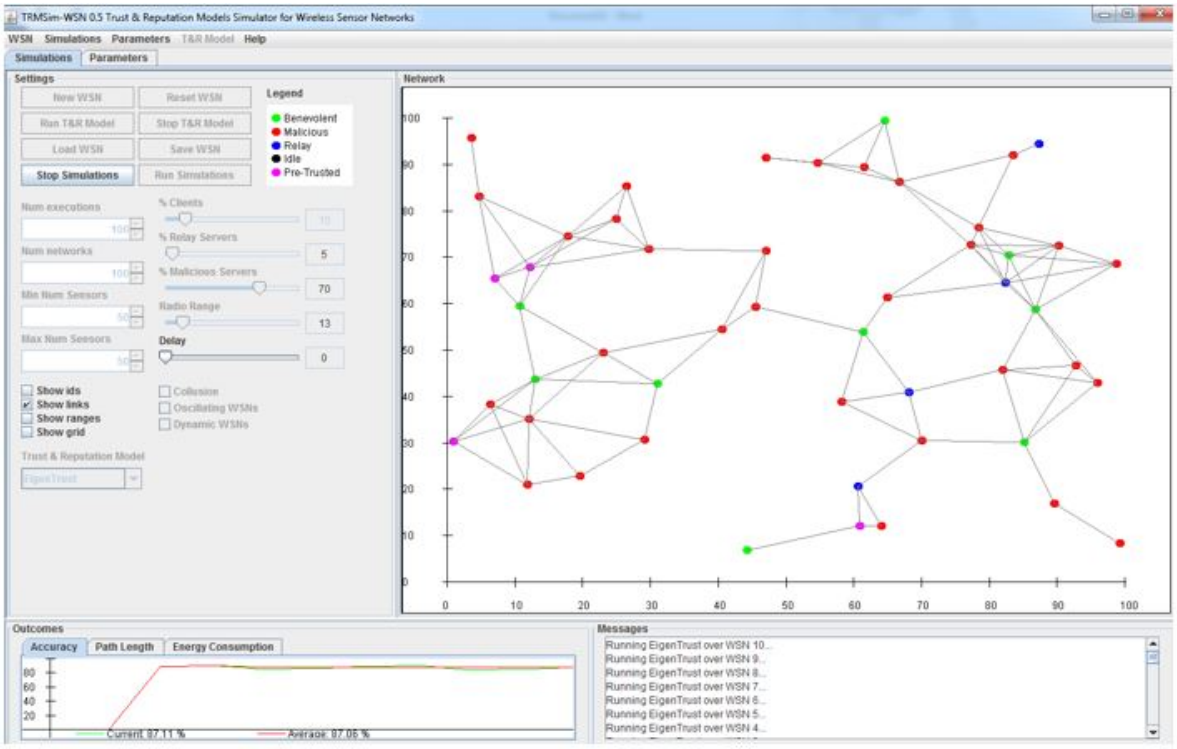


Figure 3.4: TRMSim-WSN Simulator Screenshot

TRMSim-WSN Simulator: Trust and Reputation Model Scheme

Every trust and reputation algorithm has its own specific characteristics and requirements; nonetheless, their pattern and abstract scheme can be generalised as presented in Figure 3.5. The figure presents the series of transactions of a trust model in a distributed system [2]. TRMSim-WSN, among other trust simulators, operates based on this scheme. The first method is responsible for gathering information from other peers

in the network for trust evaluation. This includes gathering local information (direct experience) and global information through indirect experience or recommendation. Based on the collected information in the first method, the score and ranking methods are used to score each peer along the path to a service-providing peer (server).

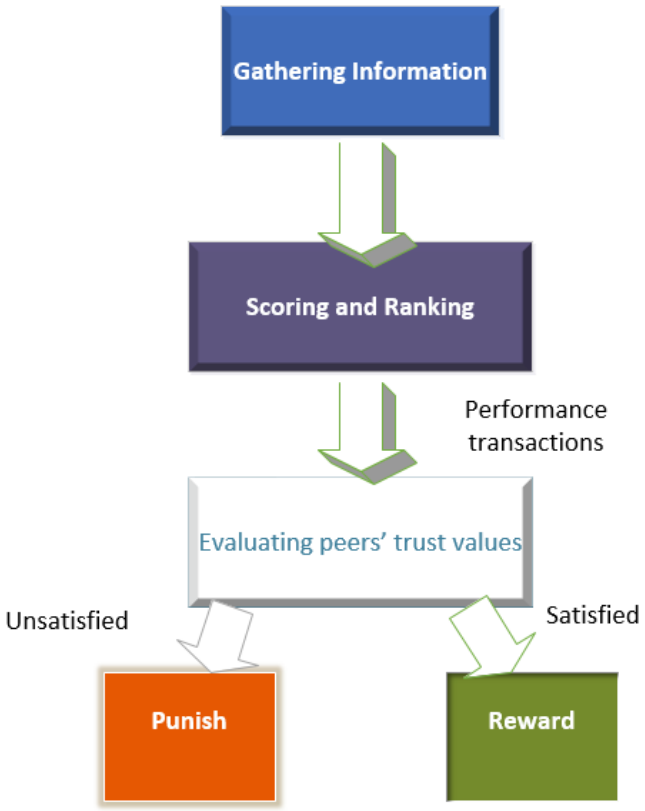


Figure 3.5: Generic Trust and Reputation Model Scheme

The result of ranking the trust level of the peers is that this step will return the most trustworthy service provider. The transactions and evaluation method can then be applied for the peers to get the required service from the selected most trustworthy peers (peers with a higher-ranking score). After the transactions, the receiving peers can then evaluate the service received from the service provider and score it accordingly (higher, lower) depending on the trust evaluation method. Finally, the punish and reward

methods perform the function of rewarding good serving peers and punishing the peer that is providing less quality service. It is however, worth emphasizing that some trust algorithms do not apply the reward and punishment phases in trust evaluation.

TRMSim-WSN Simulator: Main Classes and Reputation Models Interface

Figure 3.6 presents the diagram of the main classes used with the TRMSim-WSN simulator. As can be observed, both the client and server sensors are both subclasses of the sensor class with a client peer requiring a service from the server; therefore, every client peer uses its trust and reputation model to evaluate the servers, search for the most trustworthy service provider and punish or reward the service providers.

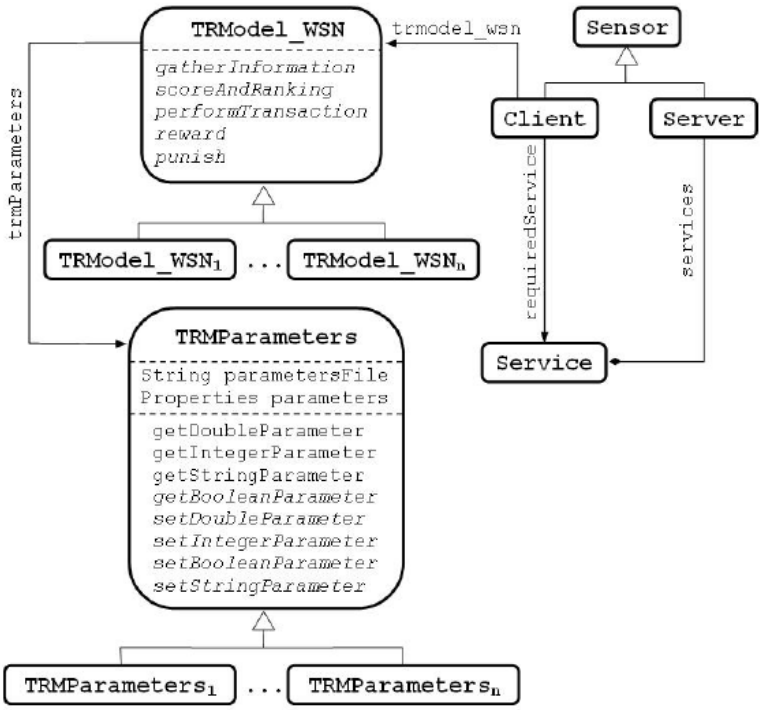


Figure 3.6: TRMSim-WSN Simulator: Class Diagram of Main Classes of the Generic Trust and Reputation Models Interface [2]

Although TRSim-WSN has been designed to model the peers trustworthiness based on the successful message transaction between the peers, it is also designed to adapt

quickly and to integrate a new trust model with the addition of few classes. However, it has some limitations for addressing the research objectives of this study. For example, TRSim-WSN does not have routing and network performance modules (which can report on delivery ratio, message latency, the number of packets received, packets drop, etc.). Therefore, drawing a conclusion based on the authenticity of the packets sent and received by the peers, may not accurately reflect the scenario of the network routing performance. Furthermore, TRSim-WSN does not have mobility modules, which limits its power to model the dynamic routing behaviour of the peers while in motion. Perhaps the most serious disadvantage of TRSim-WSN in answering the desired questions of this research is that, it does not allow the researcher to implement different wireless peer interface mechanisms and it is challenging to reconfigure the malicious peers to reflect the characteristics of misbehaving peers in the network. Therefore, we sought to identify a different tool that could satisfy some of the additional objectives of the study.

3.1.4 Opportunistic Network Environment Simulator (ONE Simulator)

The Opportunistic Network Environment Simulator [3] (popularly known as the ONE simulator) is a communication networking system that enables communication between peers in a setting where there are no end-to-end paths between peers in the network. The goal of the simulator was to add more realism to the simulation of a routing protocol in an intermittently connected P2P network design. Various related studies have adopted the use of the ONE simulator [167, 168] especially in the design of Delay Tolerant Networks (DTN). Figure 3.7 presents an overview of the whole process of the ONE simulator. For the purpose of this research, we created a trust-based internal routing logic adapted from the TRSim-WSN simulator and we incorporated it into the ONE internal routing module. The internal routing module is a routing engine that

performs operations on the messages in the ONE simulator and it is a module that determines where the messages or bundles can be forwarded, based on the received connectivity data and routing data. In our experimental studies, when a peer wishes to transfer messages to other peers, it will receive the trust related data, peer connectivity data and peer buffer data for the trust decision before it starts the transfer, which in turn forwards the request to the other nodes to seek more information. Unlike other routing protocol simulators which centre on routing simulation, the ONE simulator combines different modules such as mobility, routing simulation and visualization into one package that provides a rich set of reports and accessible development platforms.

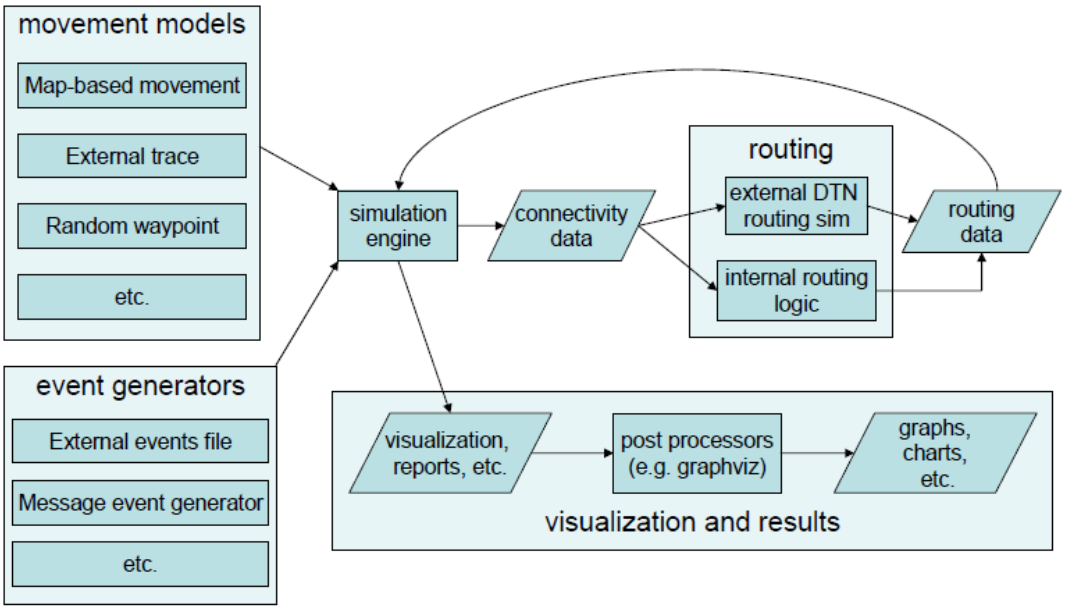


Figure 3.7: Overview of ONE Simulator [3]

Routing protocol validations require comparison with other existing protocols. The One simulator also has a variety of protocol modules such as [169, 170]. This made it easy for the researchers to develop their protocol prototypes and to compare it with different protocols for performance evaluation. It also significantly reduced the simulation development time, thus enabling the researchers to concentrate on their research

questions. Given the significant number of protocols that were already implemented in the ONE simulator and the platform to implement and to compare those protocols was a newly developed one, it will take a researcher less time to validate the aspects relevant to the questions being studied. Figure 3.8 presents a screen shot of a simple interface of the ONE simulator. The ONE simulator can be run in either GUI or batch mode. When a new routing module is created, it can be observed from the GUI intuitively. All simulation results are gathered using the output of the report modules.

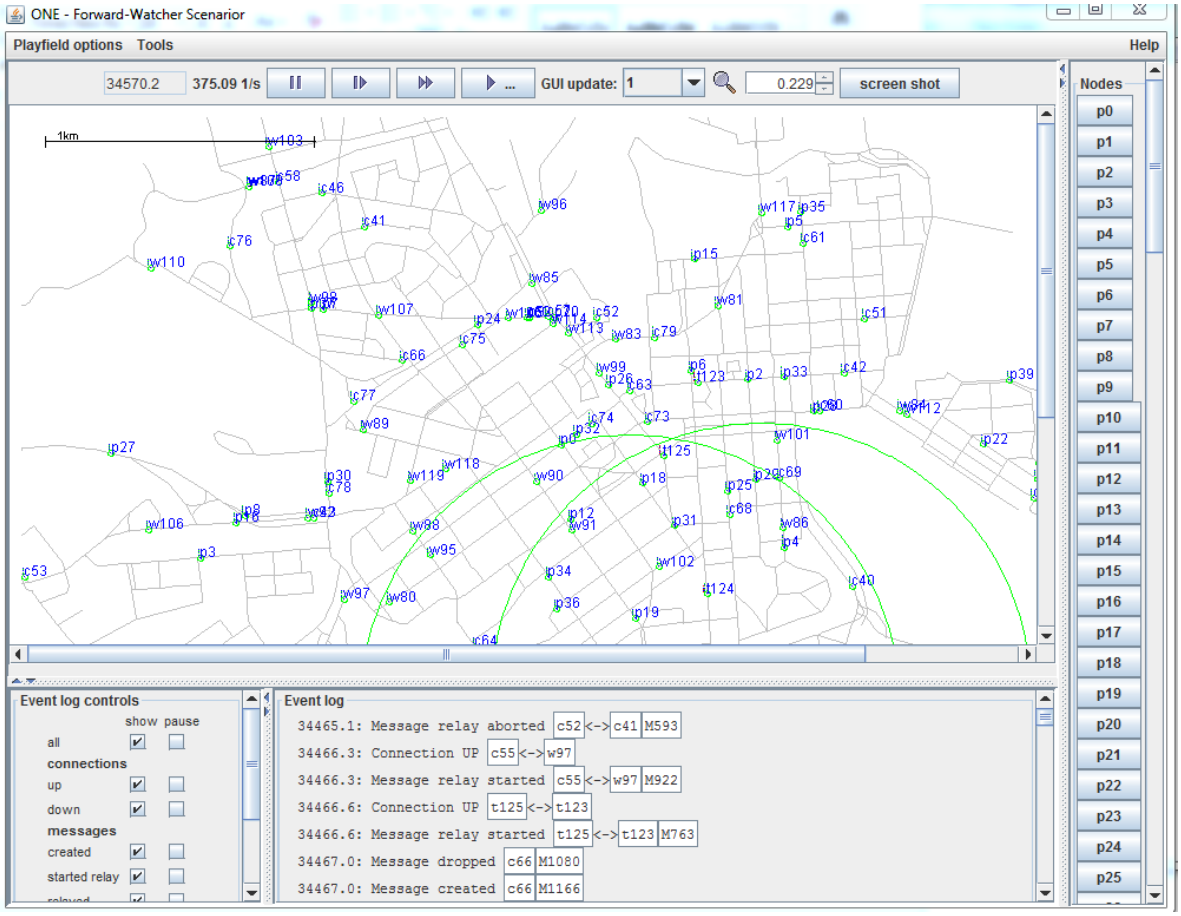


Figure 3.8: ONE Simulator Screenshot

Although, the ONE simulator is the most comprehensive tool identified for this study so far, it does suffer from a number of flaws and limitations. For example, in the ONE simulator, many real-world aspects and conditions were abstracted, discarded

or assumed to be perfect. Therefore, there are limits to how far a researcher can implement his/her ideas to reflect the detailed scenarios of the physical environment since such simulation tools tend to overlook some physical factors and constraints. All the studies reviewed so far however, suffer from the fact that routing simulators have limitations mimicking physical environmental conditions. Similarly, the ONE simulator is not purposely a trust-based routing simulator. Therefore, implementing a trust and reputation routing algorithm requires additional programming skills to either incorporate existing trust algorithms or to develop a new one. Another limitation of the ONE simulator is that the simulation environment lacks the details of the lower layers, such as MAC layer and physical layer. For example, when two peers are in the transmission range of each other, they can communicate at whatever speed is configured. Nevertheless, this feature made it possible for us to implement our proposed Forward-Watcher routing scheme presented in Chapter Seven, since the radio devices that the peers use in the simulation are regularly turned on, whereas, in real-world scenarios, they are often switched to idle mode to save battery power.

3.1.5 Evaluation

So far, little work has been done to establish a general analytical metric for reputation systems; similarly, there is no customarily recognised evaluation benchmark that one can use to compare different mobile wireless protocols and models under certain conditions and common representatives [171]. Nevertheless, some related studies used the ONE simulator in evaluating DTNs protocols, see for example [172, 173, 174]. Thus, we adopted some of the techniques used by different related studies: more specifically the work of [174] and [175] for evaluating our proposed solutions. We evaluated our proposed solution in comparison with other protocols to determine the average-case

performance of the models. To achieve this, we ensured that the implementation environment of our protocols supported our assumptions and the desired output of the protocols. Since we based our proposed contributions on making predictions, it is, therefore, important that the models we proposed, the assumptions we made and the process of developing the research outcomes, were realistic and related to the physical environment. In this regard, we employed the use of empirical data analysis to study the Wireless Local Area Network (LAN) traces and incorporate the traces in the simulator for protocol evaluation in comparison with other solutions. Also, we optimized the attacking models with optimal attack strategies so that we could optimally evaluate the efficacy of our proposed schemes in comparison with other existing protocols. For this purpose, we evaluated our proposed schemes using delivery ratio, protocol overhead and average message latency, since they are the performance evaluation metrics used in related studies including [113],[175], [176],[177],[178], and [172].

3.1.6 Traces Analysis Framework for Model Evaluation

We used the presented traces analysis framework in Figure 3.9 as a guiding methodology in our empirical data analysis. All the traces were collected from an extensive traces library as described earlier. We then represented the collected data into a network representation (adjacency matrix) to analyse various aspects of user mobility, contacts and the dynamic encounter between the peers. Based on the direct inference of the finding in the traces analysis we proposed a transitive routing protocol as presented later in this thesis.

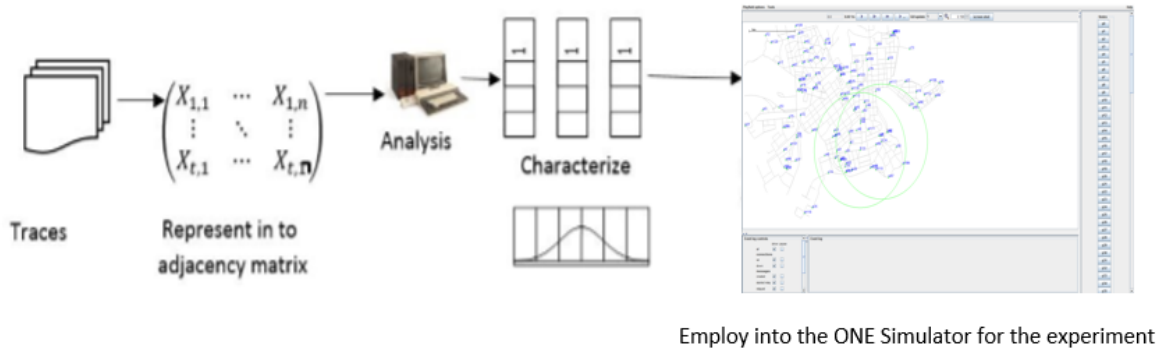


Figure 3.9: Illustration of the Traces Analysis Frame Work

3.2 Incorporating Our Proposed Schemes into DTN Routing Protocol System for Evaluation

Keeping in mind the challenges and the feasibilities of incorporating our proposed schemes into different network scenarios, we itemised some of the advantages associated with implementing our proposed solution in the ONE simulators for Opportunistic Networks as listed below.

- Originally, the concept of opportunistic routing was introduced by Biswas and Moris in their proposed protocol, Expected Opportunistic Transmission Count (ExOR). The opportunistic routing scheme aimed at exploiting the diversity of multi-hop networks that allow nodes that overhear the message transmission to simultaneously forward the packets, or use the forwarding information while making routing decisions. Our proposed Forward-Watcher model presented in Chapter Seven posed similar design principles: that the forwarding decisions between peers in wireless multihop depend on the peers ability to overhear the messages forward of their corresponding subjects.

- DTNs are designed for message forwarding from the source to the destination. Based on the conditions of the nodes selection strategy, any selected peer can

continue forwarding the packets further towards the destination while meeting certain conditions. All the proposed forwarding schemes presented in this thesis have similar properties of forwarding a message from the message source until it reaches the destination through multiple forwarding of messages by the peers in the network.

- Any DTN peer may generate a message for any other peer and may also carry a message destined from other peers. Similar to the proposed forwarding schemes in this thesis, every peer in the network can randomly generate a message and forward it toward the destination, and also can serve as a message carrier generated by other peers.

- The Opportunistic routing consists of two main components: forwarder set selection process and forwarder set prioritisation. In our proposed forwarding schemes, we modelled the forwarder set based on the peers subjects (the neighbours of the message carrier), and forwarding prioritisation builds on the aggregated trust level of a peer.

The evaluative model presented in Figure 3.10 shows the mode of evaluation of the experimental phase in this thesis. As presented, the evaluation model covers two main aspects. One aspect of the evaluation model shows the analytical modelling and empirical data analyses. In this regard, we obtained the traces used in this study from the Community Resource for Archiving Wireless Data at Dartmouth (CRAWDAD) [179] for empirical data analyses. To our best knowledge, CRAWDAD is one of the most well-known archives for wireless traces established for the purpose of resource sharing in a community that meets the needs of this research. We then represented the collected data into a network representation (adjacency matrix) to analyse various

aspects of user mobility, contacts, and the dynamic encounters between the peers. Based on the direct inference of the findings in the traces analysis, we used the results of our analysis to propose a new data forwarding strategy.

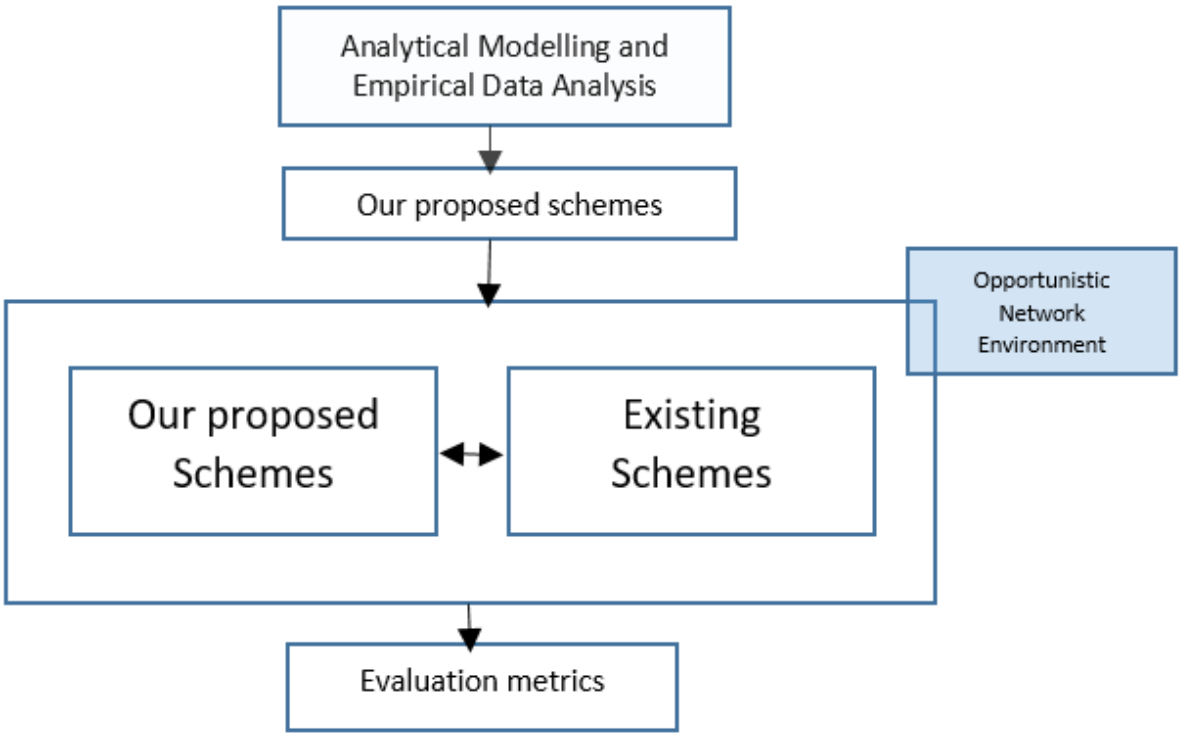


Figure 3.10: Evaluation Framework

The second part of the evaluation model shows the implementation of our proposed system and comparison with other existing routing protocols. In each chapter in the thesis, we implement the proposed contribution in the Opportunistic Network Environment and evaluate its performance with other solutions in the literature. So far, little work has been done to establish a general evaluation metric for trust-based routing protocols; similarly, there is no customarily recognized evaluation benchmark that one can use to compare different trust and reputation models under certain conditions and common representatives [171].

3.3 Chapter Summary

This chapter presented the overall research design and the detail of the iterative processes of conducting the study in this thesis. Given the importance of the research methodology in the choice of research instruments, in this thesis, we use Design Science Research Methodology (DS) for conducting this research. One of the reasons why we adopted the DS research methodology was it incorporates principles, practices and procedures required to carry out scientific research related to this study. In this chapter, we presented a justification for each step, method, and tool used in conducting this study. The chapter also presents high-level diagrams and the iterative processes involved in conducting this research. The chapter also presents the different evaluation techniques used in this study.

Chapter 4

Transitivity and Network Performance Metrics Analytical model

In this chapter, we hypothesise that in the design of a trust-based routing protocol, the exploration of the peers routing attributes could significantly improve trust evaluation accuracy. In this regard, we studied the properties of complex networks and their impact on trust and reputation propagation and evaluation. We started by illustrating the structural transitivity in the network and its approximation. We then proceed to present the theoretical and analytical relationship between trust and reputation model accuracy, average structural transitivity between peers, average shortest path between peers and energy consumed by peers for trust and reputation propagation and evaluations. The experimental studies using simulation have further supported the results of the analytical study. In this chapter, we are paving a new angle of research on exploring the complex network properties impact on trust and reputation evaluation between wireless peers.

4.1 Background

To remedy the flaws of the existing trust-based routing scheme discussed in Chapters One and Two, we proceed to explore different complex network metrics and models that influence trust and reputation evaluation.

Recently, network science has emerged as a new interdisciplinary field of study that allows scientists and engineers to analyse different network concepts and the connection among elements of the complex agent systems associated with large networks. In simple terms, a network is a collection of vertices or elements that are connected by links [56]. In principle, such a high level of abstraction can be applied to any system of agents, thereby providing a conceptual representation of interrelationships between interacting agents or peers.

Some related studies, including [180], proposed a trust-based recommendation using topological attributes (vertex similarity between peers) based on the intuition that a good peer to seek a recommendation from, is a peer that is connected to many neighbouring peers. On the other hand, the study of trust and reputation models in routing protocols deals with the local and global routing behaviour of the peers. It is however, important to emphasise that the network approach also deals with mapping the interactions between peers. Therefore, the detailed properties of each peer (local information of a peer), and network level (global information) can give substantial information about the behaviour of interacting peers for proper trust propagation and trust evaluations between peers in the network [181].

We drived our inspiration from the view of the so-called "network thinking" paradigm which was recently adopted by many researchers as an analytic technique used to study the concepts of interacting agents in the contemporary view of complex networks.

4.2 Transitive Connectivity For Trust Propagation and Evaluation

Several trust and reputation models have been proposed around the idea that connectivity between peers has a significant effect and can influence trust propagation behaviour in P2P networks [182]. Also, trust inference, which is one of the mechanisms for building a trust chain between peers, is a relation-driven phenomenon. Therefore, understanding a relationship that infers trust between peers who are directly or indirectly connected might be an important contribution in peer trust modelling and evaluation. Here, there are three main issues that need further exploration: the first issue is which category of the peers relationship (connectivity) can facilitate effective trust evaluation between peers and by extension can enhance collaborative routing decisions in P2P wireless networks. The second issue, is to investigate whether there is any correlation between the identified peer relationship (connectivity) and network performance metrics which are the essential consideration in the design of routing protocols. Third, routing selection algorithms should be introduced based on the identified peers relationships or connectivity.

In this chapter, we attempt the first two questions, and attempt the third question in Chapter Six. We study structural transitivity for trust and reputation evaluation between wireless peers. We base our notion on the assumption that the trust and reputation evaluation between wireless peers is not merely a function of trust models, but also a network-wide activity in which the network structure matters. We propose that the presence of a transitive relation anchor (transitive-chain) in a network of peers is more likely to promote an effective trust and reputation evaluation process. That is, when the peers are connected in a transitive form, they will be more likely to facilitate

the trust recommendation or referral process, thus providing an effective trust evaluation system and further yielding good routing performance between the peers.

Additionally, to obtain a derived metric that can quickly and intuitively give an indication of the relationship between structural transitivity, network performance in relationship trust and reputation evaluation. We derived the mathematical relationship between structural transitivity and average shortest paths, and average network efficiency.

The studies in this chapter collects the combined metrics of network performance, and trust evaluation in a style that focuses on principles that are likely to be valuable in trust-based routing protocol design. Furthermore, we believed that a fast and efficient trust-based routing algorithm could be realized using the presented performance matrix-based model.

Before defining transitivity in our network model, let us look at the concept of trust transitivity. Essentially, the properties of trust propagation on networks, based on a simple metric of trust transitivity, can be a requirement for the viability of global trust propagation in large systems [183]. When a trust relationship between peers is transitive, the trust extends beyond the directly trusted and the trusting peer to any other transitively trusted peer in the network. An illustration of the transitivity trust inference in the expression below can be understood as the essential elements of trust propagations, stating if $p\,T\,q \wedge q\,T\,r$ (meaning if p trust q, and q trust r) then, there exist the possibility of q to refer r to p, so that p can trust r as well. For simplicity, this can be illustrated as follows: $\forall\, p,\, q, \in N : p\,T\,q \wedge q\,T\,r \;\therefore \exists\, p\,T\,r$.

Therefore, this can be understood as, in a given wireless network $G = (N, L) : p, q \in N$ and $L \subseteq \{(p,q)\}|p, q \in N, : p \neq\ q\}, \forall\{(p,q)\} \in L\colon \{(p,q)\} \wedge \{(q,r)\ \in L \therefore \exists\{(p,r)\} \in L$

Where L : represents the wireless connection between the peers.

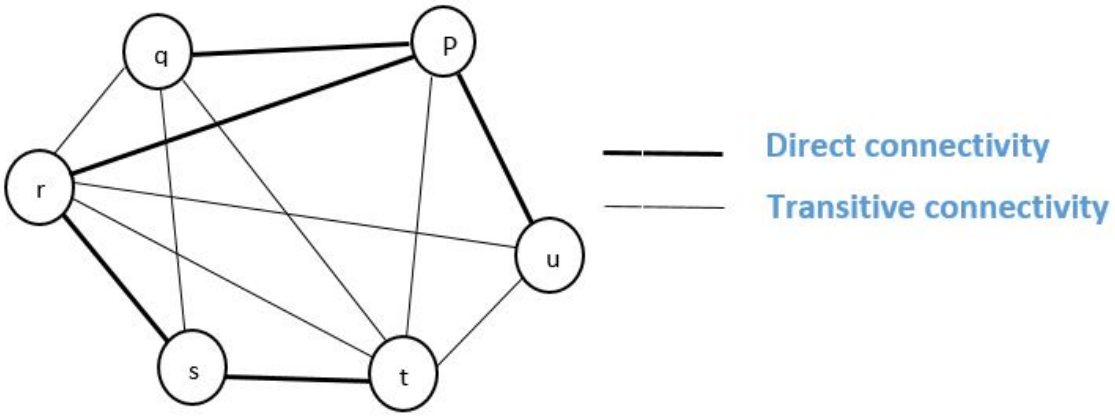


Figure 4.1: Network Transitivity Model

4.2.1 Transitivity Network Model

In particular, we are more interested in the proportion of transitive relations (that express a degree of balance in the network), which most theorists have proposed as an "equilibrium" or natural state toward network and structure formation that tends to efficiently promote trust and normative relationships between the actors in the network [184].

Consider the diagram in Figure 4.1, where node p and q are directly connected with each other. In the first place, q can interact with r based on a recommendation or referral from p; likewise through a recommendation from p, r can easily reach to u based on the transitive recommendation or referral from p. Also, r can reach to t through transitive referral from s. From the figure, it can be seen that every agent can easily trace a corresponding agent either through direct connection or through a transitive connection. This also expresses the fact that, if the peers are transitive anchor connected, they can easily reach each other with less effort and within the shortest possible distance.

