Reliable and trust-based forwarder selection for a class of multi-hop networks

Thesis submitted in partial fulfilment of the requirements
for the award of the degree of

Doctor of Philosophy

in

Computer Science and Engineering

by

Amrita Bose Paul

Under the supervision of

Dr. Santosh Biswas
Dr. Sukumar Nandi

Department of Computer Science and Engineering

Indian Institute of Technology Guwahati

Guwahati - 781039, India

FEBRUARY, 2019

Dedicated in Memory of

Bapi

Deep in my heart

You will always stay

Loved and remembered

Everyday

Declaration

I certify that

- The work contained in this thesis is original and has been done by myself and under the general supervision of my supervisor(s).
- The work reported herein has not been submitted to any other Institute for any degree or diploma.
- Whenever I have used materials (concepts, ideas, text, expressions, data, graphs, diagrams, theoretical analysis, results, etc.) from other sources, I have given due credit by citing them in the text of the thesis and giving their details in the references. Elaborate sentences used verbatim from published work have been clearly identified and quoted.
- I also affirm that no part of this thesis contains plagiarised contents to the best of my knowledge and I understand and take complete responsibility if any complaint arises.
- I am fully aware that my thesis supervisor(s) are not in a position to check for any possible instance of plagiarism within this submitted work.

February 22, 2019 Amrita Bose Paul

Department of Computer Science and Engineering
Indian Institute of Technology Guwahati
Guwahati - 781039, India

Certificate

This is to certify that this thesis entitled "**Reliable and trust-based forwarder selection for a class of multi-hop networks**" submitted by **Amrita Bose Paul**, in partial fulfillment of the requirements for the award of the degree of Doctor of Philosophy, to the Indian Institute of Technology Guwahati, Assam, India, is a record of the bonafide research work carried out by her under our guidance and supervision at the Department of Computer Science and Engineering, Indian Institute of Technology Guwahati, Assam, India. To the best of our knowledge, no part of the work reported in this thesis has been presented for the award of any degree at any other institution.

Dr. Santosh Biswas
Associate Professor
Email : santosh_biswas@iitg.ernet.in
Phone : +91-361-2582364

Dr. Sukumar Nandi
Professor
Email : sukumar@iitg.ernet.in
Phone : +91-361-2582357

Acknowledgements

The road that has led to this point of my life has been long and winding, often riddled with hurdles which seemed impossible to overcome. It was the support and guidance of all the people in my life which helped me during those difficult times, for which they will forever have my gratitude.

This thesis is the result of a perfect working relationship with my supervisors Prof. Sukumar Nandi and Dr. Santosh Biswas, to whom I am eternally grateful. Prof. Nandi has been my friend, philosopher and guide since my M.Tech days, sharing his insight and guidance whenever I have needed it. His confidence in me and his words of encouragement are the two pillars which kept me string during the most critical hours of this long academic journey. He has been a guide in the true sense, in both academics and in life, providing support and words of kindness whenever balancing a career, family, personal health and research became difficult. For pushing me to be the best version of myself and always having faith in me, I owe him thanks.

I have been very fortunate to have Dr. Santosh Biswas as my thesis supervisor. His invaluable guidance during the formulation of my research ideas while providing me the autonomy of exploring those ideas on my own, played a crucial role towards the successful completion of my PhD work. It was his motivation that pushed me to continue working even when I felt like I had hit a dead end. I would also like to thank him immensely for his guidance on my research papers and for his invaluable advice and feedback while improving and addressing my journal papers' reviews. His work ethic and enthusiasm that he brings to any project are only some of the lessons he has taught me, which I am confident will help me in the future. For his constant monitoring, training and most of all, unwavering support, I will always remain indebted to him.

I take this opportunity to express my sincere thanks to Dr. Sandip Chakraborty, Astt. Professor, Dept. of Computer Science and Engineering, Indian Institute of Technology Kharagpur (IITKGP), for his collaboration on this research topic and suggestions during my research work. This experience was not only enjoyable but also expanded my vision of the research area.