Transitivity Coefficient Approximation

Given a network $G = (N, L)$ consisting of peers $N = \{p, q, r\}$ and the set of communication links between the peers $L \subseteq \{(p, q)\} : p, q \in N$, and $p \neq q$. Therefore, the transitivity coefficient between the peers in the network is given by the proportion of links between the peers within its neighborhood divided by the maximum number of links that could exist between the peers.

If we denote the number of immediately connected neighbours or (clique members) of peer p as $n_p : n_p = \{q : \{(p, q)\} \in L \wedge \{(q, p)\} \in L\}$: $\{(p, q)\}$ is distinct from $\{(q, p)\}$. For each peer $p \in N$ there are possible number of distinct wireless interface connection $n_p(n_p - 1)$ that could exist among the peers within the neighbourhood of peer p. Therefore, we can define the local transitive coefficient of peer p $T_{coef(p)}$, by the proportion of the exact interfaces between its neighbours divided by the number of interfaces that possibly could exist between them as presented in equation (4.2).

$$T_{coef(p)} = \frac{2\{|\{p, q\} : p, q \in N_p, \{(q, p)\} \in L|\}}{(n_p(n_p - 1))} \tag{4.1}$$

Throughout this thesis, we are considering the undirected graph for network modelling; thus, to approximate the local and global transitivity in a given network, we use the clustering coefficient metrics to determine the degree of clustered peers. Here, we rely on the assumption that for undirected graphs, the weighted clustering coefficient is simply transitivity as inferred in [185]. Depending on the strength of interdependency between network members, the clustering coefficient can reveal the transitivity level and interdependency between connected peers. Therefore, the average global clustering coefficient of the network can be estimated as the average transitivity coefficient of the network [186].

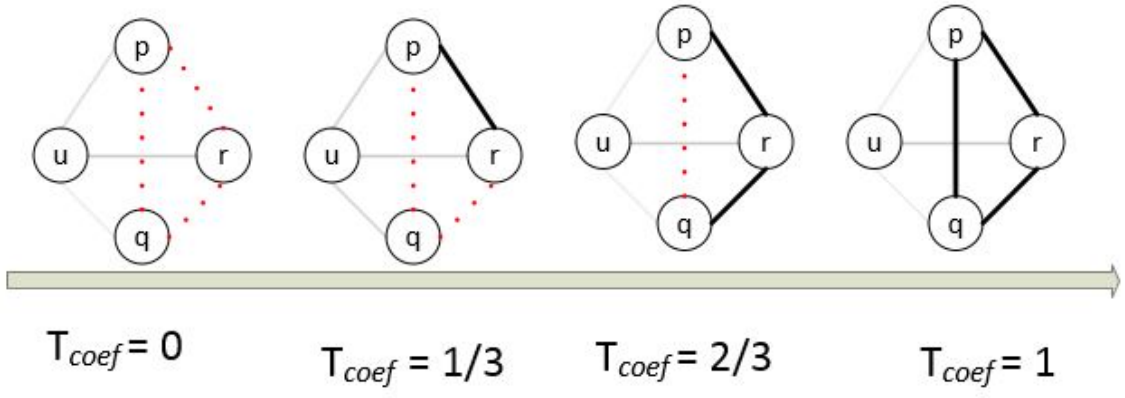


Figure 4.2: Transitivity Illustration

$$av.Tra(N) = \frac{1}{n}\sum_{p=1}^{n} T_{coef(p)} \tag{4.2}$$

4.3 Transitivity and Network Performance Modelling

In the previous subsections, we discussed the relationship between trust propagation strategy and the transitivity relationship between peers. In this section we are interested in seeing the relationship between transitivity and network performance metrics which by extension are properties of efficient trust-based collaborative routing.

From the diagram in Figure 4.2, it can be observed that as the edges (connectivity) between the peers increase, the structural transitivity increases. For example, by adding a connectivity between p,r the transitivity coefficient increases from zero to one-third etc.

4.3.1 Transitivity and Shortest Path Model

Let us first consider the distance among wireless peers in the network; and by distance here, we mean wireless distance between the peers based on peers radio interface ranges. We therefore, consider the definition of the shortest path metric of the undirected, unweighted network, which we can derive from equation (4.3) as follows:

$$Av.SPath(p- > q) = \sum_{p,q \in N} \frac{Dis(p,q)}{n(n-1)} \tag{4.3}$$

i.e,. the shortest path between p and q is the average shortest path between the two peers and n represents the number of hop counts between p and q.

Also, as presented in Chapter Two, transitivity characterizes the local cohesiveness of networks as well as the propensity to form clusters of interconnected peers [187]. Therefore, one can deduce that the more the peers are clustered, the higher the cohesivity between the peers and the less effort it takes peers to spread aggregated trust (reputation) among peers, for trust evaluation [188].

Also, as presented in chapter two. The transitivity characterizes the local cohesiveness of networks as well as the propensity to form clusters of interconnected peers [187]. Therefore, one can deduce that the more the peers are clustered, the higher the cohesivity between the peers and the less effort it takes peers to spread aggregated trust (reputation) among peers, for trust evaluation [188]. In addition, we can define the closeness centrality of the peers in the network as follows:

$$CC(p) = \frac{n-1}{\sum_{p \neq q} Dis(p,q)} \tag{4.4}$$

Where $Dis(p,q)$ denotes the distance between p and peer q. From equation (4.4) and 4.2, we can deduce that a small average shortest path length between the peers yields

a large structural transitivity coefficient between the peers in the network. Therefore, the higher the average transitivity between the peers the higher the closeness centrality between the peers in the network.

4.3.2 Transitivity and Energy Model

Among others, energy consumption, data rate and transfer time are parameters that are essential in trust-based routing protocol design. Therefore, it is important to discern a better understanding of energy efficient network operation for proper trust-based routing protocol design.

Compared to traditional security solutions (hard security solutions), trust and reputation models are relatively better regarding energy overheads. However, the process of reputation aggregation, and evaluation of trust-based routing involve a series of messages transferred between wireless peers. Therefore, taking into account the energy model while designing the trust and reputation model is essential. As presented in [189] the energy needed for the two peers to communicate in wireless network settings is a function of the distance between the source peer and the destination peer.

$$E(p->q) = Dis(p,q)^{\alpha} + pow \tag{4.5}$$

i.e., the energy needed for two peers p and q to communicate depends on the distance between them and the processing power as indicated in equation (4.5) where α denotes the media attenuation coefficient factor and pow denotes the processing power. Thus, for the design of a trust-based routing protocol, the presented energy model can be understood in two ways. Firstly, if a peer is located at a nearby location of other peers,

then it results in a reduction in the number of hops between the peers. Therefore, that condition can help in reducing the total energy and bandwidth consumption to forward messages and in minimizing the convergence of trust data (reputation). Secondly, the lower hops counted from the sources to the destination, can reduce message latency.

4.3.3 Network Efficiency Model

Some of the challenging aspects of designing trust-based routing protocols which work in a collaborative fashion, include network efficiency and peer energy depletion while trying to identify and establish communications with other peers in the network. Subsequently, the design of trust-based routing protocols is not limited to only one set of elements (peers) but includes an inter-relationship between the peers (i.e., links) and how efficiently the peers can communicate (exchange trust data or reputation). Furthermore, the ability of the network to resist structural attacks or structural vulnerability exploitations (failure of a networks' topological structure) depends on the efficiency and structural balance of the network [190]; i.e. how the network of peers can resist node failure or link failure [191].

Additionally, a good design principle of a trust-based routing protocol should take into consideration the characteristics of attacks such as Sybil attacks, blackhole attacks, wormhole attacks, etc. These types of attacks can cause a section of the network or some peers in the network to malfunction or to be converted into attacking peers. Therefore, understanding the nature of an efficient network structure that can withstand the presence of compromised nodes or links in the network by using trust-based routing design is essential [192]. Network efficiency is a measure of how efficiently peers can exchange information, which can be applied to both local and global scales in a network. Therefore, we define the network local efficiency as the inverse of the average

shortest path (as described in equation (4.3)) between the peers in the network.

$$E_{loc}(N) = \frac{1}{n} \sum_{p \in N} E(N_p) \tag{4.6}$$

where N_p is the local sub graph consisting only of a peer p's immediate neighbors (peers in the same transmission range with p), but not the node p itself and $E_{loc}g$ is the local efficiency between p and q and $dis(p,q)$ is the shortest distance between the two peers. Therefore, the average network efficiency of the network can be defined as in the following equation (4.7), where n denotes the total number of peers in a network and $dis(p,q)$, denotes the length of the shortest path between a node p and another node q.

$$Eg = \frac{2}{n(n-1)} \sum_{p,q \in N}^{n} \frac{1}{Dis(p,q)} \tag{4.7}$$

4.3.4 Transitivity and Network Performance Analytical Models

To put all the pieces together, we can analytically establish a relationship between the models we have introduced (transitivity, shortest path, energy and network efficiency) as follows:

- From the average transitivity model in equation (4.2); the closeness centrality in equation (4.4) and the average shortest path model from equation (4.3) it is not difficult to see that for any given network with a fixed number of links and nodes, the relationship between average transitivity and the shortest path between the peers is directly proportional. This is consistent with the finding in [193].

- From equation (4.7) above, we can see that the relationship between average network efficiency and average distance is related by inverse variation. In other words, as one becomes larger the other becomes smaller. i.e., the lower the shortest path

(minimum distance between the peers in the network), the higher the efficiency of the network.

- Subsequently, from the energy model in equation (4.5), and the average shortest path equation in (4.3), we can observe a directly proportional relationship between energy and the average shortest path; i.e., the lower the average shortest path between the peers in the network, the lower the amount of energy needed for the peers for trust propagation, trust evaluation and messages transfer between the peers.

- Therefore, we can analytically establish a relationship between structural transitivity and the energy model as *inversely proportional* and the relationship between average structural transitivity and the network efficiency model as *directly proportional relation.*

To determine the accuracy of our proposed model's implementation, we keep the density of the network fixed. We define network density as the portion of the potential connections in a network that are actual connections. We calculate the average network density of the network g as the percentage of links present in the network with the following equation (4.8). Where L represents the links present in the network and n represents the number of nodes in the network.

$$Av.D = \frac{L}{n(n-1)} \tag{4.8}$$

4.4 Simulation Studies

To evaluate the presented analytical model, we adopted the Eigen Trust algorithm to simulate the transitivity model for efficient trust propagation in a given network of wireless devices. The Eigen Trust algorithm is a self-policing trust and reputation management model developed to overcome the peer-to-peer authentication problem. The model aims to assist the peer members of the network to choose the most reputable and trusted peers for routing decisions.

We used the TRMSim-WSN [2] simulator for the experiment. TRMSim-WSN is a Trust and Reputation Model Simulator for Wireless Sensor Networks (the details of TRMSim-WSN can be found in the Methodology chapter). In the simulation studies, we consider a traditional WSN peer-to-peer based network which comprises malicious nodes, benevolent nodes and relay nodes within the area of $100X100M^2$, with each node having a radio range of 10M. The nodes in the network sends and receives data from their neighbouring node with equal traffic.

We have simulated the Eigen trust model, because it is one of the most widely known trust and reputation models. The model is developed in such a way that each peer in the network observes and takes notes about its interaction with the corresponding neighbours in the network. The local and global trust value of a peer can be computed when determining the reputation level of the peer. We generated six different random regular networks using NetworkX [194], a python graph package with the following settings: 50 nodes and 150 links with each node having an average degree of six (6).

Table 4.1: Simulation Variables

Model	NS	NE	% M	% C	PP	PW	ξ	ZP
Eigen Trust Model	50	10	70	15	0.3	5	0.1	0.2

Table 4.2: Definition of Terms of Table 4.1

NE	number of model execution
NS	number of sensors
%M	percentage of malicious peers
%C	percentage of client
W	simulation window size
ξ	epsilon
PP	pre-trusted peers percentage
ZP	zero probability

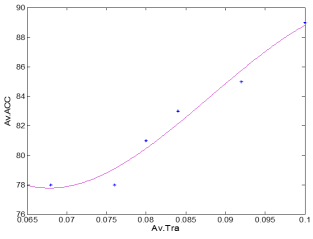
We then transferred the metrics to the TRMSim-WSN model for the modelling of trust and reputation behaviour and energy efficiency for the six generated network topologies as presented in Table 4.3 for six different scenarios so that the position of the links in the network will behave dynamically and take the reading of each simulation scenario. We set up the TRMSim-WSN with the parameters as shown in Table 4.1. We use the equation (4.2) and equation (4.7) to compute the average transitivity coefficient of the network ($av.Tra$) and the average network efficiency using equation (4.7) respectively for every simulation scenario as presented in table 4.3.

Table 4.3: Result of the Simulations

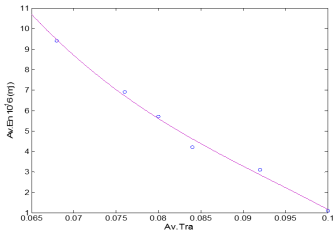
Variables	scenario 1	scenario 2	scenario 3	scenario 3	scenario 5	scenario 6
$Av.Tra$	0.068	0.076	0.080	0.084	0.092	0.100
$Av.Spath$	2.360	2.350	2.320	2.310	2.300	2.250
$Av.D$	0.122	0.122	0.122	0.122	0.122	0.122
$Av.Acc.$	78%	78%	81%	83%	85%	89%
$Av.En$	$9.4X10^{16}$	$6.9X10^{16}$	$5.7X10^{16}$	$4.2X10^{16}$	$3.1X10^{16}$	$1.1X10^{16}$

Table 4.4: Summary of Table 4.3

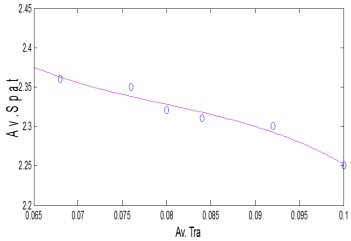
$Av.Tra$	Average Transitivity coefficient
$Av.Spat$	Average Shortest path
$Av.D$	Average Density
$Av.Acc$	average Accuracy of the model Implementation
$Av.En$	Average energy consume by each peer



(a) Average Transitivity Coefficient VS Average Trust and Reputation Model Accuracy



(b) Average Transitivity Coefficient VS Average Energy Consumed by the peers



(c) Average Transitivity Coefficient VS Average Shortest Path between the peers

Figure 4.3: Average Transitivity VS: (a) Average Trust and Reputation Model Accuracy (b) Average Energy onsumed by the Peers (c) Average Shortest Path

From Table 4.3 above, we can see that while the density of the network topology is fixed with the value 0.122, the average transitivity changes with the corresponding change in the trust and reputation model accuracy. Also, it can be observed that an increase in the average transitivity causes an decrease in the average shortest path between the peers in the network.

Figure 4.3(a) presents the observed average transitivity coefficient and average trust and reputation model accuracy of the simulation. The average model accuracy is defined as the total possible accuracy of all the peers in the network to locate the corresponding benevolent peers in the network. This tells us that the more the peers are connected to a transitive anchor, the higher the accuracy of trust model implementation (trust propagation and trust evaluation).

Another interesting observation is with regard to the total amount of energy consumed by the peers during the simulation studies, from the graph of Figure 4.3(b), we can observe the results of the simulation study of the average transitivity coefficient vs energy. We observed that with an increase in the average transitivity coefficient, the amount of energy consumed by the peers reduced significantly. Thus, it requires the peers to spend less energy in the process of locating the good behaving peer.

Figure 4.3(c) shows the relationship between the average transitivity and the average shortest path between the peers. Based on the result of the simulation we deduced that, the more the peers are connected in a transitive connectivity, the path length decreases. Thus, the results suggest that, the higher the transitive connectivity between the peers in the network, the easier it is for the peers in the network to trace a benevolent peer efficiently. That is to say that, the more the network characterizes by transitive closure, the easier it is for the nodes to propagate the trust data, evaluate other peers trust levels and locate a trusted node with less energy.

4.5 Chapter Summary

This chapter investigated the impact of the transitive connectivity between peers on the accuracy of trust and reputation models' execution (Eigen Trust). The study in the chapter also presents the impacts of transitive connectivity and the energy efficiency of the trust and reputation model implementation. As illustrated in the analytical and simulation studies the more the network is characterized by transitive connectivity between the peers in the network. The higher the transitive connectivity coefficient between the peers, the faster the peers manage to locate the benevolent node in the network with less energy spent because the protocol enables the peers to locate behaving peers using the shortest possible path. Based on the theoretical, analytical and simulation studies observed in this chapter, one can formulate the overall considerations of trust-based routing in wireless networks. The findings of this chapter suggest that we can assume [but have not yet proved] that the transitivity scaling factor can equally be applied in the design of a trust-based routing protocol for efficient trust evaluation between the peers. Further investigation is needed to determine the effect

of the transitivity scaling factor for trust propagation and evaluation.

Chapter 5

DATM: A Dynamic Attribute Trust Model for Efficient Collaborative Routing in Wireless Mobile Networks

In this chapter, we hypothesise that in a trust-based routing protocol, it will be an additional trust evaluation for reliability if peers can take into consideration their partners attributes' status in addition to the trust relationships for routing decisions. We propose DATM protocol; a trust-based scheme to enforce collaborative behaviour in wireless mobile networks taking into consideration the peers' attributes for an efficient routing scheme. Since the peers' routing attributes vary dynamically, our proposed model must also accommodate the dynamic changes of peers' attributes and behaviour. We introduce a personalised similarity algorithm for peers' attributes modelling as a scaling factor for trust evaluation. The relative comparison of the DATM and protocol using simulation shows the improved performance of our proposed model in terms of messages delivery, messages overhead and average latency.

Our contributions in this chapter include: a) the introduction of the notion of quantifying the peers' routing attributes (buffer) as a scaling factor for trust evaluation between the peers; b) the introduction of generalise peers' personalise similarity model

for trust and reputation evaluation and c) a generalised trust model that evaluates peers' forwarding ability and peers' attributes for trust evaluation (DATM).

5.1 Background

The motivation to solve the problems related to peers' routing misbehaviour drives from the strong binding between collaboration among peers and cooperative behaviour, so that the peers can collectively participate in routing activities [195, 53]. Peers communicate with their own neighbours (i.e., nodes in their radio ranges) directly by wireless links. Nevertheless, non-neighbouring peers can equally communicate by using other intermediate peers as relays which assist them in forwarding the packets toward destinations. Therefore, every member of the network is expected to contribute in the routing process. However, the members of the community might not have information about the routing behavior and the status of other members. Therefore, we give credence to the fact that trust and reputation is a good measure of peers' contributions to the network and it can be used to establish a behavior aware predictive model [25].

Subsequently, in our previous work [28], we proposed that the correct operation of the network devices requires not only trust relationship as a deciding factor in routing decisions, but it also requires each node to be reliable in terms of resources and routing handling ability which we referred to as peers' attributes. Further, we understand, that, in an environment where the peers' attributes such as bandwidth and buffer space are infinite, different flooding-based collaborative routing protocols (e.g., Epidemic routing protocol) [196] can give an optimal solution (in terms of delivery ratio and latency), since the message carrier will keep on spreading the message copies until the message reaches the destination. However, in most cases, the peers' resources are limited. Thus it will be a great value to have an alternative solution in the case where such resources

or attributes are limited.

Ordinarily, in different wireless networks' settings such as Mobile Adhoc Networks (MANETs), Wireless Sensor Networks (WSNs), peers' are expected to utilise their limited resources for routing functions (next peer selection, data forwarding, etc.) with the probability of higher packet deliverance. At a point in time, a peer may succeed in launching an attack that can cause a node to either fail to respond on time, drop the packets or engage in collaboration with attacking peers for malicious attacks. Also, peers in wireless P2P networks drop their received packets that they are supposed to forward due to selfish behaviour (for example, in an attempt to minimise the utilization of resources) [10] or due to their limited resources [197]. In this regard identifying a corresponding non-selfish peer (based on the peers' routing history) and reliable peer (a peer with available resources) is essential.

In principle, peers' misbehaviour that can influence packets' forwarding in the network may generate from numerous events such as simple selfishness of peers [198], faulty nodes, attacking peers, network congestions or perhaps any form of non-cooperative behaviour. But recent studies [199][200] have suggested, that one of the basic requirements for keeping the network functional and operational is to enforce peers' contributions through a collaborative mechanism.

In this chapter, we argued that even in cases where trust and reputation mechanisms are in place, to some extent achieving a collaborative mechanism requires the instantaneous knowledge of peers' reliability among the neighbouring peers for an efficient routing mechanism.

To support our argument, consider the case of Self-Organization in Autonomous Sensor/Actuator Networks that have peers with temperature sensors and cooling mechanism controls [201]. The actuator periodically receives temperature readings from the sensors. Based

on the readings, the actuator can trigger a cooling mechanism whenever it detects a neighbouring device reporting the temperature that is higher than the assigned threshold. Since the sensors can only transmit the data according to their transmission ranges, a collaborative routing mechanism is needed based on a "trust chain" where peers can keep forwarding the received messages to the peers they trust in the network until the messages reach the actuator (destination). Assume that a particular peer p detects a temperature above the threshold, then it must report the temperature value to the actuator. In the event where peer p forward its readings to peer q, and peer q is the most trusted peer in the eyes of peer p. However, instead of peer q forwarding to the actuator, it drops the packets due to its limited resources, the actuator may never detect the accurate reading of the temperature for it to activate the cooling mechanism. But if peer p can instantaneously understand the reliability (resources level) of peer q, probably it might forward the packets to other peers instead to peer q.

Another example; consider an application in which QoS is of particular importance for the transport of traffic with special requirements or an application that has certain compelling Quality of Service (QoS) requirements (e.g., video streaming). In those applications, if a peer fails in data forwarding, the entire network performance may be affected; or if the failing or non-cooperating peer is not quickly detected, that behaviour can generate a significant loss of QoS. Likewise, when the peers fail to operate as expected, a peer might fail to deliver (drop) some packets or the packets might arrive at the destination when the destination peers' buffers are already full. Resultantly, the receiving application may ask for this information to be retransmitted, possibly causing severe delays in the overall transmission.

We propose A Dynamic Attributes Trust Model for Efficient Collaborative Routing

(DATM) [202] which is a trust-based scheme to enforce collaboration taking into consideration the peers' attributes for an efficient routing scheme. We see that our approach is a generic mechanism that can be integrated into any packets' forwarding strategy, or network management functions.

5.2 DATM: Trust and Reputation Concepts

In this chapter, we define trust as the confidence that a peer has about the reliability and cooperation of its neighbouring peers; i.e., the likelihood a peer can forward the received messages to its neighbours or to the destinations. Therefore, trust establishment between the peers is not limited to the peers' routing behaviour but include the peers' characteristics or attributes. Based on the aggregated trust values, a peer can avoid sending data packets to the corresponding peers that are not likely to cooperate in routing the messages or that are not reliable to handle the routing tasks. Such trust value represents the degree of the trust that other peers in the network can have on a given peer based on its routing behaviour.

In DATM, we used the *direct observations* from the information of delivery vectors for the computation of local trust values which can be calculated directly from the subjects' observations. We used the term subject to refer to a neighbour that is within the wireless transmission range of another neighbour. Also, we based our assumptions on the fact that, the frequent encounter between peers in a mobile network can represent how likely it is that a peer can deliver a message to the destination as inferred by many social aware routing protocols including [203, 61]. Thus, the peers that frequently meet can update their delivery vectors on a regular basis.

The scheme propose in this chapter involves three main components namely: *Delivery and attributes' summary vectors exchange*, *Local trust evaluation*, and *peers' attributes*

modelling for global trust evaluation. We describe below the details of each DATM' components.

5.2.1 Delivery and Summary Vectors Exchange in DATM

This involves the exchanges of delivery information between peers and the peers' attributes summary upon encounter. The delivery information of the peers comprises the peers' encounter history (recently encountered peers), and the details of the messages received and forwarded by a peer. The status of the received messages include the binary status of Messages' IDs recently received; if the message IDs' status is 0, meaning the message has been forwarded by a peer (no longer in the peers' buffer), while if the messages' status is 1, a peer did not forward the message yet. Therefore, every peer will maintain the status records of its recently received messages of the peers it has encountered (reasonably) recently. Also, peers maintain their subjects local trust information in their *delivery vectors* . In this regards, we opted the data structure of the delivery predictability metrics proposed in [204] with additional modifications as the peers' delivery vector for the implementation of our proposed system. Based on the information in the delivery vectors, the peers can evaluate their subject encounters with the packets' destination for local trust evaluation (as described later in section 5.2.2).

On the other hand, the exchange of peers' attributes summary involves the exchange of the peers' resources' information. Peers can exchange their attributes summary vectors' information ($A_p = \{a_1 = v_1, a_2 = v_2, ..., a_i = v_i\}$) containing their resources' details. The additional information in the attributes summary vectors is used for the peers to update their subjects about their reliability status (as described later in 5.2.3). Every

peer exchanges the summary and delivery vectors with other contacted peers and updates its list on each connection. The illustration of delivery vector and attributes summary vectors exchange can be seen in Figure 5.1. Therefore, after a free configured time interval, every peer can be expected to possess the delivery vectors and attributes summary vectors of its subjects. In the later section, we will demonstrate how the combined information from *delivery vector* and *attributes summary vector* can be used for reliable local and global trust evaluations.

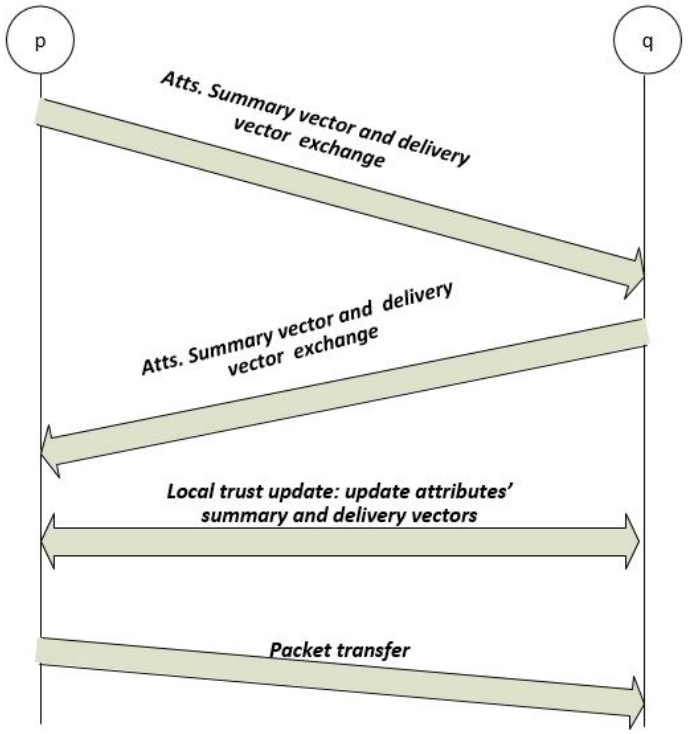


Figure 5.1: Delivery and Summary Vectors Exchanges Illustration

5.2.2 Local Trust Evaluation in DATM

This section describes how the local trust value can be computed based on the peers' exchange of delivery vectors described earlier. A peer can evaluate its neighbours or other peers, depending on their track records and previous encounters with the packets' destination (if any). Each peer maintains the status of its most recently received and

forwarded packets' IDs. To compute the local trust values, the peers can access the success of their previous transactions from the details in their subjects' delivery vectors. When two peers p and q interact, they can establish a local trust between themselves upon encounter. Each peer will check the corresponding delivery vector of its subjects to access the local trust of its subjects based on the following conditions:

- if the status of the previous messages transactions between *trustor* and *trustee* is 0 (meaning a packet received by a *trustee* is no longer in *trustees'* buffer), and there was a recent encounter between a *trustee* and other peers in the network (probably the packets' destination); we assume that the outcome of the transaction is satisfactory.

- if the status of the previous messages received by a *trustee* shows it's still in its buffer (meaning the messages status is 1) while the trustee is not the destination of the message and there was no recent encounter between *trustee* and other peers in the network, then the outcome of the transaction is considered as a neutral or undecided.

- if the status of the previous messages received by a *trustee* shows it is still in it's buffer, while there is an encounter history of a *trustee* meeting the messages destination the outcome of the transaction is considered to be not satisfactory.

- in the event where peer p is meeting a peer q for the first time, peer p can assign an initial trust value $t_q^{(0)} = \begin{cases} \frac{1}{|init|} : q \in n_{preT}, \\ 0, \, otherwise, \end{cases}$.

For example, let $t_{p,q}$ be the trust value that peer p places in peer q based on its priori experience with peer q, where $t_{p,q} \in \langle 0, 1 \rangle : p \neq q$. Each time peer p encounters peer q, peer p can assess the trust level of peer q based on their encounter delivery

vectors exchanges. If the encounters history is not satisfactory it will be considered as a negative experience, therefore the local trust value ($t_{p,q}$) between p and q will decrease; while if the encounter history between the peers is satisfactory, then it will be considered a positive experience and the ($t_{p,q}$) will increase [205]. If the peers' transaction is undecided, it will have no effect in the peers' trust evaluation. Therefore, $sat(p,q)$ represents the number of satisfactory encounters between peer p and peer q while $unsat(p,q)$ represents the total number of unsatisfactory encounters between peer p and peer q. Evidence of trustfulness is manifested by the encounters history exchange between the peers. Thus, the resultant local trust value between the peers can be computed as $C_{p,q} = sat(p,q) - unsat(p,q)$. The normalised reputation can be computed as:

$$t_{p,q} = \frac{max(C_{p,q}, 0)}{\sum_q max(C_{p,q}, 0)}, ||\vec{t_p}|| := \sum_{q=1}^{N} t_{p,q} = 1 \tag{5.1}$$

The global trust equation (with no reliability scaling factor) peer p can place on peer q based on the feed back of peer r about the previous routing behaviour of peer q can be presented in the following equation 5.2.

$$T_{p,q} = \sum_r t_{p,r} t_{r,q} \tag{5.2}$$

Therefore, each peer will maintain the global trust vectors of its subjects as follows:

$$\vec{t_p} = (t_{p1,....,t_{p,N}})^T, 0 \leq t_{p,q} \leq 1 \tag{5.3}$$

The General trust algorithm presented in Algorithm 1 presents the simple procedure of peers' trust values aggregations and ranking. Initially, the message holder (say peer p),

will get the local observations of its subjects (say peer q), $t_{p,q} : t_q^{(0)} = \frac{1}{init_q}$. Peer p will also send its local observations about peer q to all its neighbours ($r \in n_p$), and request their observations about peer q as well. Therefore, the resultant global observations of peer p about peer q can be computed using the presented equation 5.2 as shown in algorithm 1.

Algorithm 1 General Trust Algorithm Forward

while *peer p is a message holder* **do**
  for *each peer q* $\in n_p$, **do**
    Get $t_{p,q} : t_q^{(0)} = \frac{1}{init_q}$;
    Send $t_{p,q}$ to all peers $r \in n_p$;
    query $r \in n_p$ to return $t_{r,q}$;
    compute $T_{p,q} = \sum_r t_{p,r} t_{r,q}$;
    Rank $T_{p,q}$;
  end
end

To secure the implementation of DATM, we deviced the trust value of the peers to two basic principles; (1) the trust value of a peer is computed in a distributed passion. Thus a peer does not have access to its trust information where it can be subject to alterations. (2) the trust value of a peer is computed by more than one peer so that malicious peers cannot succeed in white washing attacks.

5.2.3 Peers' Attributes Modelling For Global Trust Evaluation

Here, we discuss the peers' attributes modelling and its inclusion in the global trust evaluation. In our proposed system, the attributes of peers are dynamically evaluated for peers' reliability evaluation based on the information in the attributes' summary vector. The attributes of a peer are characterised by the peers' resources (e.g. energy) and peers' routing capability (buffer size). Also, the peers' attributes values can be static (e.g., CPU speed, peers' memory size) or dynamic (e.g., free memory, energy level, free percentage of buffer occupancy, etc.). In our proposed model, the peers' attributes that

are characterised by dynamic attributes are re-calculated at peers' contacts when the attributes values changes significantly. To generalise the model, the peers' attributes can be assigned to a peer to describe its available hardware and software resources. For example, the peers can be assigned a storage capacity as an attribute and edges can be assigned a parameter like bandwidth, delay, etc.

Attributes Modelling:

Given a set of peers' attributes A, the function $a : V \longrightarrow \mathbb{R}_{+}^{\{|A|\}}$ assigns to each peer a list of its attributes values $A = \{a_1 = v_1, a_2 = v_2, ..., a_i = v_i\}$. Each attribute $a_i \in A$, has a value $v_i : v_i \in \mathbb{R}^{+}$. We can represent the tuple of the peer q attributes as (a_q). Where $a \in A$ represent the attribute value of peer q. We can subsequently represents possible maximum attributes value of peer q attributes as $\tau_{max}(a_q)$ and the current attributes value as $\tau_{curr}(a_q)$. By current attribute; means the most rescently computed attributes' value. We can also define the threshold (δ) as the minimum reliability impact required for the peers to be considered as a message carrier in the network. Further, we assumed that the peers' attributes values are quantifiable data, therefore, can be evaluated. Based on the two attributes' values (maximum possible attribues' value and the current attributes values) of peers, we computes the attribute scalling factor using equation (5.4).

$$a_q = \frac{\tau_{max}(a_q) - \tau_{curr}(a_q)}{\tau_{max}(a_q)} \tag{5.4}$$

From the resultant global trust algorithm presented in equation (2.3) and the attributes' model equation (5.4), we introduce an attributes' scaling factor to represent the level at which a peer is reliable for efficient routing handling. For example, the resultant Global-Reliability trust value between peer p and q can be computed using the following

equation (5.5).

$$\hat{T}_{p,q} = a_q * \sum_r t_{p,r} t_{r,q} \tag{5.5}$$

Where a_q represents the attributes of peer q computed by peer p and $\hat{T}_{p,q}$ represents the transitive global trust of peer q computed by peer p .

5.3 Protocol Implementation

In this section, we discuss the protocols' implimentation using an opportunistic network environment simulator [206]. For the details of ONE simulator, we refer the reader to chapter three of this thesis. The Opportunistic Network Environment simulator models store-carry-forward networks, thus at each transaction between the peers, the intermediate peers only hold the messages that can fit into their buffer sizes. In the event where the peers' buffer space is occupied, the peers will drop the packets. The simulation studies are grouped into the following two parts: Firstly, we evaluated average attributes' as a scaling factor for trust evaluation. Secondly, we implemented our proposed simple similarity algorithm to capture the relative attributes' similarity as a scaling factor for trust evaluation. We then compare the performance of the DATM and PROPHET protocols [204] in terms of total messages delivered, messages overhead and average latencies. PROPHET is known as Probabilistic routing protocol using history of encounter and transitivity (PROPHET); a Probabilistic Routing Protocol using History of Encounters and Transitivity. PRoPHET is a variant of the epidemic routing protocol for intermittently connected networks that operates by pruning the epidemic distribution tree to minimize resource usage while still attempting to achieve the best-case routing capabilities of epidemic routing.

5.3.1 Average Attributes' Scaling Factor For Trust Evaluation

In this phase, we compare the performance of the trust model with a naive attributes' scaling factor (average attributes' values) and a trust model with no attributes' scaling factor. This is to enable us to understand the influence of the peers' attributes in trust evaluation. We assigned to each DTN peer a set of basic attributes such as buffer size, radio interface and energy consumption to implement our proposed trust algorithm. In an ideal situation, all the peers are expected to behave normally and forward the data packets accordingly unless some reasons exist, such as non-availability of buffer space for a peer to store the packets for future forwarding, and limited resources. Therefore, we seek to understand how the peers' buffer occupancy can be modeled as an attributes' scaling factor for peers' trust evaluation. The objective of our solution is to maximise the data delivery performance between peers; thus a peer should be able to make an accurate decision in choosing a corresponding peer for routing tasks handling. Therefore, we explored the DTN peers' buffer size for the implementation of our proposed model. Worthy of consideration is how a peer maintains its buffer space allocation in our model when sending or receiving a data packet (i.e., increase or decrease). First of all, we assigned each peer a buffer size with a maximum limit of $Max(X_p) = 50MB$ and a minimum limit of $5MB$ of buffer space a peer can possess. Each peer maintains a buffer of content chunks which it attempts to fill by contacting other peers in the network.

At the initial stage, we implemented the non-reliable trust algorithm presented in equation (2.3) and a reliable trust algorithm presented in equation (5.5). We assigned the pre-trusted peers percentage = 0.3, pre-trusted Peers Weight = 0.25 and zero trust node selection probability = 0.2. For the implementation of a reliability-based trust model, we assigned the attributes (buffer) threshold as $5MB$. Any peer with a limited buffer

size less than the *threshold* will not be considered in routing selection. We created five scenarios in which the peers can create messages of different sizes (500k, 1M, 1.5M, 2M, and 3M) with each message carrying the source and the destination addresses.

As discussed in [207], the available size of the peer's buffer determines its routing capacity and its reliability for packets forwarding in collaborative routing. Also, the unavailability of the buffer memory may induce peers in the network to fail in the process of data forwarding which degrades the performance of the network [111].

Decision Making for Next-Peer Selection Strategy

For our routing selection strategy, we consider a mobile network of DTN peers consisting of peers $\{p, q...., n\}$ with each peer creating a message in a uniform distribution over time. Each created message (m_p) created by peer p has a set of information such as the source and destination IDs, the time since the message was created and the Time-To-Live (TTL), that is time-out value, which specifies when a message is no longer valid so that it can be deleted from the buffer of the message carrier.

Peers communicates with their subjects using a *multiple copy policy*. We assume that the peers move in a predictable fashion based on repeating behavioural patterns. Thus, the contacts between peers are predictable. Figure 5.2a and 5.2b presents the performance comparison of our proposed attributes' based trust model and non attributes based trust model with a varying number of message sizes and attributes' scaling factor thresholds (δ). We assigned $(\delta) = 5MB$ and $10MB$ to enable us to understand how the peers' buffer (percentage of buffer occupancy) as a scaling factor can influence the trust evaluation between peers. We, therefore, define the threshold (δ) as the minimum reliability impact required for the peers to be considered as a message carrier. From Figure 5.2a and 5.2b we can notice higher delivery ratios in the reliability based trust

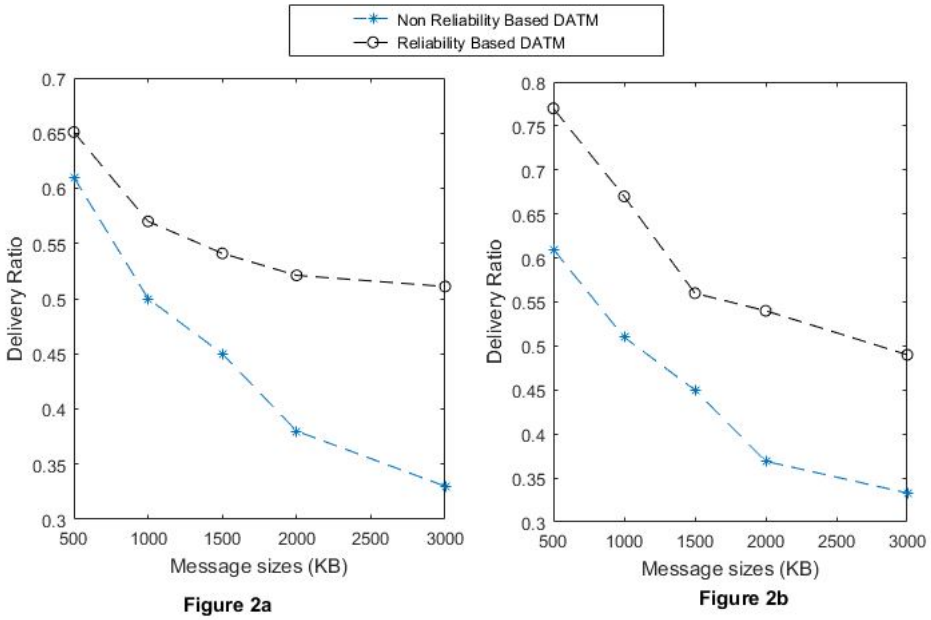


Figure 5.2: Performance Comparison of the Reliability Based Trust Model vs Non Reliability based trust model with varying sizes of attributes' threshold; Figure 3a is when (δ) = 5M, Figure 3b is when (δ) = 10M

model in comparison with the nonreliability trust model (Eigen Trust with no attributes' scaling factor). We define delivery ratio as the number of packets successfully received by the destination divided by the number of packets sent by the sources.

The figures show that a large enough message will result in reducing the delivery ratio for both the reliability and the non reliability trust-based protocols due to the possibility of message congestions. However, the reliability based trust model shows significant improvement. This is expected since, in the reliability trust model, the peers only choose the corresponding routing partners with relatively higher buffer sizes (more reliable to deliver the packets) in addition to the truthfulness of the peers. Moreover, from the two figures, one can notice that the delivery probability favors the increases in the threshold (δ) (minimum buffer occupancy for the peers to be considered as the message carrier). This shows that the peers' buffer is an important factor for trust evaluation and our proposed reliability trust model is efficient in identifying the peers with less

buffer occupancy for routing decision; thus it is actually reasonable that this occur.

5.3.2 Personalised Reliability Feedbacks Similarity Estimation

In this section, we extend the attributes' model (presented in sub section 5.2.3) to handle different dishonesty and falsification of the peers' attributes estimations using a simple similarity algorithm. Therefore, we first extend the naive average attributes' scaling factor using a personalized similarity model of peers attributes. We propose a personalized similarity metric so that the peers can rate the attributes' feedback provided by another peer through its personalised attributes.

Concretely, a peer can use a personalised similarity between itself and its subjects to weight the attributes' feedbacks provided by other peers in the network. The notion of integrating the similarity of attributes in our proposed protocol is to provide a flexibility and stronger predictive value and to give more reliability weight to similar peers in the network. The concept can also act as a defence mechanisms against potential malicious peers that can falsify their attributes in order to get an advantage (by advertising the higher attributes value)[208]. Using personalise reliability similarity, will result in low chances for dishonest peers to be considered in routing selection. This is particularly possible when the peers in the network or clique members are homogeneous devices or when measuring the attributes similarity between the members in a clique and the attacking peer is from outside the clique.

Given the peers' attributes model presented in section 5.2.3, we can compute the similarity between the peers attributes. Assume that the maximum sizes of the peers' attributes as defined in equation (5.4) are denoted as: for peer p as $\tau_{max}(a_p)$, and for peer q as $\tau_{max}(a_q)$. Each time peer p and peer q exchange their summary vectors of attributes values, peer p can compute the difference between its attributes value and

that of peer q which can be normalised with the maximum possible attributes level as follows in equation (5.6).

$$d_{(a_p,a_q)} = \frac{\sum_{i=1}^{n} |a_{pi} - a_{qi}|}{\sum_{i=1}^{n} \tau_{max}(a_{pi}, a_{qi})} \tag{5.6}$$

Therefore, the similarity between peer p and q attributes' can be evaluated in the following equation(5.7). $S_{(A_p,A_q)} = 1 - d_{p,q}$ which can be represented as follows:

$$S_{(A_p,A_q)} = 1 - \frac{\sum_{i=1}^{n} |a_{pi} - a_{qi}|}{\sum_{i=1}^{n} \tau_{max}(a_{pi}, a_{qi})} \tag{5.7}$$

Where $\tau_{max}(a_{pi}, a_{qi})$ is the maximum of $\tau_{max}(a_{pi})$ and $\tau_{max}(a_{qi})$.

Attributes' Similarity Model Illustration

To help grasp our proposed concept, consider the diagram in Figure 5.3 and table 5.1. Assume that using a trust and reputation algorithm, peer p want to forward the message of size 6MB to either of the two peers (q, r), and the trust level that peer p places in peer $q = 0.76$ and that of $r = 0.8$. Apparently, based on the trust level of the two peers, peer p is more likely to forward the message to peer r since the trust value of r is greater than that of q. However, looking at the attributes of the peers (buffer size), forwarding the message to peer r, might not be a better option since it is likely to drop the message due to its limited size of 4MB. Therefore, for peer p to look beyond the trust value of their subjects (to include the attributes) in routing decision, might be additional trust evaluation reliability. Bearing the above hypothesis in mind, we present the resultant reliability trust model with a similarity of peers attributes (presented in equation (5.8))

as a scaling factor for global trust evaluation. In the next section, we present the DATM protocol with a personalised reliability feed back similarity implementation.

Based on the presented similarity model one can see that the peers' attributes can

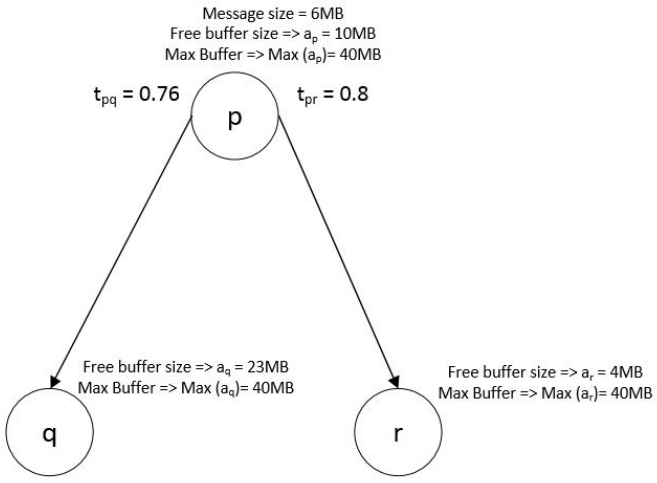


Figure 5.3: Illustration of a simple scenario

be computed dynamically, distributed fashion and on the fly. Looking at the presented simple scenario and the analytical similarity model with an illustration of the presented simple scenario can be seen in table 5.1. From the computed attributes similarity, one

Table 5.1: Simple Scenario

Buffer size similarity	$S_{p,q}$	$S_{p,r}$
$t1$	0.825	0.35
$t2$	0.625	0.95

can deduce that at $t1$, the peers' attributes' similarity is greater between p, q with the value of 0.825, whereas at $t2$, the peers' attributes similarity is more related between that of p, r.Based on proposed model implementation, the peers' are able to choose a corresponding peer with the highest similarity in terms of attributes in addition to the reputation between the peers.

Attributes' Similarity Scaling Factor for Trust Evaluation

We now describe how the presented trust metrics can be integrated for global trust evaluation using the presented similarity algorithm. For simplicity, we assume that each peer updates its delivery vectors periodically while contacting its subjects. The computation of the global trust value can be viewed as a function of three parameters: (1) the delivery vectors' information which comprises the peers' history encounter and the residual information of the previous packets handle by the peers, (2) the attributes' summary vector information, and (3) the feedback from other peers (using transitivity properties)[209] . Thus, the global reputation of a peer p who receives a feedback from peer r about its subject peer q can be represented in the following equation.

$$\dot{T}_{p,q} = S_{(A_p,A_q)} * \sum_{r} t_{p,r} t_{q,r} \tag{5.8}$$

Where $S_{(A_p,A_q)}$ represents the similarity of peers' attributes as described in equation (5.7) and $\dot{T}_{p,q}$ is the resultant global reliability trust value using personalised similarity attribute.

he settings we envision in DATM with attributes' similarity as a scaling factor, is different from the previous settings of the Reliability and Non Reliability DATM trust model. Thus, the outcomes of the two models must be different. We envision a heterogeneous intermittent connected network where peers are grouped based on their attributes and characteristics. This is to enable us to explore more on the peers' attributes similarity as a scaling factor for trust evaluation. Each group having a different maximum and minimum number of buffer occupancy. We assume that the varying attributes sizes can serve as a means by which peers can filter the false attributes' scaling factor or the peers that are not participating in the network for the resources' reservations (selfish peers). Therefore, any peer with distinct attributes size, will have less opportunity to be considered as a message carrier by other peers in the network.

Further, we compare the performance of the DATM protocol with the well-known PROPHET routing protocol [204] with the same settings as presented earlier and with the same optimal scheduling buffer management policy (FIFO)[210]. In both scenarios, peers posses uniform average wireless interfaces of 50m and 80m within the simulation period of 43200s. Peers move in a random way point mobility model [211]. We used a scenario consisting of a total of 98 devices. When a message arrives at a particular peer, a peer will buffer the message for a while awaiting to meet the appropriate peer to forward the message to. We assigned a fixed resultant trust level *threshold* of (δ= 0.85), so that peers can only forward the messages to the peers with the trust value higher than the *threshold*(δ). Further, we address the problem of new peers who are joining the network through assigning them a pre-trusted peers' weight (initial trust value of 0.25) as described earlier.

The simple peer selection strategy used by DATM in our simulation worked fairly well, since it enables a peer to route the data packets to its corresponding subjects with the trust values greater than the assigned threshold.

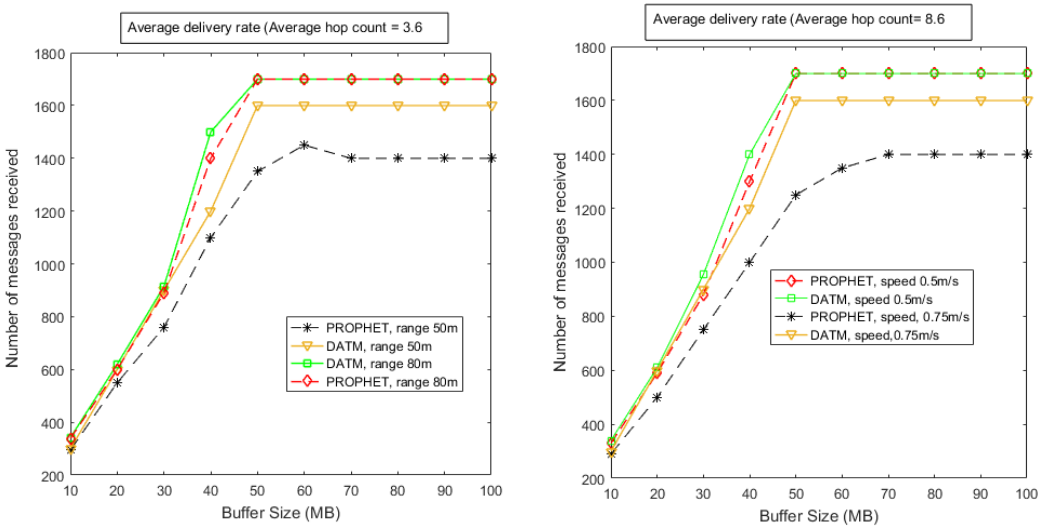


Figure 5.4: Performance Comparison of the DATM vs PROPHET Protocols for Messages Delivered: Wireless Range of 50m and 80m

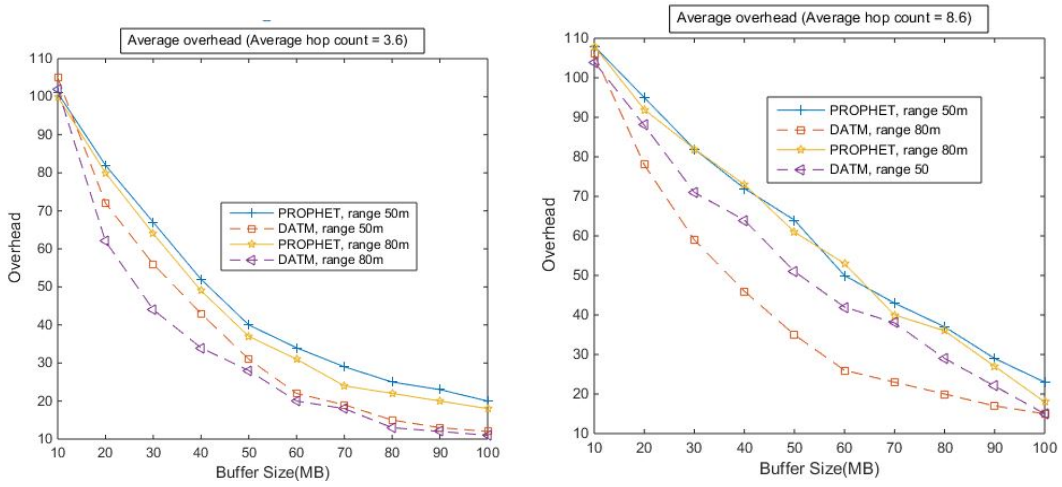


Figure 5.5: Performance Comparison of the DATM vs PROPHET Protocols for Messages Overhead: Wireless Range of 50m and 80m

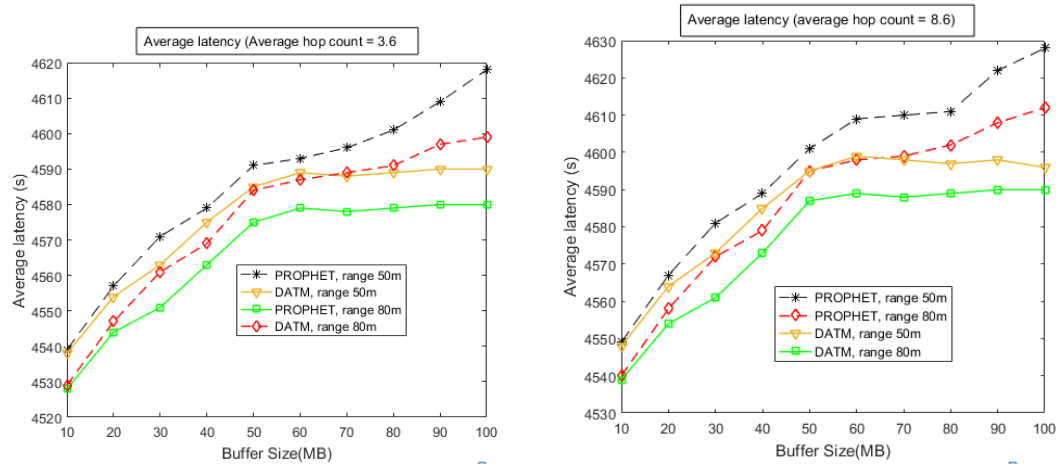


Figure 5.6: Performance Comparison of the DATM vs PROPHET Protocols for Average Latency: Wireless Range of 50m and 80m

Initially, we observed the delivery rate of the two protocols in the described simulation scenarios. The outcomes of the two protocols can be seen in Figure 5.4, 5.5 and 5.6. Each of the two graphs has different hop count settings, and with two different communication ranges. From the graphs, it can be observed that the delivery rate varies according to the peers buffer sizes. It is easy to see that for both protocols, the delivery rates behaviour of peers are similar; the sizeable buffer size yields higher

delivery rates. This is however, possible since the larger the peers' buffer sizes the more messages can be buffered, thus, the possibility of messages dropping will be less. However, the DATM protocol exhibits slightly higher performance especially with short communication ranges. This might be connected to the additional attributes' intelligence awareness of the DATM protocol; since peers can dynamically understand the status of their subjects. Also, from the two graphs, it can be observed, that the delivery rate is affected by an increase in the number of hop counts. This is also possibly due to the fact that the higher the hop counts, the higher the possibility of the messages to visit many peers before reaching the destination, causing peers' resources to be wasted and by extension can lead to message drops.

The overhead of the two protocols is illustrated in Figure 5.5. Note that the higher the buffer space, the less the overhead in both protocols. This is because the delivery rate of the protocols increases with the increase in buffers' sizes. We calculated the overhead as $M_{OH} = \frac{N_{mf} - N_{md}}{N_{md}}$. Where N_{mf} represents the number of messages forwarded, and N_{md} represents the number of messages delivered. From the two figures, it can be observed, that the DATM protocol has significant less overhead relative to PROPHET. This is however possible since any routing protocol that achieved better performance relating to delivery rate is the protocol that has the lower overhead.

Further, since both DATM and PROPHET are message *multi copy* protocols (replica); the per node messages' replica is expected. However, we inferred that the DATM protocol limits the messages replication by forwarding the messages to the specific peers that has higher chances to deliver the message (peers with higher trust value and similar attributes in the eyes of the forwarding peer). Therefore, it is anticipated, that this will take place.

Moreover, in a classical formulation of the flow assignment and routing problem in

wireless communication networks, the performance measure to be minimised is that of average messages latency over all sources to destination peers. Therefore, reducing the average latency improves the performance and the quality of communication between the peers. The lower the value of the average latency means the better the performance of the protocol. From the graphs of Figure 5.6, we see, that increasing the buffer sizes of peers in the simulation lead to the possibility of peers to exchange almost all the messages before reaching the destination. This will no doubt cause a redundant relay by other peers, leading to a higher latency. We calculated the message latency as the time between the creation of a packet and its delivery to the destination. Furthermore, the messages that were supposed to be dropped in the event of smaller buffer size can reside in the buffer before being delivered to their destination. This can equally be seen in Figure 5.6, where both the protocols DATM and PROPHET revealed a similar pattern in the average latency for different buffer sizes. However, as the peers' buffer grow, the DATM protocol exhibit less latency. This is because, in the DATM protocol, the peers can achieve a better routing distribution strategy since each peer can dynamically detect a corresponding reliable peer for a routing decision which by extension reduces the queuing delays.

5.3.3 Theoretical Analysis of the DATM Protocol

The DATM protocol can be thought of as a forwarding decision layer on top of different routing protocols in mobile applications. DATM involves a message sender and one or more message receivers that are in the same transmission range. The primary goal of introducing the personalised similarity model is to minimize the advantage that a misbehaving peer can get if it attempts to falsify its attributes status in our proposed trust system. One possible solution to mitigate such problem is to enforce cooperation among peers so that every peer will find it less worthy to falsify its attributes. As

described in section 5.3.2, there is no advantage for any misbehaving peer to falsify its attributes due to the inclusion of attributes' personalised similarity scaling factor in the model. Further, the global reputation value is hard to falsify or mimic since the increase in trust value is acquired through attributes' information, trust scoring and history of peers' encounters. From the model, a persistent malicious behavior and the lack of available resources can affect the reputation value of the misbehaving peers, leading to the exclusion of non-trustworthy peers and non-reliable peers in routing decisions.

5.4 Chapter Summary

The proposed DATM protocol in this chapter extends the implementation of trust-based collaborative routing in Intermittently Connected Mobile Networks. This was achieved through the inclusion of personalised attributes' similarity feedback as a scaling factor for trust evaluation. Thus, the DATM protocol has several advantages over traditional trust-based routing schemes, which include the peers' being aware of the instantaneous routing ability of their subjects and the improved performance in comparison with the PROPHET protocol. Despite the simplicity of the DATM protocol, we believe that our approach is a step toward improving the intelligent routing decisions in mobile wireless networks, and to overcome the shortcomings of other trust-based collaborative routing schemes. The outcomes of the simulation studies have shown, that the DATM protocol is more suitable for dense wireless mobile networks where the peers are in frequent contact (e.g., city traffic scenario and with a relative sizeable wireless range). One fundamental question is what are the implications of our proposed DATM for the design of practical wireless collaborative routing schemes? The main implication is that the protocol designers can focus their design on exploring different attributes

and properties of the dynamic mobile network (e.g., peers' energy level, peers' spatial distribution and intermittent connectivity, etc.), and include these properties in the routing decision process. Clearly, based on the outcome of DATM, the peers' buffer occupancy is likely to be a key feature for understanding peers' reliability in routing handling. In the future work we intend to explore, in detail, how we can integrate multiple weighted peers' attributes as a utility factor for peers' trust evaluation. Such scheme will aim to quantify the weight of peers' attributes and the routing circumstances for proffer forwarding decisions. Further, we intend to examine different routing attacks and to study the resilience of DATM against malicious peers.

Chapter 6

A Transitive-Aware Trust-based Protocol for Mobile Opportunistic Networks

In this chapter, we hypothesise that relative comparisons of the proliferation of peers' transitive connectivity can give a meaningful basis for determining a good relaying peer to forward packets toward the destination with less effort. As presented in Chapter Two, the uncertainty in nodal mobility and the characteristics of mobile networks with frequent network disruption make the design of a trust-based routing scheme a challenge since the peers must deal with different networks and peer conditions. Despite a lot of efforts made by previous researchers in the design of trust-based routing for efficient collaborative networks, there are few related studies that focus on the peers' connectivity as an element of trust-based routing decisions. In this regard, we foresee that, exploring the existing user mobility traces for understanding the patterns of peer contacts and connectivity structure within an arbitrary mobile wireless network, can provide a new outlook in trust-based routing protocol design. We propose and validate a trust and reputation scheme that takes into account the peers' transitive connectivity to improve routing performance in mobile opportunistic environments. We drive this

notion from the findings in the recent studies on transient connected components components [175], human mobility [176], and community structure, as a routing metric for mobile networks.

In this chapter, based on the WLAN collected traces, we presume that when two peers meet, during the overlapped time intervals, the peers' encounter can possibly facilitate direct connectivity and communication through a trust-based transitive forwarding strategy. The results of this study demonstrate that peer connectivity in the network is a characteristic that can influence peer routing performance. Subsequently, our proposed trust-based protocol takes into account the similarity of peer connectivity as a scaling factor for peer trust evaluation. Furthermore, our analysis shows that our proposed protocol only forwards the message to companions with a higher probability of delivering the message, thus improving the delivery ratio and minimizing latency.

Our contributions in this chapter are characterised as follow:

- We analytically explore the existence of transitive connectivity between peers in MSNs based on the derivation of connectivity traces. From the analytical studies and theoretical analysis in this chapter, we realised that a transitive connectivity periodically appears in the traces of MSNs.

- Based on the identified transitive connectivity property from the traces, we then proposed a new transitive data forwarding strategy which considers the similarity of transitive connectivity between peers. Our proposed transitive forwarding strategy gives preference to the peers with increasing transitive connectivity similarity to the messages' destination to improve the chances of delivering the message to the destination. Thus, through simulation and theoretical analysis, we show that transitive contact opportunities between the peers can increase the routing performance of wireless devices.

6.1 Background

Recent studies revealed that there exist a pattern of community structure in the real network of mobile devices [175]. Peers make contact and interact with other peers to form connected components which can enable peers to contact each other through multi-hop wireless connections. Further, recent studies have shown that the use of social metrics and Complex Network Analysis (CNA) such as peer centrality estimation for computing the comparative centrality of two encountering peers [212] [213] and the similarity of the peer behavioural profiles based on the mobility preferences [176] can be exploited to provide an effective solution to improve peers' forwarding decisions.

As we have presented in Chapter Four, the more connections a peer has, the more likely it is to acquire new connections; and the more likely it is to route the message across the network and serve as a good relaying peer in the network. One possible explanation behind this might come from the notion of power law distribution; i.e., the network theory of "the rich get richer" and "the poor get poorer" [214]. This can be understood based on the fact that a peer with more neighbours (connected peers) is more likely to get more connections. In a similar way, a peer with less connectivity is less likely to be connected to the network.

On the same vein, one of the basic measures to describe the mobile wireless peers' connectivity is the distribution of links (established wireless connections with other neighbours) per network node and the number of shared neighbours among the peers. However, to investigate peer connectivity of a mobile network setting between wireless peers, it is essential to understand the basic principles behind peers' contacts, peers' mobility patterns and the frequency of peers' contacts (the number of times a peer encounters other peers).

For example, consider the diagram in Figure 6.1, which illustrates the encounters

between the two mobile peers, p and q who move in opposite directions (toward each other), with each peer having a diameter range of 10m moving at a velocity of 0.75m/s. It can be noticed that the contacts and connectivity between the peers depend on three factors. The first factor is the diameter of the peers (wireless range covered); with a diameter = 10m, it will take the peers a minimum window contact opportunity of only 26.7s to overlap each other (to go out of range of each other), and when the diameter of the devices is 15m each, and with the same velocity of 0.75m/s, the contact opportunity can be up to 40s. Here, we note that the contact time is the time it takes the peers to discover each other and establish a communication channel. Although this is trivial, it can be noticed that the devices' wireless ranges influence the devices' contact duration and connectivity.

The second factor is the speed of the devices. With the increase of the peers' speed, the minimum contact time decreases. The third factor which is related to our interest is the frequency of contacts between the peers (this will be covered in detail in subsequent sections).

Based on the outcomes of related studies, we realised that the contacts' frequency dis-

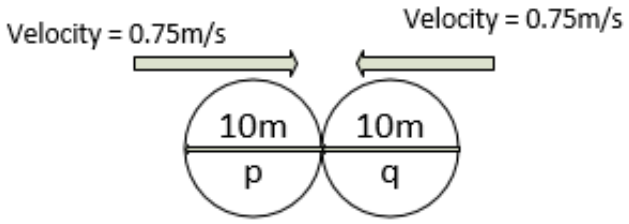


Figure 6.1: Contacts Illustration

tribution could serve as a utility measure of probabilities of peers' meeting the correct messages' destination while serving as a message carrier[215]. In this regard, we see that there is still ample need to explore and understand the irrefutable properties of

transitive connectivity based on the contact frequency distribution between peers for the design of an efficient trust-based routing protocol. Therefore, we seek to look at the processes of peers' contacts, and peers' connectivity as an element of peers' routing trustworthiness evaluation.

However, to investigate peers' contacts and connectivity for the design of a trust-based routing protocol, it is essential to answer several questions: for instance, are the contacts between wireless mobile devices persistent enough to serve as an element for understanding peers' connectivity patterns? If yes, how can the peers' contacts be appropriately captured, summarised and represented adequately to understand the peers' connectivity pattern? The last question is: "Can the peers' connectivity be leveraged to serve as a meaningful prediction of nodal mobility for a trust-based routing forwarding strategy?".

To attempt to answer these questions, we divide the chapter into two parts. In the first part, we analyse large-scale existing user mobility traces of WLANs. This enables us to understand that a certain pattern of connectivity exists among mobile peers based on the empirical data analysis. In the second part of the chapter, we use the implicit structure of peers' connectivity patterns as a trust-based forwarding element.

The stimulus of the study in this chapter is somewhat allied to the families of Geographic Forwarding Protocols; a form of routing forwarding scheme based on the Spatial analysis of the peers; such as topological, geometric, or geographical position of the peers and messages' destinations. Normally, in this type of forwarding scheme, a forwarder set is selected based on the proximity between the messages' destination and relay peers. Thus, the selected candidates can be ranked based on their geodesic distance to the target peer. To explore some related studies of interest see for example the work of [113], [175], [176], [177], [178], [172], and [216]).

While we acknowledge the previous contributions by different scholars in the field, the major differences between our work and theirs include (i) in our proposed solution, connectivity is not a solitary element of the routing decision: the peers' routing history is also a contributing factor, and (ii) our connective model required peers to exchange their local connectivity information (no global connectivity information is required) based on peers' efforts.

6.2 Network Model and Assumptions

We represent an Opportunistic Mobile Network (OMN) as $G = (N, L) : N = \{p, q, ..., r\}$ and $L \subseteq \{(p, q)\} : p, q \in N$, and $p \neq q$. Let the transmission range of peer p be $\iota(p)$ and the distance between peer p and peer q be d_{pq}. Therefore, the two peers p and q are direct neighbours if and only if $d_{pq} \leqslant \iota(p)$. Let n_p denotes the set of peers that are direct neighbours of peer p and within the cluster area of p, with area an equation $A(p) = \pi(\iota n)^2$. We assumed that, for the communication between peer p and peer q to be successful, the following condition must be satisfied: (i) $d_{pq} \leq \iota(n)$ (receiver is within the communication range of the sender) and any peer r such that $d_{rq} \leqslant \iota(r)$, is not transmitting (i.e, the receiver is free of interference from any other possible sender). In other word, peer p can successfully transmit the message to q if p is a neighbour of q and no other of q's neighbours is transmitting to peer q simultaneously. Also, we define the set of messages created in the network as M: $m.sc$, $m.d$ and $m.ttl$ represents the message sources, messages destinations and messages Time-To-Leave respectively, $\forall m \in M$.

We describe the traffic model for the network as follows: each peer in the network can be a source and a destination of a message when a peer creates a message, and it can forward it to its neighbours or the destination. A receiving peer can either forward the

message, or absorb the message if it is a destination. Further, we assumed that each peer profiles its degree of connectivity by keeping track of its encountered peers and its regular connectivity status. This is an individual effort by each peer with no interaction from other peers.

Additionally, for peers to maintain the track of their transitive path, peers can perform a neighbour discovery to enable mobile peers to transmit and listen for beacons (scanning). Since the process of neighbour discovery in a mobile network is nontrivial, we assume that the neighbour discovery process is a randomized beacon scanning discovery procedure. This is also to enable us to relax the possibility of collisions since peers can operate asynchronously. For the details of the randomised neighbour discovery asynchronous algorithm that supports our assumptions see[217].