I am also highly grateful to my Doctoral Committee members, Prof. Heemange Kapoor, Dr. Sonali Chouhan, and Dr. Sanasam Ranbir Singh, for their invaluable time and support in evaluating my work progress in different stages. I extend my gratitude to the thesis reviewers, Prof. Manik Lal Das from Dhirubhai Ambani Institute of Information and Communication Technology and Prof. Mohammad Zulkernine from School of Computing, Queen's University Kingstone. I owe my sincere thanks to Prof. Diganta Goswami, the former Head,

and Prof. S.V. Rao, the present Head of the Department of CSE, for providing a healthy research environment in the department, and support my research works in many ways.

I take this opportunity to express my heartfelt gratitude to Prof. Gautam Barua, the past Director of the institute; Prof. Gautam Biswas, the present Director of the institute; all the Deans and other administrative staff of IIT Guwahati, whose collective efforts have made this institute a place for world-class studies and research. I also express my sincere regards to the respected faculty and staff of the CSE department for their extended help in terms of technical and official support.

I would like to express my thanks to Pravati, for her kindness in allowing me to share her hostel room during my comprehensive examinations. A special thanks for Suddhasil and Niladri, for their collaboration and cooperation with several research related activities. Among my other peers at the CSE department, I would like to thank Ferdous, Lipika, Shilpa, Mayank, Subhrendu, Shounak, Pradeep, Basant, Piyoosh, BalaPrakash, Saptarsi, Sukaran, Khusboo, who deserve acknowledgement for their love, support and for being a part of this wonderful journey of doctoral research. I would also like to thank everyone who has helped me directly or indirectly in my PhD journey and whose names I did not mention here. I sincerely acknowledge all of your efforts too.

I appreciate my employer, the Secretary (Education Dept), for allowing me to pursue my research work along with my full-time employment duties. The cooperation received from my colleagues, Dr. Maushumi Barooah, Dr. Jyotiprakash Goswami and Dr. Subhrajyoti Bordoloi, of Dept. of Computer Applications deserves due acknowledgement and appreciation.

I also take this opportunity to express my sincere thanks to my friend Er. Pradeep Mittal, Executive Director, NBCC, Delhi, for motivating and inspiring me to go for higher studies at a later stage of my teaching career. My heartfelt gratitude to Dimbendra Mohanta Sir, Prof., Dept. of Mechanical Engg., AEC, for having the patience to listen to my ramblings.

Without the constant support of my family members, completion of this PhD would have remained a dream. I would like to thank my husband Dr. Satyajit Paul for his constant support, motivation and never ending humor during this doctoral journey. I would also like to express my gratitude to my mother-in-law and sister-in-law for their constant support which provided me with a sense of security and enabled me to concentrate on my research work. I am sincerely obliged to my mother, who has always encouraged me to strive for the best things in life. My brother and sister deserve a special note of thanks for their love, care and trust in me which helped me to overcome all the tough situations in life, and will always inspire me to move forward towards my destination. I would also like to extend my sincere thanks to all my domestic helpers, who extended their support from time to time during my PhD journey.

The highest amount of acknowledgment goes out to my daughters Riyam and Priyam. Some times I feel that I have even taken the time slot meant for them to achieve my dream. Their sacrifices ensured that no obstacles could hinder the pace of my journey starting from M.Tech to PhD. Their belief in my abilities helped me succeed throughout my late academic career. Thank you, Riyam and Priyam, for being so kind, generous, supportive, caring and for all your love. This thesis is a culmination of your sacrifices!

This acknowledgement would be incomplete if I did not mention my pets, who have been stress relievers in every aspect of my life. Their unconditional warmth and love is the secret of my energy.

Last but not the least, I would like to thank the Almighty for his grace and blessings which enabled me to successfully complete my PhD journey.