Since it is difficult for peers to have transitive connectivity path information of all members in the network pro-actively, peers are only aware of their connectivity status when they have no message to forward. We assume that peers' clique members always move together in a predictable fashion as identified in the traces' analysis presented in Section 6.2.3 later in this chapter.

6.2.1 Description of Data Sets Used for Traces Analysis

In this section, we present our conducted analysis of a user mobility traces' pattern and its implication on the routing protocol design. Initially, we study the social contacts' patterns of five different collected traces of Wireless Local Area Networks (WLAN). We obtained all the collected traces used in this study from the Community Resource for Archiving Wireless Data at Dartmouth (CRAWDAD)[179]. To our best knowledge, CRAWDAD is one of the most well known archives for wireless traces established for the purpose of resource sharing in a community that meets the needs of this research. We analyse five data sets: (i) Bluetooth encounters between 72 short range nodes from

the Cambridge infocom2006 traces (ii) Bluetooth encounters between 52 mobile nodes from the Cambridge content traces, (iii) Bluetooth encounters between 41 mobile nodes from the Cambridge infocom traces, (iv) Bluetooth encounters between 12 mobile nodes from the Cambridge traces, and (v) Bluetooth encounters between 9 mobile and stationary nodes from the Cambridge imote/intel traces, [218].

In all the collected traces, when two users are within Bluetooth connectivity range (typically less than 10 meters), a Bluetooth connection is established between the user devices. It takes each imote approximately 5 to 10s to perform the complete scanning on a periodic basis for a device. In each collected trace, a valid encounter between the devices is represented as "up" (meaning the two devices connect when they meet), and a non-valid encounter is represented as "down" (meaning, even though the peers have a contact they did not connect). Since our interest is in the peers' connectivity, we therefore extracted all the valid encounters. Thus, we ignored the contacts during which the peers were not connected.

Table 6.1 summarises some important facts about the traces. Each data contains the steps for the derivation of the connectivity trace based on the peers' valid encounter as described earlier. We then leverage this information to understand the potential transitive opportunities of communication between the peers. We based our assumptions on the fact that the peers in wireless mobile can communicate with each other (with no infrastructure). Therefore, our proposed protocol6.3 do not involve the use of infrastructure for communication.

Table 6.1: Traces Summary

Traces	**Net. type**	**N. of devices**	**N. of contacts**	**Duration**
72 imote/infocom2006 traces	Bluetooth	72	128979	3.87 days
52 imote/content traces	Bluetooth	52	10873	11.43 days
41 imote/infocom traces	Bluetooth	41	22459	2.94 days
12 imote/cambridge traces	Bluetooth	12	4228	5.27 days
9 imote/intel traces	Bluetooth	9	1364	4.16 days

6.2.2 Peers' Direct Connectivity Frequency Distribution Estimation

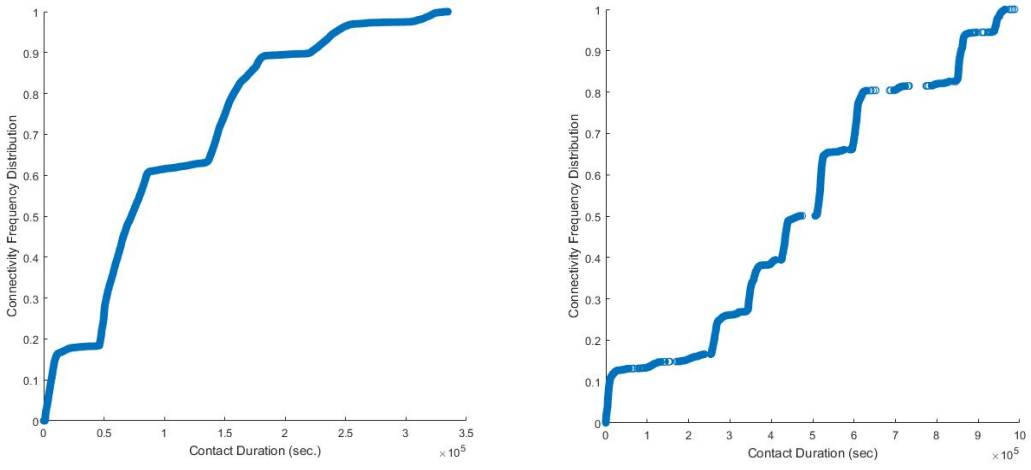
From the presented traces' summary in table 6.1, one can observe that there are thousands of frequent contacts between the users. Thus, understanding the pattern of the opportunistic contacts between the peers can be extremely challenging. Therefore, we model the pairwise contacts information which can be directly obtained from the traces. This can also be represented rather straightforwardly by the frequency distribution of the peers' connectivity concerning the contacts' durations.

In this regard, we only consider pairwise contacts in which the peers are connected. We, therefore, formulate each pairwise contact process as connectivity between the peers. Thus, we define the connectivity frequency distribution as the number times the peer contacts (or connectivity) occur between the peers. We perform the calculation of all pairs of peers' connectivity frequency distribution to arrive at Figures 6.2 and 6.4. The connectivity frequency distribution shows us a summarised connectivity of the peers at each contact time and the number of occurrences throughout the traces experiments' duration.

Looking at the graphs of Figures 6.2, 6.3 and 6.4, we have two observations: the first observation is with regards to the stability of peers' connectivity at a certain period. It can be seen from all the graphs of the traces, that the peers exhibit similar connectivity frequency distribution patterns. It can also be seen that the connectivity frequency

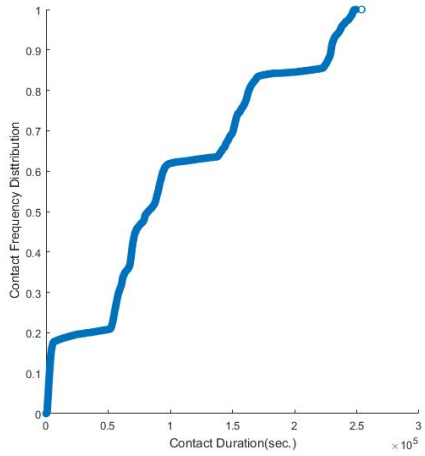
distribution is not sensitive to the change of time. One possible implication of this is that the peers' connectivity frequency distributions are stable within a certain interval of time and peers usually have frequent contact with each other. Taken together, this suggests that if we can be able to identify the pattern of the peers' connectivity, with similar duration, it can serve as a means of predicting the peers' connectivity states.

The second observation is related to the properties of transitive connectivity patterns. For example, looking at the degree distributions from the graphs of Figure 6.5 and 6.7, we observed that the connectivity pattern of the network is *scale free pattern*, that some nodes (obviously few), have more connections than others, and that the network as a whole has a power law distribution.



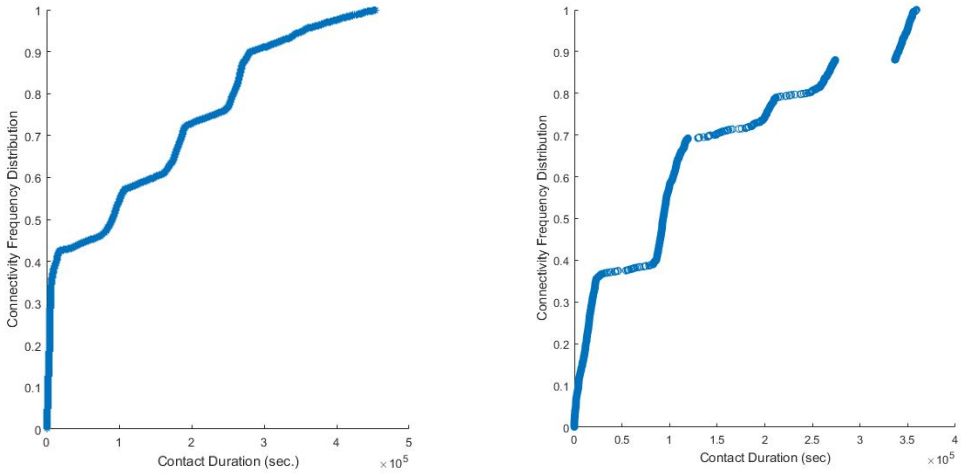
(a) 72 imote/infocom2006 traces (b) 52 imote/content traces

Figure 6.2: Connectivity Frequency Distribution of 72 and 52 Nodes



(a) 41 imote/infocom traces

Figure 6.3: Connectivity Frequency Distribution of 41 Nodes



(a) 12 imote/cambridge traces

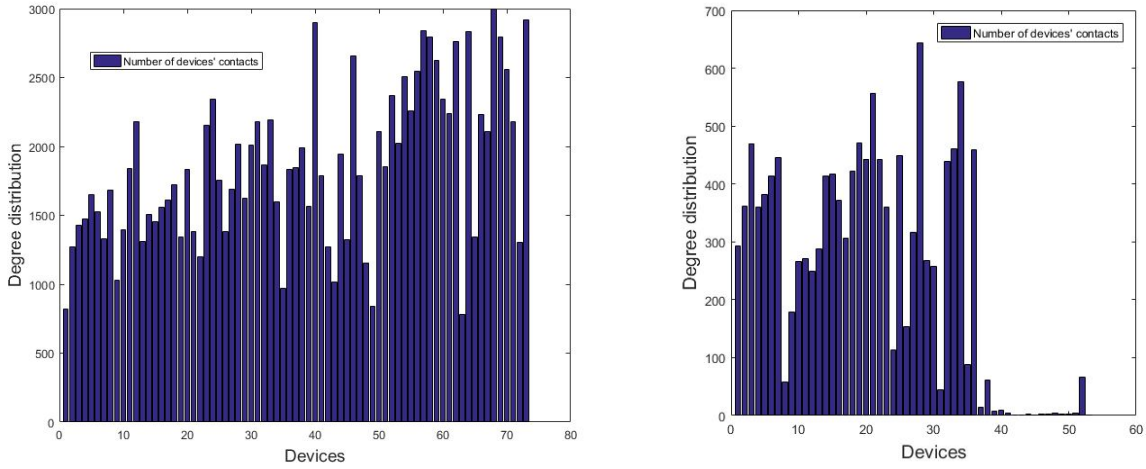
(b) 9 imote/intel traces

Figure 6.4: Connectivity Frequency Distribution of 12 and 9 Nodes

Although the traces show, that, the peers do not have a homogeneous distribution of the degree that regular or random networks have, the resulting graphs showing that the pattern of the degree distribution of nodes is between the regular and random networks. This property, however, is shared by many real world networks and is often called the small world property. This notion has been popularised by different terms like the "six

degrees of separation" between any two nodes; meaning peers are typically connected by a chain of six or fewer edges in a social network [219].

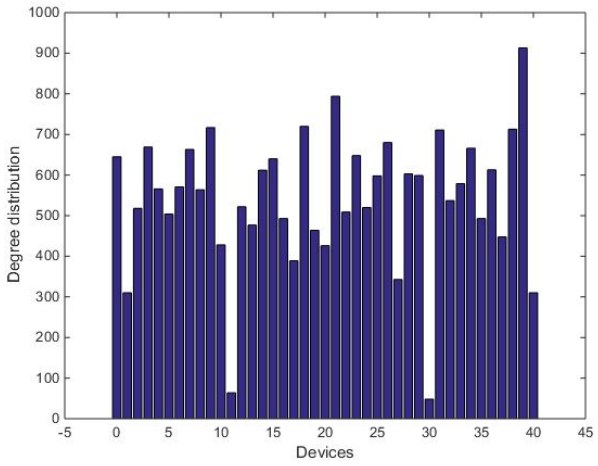
The small world properties realised in the traces, revealed that any two nodes having a common neighbour are more likely to be neighbours: in other words, they are connected by a transitive edge. The evidence from the collected traces appear to support our previous assumptions that there may be a transitive connectivity pattern in the real network traces. There would, therefore, seem to be a definite need to approximate the transitivity appearance from the traces.



(a) 72 imote/infocom2006 traces

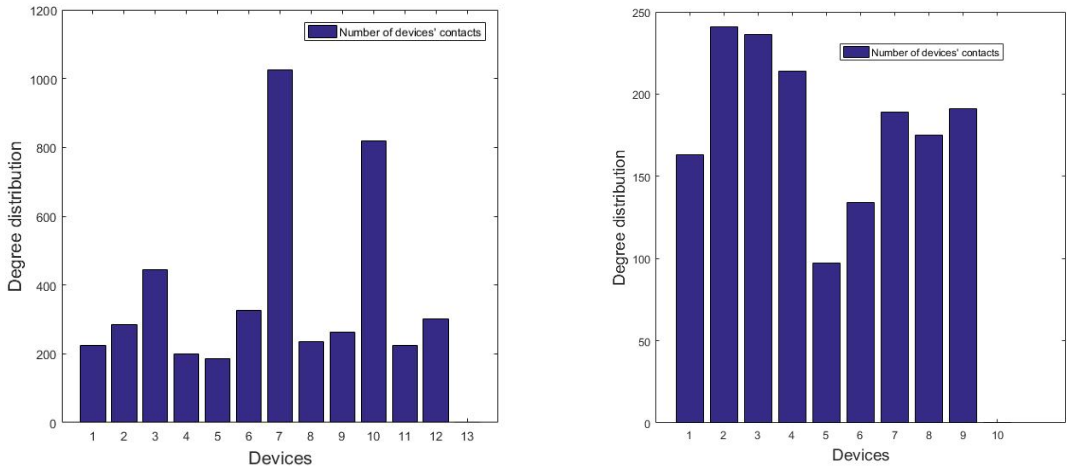
(b) 52 imote/content traces

Figure 6.5: Degree Distribution of 72 and 52 Nodes



(a) 41 imote/infocom traces

Figure 6.6: Degree Distribution of 41 Nodes



(a) 12 imote/cambridge traces

(b) 9 imote/intel traces

Figure 6.7: Degree Distribution of 12 and 9 Nodes

6.2.3 Transitive Connectivity Appearances Pattern Approximation

In this section, we analyse the appearance of transitive connectivity (contacts) in all the five collected traces. Although there are many possible patterns that can be understood from the traces in a more complex way, our focus is mainly on the transitive contacts in this work. In this regard, we formulate the transitive appearance patterns using

the matrix algebra procedure (UCINET 6.614) that satisfies the condition, $\forall\{(p,q)\} \in L\colon \{(p,q)\} \wedge \{(q,r) \in L\} \therefore \exists\{(p,r)\} \in L$.

We achieved this by counting both the weak transitive contacts (transitive connectivity with two legs) and the strong transitive closure (transitive connectivity with three legs) of each device using the following transitivity coefficient approximation model and assumptions.

If we denote the set of immediately connected neighbours or (clique members) of peer p as $n_p = \{q : \{(p,q)\} \in L \wedge \{(q,p)\} \in L\}$, $\{(p,q)\} = \{(q,p)\}$; meaning the edge between p to q is the same as between q to p (undirected and unweighed). We assume that, there is no multiple edges between peer p and peer q; therefore if two peers p, q are directly connected with an edge $\{(p,q)\} \in L$ there is no other connection between them. Also, we assume that there are no loop connections on G. Also, for each peer $p \in N$ there are possible number of distinct wireless interface connection $n_p(n_p - 1)$ that could exist among the peers within the neighbourhood of peer p.

Therefore, we define the local transitive coefficient of peer p $T_{coef(p)}$, by the proportion of the exact interfaces between its neighbours divided by the number of interfaces that possibly could exist between them as presented in equation 6.1.

$$T_{coef(p)} = \frac{2\{|\{p,q\} : p,q \in N_p, \{(q,p)\} \in L|\}}{(n_p(n_p - 1))} \tag{6.1}$$

Although we acknowledge the non-perfect nature of transitivity (partial transitivity) for example, the fact that peer p is connected/contacted to peer q, and q is connected/contacted to peer r does not guarantee that peer p is connected to r as well, but, one can argue that it makes it much more likely for p to connect to r. That is, the friend of my friend is not necessarily my friend, but is far more likely to be my friend than some randomly chosen member of the population.

Table 6.2, presents the summary of transitive connectivity of the collected traces. From

Table 6.2: Transitive Connectivity Summary from the Traces

Traces	9 imotes	12 imotes	41 imotes	52 imotes	72 imotes
Total Number of Connectivity	1364	4228	22459	10873	128979
No. of Transitive Connectivity with at least 2 legs	84	220	10318	8038	61981
No. of Strong Transitive Con. (with all 3 legs)	84	215	9549	4599	58896
% of Weak Transitive Con. with 2 legs	6.15	5.20	46	74	48
% of Full Transitive Con. with all 3 legs	6.15	5.08	42.5	57.22	45.7
Network Density	0.800	0.840	0.867	0.426	0.981

the table, it is easy to see that the transitive connectivity between the mobile devices exists in the traces, though in a small-scale as in the case of *9 imotes* and *12 imotes* with week transitive connectivity of 6.15% and 5.20% respectively. But with increasing number of devices, the percentage of both week and strong transitive connectivity of the peers in the network changes significantly up to 46%, 74% and 48% for *41 imotes 52 imotes* and *72 imotes* for weak transitive connectivity respectively. For a full transitive connectivity, the percentages are 42.5%, 57.22% and 45.7% for *41 imotes 52 imotes* and *72 imotes*.

The result of this analysis clearly revealed the existence of transitive connectivity among peers; **and it subsequently establishes that the transitive connectivity between wireless mobile peers is a stable behavioural feature of peers in the real WLAN networks**.

Further, from Figure 6.8, 6.9 and 6.10 it is not difficult to observe the similarity pattern of the peers' transitive closure; meaning the number of perfect/full transitive closures made by each peer in the experiments. Thus, we observe that the average numbers of strong transitive connectivity formed by the peers in the network are relatively similar; this elucidates that the traces of all the devices exhibit a similar pattern of transitive closure connectivity between devices. Therefore, estimating the similarity of transitive connectivity of the nodes, can lead to a further observation about member communities

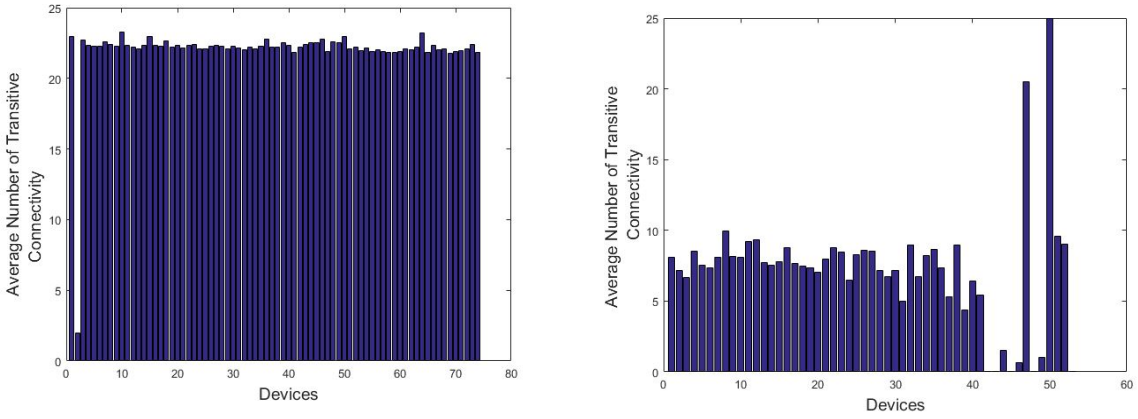
or neighbours of a particular peer. Thus, we presume that once the transitive connectivity similarity between a pair of peers is obtained, it can serve as a reasonable predictor for the connectivity between the peers for some period shortly. Meaning, perhaps, **the peers that can be reached through the transitive connectivity chain can be either members of the same community, or they share some neighbours, and they can become good communicating partners**.

We acknowledge that our assumptions may not be completely accurate in all the cases since there can be scenarios in which even if the peers are directly or transitively connected, still there is no data transfer between the peers, due to some reasons.

However, it can be observed that in network settings where peers' direct contacts are limited, the transitive contacts chain might help in data transfer between the peers. In this regard, we postulate that the relative comparisons of the proliferation of peers' transitivity coefficients might give a meaningful basis for determining a good relaying peer to forward a message towards the destination. We envision that such a comprehensive approach has two advantages:

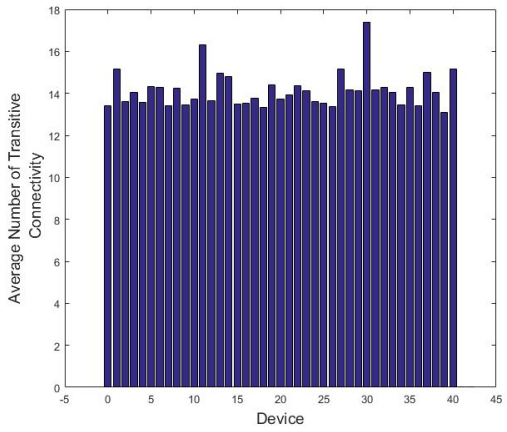
- It will precipitate the discovery of the peer with similar behaviour and mobility patterns with the message destination for efficient collaborative routing.
- It stimulates a behaviour-aware message routing protocol whereby each peer will determine a corresponding peer with similar behaviour with the message destination as a relay.

We next discuss in detail how we estimate the similarity of the peers' connectivity patterns for a proper connectivity routing strategy.



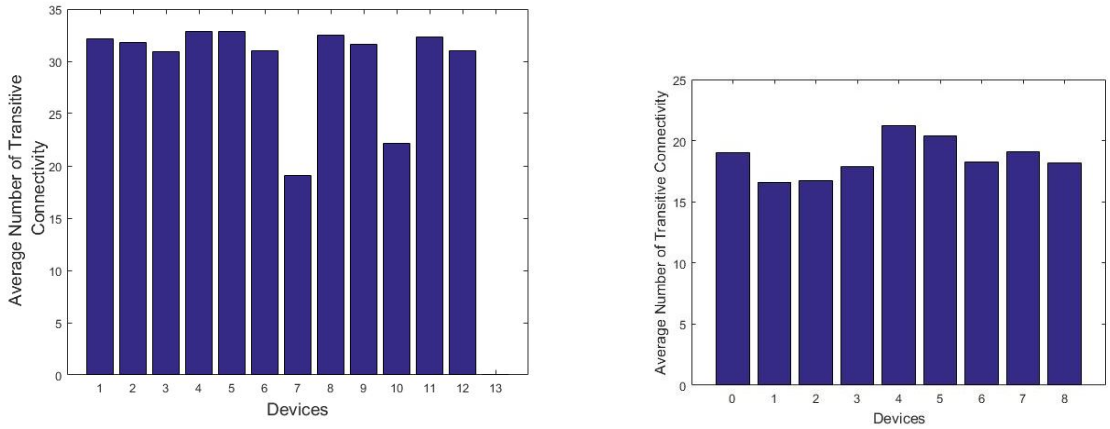
(a) 72 imote/infocom2006 traces (b) 52 imote/content traces

Figure 6.8: Transitive Connectivity Distribution of 72 and 52 nodes



(a) 41 imote/infocom traces

Figure 6.9: Transitive Connectivity Distribution of 41 nodes



(a) 12 imote/cambridge traces (b) 9 imote/intel traces

Figure 6.10: Transitive Connectivity Distribution of 12 and 9 nodes

6.2.4 Transitive Connectivity/Contacts Similarity Model

To some extent, the similarity regarding frequent contacts visiting locations of interest is often seen as major factors for connectivity in many real-world networks including DTN and Social Mobile Networks. One possible reason that supports this notion, is people tend to connect those sharing similar tastes, social backgrounds, interests and beliefs, and also similar popularity. This is often expressed as love of the same' or Birds of a feather flock together'; that is the tendency of individuals to associate and bond with similar others which can be treated synonymously with transitive connectivity similarity in the context of a network of devices [24]. More so, the similarity of peers' connectivity can serve as a network formation model, since it can also reproduce the commonly perceived power law or scale-free distribution of sparsely connected networks as described earlier.

In this section, we started by modelling the basic similarity between a pair of peers regarding frequent contacts with messages' destination to access the future encounter between a relay and the message destination. We define a specific function $S(q, d_{es})$ that expresses a similarity between peer q (a potential relay) and message's destination

within the range of [0,1]; such that if peer q frequently encounters a message destination, then it is probably a good relaying peer for the message meant for the destination. This implies that the more frequent peer q meets messages' destination the more the value of $S(q, d_{es})$ will be closer to 1. On the contrary, if peer q do not have any previous encounter with the messages' destination, the value of $S(q, d_{es})$ will be 0. To achieve this, we apply the extension of coefficient similarity (Tanimoto) [220] which can compute the degree of overlap between elements' vectors and is widely used in computational intelligence [221] for measuring the specific transitive similarity between any two sets of items. Therefore, we model contacts between peers with a binary vector of edge elements represented by 1 or 0; indicating that the two peers had a connectivity or not, respectively. Note, that in our experiment connectivity means contacts since we are dealing with a mobile network. Therefore, the transitive similarity of the two peers, q and d_{es} can be expressed as:

$$S(q, d_{es}) = \frac{\vec{v}_q \cdot \vec{v}_{d_{es}}}{||\vec{v}_q||^2 + ||\vec{v}_{d_{es}}||^2 - \vec{v}_q \cdot \vec{v}_{d_{es}}} \tag{6.2}$$

Note that the term $\vec{v}_q \cdot \vec{v}_{d_{es}}$ express the number of contacts' between the two peers (common encountered peers), and $\vec{v}_q$ and $\vec{v}_{d_{es}}$ represents the total contacts of peer q and messages' destination respectively. Also note that the maximum value of similarity [upper bound similarity] can be reached when the two peers are only encountered each other, having no contacts otherwise. That is when $\vec{v}_q \cdot \vec{v}_{d_{es}} = 1$. In that case, the resultant $||\vec{v}_q||^2 = 1$ and $||\vec{v}_{d_{es}}||^2 = 1$. Subsequently, we can define the transitive contact similarity between the two peers as shown in equation 6.3.

$$TS(q, d_{es}) = \frac{1}{deg(q) + deg(d_{es}) - 1} \tag{6.3}$$

Whereas, if there is no common encounter between the two peers the resultant

$S(q, d_{es}) = 0$; means the number of similar encountered peers between q and Sd_{es} is 0 [lower bound similarity]. In this case, there is no similar contact between the peers. Thus, the resultant similarity between them is 0. Thus, our basic transitive-similarity measure can be defined in the following equation (6.4).

$$T\dot{S}(q, d_{es}) = \begin{cases} 0, if\ \{(q, d_{es})\} \notin L \wedge \{(d_{es}, q)\} \notin L, \\ \frac{\vec{v}_q \cdot \vec{v}_{d_{es}}}{deg(q) + deg(d_{es}) - \vec{v}_q \cdot \vec{v}_{d_{es}}}, \text{ otherwise,} \end{cases} \tag{6.4}$$

Based on equation 6.4, it can be observed that the similarity value between peers who had never encountered each other and had no common encountered peers is 0.

6.3 Trust Transitive Forwarding Algorithm

We have shown that the presented trust algorithm (in Chapter Five) can provide each peer in the network a unique global trust value based on the peer's routing history in the network. Thus, a peer can evaluate its subjects or other peers, depending on their track records and previous encounters with the message destination (if any) or any other peer in the network. When two peers, p and q, interact, they can establish a local trust between themselves upon encounter.

Let $t_{p,q}$ be the trust value that peer p places in peer q based on its priori experience with peer q, where $t_{p,q} \in \langle 0, 1\rangle : p \neq q$. Each time peer p encounters peer q, peer p can assess the trust level of peer q based on their encounter delivery vectors exchanges. If the encounters history is not satisfactory it will be considered as a negative experience, therefore the local trust value ($t_{p,q}$) between p and q will decrease; while if the encounter history between the peers is satisfactory, then it will be considered a positive experience and the ($t_{p,q}$) will increase. If the peers' transaction is undecided, it will have no effect in the peers' trust evaluation. Therefore, $sat(p, q)$ represents the number of satisfactory encounters between peer p and peer q while $unsat(p, q)$ represents the total number

of unsatisfactory encounters between peer p and peer q. Each peer will check the corresponding delivery vector of its subjects to access the local trust of its subjects based on the following conditions:

- if the status of the previous message transactions between *trustor* and *trustee* is 0 (meaning a message was received by a trustee but is no longer in the trustees' buffer), and there was a recent encounter between a *trustee* and other peers in the network (probably the message destination), we assume that the outcome of the transaction is satisfactory.

- if the status of the previous messages received by a *trustee* shows it is still in its buffer (meaning the messages' status is 1) while the trustee is not the destination of the message and there was no recent encounter between the *trustee* and other peers in the network, then the outcome of the transaction is considered as neutral or undecided.

- if the status of the previous message received by a *trustee* shows it is still in its buffer, while there is an encounter history of a *trustee* meeting the message destination, the outcome of the transaction is considered to be not satisfactory.

- in the event where peer p is meeting a peer q for the first time, peer p can assign an initial trust value ($init(q)$) to peer q.

Evidence of trustfulness is manifested by the encounters history exchange between the peers. Thus, the resultant local trust value between the peers can be computed as $C_{p,q} = sat(p,q) - unsat(p,q)$. The normalised reputation can be computed as:

$$t_{p,q} = \frac{max(C_{p,q}, 0)}{\sum_q max(C_{p,q}, 0)}, ||\vec{t_p}|| := \sum_{q=1}^{N} t_{p,q} = 1 \tag{6.5}$$

The global trust equation (with no reliability scaling factor) peer p can place on peer q based on the feed back of peer r about the behaviour of peer q can be presented in the following equation 6.6.

$$T_{p,q} = \sum_{r} t_{p,r} t_{r,q} \tag{6.6}$$

Therefore, each peer will maintain the global trust vectors of its subjects as follows:

$$\vec{t_p} = (t_{p1,\ldots,t_{p,N}})^T, 0 \leq t_{p,q} \leq 1 \tag{6.7}$$

Algorithm 2 Compare-and-Forward Trust Algorithm Phase I

while *peer p is a message holder* **do**
  for *each peer* $r \in n_p$ **do**
    Get $t_{p,r}$;
    Send $t_{p,q}$ to all peers $r \in n_p$;
    query $r \in n_p$ to return $t_{r,q}$;
    compute $T_{p,q} = \sum_r t_{p,r} t_{r,q}$;

    if $T_{p,q} \geq Trust\_threshold$ **then**
      Elect q as a message holder;
      send a message to q;

    end
    /* do nothing and go to the next peer;
  end
end

Algorithm 3 TRUST ALGORITHM Forward Phase II

if *peer p has a message to send to* d_{es} **then**
  if *(*$\{(p,q)\} \wedge \{(q,d_{es})\} \in L$*)* **then**
    Initiate compare-and-forward trust-algorithm ()
  end
  else
    /* forwarding decision will include the transitive coefficient similarity with the destination peer. */
    Initiate Trust-Transitive-Forward ()
  end
  if *the message time* $t > m.ttl.$ **then**
    Delete message and related data;
  end
end

Algorithm 4 TRUST-TRANSITIVE -Forward Phase III

Initiate Trust-Transitive-Forward ()
while *the message is not sent* **do**
  for *each encountered peer q* **do**
    if $T_{\dot{S}(q,d_{es})} > T_{\dot{S}(p,d_{es})}$, *and q is a message holder = false* **then**
      Get $t_{(p,q)}$
      compute $T\_Trust_{(p,q)} = T_{(p,q)} * T_{\dot{S}(q,d_{es})}$
      if $T\_Trust_{(p,q)} \geq Trust\_threshold$ **then**
        Elect (q) as a message holder
        forward message to peer q
      end
      else
        do NOTHING and go to the next peer;
      end
    end
    else
      do NOTHING and go to the next peer;
    end
  end
end

$T\_Trust_{(p,q)}$ resultant transitive trust value

$n_p \longleftarrow$ the set of peers in p wireless range

$n_r \longleftarrow$ the set of peers in r wireless range

Algorithm (2) presents the pseudocode of the basic trust algorithm forward Phase I. As it can be seen, implementing the proposed algoritm is simple. Using the algorithm, the message carrier can forward the message to a peer with a trust value greater than the threshold. The pseudocode in algorithm (3) presents the extension of algorithm (2). For the purpose of illustration, let us assume there is a message created by peer p who wants to forward the message to peer d_{es} through a relay peer q. From the presented algorithms, there are two possible phases in which a peer p can forward message to destination d_{es}: in the first phase, peer p can forward the message to the destination if they are in direct contact with peer q; if the message carrier detects the presence of the message destination in the connectivity status of the relaying peer. In this regard, a simple trust algorithm compare-and-forward could be initiated, algorithm (2). In this regard, a process of message forwarding can be achieved without including the transitivity similarity coefficient.

In the second phase, if the relay is not in the same transmission range with the destination peer, the message carrier will have to compare its transitive contacts' similarity with the destination peer, and that of the relay with the destination peer. In this regard, the process of Trust Transitive Forwarding Algorithm can be invoked. Looking at algorithm (3) and the pseudocode in algorithm (4), starting from the message sender, if peer p is currently holding the message, it will ask for a contact list of each encountered peer for the comparison with its transitive contacts' similarity with the message destination. If the encountered peer is more similar to the target in terms of the *transitive proximity* (i.e., $T_{\dot{S}(q,d_{es})} > T_{\dot{S}(p,s_{es})}$), and the resultant computed transitive trust value $T\_Trust(p,q)$ is greater than the assigned trust threshold, then, the responsibility of forwarding the message will be passed to the encountered peer.

Based on the presented algorithm, one can observe that in the presence of multiple

neighbouring peers, a message carrier can only send a message copy to peers who are trustworthy (have a record of successful message delivery) in the network and have higher chances to encounter the message destination through either direct connectivity or transitive connectivity. Therefore, in an ideal Opportunistic Network Environment the presented model can form an inherent ramp for the messages to follow to reach the destinations with less effort. Note that the message carrier will keep on evaluating every contacted peer and replicate the message as long as *m.ttl* is valid. Thus, a message carrier can forward a messages' multiple copies (*replica*) to the relaying peers making the protocol a multi-copy routing scheme. The strategy design in our proposed solution can be seen in the pseudo-code presented in the algorithms (2),(3) and (4). Although, in our proposed protocol, multiple copies are generated in the network, this is only possible if the evaluating relay peer is trustworthy, and there is a higher chances of the relay meeting the messages' destination. Therefore, the only possible encounter that involves message transfer is the encounter with a trustworthy peer that can deliver the message to destination, reducing unnecessary overhead. Consequently, our scheme yields fewer replicas which by extension can improve resource usage. Further, in our proposed scheme, since a peer can only replicate a messages' copy to another, if the routing quality (resultant transitive trust forward value) of the latter is greater than the assigned trust evaluation threshold, a trustworthy transitive routing path can be optimised. Thus, a transitive aware trust-based protocol is achieved.

6.4 Performance Evaluation

In this section, we discuss the conducted simulations with the results obtained. For the simulation, we assume interpersonal communication between mobile devices using

smart phones or similar devices with a blue tooth of 2Mbit/s net data rate and 10m wireless range. Each device has up to 100 MB of buffer for storing messages except the malicious peers. Peers move in the terrain of 8399 x 7300m (see Figure 6.11). We ran the trace-driven simulations with the collected traces as pedestrians by the collected traces' connection events. Each device moves with a speed range of $0.5m/s$ and $0.75m/s$ using the simulation parameters presented in table 6.3.

To understand the delivery performance of our protocol, we use the varying message TTL ($m.ttl$) of $300, 600, 900, 1200$ and 1500 minutes. Thus, we define the message delivery ratio as the proportion of messages successfully delivered to the destinations before the messages' TTL expires. We calculated the transmissions' overhead as the total number of messages spread to the message holders and delivered to the destination. We use the *Trust_threshold*=0.85 and initial trust weight ($init = 0.25$) for implementing our proposed T-Trust forwarding strategy. However, if one desires more reduction in the messages' copies (overhead), setting higher threshold provides less overhead, though at the expense of delivery ratio. We evaluated our proposed solution with three well known opportunistic environment protocols namely *Epidemic*, *dLife* and *Bubble Rap*.

- **Epidemic routing** [196]: Upon an encounter between peers, the message carrier always forwards the message to the peers that do not have the messages' copy. Since, this protocol has a good performance in terms of delivery ratio, we consider the epidemic approach as the upper bound regarding delivery ratio.

- **Bubble Rap**[172]: The Bubble Rap forwarding strategy uses centrality, community and interaction of users to enhance delivery performance in Mobile Opportunistic Networks. In the Bubble Rap protocol, the message is always forwarded to the most central peer (a node with higher centrality) until the message reaches the destination peer.

- **dLife** [216]: With the dLife protocol, the dynamic change of the peers' mobility behaviour is a metric to determine the message carrier through keeping track of peers' social interaction levels concerning peers' contacts and connectivity.

To provide a fair comparison and to show the possibility of integrating another routing mechanism with our proposed transitive trust forwarding schemes, we ensure all the protocols settings, and random messages' creation strategy are the same and under the same conditions.

To explore the effect of untrustworthy peers as described in our model, we assigned to each simulation scenario a specified number of malicious peers. For the 72 imotes/intel traces, 52 imote/Cambridge traces and 41 imotes/imforcom traces we assigned 5% of peers to be malicious peers, while for the 12 imotes and 9 imotes traces we only assigned 2 malicious peers each. We achieved this by configuring the malicious peers with a limited buffer space of 2MB only, meaning the peers can create a message of size 500KB to 1MB, but they cannot handle the messages from other peers, due to the limited capacity. For the simulation period, we configured 72 imotes traces for 334368 seconds, 52 imotes traces for 987552 seconds, 41 imotes' traces for 254016 seconds, while for 12 imotes' traces, 455609 seconds, and 9 imotes' traces, 359190 seconds.

Note that the malicious behaviour of the peers configured in our experiment is not a perspicacious type of attacks where peers can spoof, other peers IDs, or collude in attacking other peers. The malicious peers only drop their received message due to their limited resources making them be non-trustworthy peers in the network.

The evaluation results in Figure 6.12 and 6.14 shows the average of messages' delivery ratio of 1000 simulation with 95 % confidence interval.

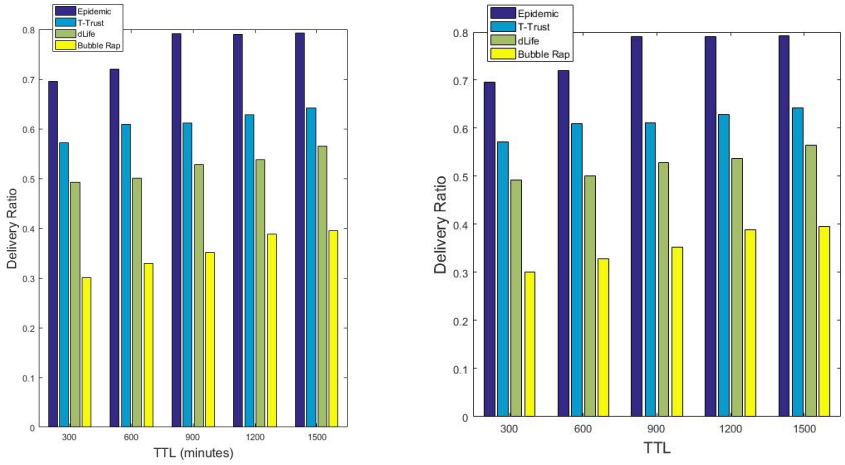
From the figures, it can be observed that the delivery ratio of epidemic protocol outperforms *T-Trust, dLife* and *Bubble rap* protocols. The Epidemic routing protocol

Table 6.3: Simulation Parameters

Messages' TTL (minutes)	300,600,900,1200,1500
Messages' generation interval (seconds)	25-35
Number of interface per peer	2
Buffer Sizes of trustworthy peers	100MB
Buffer Sizes of non trustworthy peers	2MB
Peers' interface	Blue tooth
Message sizes	(500kB - 1MB)
Pre-trusted Peers Weight	$init = t_p^{(0)} = 0.25$

takes advantage of messages' random replications through *spreading* the messages' copies with any encountered peers. Subsequently, messages can easily reach the various destinations causing the increase of messages average delivery ratio in comparison with *T-Trust, dLife and Bubble Rap* up to 19%, 37% and 53% respectively.

When comparing the performance of *dLife* and *Bubble rap*, *dLife* performs up to 22% in comparison with the *Epidemic* protocol as it is possible for peers (using) *dLife* protocol to capture dynamic contacts of peers for routing selection.



(a) 72 imote/intel traces (b) 52 imote/cambridge traces

Figure 6.12: Performance Comparison of T-Trust With *dLife* and *Bubble rap*: Delivery Ratio, 72 and 52 Imotes

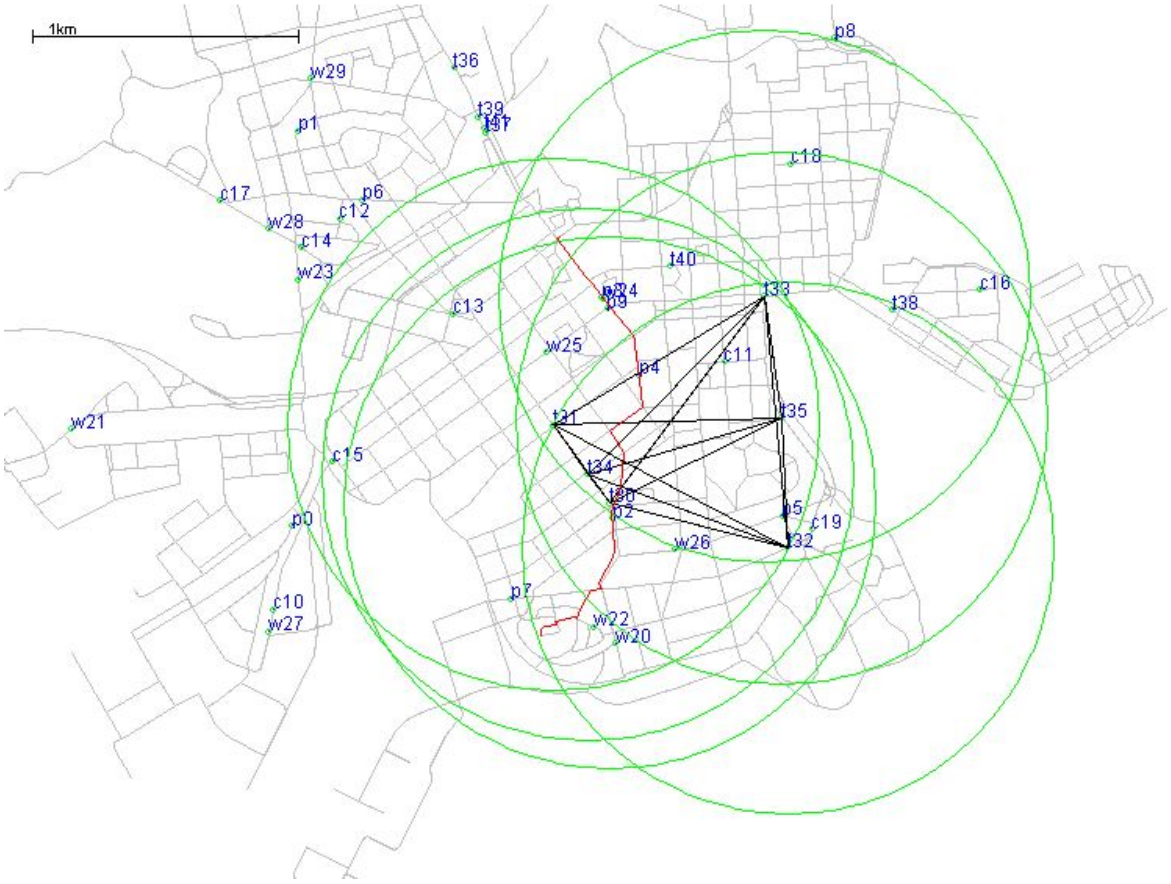
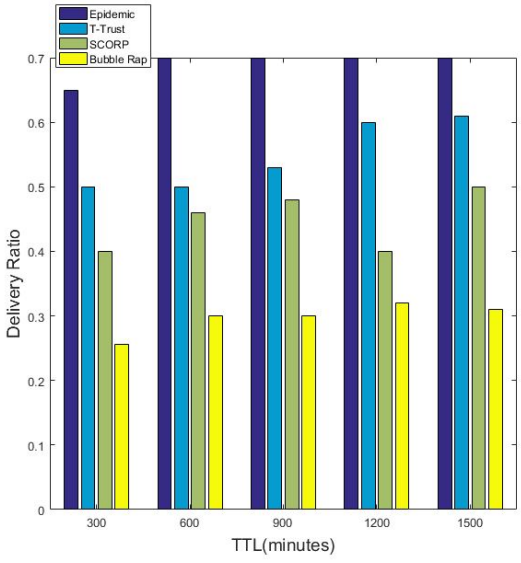
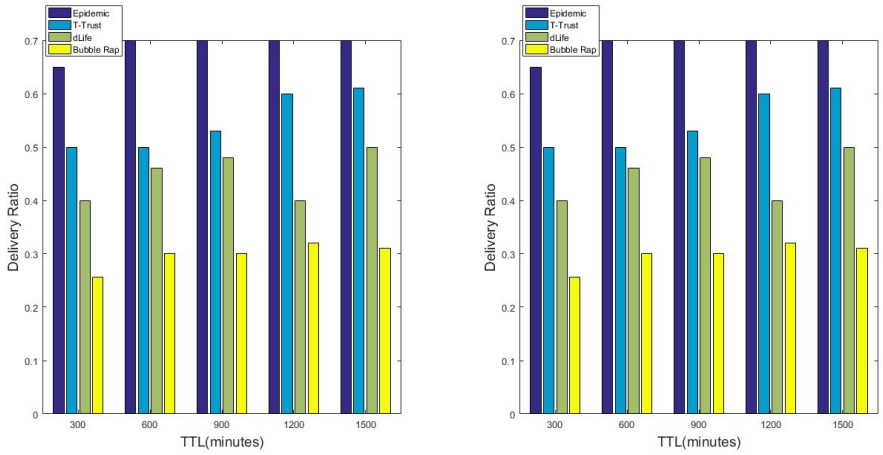


Figure 6.11: Simulation map (Numbers Represents the Nodes, Circle Represents the Nodes' Wireless Range)



(a) 41 imote/infocom traces

Figure 6.13: Performance Comparison of T-Trust With *dLife* and *Bubble rap*: Delivery Ratio, 41 Imotes



(a) 12 imote/content traces (b) 9 imote/infocom2006 traces

Figure 6.14: Performance Comparison of T-Trust With *dLife* and *Bubble rap*: Delivery Ratio, 12 and 9 Imotes

Perhaps the performance of **Bubble Rap** is affected since the protocol relies on the peers' global centrality[172]. To rationalize this opinion we calculated the average centrality of all the traces' connectivity and found that the traces' centrality are 5.267%, 9.668%, 10.346% 8.459% and 18.188% for 72 imotes/intel traces, 52 imotes/Cambridge traces, 41 imotes/infocom traces,12 imotes/content traces and 9 imotes/inforcom2006 respectively. Thus, most messages' were generated in low centrality peers causing the messages to probably not reach the destinations.

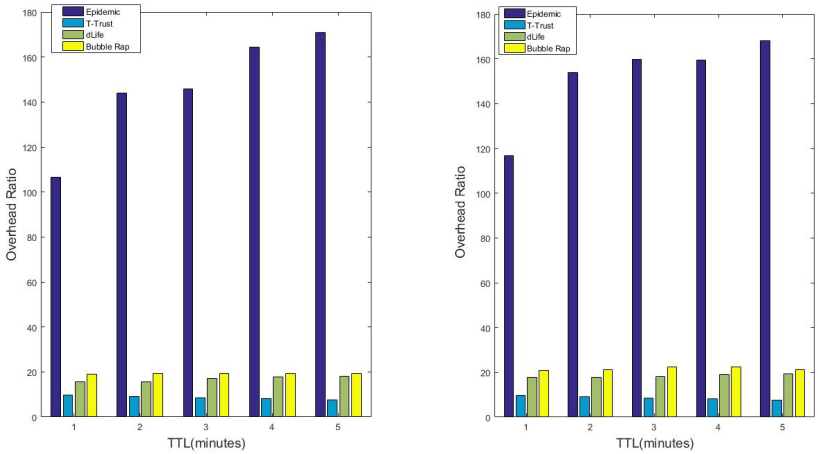
On the other hand, the T-Trust forwarding strategy takes advantage of (i) identifying a trustworthy based on the peers' previous message forwarding and (ii) transitive contacts among peers to replicate the message to the relay peers. This made it possible for peers to detect and exclude the malicious peers in the forwarding lists and quickly disseminate messages in the network. Probably, the reason *T-trust* suffers the decrease in delivery ratio in comparison with *Epidemic* protocol is due to the limited number of messages forwarded, which increases with an increase in TTL. This made it possible for a few messages to be discarded, perhaps due to the limited buffer sizes. However,

it can be observed that with the increase in TTL the message delivery ratio is slightly increasing, though this is applied to all other protocols.Therefore, when making overall comparisons in terms of message delivery ratios, it is clear that the T-Trust forwarding strategy has the best performance since it achieves a higher delivery ratio than when using the *Epidemic* protocol. This confirms our previous observations that through evaluating the trustfulness of the peers in terms of data forwarding, and the exploration of similarities between the relay and message destination might increase message delivery probability in an Opportunistic Network Environment.

Looking at the protocol overhead in Figure 6.15 and 6.17, *Epidemic* protocol creates the highest messages' replica as the peers keep on spreading the copy to any contacted peers. However, *dLife* protocol creates the messages' replica based on peers' important and social ties between encountered peers and the messages' destination (i.e., communities formed by the peers based on the pre-defined contact duration).

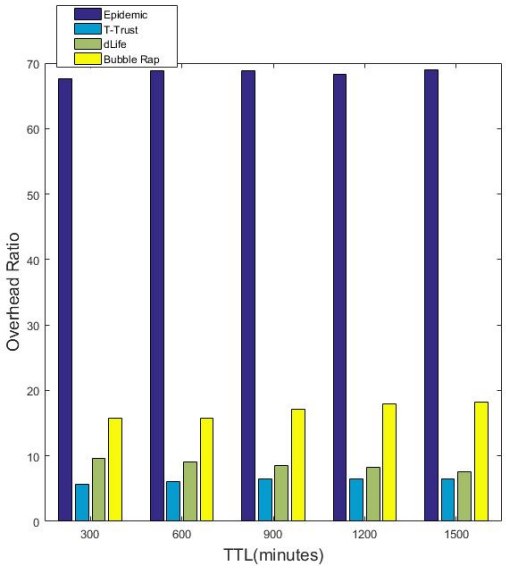
Subsequently, looking at the identified community structure in the traces which represents how cohesive peers are connected and form community structures in the network[214]. This explains why the *dLife* protocol produces between 20% and 11.9% replica higher than the T-Trust protocol, 60% and 56% fewer replicas than the *Bubble Rap* and about 87% less replica than *Epidemic*.

From the resultant T-trust model, it is easy for the peers to identify the trustworthy peers and who do not have the messages' copy in the network. Therefore it is expected for the T-Trust to produce fewer messages' replica as realised in the simulation studies. The results demonstrated that T-Trust creates 89%, 2%, and 39% less replicas than the *Epidemic*, *dLife* and *Bubble Rap*, respectively.



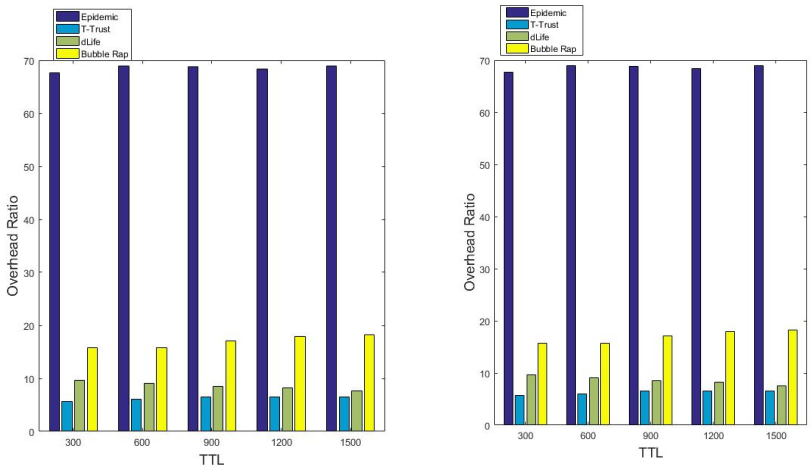
(a) 72 imote/intel traces (b) 52 imote/cambridge traces

Figure 6.15: Performance Comparison of T-Trust With *dLife* and *Bubble rap*: Messages Overhead, 72 and 52 Imotes



(a) 41 imote/infocom traces

Figure 6.16: Performance Comparison of T-Trust With *dLife* and *Bubble rap*: Messages Overhead, 41 Imotes



(a) 12 imote/content traces (b) 9 imote/infocom2006 traces

Figure 6.17: Performance Comparison of T-Trust With *dLife* and *Bubble rap*: Messages Overhead, 12 and 9 Imotes

6.5 Chapter Summary

We have presented in this chapter,a routing decision-making process which consists of a sequence of two independent pieces of information: (i) the trustfulness of the relaying peer (in terms of message delivery) and (ii) the transitive contact information of the relaying peer with the message's destination. In other words, our trust model exploits peers' connectivity information with the destination and also with peers' routing history.

The presented approach in this chapter suggests a new perspective in trust-based routing model studies and a new way of interpreting peers' connectivity and offers insight into how peers' connectivity can be construed as additional information for the development of trust and reputation protocols.

Our trust-based protocol design allows the peers to identify the matchless peer in the midst of other peers to maximise message delivery and minimise overhead. The result of this study backed by the simulation validation demonstrated that our approach has

several advantages in comparison with *Epidemic* protocol regarding messages' overhead(number of the replica) and *dLife* and *Bubble Rap* in terms of delivery ratio and overhead.

Further, the result validations in this chapter shows that our proposed solution is resilient against malicious peers (peers who can drop messages while serving as relays) and achieves higher performance of delivery ratio in comparison with other approaches. Even though we implemented our proposed trust-based routing protocol in an Opportunistic Network Environment, we discern that the presented concept in this chapter can be useful in the design of Intelligent vehicular ad-hoc network protocols, Delay Tolerant Network Protocol, Mobile Wireless Sensor Network protocols and many related efficient forwarding strategies in wireless networks.

Chapter 7

Forward-Watcher Trust Model Protocol

In this chapter, we hypothesise that through properly distributed network observations, routing listening and gathering statistics of routing history efficiently, peers' routing performance can be enhanced by making better routing decisions, and thus improve network performance. We propose a Forward-Watcher trust evaluation scheme: a statistical approach to learning peers' routing patterns based on the encounter/proximity between wireless peers for trust evaluation. We present a scheme by which the peers can dynamically understand the changes of their subjects' routing patterns and behaviour to enforce cooperation between peers. Our focus in this chapter is on learning peers' routing forwarding ability that gets better with time (as the peers learn). For our contribution in this chapter (i) we introduce four important metrics for peer trustworthiness evaluation that are linked to learning peer routing history based on message (messages' beacons) overhearing for trust evaluation between peers (ii) we introduce a model for evaluating the probability of the peers' forwarding and receiving potential for local trust evaluations (iii); we present a correlation matrix for evaluating peers' global trust value; and (iv) we leverage our presented attributes' similarity analytical model (see section 5.2.3 in chapter five), and transitivity model (section 6.2.3 chapter six) for

attribute and transitivity analysis. The advantage of the proposed Forward-Watcher approach is that through routing history created by the peers, they can statistically predict the future behaviour of their corresponding routing partners. The concept can also serve as an underpinning and a cornerstone for developing self-cooperative protocols in wireless mobile networks using statistical analysis and correlation matrices.

7.1 Background

Different techniques of trust-based message forwarding strategies use incentive mechanisms to enforce cooperation and peers' fair contributions in the routing processes[222] [223, 224]). Similarly, many incentive forwarding strategies proposed in the literature are based on the reciprocity mechanism: an act of giving back or reciprocating the kind of treatment an actor received from others [225]. Traditionally, the incentive forwarding scheme assigns a trust ranking to peers based on their previous cooperation in the network and propagate the peers' reputation in the network.

For example, the work in [226] proposed incentive-compatible payment mechanisms based on a credit-based system where peers participate in a path revelation game. The mechanism allows the underlying routing protocol to discover the most efficient paths for message transfer between peers. When making forwarding decisions, peers are paid for message forwarding, and the message destination makes the rewarding decision.

In addition, the work in [227] proposed a mechanism to discourage selfish behaviour based on the principles of barter (exchange of good services). The barter cooperation mechanism is a game-theoretic model of trade between peers who exchange messages when in contact so that the utility of each peer is maximised, based on its message exchanges with other peers in the network. However, we understand that some of the

problems associated with incentive schemes proposed in the barter cooperation mechanism include (i) the possibility of non-trustworthy peers creating arbitrary contributions and assigning them to malicious peers (e.g., *Black hole*, *Sybil* peers), (ii) the processes of peer incentives or contribution management may add additional complexity to trust-based protocols.

Another important question posed in the work of [228] which we found slightly related to our scenario of interest (mobile opportunistic environment), is how the network can enforce peer cooperation using incentive mechanisms in dynamic and intermittent network settings. The author proposed a reward scheme that provides incentives named *in-network realisation*, using peers' transit behaviour and trust ranks, which in turn, translate the peers' ranking into a message priority. We see that such an approach is potentially a promising mechanism; however, the main components of the schemes' *rank manipulation* have a mix-up. For example, in the rank manipulation process, the relaying peers are only rewarded when the message is successfully delivered to the destination. The destination peer can then reward all the relay peers that participated in the message-sending based on the populated list of the forwarders in the message header list. In such a reward strategy, any peer can readily promote its reputation by adding its ID to every message header it receives, and it can also add the IDs of other peers who did not contribute to the message-relaying process. In this regard self-promotion among peers can affect the reputation integrity of the scheme [229].

Therefore, we postulate that through properly distributed network observations, routing listening and gathering statistics of routing history in an efficient way, a reciprocity trust forwarding algorithm can be realised for better routing decisions, and it can improve network performance.

On the other hand, the routing requirements of different network applications and architecture can be different: some applications require a unicast routing service, where, for example, a source can send a message to particular destination correctly. But some applications require a more specific routing service that promotes the message source to route the message to a certain group of peers identified by their geographical location (e.g., Geocast Routing) [230]; or traditional wireless broadcast transmissions where multiple peers can possess a copy of a message, though it is intended for a different receiver.

Some of the applications of broadcast wireless communication routing schemes include ubiquitous sensing applications in future large-scale low power IoTs [231][232]; design and analysis of pairing protocol for bluetooth[233], networked sensors in the infrastructure, simple wireless sensor networks and delay tolerant network applications etc.

Subsequently, the features of wireless media broadcast have been exploited widely in the literature for the design of efficient cooperative routing protocols (see for example the work of [234][235][112]).In these types of networks, peers inside the transmission range of a sender can obtain a copy of the message forwarded to the intended receiver. For example, consider an IoT network equipped with a Bluetooth devices [236], Due to the recent low energy implementation and short range in mobile devices, peers can broadcast a beacon signal actively in the network. In the event the users of a mobile device have their Bluetooth turned on, they can receive nearby beacon signals which can trigger a notification or other behaviour in the network [237].

Nevertheless, we identified some challenges associated with the design of trust-based routing protocols in a wireless broadcast environment: (i) how can a peer learn the forwarding patterns of its subjects? (ii) can the peers' forwarding behaviour be appropriately consistent to give a substantial basis for the prediction of the peers' reliability

in handling the routing task? (iii) how adequately can a peer understand its subjects' forwarding and receiving patterns for trust evaluation? To answer these questions, we propose a statistical approach to learning the peers' routing patterns and histories for trust evaluation between the peers in a network. Our focus is on learning peers' routing forwarding ability that gets better with time (as the peers learn).

7.1.1 Models' Requirements

We established four main design principles for our proposed model:

- The model should be dynamic so that a significant change of a peers' forwarding in comparison with its receiving patterns can affect the change of its trust values in the network.

- The system should not assign undue advantages to newcomers (no free initial trust value to newcomer peers). Instead, the peers' attribute can serve as their initial trust value. In other words, the trust and reputation computation should be based on multiple transactions and peer attributes at the required level of routing performance.

- The model should be distributed and self-policing. There should be no central coordination point between the peers, and the trust evaluation should be based on the peers' discretion and observations. Also, the peers should define and enforce what they consider an acceptable level of performance while evaluating other peers in the network.

- The model should have minimal overheads.

Having identified the models' requirements, the next section discusses its underlying assumptions.

7.1.2 Models' Assumptions

To understand the notion of our proposed Forward-Watcher scheme we have to assume some specific requirements as follows:

- Broadcast transmission, conflict-free transmission and multi-hop message propagation in a store-and-forward manner instead of a continuous flow of information.
- Each peer has a unique ID and it cannot be spoofed.
- The network is dense enough that each peer has at least two one-hop neighbours.
- When the peers are in network operation mode, they are in promiscuous mode. i.e., they can overhear their subjects forward.

The next section in this chapter demonstrates the proposed Forward-Watcher scheme.

7.2 Forward-Watcher Trust Model

In the Forward-Watcher scheme, each peer monitors the receiving and forwarding behaviours of its neighbours, then assigns the reputation values to them based on their observed behaviour. Figure 7.1 shows a simple illustration of Forward-Watcher. The vertices correspond to peers in the network, and the edges represent a wireless connection between peers. The edge between peers exists based on two conditions: (i) if they are in proximity or in the same transmission (i.e., they can overhear their neighbours' forwards using simple broadcast) (ii) if the peers are transitively related (please refer to Chapters Four and Six to see the transitivity model used) with one hop between them; meaning the wireless range overlap can still make it possible for the peers to overhear their subjects' forwards. The positive real number $t \in [0, 1]$ is the local trust level that peer p places in peer q; with $t_{p,q} = 0$ means peer p consider peer q as untrustworthy, and

$t_{p,q} = 1$ indicate that peer p fully trusts peer q. In our proposed model, the trust level of p on q depends on three elements, namely, (i) the peers' forwarding and receiving ability (ii) the peers' delivery predictability and (iii) the peers' ability to forward the message on time. In the subsequent section, we will see how this information can be leveraged for learning peers' routing behaviour for trust evaluations.

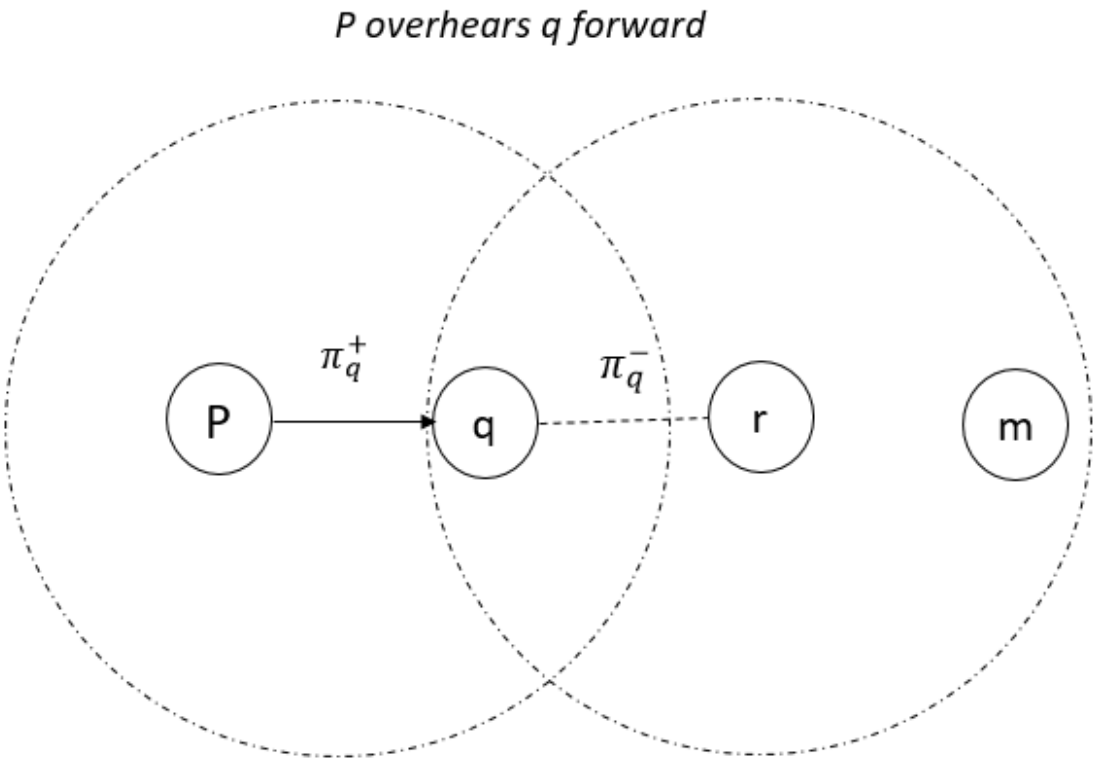


Figure 7.1: *Forward-Watcher Illustration*

7.2.1 Learning Peers' Routing Behavior for Local Trust Evaluation Based on *Forward-Watcher*

In this subsection, we present the mechanism of learning peers' routing behaviour; forward and backwards (Forward-Watcher) for mitigating a peers' malicious or malfunction effects in the network. For the purposes of illustration and modelling of our proposed system, consider the diagram in Figure 7.1. Suppose peer p wants to forward

a message to peer r; however, peer p cannot forward the message all the way to peer r, but it can listen on peer q traffic. Thus, whenever peer p transmit a message meant for r to q (peer q serving as a relay), peer p can often tell whether peer q forwarded the message to r or perhaps if peer q receives messages' from any other peer in the network. Thus, peer p can notice both the receiving and forwarding of peer q. Also, peer p can possess the copy of the message forwarded by peer q.

We assume that the links between the peers are not encrypted, and the channel quality between the peers is good for the peers to listen. If the outgoing link or forwarding potential of peer q to neighbour r is denoted as Π_q^-, we can, therefore, denote its incoming traffic, i.e., the one received from peer p as Π_q^+. The details of *Forward-Watchers'* phases are presented below:

- **phase 1:** Peer p can forward the message to peer q having contact/proximity with peer q who is in its transmission range and has higher chances to meet the messages' destinations. This can be understood through the exchange of peers' delivery predictability as described in chapter five (please refer to 5.2.1 for the details on the peers' delivery exchange). The reason for choosing the exchange of delivery predictability is for the peers to include the probability of the relaying peer meeting the messages' destination. Thus, peers can exchange out-of-bounds information which can enable the peers to know more about their corresponding routing partners.

- **phase 2:** During the first encounter (proximity) between the peers, each peer will get the attributes values of its subjects as described in detail in chapter five (please refer to section 5.2.3 for the detail on attributes similarity evaluation between the peers). The peers can then compute the similarity of their attributes and that of their subjects. In this regards, the resultant similarity value is regarded as an

incentive value or initial trust (based on the similarity of the peers' attributes) (*init*). Subsequently, when peer p encounters peer q (direct encounter), peer p can forward the data to peer q; this will be further referred to as peer q's receiving potential. Also, each time peer p forwards a message to peer q, it will increment the value of (Π_q^+).

- **phase 3:** Peer p will maintain a currently sent message in its buffer to compare the overhead message with the transmitted message. If the messages are matched then peer p will discard the transmitted message and increment peer q forwarding potential (Π_q^-); otherwise, peer p will decrement peer q forwarding potential. This method will help peer p to detect whether peer q has change messages' payload or the message header and to determine whether peer q have successfully forwarded the correct message to the next peer or the destination.