February 22, 2019 Amrita Bose Paul

Abstract

With the advancement of a variety of innovative and pragmatic application domains of wireless networks, ranging from Wireless Mesh Networks (WMNs) to Delay/Disruption Tolerant Networks (DTNs), the task of multi-hop communication has become challenging than ever before. These networks are often characterized by frequent node mobility, intermittent connectivity, link failure, dynamic topology, node heterogeneity, existence of static and mobile nodes, non-contemporaneous end-to-end paths, energy and resource constrained devices etc. The conventional routing protocols available for multi-hop communication viz., Ad hoc On-demand Distance Vector (AODV), Optimized Link State Routing (OLSR), Dynamic Source Routing (DSR), and Topology Broadcast Based on Reverse Path Forwarding (TBRPF) etc., are insufficient to address such unreliable nature of the wireless medium in heterogeneous WMN or HetMesh, and DTN environments. Further, the task of routing have become much more challenging in a hostile scenario, (i.e., in the presence of "misbehaving" nodes), where behavior of nodes is unpredictable from the network as well as social perspectives. The presence of misbehaving nodes in the communicating path may cause a serious threat and thus routing becomes vulnerable to different kinds of attacks such as black hole, Denial-of-Service (DoS) and spoofing. Consequently, a communicating node has to be cautious while making forwarding/routing decision in the network. These situations create new challenges for designing reliable and secure routing solutions in the congenial as well as in the hostile environments of HetMesh and DTNs. Motivated by these limitations, in this thesis, we have made an attempt to exploit the intrinsic characteristics of multi-hop wireless networks for addressing the routing challenges of heterogeneous WMNs and DTNs in a congenial (i.e, all nodes are benign and follow the normal routing functionality) as well as in a hostile environment (i.e., in the presence of misbehaving nodes, both malicious and selfish).

The thesis consists of four distinct contributions. As the first contribution, a unified path determination scheme called *Adaptive Path Selection Scheme* (Adapt-PSS) for high throughput heterogeneous WMNs (HetMesh) has been proposed. In Adapt-PSS, a novel resilient path metric called "Multi-Attribute Adaptive Path Metric" (MAAPM) is defined by combining the multiple path selection criteria to make the path selection process adaptive. The performance of Adapt-PSS is evaluated through testbed as well as large scale simulation experiments and a comparative analysis with the existing routing protocols of mesh networks

has been carried out. The results not only exhibit performance enhancements of Adapt-PSS in terms of throughput, packet delivery ratio, delivery overhead and end-to-end delay, as well as it also inferred the resiliency and scalability nature of the scheme against increased traffic load and client mobility rate.

The second contribution of the thesis proposes a novel seasonality aware adaptive forwarding technique called *Seasonality Aware Social-based* (SAS) forwarding in a people-centric DTN. The proposed work introduces a new measure of "tie-strength" which is derived from the seasonal behavioral pattern among the node contacts in real mobility traces. SAS invoked a weighted Katz index based similarity measure, where tie-strength is used as a link weight, and ego-betweenness centrality to evaluate a utility value of an encountered node. Based on this utility, SAS decides the competency of a candidate node for being selected as a next-hop message carrier in DTN routing. Simulation results exhibit performance benefits of SAS against baseline social-based forwarding techniques in DTNs.

The third contribution of the thesis proposes a novel unified trust-based forwarder selection framework in a hostile environment of HetMesh. The proposed framework, called *Trust-Based Multiple Criteria Decision Making* (TB-MCDM), takes into account multiple trust-measuring criteria for trust quantification and uses a "Multiple Criteria Decision Making" (MCDM) technique for assessing the trustworthiness of each individual node in the networks. Simulation results demonstrate TB-MCDM's robustness against various security attacks that attempt to disrupt the functionality of the proposed framework. Further, TB-MCDM's performance against different routing metrics has proved its' efficiency in a hostile HetMesh scenario.

As a final contribution of the thesis, a novel unified trust-based next-hop carrier selection framework called *Multi Attribute Trust Evaluation and Management* (MATEM) is proposed for DTN routing security. The salient feature of MATEM is that, it not only integrates multi-criteria decision making technique with multiple trust measuring criteria having conflicting requirements and goals, it is also able to cope with uncertainty, long delay, and social selfishness for choosing a next-hop carrier in a hostile DTN dynamically. The performance of MATEM has been evaluated and analyzed through an extensive set of simulations and a real testbed implementation. Results generated from simulations and the real testbed verified the usability and user acceptance of MATEM in DTN-based applications viz., Pocket Switched Networks (PSNs) or Mobile Social Networks (MSNs), for ensuring security, reliability and pervasiveness. Moreover, the performance results also inferred the Quality-of-Service (QoS) requirements of DTN routing amidst uncertainty.