7.2.2 Forward-Watcher: Local Trust Evaluation Based on the Peers' Direct Observations

In this section, we describe Forward-Watcher local trust evaluations. By the local trust, we mean the aggregated direct observations between peers. Upon an encounter between two peers (p, q), peer p can update its direct trust on peer q based on the update of the total forwarding and receiving records of peer q which can be represented as $\sum_{i=1}^{n} \Pi_{q\,i}^-$ and $\sum_{i=1}^{n} \Pi_{q\,i}^+$ respectively. However, due to the subjective nature of trust, peer p needs to include the delivery predictability of peer $q(dr_{q,Dist})$ with the destination in the trust evaluation. This is to enable peer p to determine whether peer q have a chance of meeting the messages' destination. In this regard, we leverage the proposed delivery predictability in section 5.2.1 (please refer to chapter 5). For simplicity, lets denote $\sum_{i=1}^{n} \Pi_{q\,i}^- = \Pi^{*-}$ and $\sum_{i=1}^{n} \Pi_{q\,i}^+ = \Pi_q^{*+} : \Pi^{*-} \leq \Pi^{*+}$. We can therefore define the

probability of peer q forwarding record noted by peer p presented below.

$$pr_{p,q} = \frac{\Pi_q^{*-}}{\Pi_q^{*+}} \tag{7.1}$$

Therefore the local trust value that peers p has in peer q can be computed as:

$$t_{p,q} = pr_{p,q} * dr_{q,Dist} * init * \gamma^x, 0 \leq t_{pq} \leq 1 \tag{7.2}$$

Where $init$ is the assigned initial trust value by peer p to peer q (for the first encounter between peers' only), and γ is the *aging* constant exponentiated with the time x that has elapsed since the time a peer was expected to forward a message. The messages' time slice can differ, and should be assigned based on the message' Time To Leave (TTL); the possible hop-counts and the approximate encounter interval ($[t, t + \delta t]$). In the event the message stays till time-out in the peer q buffer, it is less likely for peer q to forward the message. Thus, the peers' failure to transmit the message timely must affect its computed trust forwarding potential which will be reduced in the process. Therefore, peer p will increment the failure tally for peer q. If the number of failure tallies increases, the peers' trust value will significantly reduce which can further lead peer p to declare peer q as a misbehaving peer causing peer p to subsequently refuse to forward data to peer q. Accordingly, if a peer forwards a message to the next neighbouring peer within the expected limit of time, the peers' trust level can simply be computed as:

$$t_{p,q} = pr_{p,q} * dr_{q,Dist} * init, 0 \leq t_{p,q} \leq 1, \tag{7.3}$$

To facilitate understanding and the implementation of our proposed Forward-Watcher scheme, we present an illustration for evaluating a peers' trustworthiness and for evaluating peers' trustworthiness and healthiness based on the peers' routing behaviour (receiving and forwarding potentials) in Figure 7.2 which illustrates how the peers can

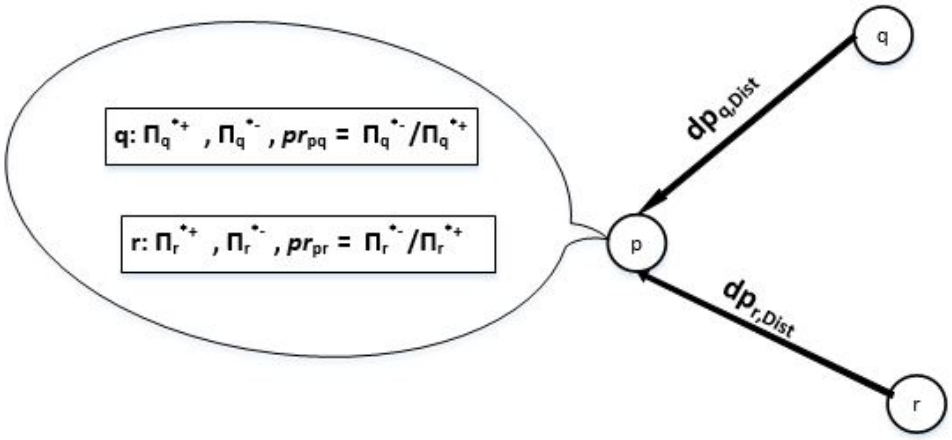


Figure 7.2: Illustration: Forward-Watcher Trust Evaluation: Direct Contact

establish the local trust lists based on their direct observations and their subjects delivery predictability. As an example, peer p can compute the trust value of peer q and peer r based on the corresponding values of $pr_{p,q}, pr_{p,r}, dr_{q,Dist}, dr_{r,Dist}$.

Therefore, we define the local trust value that peer p has in peer q as a product of the probability of peer q delivering a message it received from peer p and the peers' delivery predictability with the messages' destination. We will see later in the subsequent section how this interpretation can be used in computing the peers' global trust values.

7.2.3 Aggregating Global Trust Value and Forwarding Strategy

One challenging aspect of the presented local trust values' computation for making routing decisions is a peer might not have a holistic understanding of other peers' experiences and trust levels about a particular peer involved in a routing decision. As a result, peers can succeed in launching an attack.

For example, a malicious peer can disguise its malicious behaviour as unintentional temporary errors, or on-off attacks (most of the time it forwards all messages but occasionally it drops most or all of the messages) [139] so that it can maintain its

credibility with certain peers while causing harm to other peers. This type of exposure leaves the network open to many types of attacks [238].

To solve this problem, the peers need to understand the global routing histories of their subjects (peers' forwarding and receiving ability). In this regard, we employed a statistical technique that can reveal how strongly Π_q^{*+} and Π_q^{*-} are related. We, therefore, seek to find the correlations between the aggregated peers' forwarding and receiving records to predict relationships that can be understood between the two values (Π_q^{*-}, Π_q^{*+}).

In practice, the number of messages received by a peer in collaborative forwarding should correlate with the number of messages sent by a peer. We, therefore, seek to understand how peers' forwarding and receiving records tend to correspond, i.e., how they tend to show similar behaviour. Initially, when a peer receives a message, it buffers it upon encountering other peers who are in its transmission range, and the decision of whether to forward or not to forward the message and exactly to which peer to forward the message to, can be made.

For the purpose of illustration, consider the diagram in Figure 7.1, suppose both peer q and peer r are in the same transmission range with peer p. And there was no prior encounter between peer p and peer r, making a routing decision about a peer using similarity of peers' attributes as described in section 7.2.2 might not be enough to judge a peer. Thus it will be better to weight other peers opinion about peer r. To achieve this, we seek to measure the strength and direction of the linear relationship between the two variables: Π^{*+}, Π^{*-}. We therefore define the covariance of the peers' forwarding and receiving record as:

$$cov(\Pi^{*+}, \Pi^{*-})_q = \langle (\Pi_q^{*+} - \eta\Pi_q^{*+})(\Pi_q^{*-} - \eta\Pi_q^{*-}) \rangle \tag{7.4}$$

where

$$\eta\Pi_q^{*+} = \frac{\sum_{i=1}^{n} \Pi_q^{*+}{}_i}{n}$$

and

$$\eta\Pi_q^{*-} = \frac{\sum_{i=1}^{n} \Pi_q^{*-}{}_i}{n}$$

are the respective means of the sum of the peers receiving and forwarding records which can be explicitly written as:

$$cov(\Pi^{*+}\Pi^{*-})_{qi} = \sum_{i=1}^{n} \frac{(\Pi_q^{*+}{}_i - \eta\Pi_q^{*+}{}_i)(\Pi_q^{*-}{}_i - \eta\Pi_q^{*-}{}_i)}{n} \tag{7.5}$$

Where n represent the total number of both receiving and forwarding records of peer q. The value $cov(\Pi^{*+}, \Pi^{*-})_q$ returns the covariance between two variables Π^{*+} and Π^{*-}. From the above equation (7.5), we can understand the peers routing behaviour based on the two possible values of the resultant covariance.

The first possible value of the covariance is when the values of Π^{*+} and Π^{*-} are not correlated and the second possible value of the covariance is when Π^{*+} and Π^{*-} are correlated in some way. For uncorrelated forwarding and receiving records, the resultant value of $cov(\Pi^{*+}, \Pi^{*-})_q$ can be presented as follows:

$$cov(\Pi^{*+}, \Pi^{*-})_q = \langle \Pi_q^{*+}, \Pi_q^{*-} - \eta\Pi^{*+}\eta\Pi^{*-} \rangle = \langle \Pi^{*-} \rangle \langle \Pi^{*+} \rangle - \eta\Pi^{*-}\eta\Pi^{*+} = 0 \tag{7.6}$$

In this case, the relationship between peers' forwarding and receiving records is non-correlated, while in principle, the covariance between peers' forwarding and receiving records should be positively correlated. This condition further reveals the characteristics of a misbehaving peer in collaborative routing. i.e., when the forwarding records of a peer are not positively correlated with the receiving record of a peer.

Furthermore, if the rate at which the number of messages received by a peer is similar with the rate at which a peer forwards the number of messages, then their covariance

will be non-zero. as presented in the following equation (7.7) or (7.8).

$$cov(\Pi^{*+}, \Pi^{*-})_q > 0 \tag{7.7}$$

$$cov(\Pi^{*+}, \Pi^{*-})_q < 0 \tag{7.8}$$

From these two possible conditions, we can deduce three possible scenarios of understanding the peers' routing history and pattern: **scenario 1:** In a special case which is a solution of our interest, the number of messages forwarded by peer q is exactly the same as the number of messages received by peer q i.e, if $\Pi_q^{*+} = \Pi_q^{*-}$, then the resultant covariance between Π_q^{*+} and Π_q^{*-} can be written as follows:

$$cov(\Pi^{*+}, \Pi^{*-})_q = cov(\Pi^{*-}, \Pi^{*-})_q = cov(\Pi^{*+}, \Pi^{*-})_q = Var(\Pi_q^{*+}) = Var(\Pi_q^{*-}) \tag{7.9}$$

Where $Var(\Pi_q^{*+})$ and $Var(\Pi_q^{*-})$ represents the variance of peer q receiving and forwarding records respectively.

Looking at the condition in the above scenario 1, one can observe that in a typical store and forward routing strategy when a peer forwards a message to an intermediate peer, the receiving peer will keep the message and will send it at a later time to the final destination or another intermediate peers; therefore, a good behaving peer is expected to forward the exact amount of messages it received from other peers unless the peer itself is a destination for the message.

scenario 2: if $Cov(\Pi^{*+}, \Pi^{*-})_q > 0$, this indicates the tendency that when the peers' receiving record (Π_q^{*+}) is increasing so does its forwarding record (Π_q^{*-}). This is also a solution of our interest. However not as interesting as the solution in scenario one. In this case, a peer may be good behaving peer, but with some limitations, i.e., a peer likely dropped some few messages.

scenario 3: Likewise, if $cov(\Pi^{*+}, \Pi^{*-})_q < 0$ indicates an overall tendency that when the peers' receiving records (Π_q^{*+}) is increasing, the peers' forwarding records (Π_q^{*-}) is

decreasing or vice versa. To summarise it, this indicates the tendency that a peer is a malfunctioning or malicious since it explicitly revealed the characteristics of a misbehaving peer in collaborative routing, i.e., the number of messages received by a peer is far less than the number of messages forward by a peer.

Subsequently, our focus will be geared toward the two presented scenarios. Firstly, scenariour **1.** if $cov(\Pi^{*+}, \Pi^{*-})_q = Var(\Pi_q^-) = Var(\Pi_q^+)$ and secondly, scenariour **2.** i.e if $cov(\Pi^+, \Pi^-)_q > 0$. However, the challenges with the value $cov(\Pi_q^+, \Pi_q^-)$ are that it will be difficult to interpret the exact peer routing behaviour: whether selfish or good behaviour. Also, it will be hard to tell if a particular value of the peer q transaction record $(\Pi^+, \Pi^-)_q$ is "big" or "small", thus aggregating these values might not help much to predict the peers' routing behaviour for trust routing decisions. To overcome this problem, we therefore normalised the covariance by the product of the sum of standard deviations of the transaction records received from other peers as their opinions $(\sum_{i=1}^{n} \Pi_q^{*-}, \sum_{i=1}^{n} \Pi_q^{*+})$ to obtain the correlation between the peers forwarding and receiving records as shown in equation (7.10) below:

$$\rho(\Pi^{*+}, \Pi^{*-})_q = \frac{cov(\Pi^{*+}\Pi^{*-})_q}{\sigma\Pi_q^{*+}\sigma\Pi_q^{*-}}, -1 \leq \rho(\Pi^{*+}\Pi^{*-})_q \leq 1. \tag{7.10}$$

Where $\sigma\Pi^{*+}\sigma\Pi^{*-}$ is the product of standard deviation of the peers' forwarding and receiving records. The value of $\rho(\Pi^{*+}, \Pi^{*-})_q$ will generally increase as the inter correlations among $\sigma\Pi^{*+}$ and $\sigma\Pi^{*-}$ increase, and thus we refer it as internal consistency estimate of the reliability of peers' forwarding ability.

Furthermore, as we described earlier, the solution of our interest are two possible scenarios with the values: $cov(\Pi^{*+}, \Pi^{*-}) > 0$ and when $cov(\Pi^{*+}) = (\Pi^{*-})$. Therefore, for the possible range of the correlation in our proposed system is $0 \leq \rho(\Pi^{*+}\Pi^{*-})_q \leq 1$. Subsequently, we define the following rules in table 7.1 for describing the internal consistency of the peers forwarding and receiving records.

Table 7.1: Peers Correlation Forwarding Rules Table

Peers forwarding threshold	**Expected peers routing behaviour**
$\rho(\Pi^{*+}, \Pi^{*-}) \geq 0.9$	Excellent behaving peer
$0.9 > \rho(\Pi^{*+}, \Pi^{*-}) \geq 0.8$	Good behaving peer
$0.8 > \rho(\Pi^{*+}, \Pi^{*-}) \geq 0.7$	Acceptable
$0.7 > \rho(\Pi^{*+}, \Pi^{*-}) \geq 0.6$	Questionable
$0.6 > \rho(\Pi^{*+}, \Pi^{*-}) \geq 0.5$	Poor behaving peer
$\rho(\Pi^{*+}, \Pi^{*-}) < 0.5$	*Unacceptable*

Therefore, the global trust evaluation between the peers can be presented in equation (7.11).

$$T_{p,q} = \rho(\Pi^{*+}\Pi^{*-})_q + (1 - \rho(\Pi^{*+}\Pi^{*-})_q * t_{p,q} * \gamma^x \tag{7.11}$$

Where $t_{p,q}$ represents the local trust value computed in equation (7.2).

7.2.4 *Forward-Watcher:* Protocol Description

Forward-Watchers' trust protocol execution in dynamic topology is simplified in the flow chart presented in Figure 7.3. Initially, when two peers meet, they can exchange their delivery predictability which can enable a message carrier to evaluate the relay peers' probability of meeting the message destination. When a new peer joins the network, it can establish its initial trust through the exchange of its attributes with encountering peers. The members can then assign an initial trust value to the new arrival peer $init = S_{p,q}$ (please refer to chapter Five to see the attributes' similarity used). The subsequent local trust value of a peer can then be updated based on peers' routing history and delivery predictability with the messages' destination. The process of trust aggregation in the middle of Figure 7.3 is evaluated depending on the ability of a peer to forward the message within the interval $[t, t + \delta t]$.

The global trust evaluation using Forward-Watcher scheme can be achieved using equation (7.11) as depicted in the global trust evaluation and optimisation phase in Figure 7.3. Consequently, aggregating the opinion of other peers about the target peer

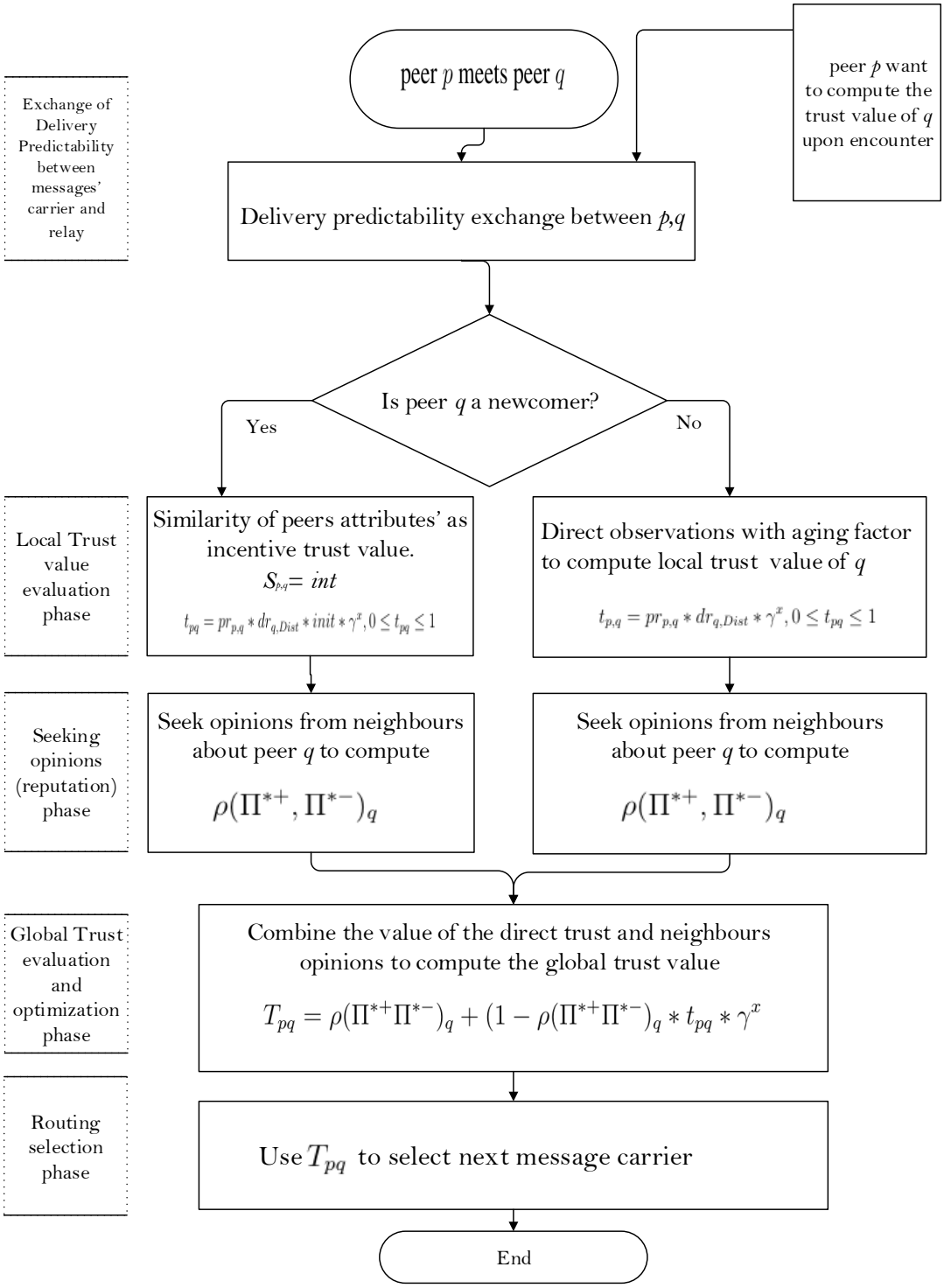


Figure 7.3: A Flowchart of *Forward-Watcher* Protocol Execution

Algorithm 5 GLOBAL TRUST FORWARD-WATCHER TRUST Algorithm

Input: $\rho(\Pi^{*+}\Pi^{*-}), dr_{q,Dist}S_{p,q}, \delta$
Output: $T_{p,q}$
while *peer p is a message holder,* **do**
  Get $\rho(\Pi^{*+}\Pi^{*-})_q$;
  Get $dr_{q,Dist}$

  if *q is a newcomer* **then**
    Get $S_{p,q} = init = t^0_{p,q}$;
  end
  Get $t_{p,q}$;
  for *every peer q, p's neighbour,* **do**
    if $\rho(\Pi^{*+}\Pi^{*-})_q \geqslant \delta, \forall q \in G : q$ *is p's neighbour* **then**
      $T_{p,q} = \rho(\Pi^{*+}\Pi^{*-})_q + (1 - \rho(\Pi^{*+}\Pi^{*-})_q t_{p,q} * \gamma^x$
    end
    do nothing and move to the next peer
  end
  Rank $T_{p,q}$;
  return $Max\ T_{p,q}$;
end

requires a peer to posses two vectors that contain the elements of the target peer forwarding and receiving potentials (Π^{*-}, Π^{*+}). This is to enable a peer to understand other peers' routing patterns based on the predictive relationship that can be exploited in practice between forwarding and receiving records of peers.

7.2.5 Managing Trust Data

The trust data for peers' trust evaluations of each peer are stored in a distributed manner as used in [239]. Each peer has a small database that stores the vectors of the received and forwarding records of its potential routing partners. Figure 7.4 illustrates the forward-watcher trust data management; which involve no central database. Therefore the data that is needed to compute the trust value of the peers are distributively stored and managed by the peers across the network.

The trust database perform three main functions: firstly, it is responsible for submitting the peers' routing record whenever requested by other peers so that other peers will receive such information for computing the global trust of a target; secondly, it is responsible for the evaluation of the peers' trustworthiness based on the received values of (Π_q^{*+} and Π_q^{*-}); thirdly, it store the target peers' routing behaviour and peers' state. Therefore the peers' trust evaluation is a dynamic process.

For the message overhearing among peers in the implementation phase, we create a simple **count_forward_module** that keep on updating every peer whenever its subjects receive and forward the messages. This is to complement the efforts of each peer to overhear the messages forwarded since the overhearing ability is not directly supported in the simulator we used in carrying out this study.

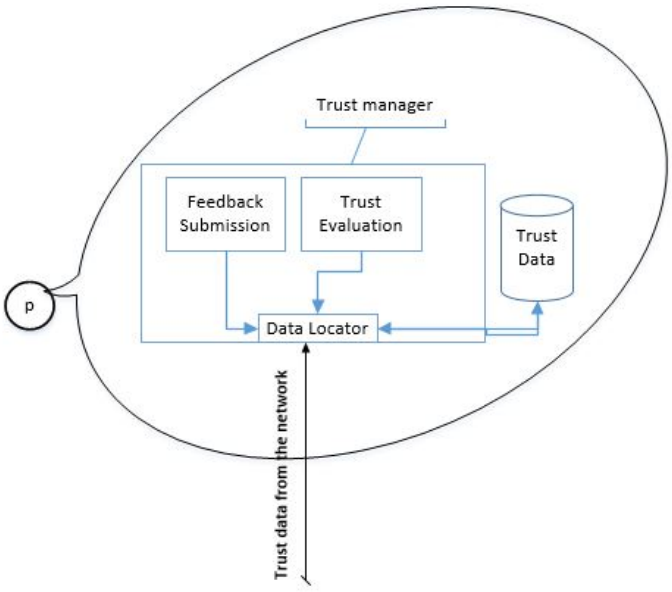


Figure 7.4: Trust Data Management Illustration

Therefore, each peer is supposed to have an up-to-date routing history (forwarding

and receiving potentials) of its subjects with the aid of count_forward_module and exchange of peers' delivery predictability. At this stage, one of the interesting questions is: should a peer maintain the global peers' routing record of every peer it meets? Here, we assert that having the peers' routing history of a dynamic subset of the peers is sufficient to quickly converge to the correct expectation for the peers' to predict the routing patterns of their subjects.

7.3 Formalizing Routing Protocol and Experiments

We assume interpersonal communication with all the peers in the network using a speed of 250kBPS for data forwarding. Furthermore, we use a mobility model based on the connectivity characteristics of a network of DTN2 peers, the mobility in this model is a random way point model [240]. Thus, peers can select a destination and move with a speed of maximum of 0.5 m/s on average(pedestrian). When a peer reaches the destination, it will then stop and select another destination.

To make a forwarding decision, a sender must have its neighbouring peers' forwarding and receiving history. Therefore, the peers' routing history exchange between the peers is necessary. When two peers meet, they exchange a message containing the IDs and corresponding routing history of the peer which the sender wishes to forward the message to. The sending peer can then use the routing history of the peers for trust evaluation and forward the message to the next peer with required acceptable trust value.

Next, if a peer has a message to forward, and it refused to forwards the message for more than the expected Time To Leave (TTL), there is a less likelihood that it will

forward the message thus minimising the possibility of the corresponding peers to overhear the message forwarding due to the mobility of the devices. We therefore assigned the protocol time scale $\gamma = 0.98$.

7.3.1 The Effect of Forwarding Threshold

Firstly, we are interested to see how the consistency between the peers' forwarding and receiving abilities will affect the network performance regarding message delivery. Therefore, we studied the impact of different forwarding thresholds of our proposed system. We designed a scenario in which a peer can forward a message to the relaying peers based on the six different possible values of the peer forwarding correlation rules as presented in 7.1. We simulated six different scenarios based on the possible ranges of $(\rho(\Pi^{*+}\Pi^{*-}))$ which we considered as the forwarding thresholds. We created four different groups of 40 peers in the network making a total of 160 non-collusive peers (with no attacking peers). Each peer can randomly create a message within the interval of 25 to 35 seconds and forward it to the next neighbouring peer based on the concept of Forward-Watcher as presented earlier.

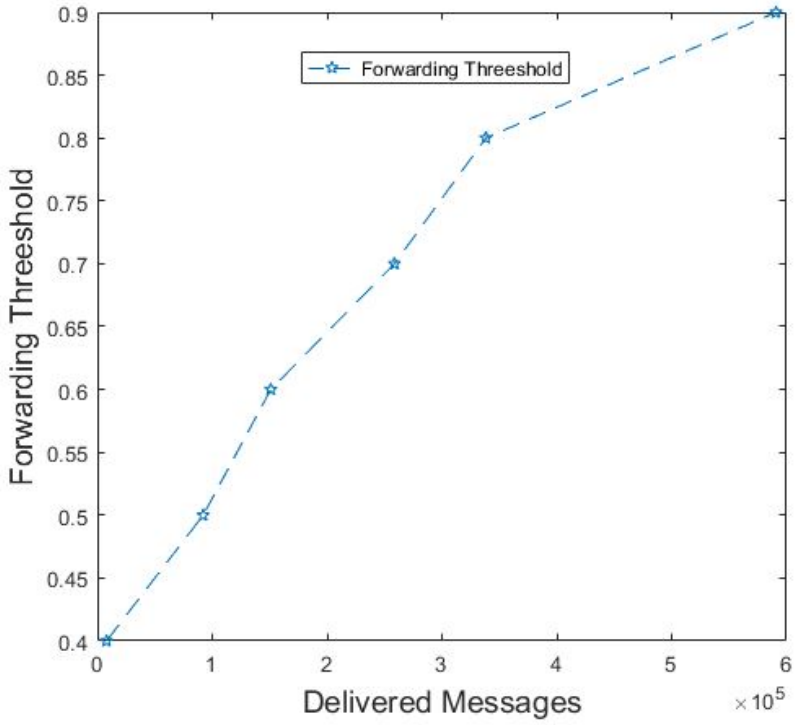


Figure 7.5: Forwarding *threshold* With Number of Messages Delivered

In each scenario, a peer can forward the data packet to the relaying peers with the possible forwarding thresholds of *Unacceptable, poor, Questionable, Acceptable, Good and Excellent behaving thresholds* as presented in table 7.1 . The graph of Figure 7.5 shows the number of messages delivered when we used different forwarding thresholds. As expected, the graph shows that the forwarding threshold had a substantial influence in determining the number of messages successfully delivered. A lower forwarding threshold limits the transfer of the message to the highly trusted peer, in that case, fewer messages were delivered. We also see that when the forwarding threshold is higher, we got a higher number of messages successfully delivered to the destinations. Thus, from the graph, we see that our proposed system is sensitive to the forwarding threshold of $\rho(\Pi^{*+}, \Pi^{*-}) \geq 0.9$ which is considered as the "excellent behaving peer" thresholds.

7.3.2 Security Evaluation of Forward-Watcher Protocol

In this section, we present the security evaluation of Forward-Watcher in a broader context. We then compare its performance with some well-known routing protocols: Spray and Wait(SnW) with six message copies and the PRoPHET routing protocol with the transitive parameter ($\beta = 0.25$).

The PRoPHET protocol uses peers' encounters history and transitivity to calculate the peers' probability of delivering messages to the destination while in the SnW the messages carrier initially spreads L messages' copies (six copies in our simulation scenarios) to L distinct "relays". If the messages' destination is not found in the spraying phase, each relaying peer carrying the message can then forward the message to the destination.

As in the case of many trust-based routing protocols, the evaluating peer computes the trust values of its subjects and determines the possible good behaving peer for data forwarding strategy. Thus, we consider two groups of peers: honest peers and malicious peers. For the honest peers, we consider the peers who actively participate in the routing process and perform the routing functions as expected. They do not drop messages for malicious behaviour nor do they create a flooding message. While for the malicious peers, we consider two different categories of malicious peers in trust-based collaborative routing: forms of Denial of Service Attacks (DoS attacks) that are common for many trust and reputation management system.

In the first category, the peers (malicious) are supposed to relay the packets, but instead, they discard the packets (Black hole peers). The second category of malicious peers is peers that can actively participate in the forwarding process, but instead of them forwarding the messages they receive, they forward fake messages (a bigger message to flood the receiving peers' resources).

Table 7.2: Network Parameters

Parameter	**Good peers**	**Black hole peers**	**Data flooding peers**
Number of peers	437,414,391,368,278	23, 46,69,92,184	23, 46,69,92,184
speed	0.5m/s	0.5m/s	0.5m/s
Movement	Random Way Mobility	Random Way Mobility	Random Way Mobility
Buffer capacity	100MB	0.2MB	100MB
Message sizes	500kb-1MB	Nil	5000KB
Simulation Time	24 Hrs	24 Hrs	24 Hrs

Table 7.2 presents the simulation parameters. We created five different scenarios with 460 total number of peers. We assigned the percentage of malicious peers to be 5%,10%,15%, 20% and 40%. All the honest peers have a similar buffer size of 100Mb while the malicious peers behave in two ways as follows:

- Black hole attack: We create a scenario in which the attacking peers neither create a message nor do they relay the messages. When ever, a black hole peer receives a message, it will simply discard it. We achieve this by assigning all the black holes peers a buffer size of 0.2MB. Meaning they cannot handle any messages from other peers due to its limited capacity. Thus the black hole peers effectively end the communication of all the messages they receive.

- A data flooding attacker: an attacking peer executes the correct Forward-Watcher protocol, but creates a message of larger size with the intention of overloading the honest peers' buffer size. We achieved this by configuring the malicious peers (data flooding peers). A flooding message is a message of size 5000KB instead of a normal message size of 500KB. This is to flood the buffer size of the peer's buffer thereby causing the network to be congested.

In the next experiment, we seek to evaluate the robustness and effectiveness of our proposed system against Blackhole attacks and data flooding attacks. In all the simulations, we see an obvious improvement in the delivery ratio, overhead and the

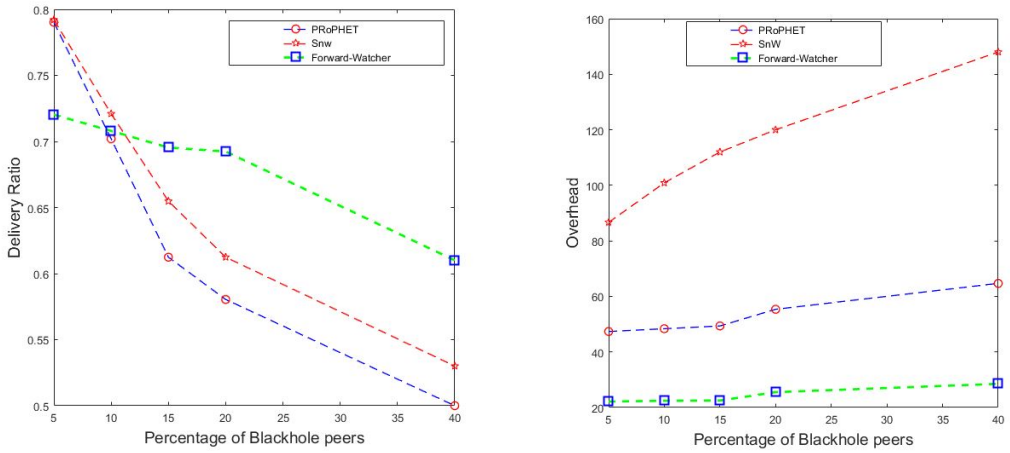
average latency between the Foward-Watcher and a network using a forwarding strategy for the the SnW and PRoPHET routing protocols.

Looking at Figures 7.6 and 7.8, first, when the percentage of malicious peers are 5%, we observe that the performance of SwN has a significantly smaller delivery ratio but higher than that of PRoPHET and Forward-Watcher. This might be due to the SwN settings in our scenario, that for every message originating at a source, the peers create six copies of the message and spread them across the network which can be received by the six relays. Also, if the messages' destination is not found in the spraying phase, the relay peers can perform a direct transmission to the destination. Thus, the possibility of having multiple relays which can forward the messages to the destination can make it achieve a higher delivery ratio in comparison with PRoPHET and Forward-Watcher protocols.

For the PRoPHET protocol, whenever there is an opportunistic encounter between the peers, the peers can exchange any bundles with the encountered peers that the peers dont already have. Therefore, if all goes well, meaning no malicious peers in the network (non-collusive network), the result of the PRoPHET, the peers can find the optimum path for forwarding the messages. The experiments proceed by repeatedly increasing the percentage of both blackhole data flooding attacking peers in the simulation runs. With the increasing percentage of attacking peers, the delivery ratio of all the protocols decreases. It can be noticed that the results of the simulation studies revealed the detection accuracy of the proposed Forward-Watcher with increasing the number of attacking peers. From the presented result in both Figures 7.6 and 7.8, we found the following: There is a sharp decrease of the delivery ratio in the case of SwN and PRoPHET and Forward-Watcher. This is however possible since, with the increase of malicious peers, the number of drop messages will increase causing the decrease in the

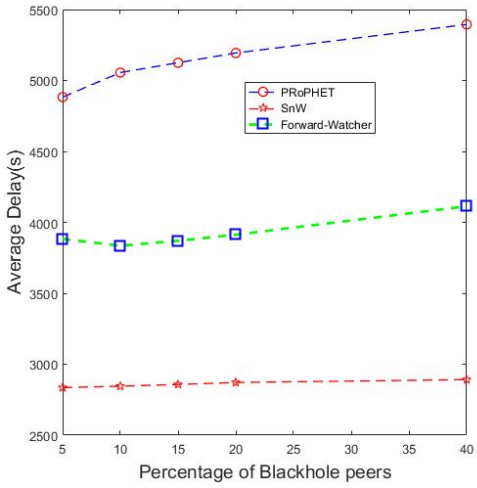
performance of the protocols.

Although the increase of attacking peers affects the Forward-Watcher as well, as can be seen from the results, the effect is not significant in comparison with two protocols (SwN and PRoPHET). This might be because our proposed system can identify the malicious peer who either drops packets or forwards flooding packets. Subsequently, the trust level of attacking peers would tend to decrease, which by extension can cause other peers to remove the attacking peers from their forwarding tables and eventually no traffic will flow to the attacking peers. On the other hand, the good behaving peers enjoy the increase in their trust value due to the higher positive correlation between their forwarding and receiving potentials.



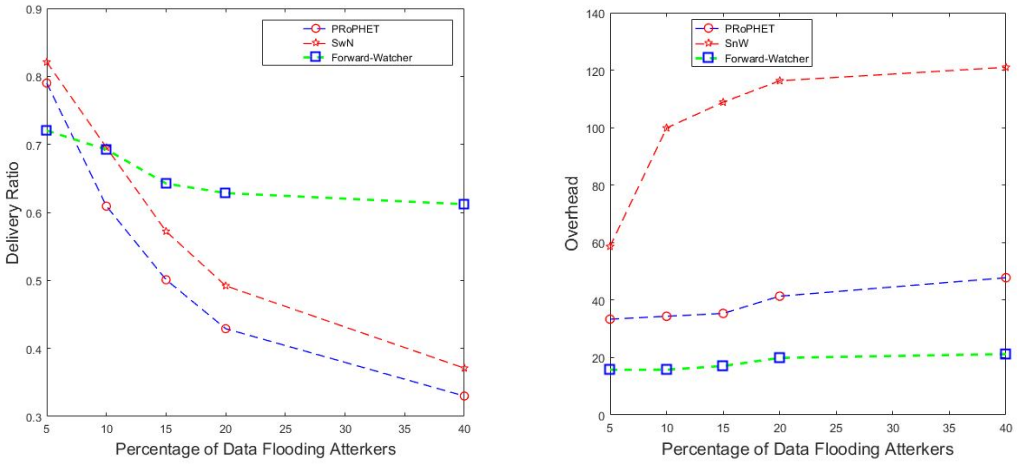
(a) Delivery Ratio Scenariou (b) Overhead

Figure 7.6: Security Evaluation of Forward-Watcher:Blackhole Attacks



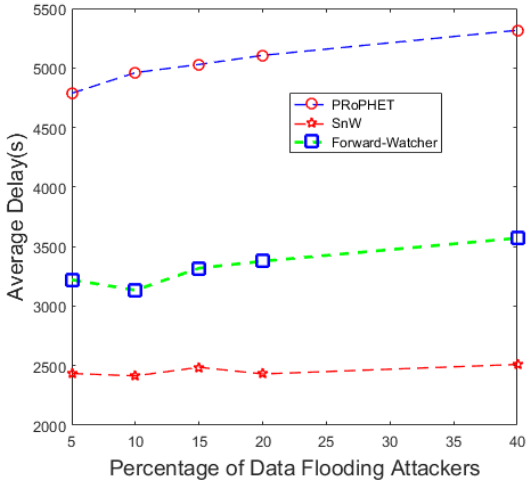
(a) Average Delay

Figure 7.7: Security Evaluation of Forward-Watcher:Blackhole Attacks



(a) Delivery Ratio (b) Overhead

Figure 7.8: Security Evaluation of Forward-Watcher:Data Flooding Attacks



(a) Average Delay

Figure 7.9: Security Evaluation of Forward-Watcher:Data Flooding Attacks

Figures 7.6b,7.7 and 7.8 b, 7.9 compare the overhead and the delay generated by our proposed protocol against the PRoPHET and SnW protocols. The results show that Forward-Watcher could effectively trade off average message latency for a significant gain in overhead with SwN. In particular, Forward-Watcher and PRoPHETs' protocols performance is lower regarding average delay in comparison with SwN with an increasing number of malicious peers. The SnW protocol exhibits less average delay compared to Forward-Watcher and PRoPHET. This may have been due to the multiple message copies (six copies) generated by the peers in the network, making it possible for the messages to successfully reach the destination with less delay.

Moreover, in terms of the messages' overhead, the Forward-Watcher performance is better. This is possible since using a Forward-Watcher, the peers can optimally select message carriers who can successfully deliver the messages to their correct destinations, thus reducing the excessive number of message copies in the network.

Here we note that there is a trade-off between average message delay and overhead between SwN and Forward-Watcher. Also, it can be noticed that in a Forward-Watcher

protocol, when the percentage of malicious peers increases, there is a slight increase in messages' average delay. This is also possible since the increase in malicious peers can lead the message carriers to spend more time searching the appropriate peers with higher trust values to relay the message to.

Another trade-off is about randomly forwarding messages without collecting network information for forwarding decisions and collecting network information for next peers selection. SwN spreads the message copies blindly to the network regardless of the trust values of the peers or the probability of the relay peers meeting the destination. Thus, peers do not exchange information before forwarding the messages which can lead to minimal delay and less average latency. On the other hand, the Forward-Watcher and PRoPHET protocols require peers to exchange information from the network, thus increasing the messages' average delay.

The exchange of peer reputations in Forward-Watcher is not laborious in comparison with that of PRoPHET protocol. This is because the peer reputation values in Forward-Watcher are accumulative; meaning the peers' reputation is incrementing if a peer behaves well and decrementing otherwise. Thus, a peer can enjoy the reputation it builds, as long as it is greater than or equal to the threshold. This may require peers to spend less effort in evaluating a peers' trustfulness and lead to less average delay; whereas in the PRoPHET protocol, each time peers meet, they need to exchange network information before forwarding the message, which perhaps might be the reason why the PRoPHET protocol average delay is higher in comparison with the Forward-Watchers'.

7.4 Chapter Summary

The presented Forward-Watcher scheme uses a peers' receiving and forwarding potential to predict healthiness and trust level of peers for data forwarding in a collaborative

routing scheme. We achieved this based on the justification that when a peer receives a message from its neighbours, its ability to forward the message on time to the next neighbour or to the destination can increase its trust level. If, however, a peer did not forward its received message on time, its trust level will be decremented, thus decreasing its chances to receive messages subsequently from the peers.

In this chapter, the result confirms that the trust scheme is an important feature in a wireless P2P transaction for peers to vanquish the effect of malicious peers. The result also shows how our proposed trust scheme is resistant to Blackhole and data flooding attacks which are forms of denial of service attacks. In our network model, the routing protocol is on-demand which means every peer has knowledge about its immediate neighbour for direct trust evaluation. Thus, the peers can use the routing information of their neighbours to mitigate the problem of malicious peers.

Worthy of consideration is that the increase of malicious peers in the network equipped with the Forward-Watcher trust scheme causes a depletion in the possible hop counts between sources and destination. This is because peers can only rely on the remaining number of trusted peers to store, carry and forward the data packets. Therefore, as the percentage of trusted peers reduces, only the messages that travel fewer hops (closer to one) are delivered since a Forward-Watcher has a mechanism of only selecting well-behaved peers as forwarders. Therefore, the increase of malicious peers causes an increase in average latency since the messages with small latency values are dropped more and more with an increase of malicious peers. Also, in the particular case of limitation of trust and reputation models in trust-based collaborative routing, we provide an alternative to the pre-trusted peers.

As we described earlier, the initial trust (*init*) which serves as the initial default reputation that was given to all or some of the peers in the network, is necessary for the

implementation of many trust algorithms. One of the key premises in the decision to include pre-trusted peers in trust evaluation was that the first few peers to join a network are often known to be trustworthy [241]. However, one might reasonably argue, that the notion of having pre-trusted peers that remain trustworthy throughout the course of their membership in the network is not reasonable. This has also been criticized by related studies [242, 241]. Subsequently, getting rid of pre-trusted peers entirely is desirable in trust-based routing. However, something must take the initial trust values' place since it is a requisite component of trust computation as previously described. From the presented routing protocol presented earlier, we have shown that in the event a peer is a new arriving peer in the network, the peers' attributes' similarity can be evaluated as an initial trust value of a peer (*init*). Therefore, the $S_{p,q}$ complements the initial trust value *init* in our proposed Forward-Watcher. Therefore even without prior trust value between the peers (e.g., a new comer in a network or a mobile environment), a peer can still build its reputation based on its attributes using the function.

Chapter 8

Conclusions and Future Work

8.1 Conclusions

The primary purpose of the study presented in this thesis was to explore trust and reputation routing problems in collaborative mobile wireless networks, and to suggest an alternative approach for improving the design of trust-based routing protocols. In this study, we developed efficient routing decision strategies to provide efficient, secure and higher quality communication between wireless mobile devices. Different from previous trust-based routing protocols in the literature, which mostly focus on the routing behaviour of the peers in trust evaluations, one of the most useful findings from this study is the notion of integrating a peers' attributes, resources and connectivity as additional trust evaluation elements. This study posited factors that influenced the reliability of the peers as additional information for peer trust evaluations. The result of this study has confirmed that a peers' attributes such as buffer sizes and transitive connectivity are important elements for trust evaluation in a network with intermittent connectivity between peers. It also suggested that the proposed Forward-Watcher approach of aggregating the peers' forwarding and receiving records provides additional benefits of limiting the effects of Blackhole and data flooding attacks, and improve mobile wireless network routing performance. Multiple evaluation methods

such as analytical modelling and simulation, empirical data analysis, theoretical analysis and comparison with other existing solutions were used to support this study. The schemes proposed in this study are summarised as follows:

To place our contributions in the context of related works, we presented in Chapter Two, the literature studies and identified challenges related to the interest of this research and our proposed schemes. Like many disciplines, the concept of trust and reputation models in computer science have developed its lexicon, partially inherited from the social sciences. Thus, in Chapter Two, we present some trust theoretic notions for our discussion about the original context of trust between agents from the social science perspective. In that regard, we present different sociological concepts of trust management, including the notion of closed structure, which further leads our discussion to the idea of reciprocity and transitivity. The chapter also presents the features of self-cooperation, self-organization and self-control mechanisms for the design of an efficient trust-based collaborative routing strategy between mobile wireless networks. Given the importance of the research design in the choice of research instruments, in Chapter Three we presented a discussion of the research design and methodology approach best suited to examine the questions of this study. The chapter presents a justification of each step, methods and tools used in conducting this study. The chapter also presents the high-level diagrams and iterative processes involved in conducting this study and how our proposed concepts were integrated and implemented into Opportunistic Network Environment Simulator (ONE) evaluation and performance analysis. To answer the first research question of this study, we sought to understand which category of the wireless peers' connectivity (contacts) could facilitate effective trust evaluation between peers for collaborative routing decisions in wireless mobile networks. In this regard, we identified the properties of complex networks and their impact on

trust, reputation propagation and evaluations. Based on the study in Chapter Four, we understood that the higher the transitive connectivity coefficient between the peers, the faster the peers managed to locate the benevolent peer in the network with less amount of energy spent. The finding in Chapter Four suggests that the transitive contacts between the peers can be a metrics element of a trust-based routing protocol forwarding strategy. Further, the finding of Chapter Four suggests that we can assume that the transitivity scaling factor can equally be applied in the design of trust-based routing protocols for the intermittent network for efficient trust propagation and evaluation. The study of Chapter Four suggests that the first research question of this study was answered. Thus, the first hypothesis of this study proved to be right.

The second question of this study seek to address how to build a dynamic trust model that takes into account the dynamic changes of peers' routing attributes for efficient trust evaluations. To answer this question, in Chapter Five we proposed a Dynamic Attributes Trust Model for Efficient Collaborative Routing (DATM): a trust-based scheme to enforce collaborative behaviour in wireless mobile networks taking into consideration the peers' attributes for an efficient routing scheme. DATM is a generic mechanism that can be integrated into any packet forwarding strategy, or network management function to enable peers in the network identify reliable, trustworthy peers for routing handling. Our proposed contributions in DATM include: i) the introduction of the notion of quantifying peers' routing attributes (buffer) as a scaling factor for trust evaluation between peers; ii) the introduction of generalised peers' personalised similarity model for trust and reputation evaluation and iii) a generalised trust model that evaluates peers' forwarding ability and peers' attributes for trust evaluation. The results of the DATM evaluation suggest that peers' buffer occupancy is likely to be a key feature for understanding peers' reliability in routing handling. One possible implication of DATM

is that the protocol designers can focus their design on exploring different attributes and properties of the dynamic mobile network (e.g., peers' energy level, spatial distribution and intermittent connectivity, etc.), and include these properties in the routing decision process. The finding in Chapter Five also suggests that the second research questions were addressed. Subsequently, Chapter Five of this thesis proved the second hypothesis of this study which says in a trust-based routing protocol, the peers' trust evaluation can be extended to the peers' routing attributes to incorporate the dynamic changes of peers' routing conditions for improving the quality of wireless peers' communications.

Inspired by the study in Chapter Four, we realised that the ability of the peers to forward the data to the correct destination was not limited to the potentiality of the message carrier having a direct contact with the message destination in a mobile wireless network. It could be extended to integrate a transitive connectivity between the peers. For example, in the event where the message carrier is not in direct contact or interfaced with the message destination, the message forwarding can be based on a chain of referral (number of possible hop counts between the message carrier and the message destination). In this situation, exploring the suitable connectivity or possible contacts with the message destination that can facilitate the successful message delivery to the destination, is essential.

Chapter Six of this thesis attempted to test the third hypothesis of this study: that the relative comparisons of the proliferation of peers' transitive connectivity can give a meaningful basis for determining a good relaying peer to forward packets toward the destination with less effort. Subsequently, the chapter attempts to answer the third research question of this thesis: how can the peers' contacts and connectivity in wireless networks be leveraged for the design of efficient trust-based routing protocol?

In this regard, we analytically explored the existence of transitive connectivity between

peers in Mobile Social Networks (MSNs) based on the derivation of connectivity traces from the real WLANs data sets. The study in Chapter Six provides significant empirical evidence that a similar pattern of transitive contacts/connectivity exists in the real data of MSNs. Based on the identified transitive connectivity properties from the traces, we then proposed a new transitive data forwarding strategy which considers the similarity of transitive connectivity between peers for data forwarding strategies. Our proposed transitive forwarding strategy gives preference to peers with increasing transitive connectivity similarity to the messages' destination to improve the chances of message carriers to deliver the message to the correct destination. Thus, through simulation studies, analytical and theoretical analysis, we showed that the transitive contact opportunities between the peers can increase the routing performance of wireless devices. The presented approach in Chapter Six suggests a new perspective in trust-based routing model studies and a new way of interpreting peer connectivity and offers insight into how it can be construed as additional information for the development of a trust-based routing protocol. Thus, the finding of Chapter Six proved the third hypothesis of this study to be right and subsequently answered the third question of this study.

Finally, the fourth question of this research asked how can the peers in wireless mobile networks learn the routing patterns of their potential routing partners to understand a peers' forwarding and receiving ability for trust-based routing protocol design?

In chapter seven, we proposed *forward-watcher* trust evaluation scheme: a statistical approach to learning peers' routing patterns based on encounter/proximity between wireless peers for proffer trust evaluation in collaborative routing. We presented a scheme where peers can dynamically understand the changes of their subjects' routing

patterns and behaviour to enforce cooperation among peers. In that regard, we introduced four important metrics for peer trustworthiness evaluation that are linked to learning a peers' routing history based on messages (packets' beacons) overhearing for trust evaluation between peers. We also introduced a model for evaluating the probability of peers' forwarding and receiving potentials for local trust evaluations based on peers' forwarding and receiving potentials. The chapter also introduced the correlation matrix for evaluating peers' global trust values. Then we leveraged our presented attributes' similarity analytical model proposed in Chapter Five, and the transitivity contact model presented in Chapter Six for attribute and transitivity analysis.

The advantage of the proposed Forward-Watcher approach is that through routing history created by peers, they can statistically predict the future behaviour of their corresponding routing partners. The concept can also serve as a cornerstone for developing self-cooperative protocols in wireless mobile networks using statistical analysis and correlation matrices. The results of Chapter Six validated the fourth hypothesis of this study; that through properly distributed network observations, routing listening and gathering statistics of routing history efficiently, peers' routing performance can be enhanced by making better routing decisions, and thus improve network performance.

8.2 Limitation of the Study

The generalizability of this study is subject to certain limitations. For example, the present study considers only the forwarding decision mechanisms between wireless mobile devices that enable peers to select a message carrier between multiple neighbours. Therefore, the entire process of building routing protocols such as routing metrics and routing table design, flow control, the MAC layer and Logical Link Control (LLC), data representation and encryption, etc., were not addressed in this thesis. Secondly, despite

the exploratory nature of this study, the development, deployment and the evaluation of the current study is limited to the use of analytical modelling, simulation and empirical data analysis. Notwithstanding this, the study suggested possible means of incorporating the findings into real life wireless mobile networks and where the proposed solutions can significantly be applied.

Another limitation of this study is that all the presented forwarding strategies proposed in this thesis are limited to the wireless mobile networks (e.g., mobile social networks) where the contacts between the peers are predictable.

8.3 Future Directions

Many interesting directions are worth further explorations in this study. We identified the following broad directions as future works of this research.

- Implementation and Deployment in Mobile Wireless Networks: One of the interesting future milestones of this research is the deployment of the proposed routing forwarding strategies in real-life environments. This can be possible through deploying the schemes in real-life opportunistic environments; mobile adhoc networks or wireless sensor networks that have characteristics of intermittent connectivity, frequent network disruptions and limited resources. Other possible applications where the proposed schemes can be more useful include secure and reliable in-network collaborative communication schemes for advanced metering infrastructure in a smart grid, a collaborative routing for wireless multi-hop networks with directional antennas and a Collaborative Driving Support System in Mobile Pervasive Environments. It will be interesting if the proposed schemes in this study can be deployed into those applications.

- Deployment in data dissemination schemes of mobile users: Current user mobility

and Social-Aware Data Dissemination in Opportunistic Mobile Networks protocol extracts users' contact information for efficient routing decisions. However, most of the schemes do not take into consideration the trustfulness and reliability of peers for security and efficiency considerations. Thus, it is recommended that further implementation steps be undertaken to deploy the proposed schemes of this research in the real-life users' mobility environment.

- There are some interesting uncovered areas in the technical aspects of this study, for example, the exchange of trust and reputation data between peers may be affected if the evaluating peer is not frequently having contact with other peers. Thus, there is a need to explore more on how the peers' trust information can be aggregated even without frequent contacts between peers in mobile networks. Also, the basis of assigning an initial trust value to any newly arriving peer in the network needs a further investigation to minimise the effect of attacking peers in the colluding network. Even though we made an attempt to replace the notion of initial trust with similarity of peers' attributes as incentive trust values for the newcomers in Chapter Seven, we still believe there is a need to devise a low-cost mechanism to enable the new peers in the network who have no prior reputation, to join the network. Therefore, the issue of free trusted peers or assigning an initial trust value to the peers is an intriguing one which could be usefully explored in further research.

- Since the strength of the message overhearing scheme depends greatly on channel characteristics such as encryption, noise, fading and signal attenuation, further research would contribute to a fuller understanding and quantify how the Forward-Watcher forwarding scheme (presented in Chapter Seven) reacts to different channel qualities and conditions between peers.

- Although the experiment of the presented study was limited to the use of Opportunistic Network Environment Simulator, Analytical modelling and empirical data analysis in opportunistic networks, the question can be raised: would similar results be obtained if the proposed schemes in this study were replicated in the design of wireless sensor networks? Thus, further research to incorporate a similar design of our proposed schemes in a large sample size of wireless sensor networks would be of value.

- In our presented trust-based schemes, messages are forwarded to peers with higher forwarding metrics (aggregated trust values and peer attributes). One possible set-back of this design is that the peers with higher aggregated trust values can be overloaded and overburdened, which can lead the peers to exhaust their resources (e.g., buffer, battery, etc.). Subsequently, it can lead trustworthy peers in the network to frequently fail in routing handling due to limited resources. In future work, we intend to develop a load balancing mechanism to ensure each trustworthy peer receives relative messages so that the peers'resources can be efficiently managed.

- Another exciting research area where the trust mechanism for the P2P system can be applied is the Distributed Ledger Technology (DLT); a digital system for recording the transaction of assets in which the transactions and their details are recorded in multiple places at the same time. Since the proposed trust-based protocols in this thesis are for heterogeneous and decentralized systems where peers are autonomous and have an intermittent presence, an obvious question may be asked, can the outcomes of this study be applied to different technology like DLT? It interests us to study further to understand how our proposed concepts can be used in the DLT and other P2P systems.

References

[1] M. A. Nowak and K. Sigmund, "Evolution of indirect reciprocity," *Nature*, vol. 437, no. 7063, pp. 1291–1298, 2005. 36, 37

[2] F. G. Mármol and G. M. Pérez, "Trmsim-wsn, trust and reputation models simulator for wireless sensor networks," in *ICC*, 2009. 68, 69, 71, 93

[3] A. Keränen, J. Ott, and T. Kärkkäinen, "The one simulator for dtn protocol evaluation," in *Proceedings of the 2nd international conference on simulation tools and techniques*. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2009, p. 55. 72, 73

[4] S. Kim, J. Han, J. Ha, T. Kim, and D. Han, "Enhancing security and privacy of tor's ecosystem by using trusted execution environments," in *14th USENIX Symposium on Networked Systems Design and Implementation (NSDI 17)*. Boston, MA: USENIX Association,, 2017, (accessed date 08,April, 2018), pp. 145–161. [Online]. Available: https://www.usenix.org/conference/nsdi17/technical-sessions/presentation/kim-seongmin 2

[5] P. Ning, "Samsung knox and enterprise mobile security," in *Proceedings of the 4th ACM Workshop on Security and Privacy in Smartphones & Mobile Devices*. ACM, 2014, pp. 1–1. 2

[6] J. Sen, "A survey on security and privacy protocols for cognitive wireless sensor networks," *arXiv preprint arXiv:1308.0682*, 2013. 2

[7] X. Zhou, Z. Zou, R. Song, Y. Wang, and Z. Yu, "Cooperative caching strategies for mobile peer-to-peer networks: A survey," in *Information Science and Applications (ICISA) 2016*. Springer, 2016, pp. 279–287. 3

[8] A. Malatras, "State-of-the-art survey on p2p overlay networks in pervasive computing environments," *Journal of Network and Computer Applications*, vol. 55, pp. 1–23, 2015. 3, 4

[9] P. Jayachandran and M. Andrews, "Minimizing end-to-end delay in wireless networks using a coordinated edf schedule," in *INFOCOM, 2010 Proceedings IEEE*. IEEE, 2010, pp. 1–9. 3

[10] D. Ye, M. Zhang, and Y. Yang, "A multi-agent framework for packet routing in wireless sensor networks," *Sensors*, vol. 15, no. 5, pp. 10 026–10 047, 2015. 3, 100

[11] P. Jayachandran and M. Andrews, "Minimizing end-to-end delay in wireless networks using a coordinated edf schedule," in *INFOCOM, 2010 Proceedings IEEE*. IEEE, 2010, pp. 1–9. 3

[12] Á. Cuevas, M. Urueña, G. De Veciana, R. Cuevas, and N. Crespi, "Dynamic data-centric storage for long-term storage in wireless sensor and actor networks," *Wireless networks*, vol. 20, no. 1, pp. 141–153, 2014. 3

[13] Y. Sun, H. Luo, and S. K. Das, "A trust-based framework for fault-tolerant data aggregation in wireless multimedia sensor networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 6, pp. 785–797, 2012. 4

[14] H. Hafi and A. Bilami, "Cooperative strategy to secure mobile p2p network," in *Modeling Approaches and Algorithms for Advanced Computer Applications*. Springer, 2013, pp. 145–154. 4

[15] M. Dener, "Security analysis in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2014, 2014. 4

[16] J. Meijuan, W. Huiqiang, F. Guangsheng, and G. Fangfang, "A trust management model for mobile p2p networks based on multiple-fuzzy theory," *International Journal of Multimedia and Ubiquitous Engineering*, vol. 9, no. 12, pp. 85–96, 2014. 4

[17] H. D. Bandara and A. P. Jayasumana, "Collaborative applications over peer-to-peer systems–challenges and solutions," *Peer-to-Peer Networking and Applications*, vol. 6, no. 3, pp. 257–276, 2013. 5

[18] M. NIFOROS, "Blockchain opportunities for private enterprises in emerging markets," International Finance Cooperation, World Bank Group, Tech. Rep., 2017. 6

[19] W. Bank, "Distributed ledger technology (dlt) and blockchain," International Bank for Reconstruction and Development / the World Bank, Tech. Rep., 2017. 6

[20] E. Ronen, A. Shamir, A. O. Weingarten, and C. OFlynn, "Iot goes nuclear: Creating a zigbee chain reaction," in *2017 IEEE Symposium on Security and Privacy (SP)*, May 2017, pp. 195–212. 6

[21] A.-S. K. Pathan, *Security of self-organizing networks: MANET, WSN, WMN, VANET*. CRC press, 2016. 6

[22] S. Kim, W. Ha, J. Seo, S. Han, and M. Kim, "A method of evaluating trust and reputation for online transaction," *Computing and Informatics*, vol. 33, no. 5, pp. 1095–1115, 2015. 6

[23] 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, no. 7, pp. 2096–2114, 2013. 7

[24] A. B. Usman, W. Liu, Q. Bai, and A. Narayanan, "Trust of the same: Rethinking trust and reputation management from a structural homophily perspective," *International Journal of Information Security and Privacy (IJISP)*, vol. 9, no. 2, pp. 13–30, 2015. 7, 140

[25] A. Naseer, *Reputation System Based Trust-Enabled Routing for Wireless Sensor Networks*. INTECH Open Access Publisher, 2012. 8, 55, 99

[26] A. Srinivasan, J. Teitelbaum, J. Wu, M. Cardei, and H. Liang, "Reputation-and-trust-based systems for ad hoc networks," *Algorithms and protocols for wireless and mobile ad hoc networks*, vol. 375, 2009. 8

[27] Y. B. Reddy, "Trust-based approach in wireless sensor networks using an agent to each cluster," *International Journal of Security, Privacy and Trust Management (IJSPTM)*, vol. 1, no. 1, pp. 19–26, 2012. 8

[28] A. B. Usman and J. Gutierrez, "A reliability-based trust model for efficient collaborative routing in wireless networks," in *Proceedings of the 11th International Conference on Queueing Theory and Network Applications*, ser. QTNA '16. New York, NY, USA: ACM, 2016, pp. 15:1–15:7, (accessed date 20/July/2017). [Online]. Available: http://doi.acm.org/10.1145/3016032.3016057 9, 99

[29] Y. Hu, Y. Wu, and H. Wang, "Detection of insider selective forwarding attack based on monitor node and trust mechanism in wsn," *Wireless Sensor Network*, vol. 6, no. 11, p. 237, 2014. 10

[30] M. Apostolaki, A. Zohar, and L. Vanbever, "Hijacking bitcoin: Routing attacks on cryptocurrencies," in *2017 IEEE Symposium on Security and Privacy (SP)*, May 2017, pp. 375–392. 10

[31] 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, no. 10, pp. 1755–1772, 2010. 10

[32] G. Swamynathan, K. C. Almeroth, and B. Y. Zhao, "The design of a reliable reputation system," *Electronic Commerce Research*, vol. 10, no. 3-4, pp. 239–270, 2010. 10

[33] R. Falcone and C. Castelfranchi, "Transitivity in trust a discussed property," 2010. 21

[34] N. Luhmann, "Familiarity, confidence, trust: Problems and alternatives," *Trust: Making and breaking cooperative relations*, vol. 6, pp. 94–107, 2000. 22

[35] W. Raub and V. Buskens, "Theory and empirical research in analytical sociology: The case of cooperation in problematic social situations," *Analyse & Kritik*, vol. 30, no. 2, pp. 689–722, 2008. 22

[36] P. G. Neumann, "Trustworthiness and truthfulness are essential," *Communications of the ACM*, vol. 60, no. 6, pp. 26–28, 2017. 22

[37] A. B. Seligman, "Trust and sociability," *American Journal of Economics and Sociology*, vol. 57, no. 4, pp. 391–404, 1998. 22, 23

[38] M. S. Ferdous, G. Norman, A. Jøsang, and R. Poet, "Mathematical modelling of trust issues in federated identity management," in *IFIP International Conference on Trust Management*. Springer, 2015, pp. 13–29. 22

[39] F. Cerutti, L. M. Kaplan, T. J. Norman, N. Oren, and A. Toniolo, "Subjective logic operators in trust assessment: an empirical study," *Information Systems Frontiers*, vol. 17, no. 4, pp. 743–762, 2015. 22

[40] M. E. Shaw, "Communication networks," *Advances in experimental social psychology*, vol. 1, pp. 111–147, 1964. 23

[41] G. Dong, J. Gao, R. Du, L. Tian, H. E. Stanley, and S. Havlin, "Robustness of network of networks under targeted attack," *Physical Review E*, vol. 87, no. 5, p. 052804, 2013. 23

[42] N. Xu, S. Rangwala, K. K. Chintalapudi, D. Ganesan, A. Broad, R. Govindan, and D. Estrin, "A wireless sensor network for structural monitoring," in *Proceedings of the 2nd international conference on Embedded networked sensor systems*. ACM, 2004, pp. 13–24. 23

[43] M. J. Neely and R. Urgaonkar, "Optimal backpressure routing for wireless networks with multi-receiver diversity," *Ad Hoc Networks*, vol. 7, no. 5, pp. 862–881, 2009. 23

[44] E. M. Daly and M. Haahr, "Social network analysis for information flow in disconnected delay-tolerant manets," *IEEE Transactions on Mobile Computing*, vol. 8, no. 5, pp. 606–621, 2009. 23

[45] R. Andersen, C. Borgs, J. Chayes, U. Feige, A. Flaxman, A. Kalai, V. Mirrokni, and M. Tennenholtz, "Trust-based recommendation systems: an axiomatic approach," in *Proceedings of the 17th international conference on World Wide Web*. ACM, 2008, pp. 199–208. 23

[46] G. Swamynathan, K. C. Almeroth, and B. Y. Zhao, "The design of a reliable reputation system," *Electronic Commerce Research*, vol. 10, no. 3-4, pp. 239–270, 2010. 23

[47] M. Tavakolifard, "On some challenges for online trust and reputation systems," 2012. 23, 66

[48] S. A. Rompf, *Trust and rationality: an integrative framework for trust research.* Springer, 2014. 23, 24

[49] A. Gutscher, "A trust model for an open, decentralized reputation system," in *IFIP International Conference on Trust Management.* Springer, 2007, pp. 285–300. 23, 24

[50] X. Li, "Achieving secure and cooperative wireless networks with trust modeling and game theory," Ph.D. dissertation, PhD Thesis, August, 2009. 24

[51] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decision support systems*, vol. 43, no. 2, pp. 618–644, 2007. 24, 25, 39

[52] A. Naseer, *Reputation System Based Trust-Enabled Routing for Wireless Sensor Networks.* INTECH Open Access Publisher, 2012. 26

[53] P. Michiardi and R. Molva, "Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in *Advanced communications and multimedia security.* Springer, 2002, pp. 107–121. 26, 99

[54] A. Srinivasan, J. Teitelbaum, J. Wu, M. Cardei, and H. Liang, "Reputation-and-trust-based systems for ad hoc networks," *Algorithms and protocols for wireless and mobile ad hoc networks*, vol. 375, 2009. 26

[55] Z. Yan and S. Holtmanns, "Trust modeling and management: from social trust to digital trust," *IGI Global*, pp. 290–323, 2008. 28

[56] R. Bouffanais, *Design and control of swarm dynamics.* Springer, 2016. 29, 82

[57] M. Backes, M. Maffei, and K. Pecina, "A security API for distributed social networks," in *Proceedings of the Network and Distributed System Security Symposium, NDSS 2011, San Diego, California, USA, 6th February - 9th February 2011*, 2011, (accessed date 29/05/2017). [Online]. Available: http://www.isoc.org/isoc/conferences/ndss/11/pdf/1_2.pdf 29

[58] Q. Han, H. Wen, M. Ren, B. Wu, and S. Li, "A topological potential weighted community-based recommendation trust model for p2p networks," *Peer-to-Peer Networking and Applications*, vol. 8, no. 6, pp. 1048–1058, 2015. 29

[59] H. Huang and G. Gartner, "Collaborative filtering based route recommendation for assisting pedestrian wayfinding." 30

[60] H. M. Chipuer and G. M. Pretty, "A review of the sense of community index: Current uses, factor structure, reliability, and further development," *Journal of community psychology*, vol. 27, no. 6, pp. 643–658, 1999. 30

[61] F. Xia, L. Liu, J. Li, J. Ma, and A. V. Vasilakos, "Socially aware networking: A survey," *IEEE Systems Journal*, vol. 9, no. 3, pp. 904–921, 2015. 30, 102

[62] R. S. Burt, "Structural holes and good ideas1," *American journal of sociology*, vol. 110, no. 2, pp. 349–399, 2004. 31

[63] T. Thenmozhi and R. Somasundaram, "Towards modelling a trusted and secured centralised reputation system for vanets," in *Proceedings of the International Conference on Soft Computing Systems*. Springer, 2016, pp. 675–688. 31

[64] A. Tajeddine, A. Kayssi, A. Chehab, I. Elhajj, and W. Itani, "Centera: a centralized trust-based efficient routing protocol with authentication for wireless sensor networks," *Sensors*, vol. 15, no. 2, pp. 3299–3333, 2015. 31

[65] J. S. Coleman, "Social capital in the creation of human capital," *American journal of sociology*, pp. S95–S120, 1988. 31, 32

[66] G. Simmel, *Georg Simmel on individuality and social forms*. University of Chicago Press, 2011. 32

[67] S. L. Engle, "Structural holes and simmelian ties: Exploring social capital, task interdependence, and individual effectiveness," 1999. 32

[68] T. Antal, P. L. Krapivsky, and S. Redner, "Dynamics of social balance on networks," *Physical Review E*, vol. 72, no. 3, p. 036121, 2005. 33

[69] N. P. Hummon and P. Doreian, "Some dynamics of social balance processes: bringing heider back into balance theory," *Social Networks*, vol. 25, no. 1, pp. 17–49, 2003. 33

[70] A. Jøsang, T. Ažderska, and S. Marsh, "Trust transitivity and conditional belief reasoning," in *IFIP International Conference on Trust Management*. Springer, 2012, pp. 68–83. 34

[71] O. Richters and T. P. Peixoto, "Trust transitivity in social networks," *PloS one*, vol. 6, no. 4, p. e18384, 2011. 34

[72] B. Cialdini Robert, "Influence: The psychology of persuasion (rev. ed.)," *New York: Quill*, 1993. 34

[73] Z. Wang, A. Szolnoki, and M. Perc, "Optimal interdependence between networks for the evolution of cooperation," *Scientific reports*, vol. 3, 2013. 35

[74] L. Akoglu, P. O. V. de Melo, and C. Faloutsos, "Quantifying reciprocity in large weighted communication networks," in *Pacific-Asia Conference on Knowledge Discovery and Data Mining*. Springer, 2012, pp. 85–96. 35

[75] E. Ostrom and J. Walker, *Trust and reciprocity: Interdisciplinary lessons for experimental research*. Russell Sage Foundation, 2003. 35

[76] D. Garlaschelli and M. I. Loffredo, "Patterns of link reciprocity in directed networks," *Physical review letters*, vol. 93, no. 26, p. 268701, 2004. 35

[77] R. Landa, D. Griffin, R. G. Clegg, E. Mykoniati, and M. Rio, "A sybilproof indirect reciprocity mechanism for peer-to-peer networks," in *INFOCOM 2009, IEEE*. IEEE, 2009, pp. 343–351. 35

[78] R. L. Trivers, "The evolution of reciprocal altruism," *Quarterly review of biology*, pp. 35–57, 1971. 35

[79] R. M. Axelrod, *The evolution of cooperation*. Basic books, 2006. 36

[80] B. Keysar, B. A. Converse, J. Wang, and N. Epley, "Reciprocity is not give and take asymmetric reciprocity to positive and negative acts," *Psychological Science*, vol. 19, no. 12, pp. 1280–1286, 2008. 37

[81] E. Elgar, "Handbook on the economics of reciprocity and social enterprise," *Beiträge zur aktuellen Wirtschaftspolitik No*, vol. 2013, p. 16, 2013. 37

[82] K. A. McCabe, S. J. Rassenti, and V. L. Smith, "Game theory and reciprocity in some extensive form experimental games," *Proceedings of the National Academy of Sciences*, vol. 93, no. 23, pp. 13 421–13 428, 1996. 37

[83] T. Squartini, F. Picciolo, F. Ruzzenenti, and D. Garlaschelli, "Reciprocity of weighted networks," *Scientific reports*, vol. 3, 2013. 37

[84] 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*. ACM, 2003, pp. 640–651. 38, 68

[85] W. Fang, C. Zhang, Z. Shi, Q. Zhao, and L. Shan, "Btres: Beta-based trust and reputation evaluation system for wireless sensor networks," *Journal of Network and Computer Applications*, vol. 59, pp. 88–94, 2016. 38

[86] K. K. Fullam and K. S. Barber, "Dynamically learning sources of trust information: experience vs. reputation," in *Proceedings of the 6th international joint conference on Autonomous agents and multiagent systems*. ACM, 2007, p. 164. 38

[87] 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*. ACM, 2003, pp. 640–651. 39

[88] R. Zhou and K. Hwang, "Powertrust: A robust and scalable reputation system for trusted peer-to-peer computing," *IEEE Transactions on parallel and distributed systems*, vol. 18, no. 4, pp. 460–473, 2007. 39, 68

[89] F. G. Mármol and G. M. Pérez, "Trmsim-wsn, trust and reputation models simulator for wireless sensor networks," in *2009 IEEE International Conference on Communications*. IEEE, 2009, pp. 1–5. 39

[90] T. Jiang and J. S. Baras, "Trust evaluation in anarchy: A case study on autonomous networks." in *INFOCOM*, 2006. 39

[91] C. J. Hazard and M. P. Singh, "Intertemporal discount factors as a measure of trustworthiness in electronic commerce," *IEEE Transactions on Knowledge and Data Engineering*, vol. 23, no. 5, pp. 699–712, 2011. 39

[92] E. Aivaloglou, S. Gritzalis, and C. Skianis, "Trust establishment in ad hoc and sensor networks," in *International Workshop on Critical Information Infrastructures Security*. Springer, 2006, pp. 179–194. 39

[93] R. K. Sinha and A. K. Jagannatham, "Gaussian trust and reputation for fading mimo wireless sensor networks," in *Electronics, Computing and Communication Technologies (IEEE CONECCT), 2014 IEEE International Conference on*. IEEE, 2014, pp. 1–6. 39

[94] J. Jiang, G. Han, F. Wang, L. Shu, and M. Guizani, "An efficient distributed trust model for wireless sensor networks," *IEEE transactions on parallel and distributed systems*, vol. 26, no. 5, pp. 1228–1237, 2015. 40

[95] J.-W. Ho, M. Wright, and S. K. Das, "Zonetrust: Fast zone-based node compromise detection and revocation in wireless sensor networks using sequential hypothesis testing," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 4, pp. 494–511, 2012. 40

[96] A. Srinivasan, F. Li, and J. Wu, "A novel cds-based reputation monitoring system for wireless sensor networks," in *2008 The 28th International Conference on Distributed Computing Systems Workshops*. IEEE, 2008, pp. 364–369. 41

[97] T. Luo, S. Chen, G. Xu, and J. Zhou, *Trust-based collective view prediction*. Springer, 2013. 41, 56

[98] Y. Wei, F. R. Yu, and M. Song, "Distributed optimal relay selection in wireless cooperative networks with finite-state markov channels," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 5, pp. 2149–2158, 2010. 41

[99] Y. Wei, F. R. Yu, M. Song, and V. C. Leung, "Energy efficient distributed relay selection in wireless cooperative networks with finite state markov channels," in *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE*. IEEE, 2009, pp. 1–6. 41

[100] Y. Wang and J. Vassileva, "Toward trust and reputation based web service selection: A survey," *International Transactions on Systems Science and Applications*, vol. 3, no. 2, pp. 118–132, 2007. 42

[101] K. Hoffman, D. Zage, and C. Nita-Rotaru, "A survey of attack and defense techniques for reputation systems," *ACM Computing Surveys (CSUR)*, vol. 42, no. 1, p. 1, 2009. 42

[102] 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, no. 10, pp. 1755–1772, 2010. 43

[103] J.-H. Cho, A. Swami, and R. Chen, "A survey on trust management for mobile ad hoc networks," *IEEE Communications Surveys & Tutorials*, vol. 13, no. 4, pp. 562–583, 2011. 43

[104] K. Govindan and P. Mohapatra, "Trust computations and trust dynamics in mobile adhoc networks: a survey," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 2, pp. 279–298, 2012. 43

[105] S. Spitz and Y. Tüchelmann, "A survey of security issues in trust and reputation systems for e-commerce," in *International Conference on Autonomic and Trusted Computing*. Springer, 2011, pp. 203–214. 44

[106] T. Bhuiyan, "Online survey on trust and interest similarity," in *Trust for Intelligent Recommendation*. Springer, 2013, pp. 53–61. 44

[107] W. Sherchan, S. Nepal, and C. Paris, "A survey of trust in social networks," *ACM Computing Surveys (CSUR)*, vol. 45, no. 4, p. 47, 2013. 44

[108] H. Mousa, S. B. Mokhtar, O. Hasan, O. Younes, M. Hadhoud, and L. Brunie, "Trust management and reputation systems in mobile participatory sensing applications: A survey," *Computer Networks*, vol. 90, pp. 49–73, 2015. 44

[109] Y. Wu, Y. Zhao, M. Riguidel, G. Wang, and P. Yi, "Security and trust management in opportunistic networks: a survey," *Security and Communication Networks*, vol. 8, no. 9, pp. 1812–1827, 2015. 44

[110] Y. Sun, H. Luo, and S. K. Das, "A trust-based framework for fault-tolerant data aggregation in wireless multimedia sensor networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 6, pp. 785–797, 2012. 45

[111] N. Li and S. K. Das, "A trust-based framework for data forwarding in opportunistic networks," *Ad Hoc Networks*, vol. 11, no. 4, pp. 1497–1509, 2013. 45, 111

[112] T. Anantvalee and J. Wu, "Reputation-based system for encouraging the cooperation of nodes in mobile ad hoc networks," in *2007 IEEE International Conference on Communications*. IEEE, 2007, pp. 3383–3388. 45, 160

[113] H. Liu, B. Zhang, H. T. Mouftah, X. Shen, and J. Ma, "Opportunistic routing for wireless ad hoc and sensor networks: Present and future directions," *IEEE Communications Magazine*, vol. 47, no. 12, pp. 103–109, 2009. 45, 76, 127

[114] V. Srivastava, J. O. Neel, A. B. MacKenzie, R. Menon, L. A. DaSilva, J. E. Hicks, J. H. Reed, R. P. Gilles *et al.*, "Using game theory to analyze wireless ad hoc networks." *IEEE Communications Surveys and Tutorials*, vol. 7, no. 1-4, pp. 46–56, 2005. 46

[115] V. Jayalakshmi and T. A. Razak, "Trust based power aware secure source routing protocol using fuzzy logic for mobile adhoc networks." *IAENG International Journal of Computer Science*, vol. 23, no. 1, 2016. 46

[116] C. T. Nguyen, O. Camp, and S. Loiseau, "A bayesian network based trust model for improving collaboration in mobile ad hoc networks," in *Research, Innovation and Vision for the Future, 2007 IEEE International Conference on.* IEEE, 2007, pp. 144–151. 46

[117] L. Sun, M. H. Karwan, and C. Kwon, "Incorporating driver behaviors in network design problems: Challenges and opportunities," *Transport Reviews*, vol. 36, no. 4, pp. 454–478, 2016. 46

[118] H. Dai, Z. Jia, and Z. Qin, "Trust evaluation and dynamic routing decision based on fuzzy theory for manets," *Journal of Software*, vol. 4, no. 10, pp. 1091–1101, 2009. 46

[119] G. Zhan, W. Shi, and J. Deng, "Design and implementation of tarf: a trust-aware routing framework for wsns," *Dependable and Secure Computing, IEEE Transactions on*, vol. 9, no. 2, pp. 184–197, 2012. 46

[120] S. Sarkar and R. Datta, "A trust based protocol for energy-efficient routing in self-organized manets," in *India Conference (INDICON), 2012 Annual IEEE.* IEEE, 2012, pp. 1084–1089. 46

[121] T. Zahariadis, H. C. Leligou, P. Trakadas, and S. Voliotis, "Trust management in wireless sensor networks," *European Transactions on Telecommunications*, vol. 21, no. 4, pp. 386–395, 2010. 46

[122] J. Sen, *Reputation-and trust-based systems for wireless self-organizing networks.* Aurbach Publications, CRC Press, USA, 2010. 47

[123] A. Rezgui and M. Eltoweissy, "Tarp: A trust-aware routing protocol for sensor-actuator networks," in *2007 IEEE International Conference on Mobile Adhoc and Sensor Systems.* IEEE, 2007, pp. 1–9. 47

[124] C. Boldrini, M. Conti, and A. Passarella, "Exploiting users social relations to forward data in opportunistic networks: The hibop solution," *Pervasive and Mobile Computing*, vol. 4, no. 5, pp. 633–657, 2008. 47

[125] A. Lindgren, A. Doria, and O. Schelen, "Probabilistic routing in intermittently connected networks," in *Service assurance with partial and intermittent resources.* Springer, 2004, pp. 239–254. 47

[126] W. jen Hsu, D. Dutta, and A. Helmy, "1 csi: A paradigm for behavior-oriented profile-cast services in mobile networks." 47

[127] S. Biswas and R. Morris, "Opportunistic routing in multi-hop wireless networks," *ACM SIGCOMM Computer Communication Review*, vol. 34, no. 1, pp. 69–74, 2004. 48

[128] R. Hou, S. Qu, K.-S. Lui, and J. Li, "Coding- and interference-aware routing protocol in wireless networks," *Computer Communications*, vol. 36, no. 1718, pp. 1745 – 1753, 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0140366413001904 48

[129] R. Ahlswede, N. Cai, S.-Y. Li, and R. W. Yeung, "Network information flow," *IEEE Transactions on information theory*, vol. 46, no. 4, pp. 1204–1216, 2000. 48

[130] M. Y. Mowafi, F. H. Awad, and M. A. Al-Batati, "Opportunistic network coding for real-time transmission over wireless networks," *Network Protocols and Algorithms*, vol. 5, no. 1, pp. 1–19, 2013. 48

[131] A. Gupta and L. K. Awasthi, "Peer-to-peer networks and computation: Current trends and future perspectives," *Computing and Informatics*, vol. 30, no. 3, pp. 559–594, 2012. 49

[132] L. Xin, "Trust beyond reputation: Novel trust mechanisms for distributed environments," Ph.D. dissertation, Nanyang Technological University, 2011. 49

[133] K. Govindan and P. Mohapatra, "Trust computations and trust dynamics in mobile adhoc networks: a survey," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 2, pp. 279–298, 2012. 49

[134] A. Naseer, *Reputation System Based Trust-Enabled Routing for Wireless Sensor Networks*. INTECH Open Access Publisher, 2012. 49

[135] Z. Wei, Y. Xiaoyong, S. Fei, T. Xianghong, and C. Binghua, "Collaborative routing protocol based on hydrodynamics for wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2015, p. 3, 2015. 49

[136] I. Maarouf, U. Baroudi, and A. R. Naseer, "Cautious rating for trust-enabled routing in wireless sensor networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, no. 1, pp. 1–16, 2010. 49, 50

[137] K. Govindan and P. Mohapatra, "Trust computations and trust dynamics in mobile adhoc networks: a survey," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 2, pp. 279–298, 2012. 49

[138] H. Alzaid, M. Alfaraj, S. Ries, A. Jøsang, M. Albabtain, and A. Abuhaimed, "Reputation-based trust systems for wireless sensor networks: A comprehensive review," in *IFIP International Conference on Trust Management*. Springer, 2013, pp. 66–82. 50

[139] G. Zhang, Y. Zhang, and Z. Chen, "Using trust to secure geographic and energy aware routing against multiple attacks," *PloS one*, vol. 8, no. 10, p. e77488, 2013. 50, 167

[140] J.-H. Cho, A. Swami, and R. Chen, "A survey on trust management for mobile ad hoc networks," *IEEE Communications Surveys & Tutorials*, vol. 13, no. 4, pp. 562–583, 2011. 51

[141] T. Eissa, S. A. Razak, R. H. Khokhar, and N. Samian, "Trust-based routing mechanism in manet: design and implementation," *Mobile Networks and Applications*, vol. 18, no. 5, pp. 666–677, 2013. 51

[142] C. Zhang, X. Zhu, Y. Song, and Y. Fang, "A formal study of trust-based routing in wireless ad hoc networks," in *INFOCOM, 2010 Proceedings IEEE*. IEEE, 2010, pp. 1–9. 51

[143] M. Momani and S. Challa, "Survey of trust models in different network domains," *CoRR*, 2010, Date accessed 29/08/2017. 51

[144] G. Swamynathan, K. C. Almeroth, and B. Y. Zhao, "The design of a reliable reputation system," *Electronic Commerce Research*, vol. 10, no. 3-4, pp. 239–270, 2010. 54

[145] R. Andersen, C. Borgs, J. Chayes, U. Feige, A. Flaxman, A. Kalai, V. Mirrokni, and M. Tennenholtz, "Trust-based recommendation systems: an axiomatic approach," in *Proceedings of the 17th international conference on World Wide Web*. ACM, 2008, pp. 199–208. 54

[146] 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, no. 3, pp. 867–880, 2012. 56

[147] J. Zhang, "Trust management for vanets: challenges, desired properties and future directions," *International Journal of Distributed Systems and Technologies (IJDST)*, vol. 3, no. 1, pp. 48–62, 2012. 57

[148] A. C. Kapadia, P. G. Naldurg, and R. H. Campbell, "Routing with confidence: A model for trustworthy communication," 2006. 57

[149] A. Kapoukakis, C. Pappas, G. Androulidakis, and S. Papavassiliou, "Design and assessment of a reputation-based trust framework in wireless testbeds utilizing user experience," in *Ad-hoc, Mobile, and Wireless Network*. Springer, 2013, pp. 1–12. 57

[150] J. F. Nunamaker Jr, M. Chen, and T. D. Purdin, "Systems development in information systems research," *Journal of management information systems*, vol. 7, no. 3, pp. 89–106, 1990. 59, 62, 63

[151] P. Menschner, *A Service Engineering Method for Knowledge-Intense Person-Oriented Services*. kassel university press GmbH, 2015, vol. 4. 59

[152] L. A. Adams and J. F. Courtney, "Achieving relevance in is research via the dags framework," in *System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on*. IEEE, 2004, pp. 10–pp. 59

[153] S. Ponelis, K. Renaud, I. Venter, and R. de la Harpe, "Deploying design science research in graduate computing studies in south africa," 2015. 59

[154] M. Preston and N. Mehandjiev, "A framework for classifying intelligent design theories," in *Proceedings of the 2004 ACM workshop on Interdisciplinary software engineering research*. ACM, 2004, pp. 49–54. 59

[155] A. Fulcher and P. Hills, "Towards a strategic framework for design research," *Journal of Engeering Design*, vol. 7, no. 2, pp. 183–193, 1996. 59

[156] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A design science research methodology for information systems research," *Journal of management information systems*, vol. 24, no. 3, pp. 45–77, 2007. 60

[157] R. H. Von Alan, S. T. March, J. Park, and S. Ram, "Design science in information systems research," *MIS quarterly*, vol. 28, no. 1, pp. 75–105, 2004. 62

[158] G. Goldkuhl, "Design theories in information systems-a need for multi-grounding," *JITTA: Journal of Information Technology Theory and Application*, vol. 6, no. 2, p. 59, 2004. 63

[159] N. Gupta and S. Grover, "Introduction to modeling and simulation," *Int. J. IT, Eng. Appl. Sci. Res*, vol. 2, no. 4, pp. 45–50, 2013. 66

[160] R. Kerr and R. Cohen, "An experimental testbed for evaluation of trust and reputation systems," in *IFIP International Conference on Trust Management*. Springer, 2009, pp. 252–266. 66

[161] E. Winsberg, "Computer simulations in science," 2013. 67

[162] R. Dardashti, K. P. Thébault, and E. Winsberg, "Confirmation via analogue simulation: What dumb holes could tell us about gravity," *The British Journal for the Philosophy of Science*, p. axv010, 2015. 67

[163] I.-R. Chen, F. Bao, M. Chang, and J.-H. Cho, "Dynamic trust management for delay tolerant networks and its application to secure routing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 5, pp. 1200–1210, May 2014. 67

[164] E. Ayday and F. Fekri, "An iterative algorithm for trust management and adversary detection for delay-tolerant networks," *IEEE Transactions on Mobile Computing*, vol. 11, no. 9, pp. 1514–1531, 2012. 67

[165] F. G. Mármol and G. M. Pérez, "Trip, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks," *Journal of Network and Computer Applications*, vol. 35, no. 3, pp. 934–941, 2012. 67, 68

[166] L. Xiong and L. Liu, "Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities," *IEEE transactions on Knowledge and Data Engineering*, vol. 16, no. 7, pp. 843–857, 2004. 68

[167] A. Keränen, T. Kärkkäinen, and J. Ott, "Simulating mobility and dtns with the one," *Journal of Communications*, vol. 5, no. 2, pp. 92–105, 2010. 72

[168] J. Karvo and J. Ott, "Time scales and delay-tolerant routing protocols," in *CHANTS '08: Proceedings of the third ACM workshop on Challenged networks*. New York, NY, USA: ACM, 2008, pp. 33–40. 72

[169] T. Spyropoulos, K. Psounis, and C. S. Raghavendra, "Spray and wait: an efficient routing scheme for intermittently connected mobile networks," in *Proceedings of the 2005 ACM SIGCOMM workshop on Delay-tolerant networking*. ACM, 2005, pp. 252–259. 73

[170] A. Vahdat, D. Becker *et al.*, "Epidemic routing for partially connected ad hoc networks," 2000. 73

[171] B. Lagesse, "Analytical evaluation of p2p reputation systems," *International Journal of Communication Networks and Distributed Systems*, vol. 9, no. 1-2, pp. 82–96, 2012. 75, 79

[172] P. Hui, J. Crowcroft, and E. Yoneki, "Bubble rap: Social-based forwarding in delay-tolerant networks," *IEEE Transactions on Mobile Computing*, vol. 10, no. 11, pp. 1576–1589, 2011. 75, 76, 127, 148, 152

[173] M. De Domenico, A. Lima, and M. Musolesi, "Interdependence and predictability of human mobility and social interactions," *Pervasive and Mobile Computing*, vol. 9, no. 6, pp. 798–807, 2013. 75

[174] W. jen Hsu, D. Dutta, and A. Helmy, "1 csi: A paradigm for behavior-oriented profile-cast services in mobile networks." 75

[175] X. Zhang, "Efficient and quality-aware data access in mobile opportunistic networks," Ph.D. dissertation, The Pennsylvania State University, 2016. 75, 76, 124, 125, 127

[176] W. jen Hsu, D. Dutta, and A. Helmy, "1 csi: A paradigm for behavior-oriented profile-cast services in mobile networks." 76, 124, 125, 127

[177] 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*. ACM, 2007, pp. 32–40. 76, 127

[178] M. Mauve, J. Widmer, and H. Hartenstein, "A survey on position-based routing in mobile ad hoc networks," *IEEE network*, vol. 15, no. 6, pp. 30–39, 2001. 76, 127

[179] D. Kotz, T. Henderson, I. Abyzov, and J. Yeo, "CRAWDAD dataset dartmouth/campus (v. 2009-09-09)," Downloaded from http://crawdad.org/dartmouth/campus/20090909, Sep. 2009. 78, 129

[180] C.-W. Hang and M. P. Singh, "Trust-based recommendation based on graph similarity," in *Proceedings of the 13th International Workshop on Trust in Agent Societies (TRUST). Toronto, Canada*, 2010. 82

[181] C. Chen, J. Zhang, R. Cohen, and P.-H. Ho, "A trust modeling framework for message propagation and evaluation in vanets," in *Information Technology Convergence and Services (ITCS), 2010 2nd International Conference on.* IEEE, 2010, pp. 1–8. 82

[182] S. Maini, "A survey study on reputation-based trust management in p2p networks," *Reputation-based P2P Survey*, vol. 1, 2006. 83

[183] G. Liu, Y. Wang, M. A. Orgun *et al.*, "Trust transitivity in complex social networks." in *AAAI*, vol. 11, 2011, pp. 1222–1229. 84

[184] F. Harary and H. J. Kommel, "Matrix measures for transitivity and balance*," *Journal of Mathematical Sociology*, vol. 6, no. 2, pp. 199–210, 1979. 85

[185] S. Borgatti, M. Everett, and L. Freeman, "Ucinet version 6.123," *Natick: Analytic Technologies*, 2006. 86

[186] T. Schank and D. Wagner, *Approximating clustering-coefficient and transitivity.* Universität Karlsruhe, Fakultät für Informatik, 2004. 86

[187] D. J. Watts and S. H. Strogatz, "Collective dynamics of small-worldnetworks," *nature*, vol. 393, no. 6684, pp. 440–442, 1998. 88

[188] R. Falcone and C. Castelfranchi, "Trust and transitivity: how trust-transfer works," in *Highlights on Practical Applications of Agents and Multi-Agent Systems.* Springer, 2012, pp. 179–187. 88

[189] C. You, T. Wang, B. Zhou, H. Dai, and B. Sun, "A distributed energy-aware trust topology control algorithm for service-oriented wireless mesh networks," in *International Conference in Swarm Intelligence.* Springer, 2010, pp. 276–282. 89

[190] M. J. Williams and M. Musolesi, "Spatio-temporal networks: reachability, centrality and robustness," *Royal Society Open Science*, vol. 3, no. 6, p. 160196, 2016. 90

[191] W. Quattrociocchi, G. Caldarelli, and A. Scala, "Self-healing networks: redundancy and structure," *PloS one*, vol. 9, no. 2, p. e87986, 2014. 90

[192] L. Abusalah, A. Khokhar, and M. Guizani, "A survey of secure mobile ad hoc routing protocols," *IEEE communications surveys & tutorials*, vol. 10, no. 4, pp. 78–93, 2008. 90

[193] C. Demetrescu and G. F. Italiano, "Dynamic shortest paths and transitive closure: Algorithmic techniques and data structures," *Journal of Discrete Algorithms*, vol. 4, no. 3, pp. 353–383, 2006. 91

[194] D. A. Schult and P. Swart, "Exploring network structure, dynamics, and function using networkx," in *Proceedings of the 7th Python in Science Conferences (SciPy 2008)*, vol. 2008, 2008, pp. 11–16. 93

[195] C. Esposito, A. Castiglione, F. Palmieri, and M. Ficco, "Trust management for distributed heterogeneous systems by using linguistic term sets and hierarchies, aggregation operators and mechanism design," *Future Generation Computer Systems*, 2015. 99

[196] D. B. Amin Vahdat, "Epidemic routing for partially-connected ad hoc networks," 2000. 99, 148

[197] F. Mari, I. Melatti, E. Tronci, and A. Finzi, "A multi-hop advertising discovery and delivering protocol for multi administrative domain manet," *Mobile Information Systems*, vol. 9, no. 3, pp. 261–280, 2013. 100

[198] 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, no. 3, pp. 867–880, 2012. 100

[199] D. Jiang, X. Ying, Y. Han, and Z. Lv, "Collaborative multi-hop routing in cognitive wireless networks," *Wireless personal communications*, vol. 86, no. 2, pp. 901–923, 2016. 100

[200] H. C. Tan, M. Ma, H. Labiod, P. H. J. Chong, and J. Zhang, "A non-biased trust model for wireless mesh networks," *International Journal of Communication Systems*, 2016. 100

[201] M. O. Abdalla, T. Nagarajan, and F. M. Hashim, "Analysis of innovative design of energy efficient hydraulic actuators," *Analysis*, vol. 3, no. 1, pp. 001–007, 2013. 100

[202] A. B. Usman and J. Gutierrez, "Datm: a dynamic attribute trust model for efficient collaborative routing," *Annals of Operations Research*, Apr, Date accessed 28/04/2018 2018. [Online]. Available: https://doi.org/10.1007/s10479-018-2864-5 102

[203] C. E. Palazzi and A. Bujari, "Social-aware delay tolerant networking for mobile-to-mobile file sharing," *International Journal of Communication Systems*, vol. 25, no. 10, pp. 1281–1299, 2012. 102

[204] A. Lindgren, A. Doria, and O. Schelen, "Probabilistic routing in intermittently connected networks," in *Service assurance with partial and intermittent resources*. Springer, 2004, pp. 239–254. 103, 109, 116

[205] A. B. Usman and J. Gutierrez, "Trust-based analytical models for secure wireless sensor networks," in *Security and Privacy Management, Techniques, and Protocols*. IGI Global, 2018, pp. 47–65. 106

[206] A. Keränen, J. Ott, and T. Kärkkäinen, "The ONE Simulator for DTN Protocol Evaluation," in *SIMUTools '09: Proceedings of the 2nd International Conference on Simulation Tools and Techniques*. New York, NY, USA: ICST, 2009. 109

[207] R. S. Prasad, C. Dovrolis, and M. Thottan, "Router buffer sizing revisited: the role of the output/input capacity ratio," in *Proceedings of the 2007 ACM CoNEXT conference*. ACM, 2007, p. 15. 111

[208] A. Bello, W. Liu, Q. Bai, and A. Narayanan, "Exploring the role of structural similarity in securing smart metering infrastructure," in *2015 IEEE International Conference on Data Science and Data Intensive Systems*. IEEE, 2015, pp. 343–349. 113

[209] ——, "Revealing the role of topological transitivity in efficient trust and reputation system in smart metering network," in *2015 IEEE International Conference on Data Science and Data Intensive Systems*. IEEE, 2015, pp. 337–342. 116

[210] A. Krifa, C. Barakat, and T. Spyropoulos, "Optimal buffer management policies for delay tolerant networks," in *2008 5th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*. IEEE, 2008, pp. 260–268. 116

[211] D. Maltz, "Dynamic source routing in ad hoc wireless networks," *Mobile Computing*, vol. 353, no. 1, pp. 153–181. 117

[212] Y. Huang, Y. Dong, S. Zhang, and G. Wu, "A centrality estimation method based on hidden markov model in social delay tolerant networks," in *2013 22nd Wireless and Optical Communication Conference*. IEEE, 2013, pp. 333–337. 125

[213] P. Yuan, H. Ma, X.-Y. Li, S. Tang, and X. Mao, "Opportunistic forwarding with partial centrality," *arXiv preprint arXiv:1208.0186*, 2012. 125

[214] B. Bai, Z. Feng, B. Zhao, and J. Su, "Benefiting from the community structure in opportunistic forwarding." *Comput. Sci. Inf. Syst.*, vol. 10, no. 2, pp. 865–876, 2013. 125, 153

[215] Z. Li and H. Shen, "Sedum: Exploiting social networks in utility–based distributed routing for dtns," *IEEE Transactions on Computers*, vol. 62, no. 1, pp. 83–97, 2013. 126

[216] W. Moreira, E. Cerqueira, and P. Mendes, "Opportunistic routing based on users daily life routine," 2014. 127, 149

[217] S. Vasudevan, M. Adler, D. Goeckel, and D. Towsley, "Efficient algorithms for neighbor discovery in wireless networks," *IEEE/ACM Transactions on Networking (TON)*, vol. 21, no. 1, pp. 69–83, 2013. 129

[218] J. Scott, R. Gass, J. Crowcroft, P. Hui, C. Diot, and A. Chaintreau, "Crawdad data set cambridge/haggle/imote/infocom2006," 2009. 130

[219] D. J. Watts and S. H. Strogatz, "Collective dynamics of small-worldnetworks," *nature*, vol. 393, no. 6684, pp. 440–442, 1998. 134

[220] T. Tanimoto, "Internal report: Ibm technical report series," *Armonk, NY: IBM*, 1957. 141

[221] T. M. L. M. De Simas, "Stochastic models and transitivity in complex networks," Ph.D. dissertation, Indiana University, 2012. 141

[222] J. Sathiamoorthy, B. Ramakrishnan *et al.*, "Design of a proficient hybrid protocol for efficient route discovery and secure data transmission in ceaack manets," *Journal of Information Security and Applications*, vol. 36, pp. 43–58, 2017. 158

[223] R. Landa, D. Griffin, R. G. Clegg, E. Mykoniati, and M. Rio, "A sybilproof indirect reciprocity mechanism for peer-to-peer networks," in *INFOCOM 2009, IEEE*. IEEE, 2009, pp. 343–351. 158

[224] P. Mohit, R. Amin, and G. Biswas, "Design of authentication protocol for wireless sensor network-based smart vehicular system," *Vehicular Communications*, vol. 9, pp. 64–71, 2017. 158

[225] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "Vanet security challenges and solutions: A survey," *Vehicular Communications*, 2017. 158

[226] B. B. Chen and M. C. Chan, "Mobicent: a credit-based incentive system for disruption tolerant network," in *INFOCOM, 2010 Proceedings IEEE*. IEEE, 2010, pp. 1–9. 158

[227] L. Buttyan, L. Dora, M. Felegyhazi, and I. Vajda, "Barter-based cooperation in delay-tolerant personal wireless networks," in *2007 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks*. IEEE, 2007, pp. 1–6. 158

[228] M. Y. S. Uddin, B. Godfrey, and T. Abdelzaher, "Relics: In-network realization of incentives to combat selfishness in dtns," in *Network protocols (ICNP), 2010 18th IEEE international conference on*. IEEE, 2010, pp. 203–212. 159

[229] A. Ismailov, "Network monitoring in delay tolerant network," 2015. 159

[230] N. Sarafijanovic-Djukic, "Collaborative routing in mobile partitioned networks," 2010. 160

[231] W.-L. Tai, Y.-F. Chang, and W.-H. Li, "An iot notion–based authentication and key agreement scheme ensuring user anonymity for heterogeneous ad hoc wireless sensor networks," *Journal of Information Security and Applications*, 2017. 160

[232] Z. Sheng, S. Yang, Y. Yu, A. V. Vasilakos, J. A. McCann, and K. K. Leung, "A survey on the ietf protocol suite for the internet of things: Standards, challenges, and opportunities," *IEEE Wireless Communications*, vol. 20, no. 6, pp. 91–98, 2013. 160

[233] S. Gajbhiye, S. Karmakar, M. Sharma, and S. Sharma, "Design and analysis of pairing protocol for bluetooth enabled devices using r-lwe lattice-based cryptography," *Journal of Information Security and Applications*, vol. 35, pp. 44–50, 2017. 160

[234] G. Bigwood and T. Henderson, "Ironman: Using social networks to add incentives and reputation to opportunistic networks," in *Privacy, Security, Risk and Trust (PASSAT) and 2011 IEEE Third Inernational Conference on Social Computing (SocialCom), 2011 IEEE Third International Conference on*. IEEE, 2011, pp. 65–72. 160

[235] X. Huang, H. Zhai, and Y. Fang, "Robust cooperative routing protocol in mobile wireless sensor networks," *IEEE transactions on wireless communications*, vol. 7, no. 12, pp. 5278–5285, 2008. 160

[236] C. Gilchrist, *Learning iBeacon*. Packt Publishing Ltd, 2014. 160

[237] R. Raheem, A. Lasebae, M. Aiash, J. Loo, and R. H. Colson, "Mobile femtocell utilisation in lte vehicular environment: Vehicular penetration loss elimination and performance enhancement," *Vehicular Communications*, vol. 9, pp. 31–42, 2017. 160

[238] Y. Chae, L. C. DiPippo, and Y. L. Sun, "Trust management for defending on-off attacks," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 26, no. 4, pp. 1178–1191, 2015. 168

[239] L. Xiong and L. Liu, "Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities," *IEEE transactions on Knowledge and Data Engineering*, vol. 16, no. 7, pp. 843–857, 2004. 174

[240] C. Bettstetter, C. Wagner *et al.*, "The spatial node distribution of the random waypoint mobility model." *WMAN*, vol. 11, pp. 41–58, 2002. 176

[241] R. Jansen, T. Kaminski, F. Korsakov, A. Saint Croix, and D. Selifonov, "A priori trust vulnerabilities in eigentrust," *University of Minnesota*, 2008,. 187

[242] V. Carchiolo, A. Longheu, M. Malgeri, and G. Mangioni, "The effects of pre-trusted peers misbehaviour on eigentrust," in *Intelligent Distributed Computing VI*. Springer, 2013, pp. 187–197. 187