Contents

List of Figures

List of Tables

List of Abbreviations

Terms	Abbreviations
AODV	Ad hoc On-demand Distance Vector
ADR	Attack Detection Rate
Adapt-PSS	Adaptive Path Selection Scheme
ANN	Artificial Neural Network
AMFD	Average Message Forwarding Delay
COAR	Community Aware Opportunistic Routing
CBR	Constant Bit Rate
DSR	Dynamic Source Routing
DTNs	Delay/Disruption Tolerant Networks
DoS	Denial-of-Service
E-AODV	Extended Ad hoc On-demand Distance Vector
FPR	False Positive Rate
FNR	False Negative Rate
HetMesh	Heterogenous wireless Mesh networks
HWMP	Hybrid Wireless Mesh Protocol
HRPU	Hybrid Routing with Periodic Updates
IP	Internet Protocol
IoT	Internet of Things
ITRM	Iterative Trust and Reputation Mechanism
IPNs	Inter Planetary Networks
LIB	Local Information Base
LA	Learning Automata

MANETs	Mobile Ad hoc Networks
MAC	Media Access Control
M-HRP	Mesh Hybrid Routing Protocol
MCDM	Multiple Criteria Decision Making
MATEM	Multi-Attribute Trust Evaluation and Management
MAAPM	Multi-Attribute Adaptive Path Metric
MSNs	Mobile Social Networks
M-OLSR	Modified Optimized Link State Routing
MPRs	MultiPoint Relays
MRC	Mesh Router Count
MRP	Mesh Routing Protocol
MOR	Multicast Opportunistic Routing
NS2	Network Simulator 2
NIS	Negative Ideal Solution
NRO	Normalized Routing Overhead
ONE	Opportunistic Networking Environment
OLSR	Optimized Link State Routing
PFM	Positive Feedback Message
PIS	Positive Ideal Solution
PDR	Packet Delivery Ratio
PRoPHET	Probabilistic Routing Protocol using History of Encounters and Transitivity
PKI	Public-Key Infrastructure
PSNs	Pocket Switched Networks
QoS	Quality-of-Service
SAODV	Secure Ad hoc On-demand Distance Vector
SAROS	Socially-Aware Reputation mechanism for Opportunistic diSsemination
SAS	Seasonality Aware Social-based
TCAODV	Trusted Computing Ad hoc On-demand Distance Vector
TOPSIS	Technique for Order Preference by Similarity to Ideal Solution

TBIR	Trust Based Intelligent Routing
TTL	Time-to-Live
TA	Trusted Authority
TB-MCDM	Trust-Based Multiple Criteria Decision Making
TCP	Transmission Control Protocol
TBRPF	Topology Broadcast based on Reverse Path Forwarding
VANET	Vehicular Ad hoc Network
WPANs	Wireless Personal Area Networks
WLANs	Wireless Local Area Networks
WMNs	Wireless Mesh Networks
Wi-Fi	Wireless Fidelity
WSNs	Wireless Sensor Networks

1

Introduction

Over the past years, a decentralized wireless network technology called Mobile Ad hoc Networks (MANETs) have received a great deal of attention and popularity for its spontaneous formation with self-sufficient, non-infrastructure and node mobility support. This type of network can be formed in isolation. Originally conceived for military applications, and aimed at improving battlefield communication and survivability, MANETs have lately emerged in many civilian scenarios. In 1990's, the proliferation of wireless technologies made it possible to afford direct network connections among user devices through Bluetooth technology (IEEE 802.15.1) for Wireless Personal Area Networks (WPANs), and the 802.11 standards family for high speed Wireless Local Area Networks (WLANs). These wireless standards allow direct communication (single-hop) among network devices within the transmission range of their wireless interfaces without the need for any network infrastructure. Gradually, the uses of multi-hop paradigm in MANETs has emerged to extend the possibility of communication among couple of network devices, without the need for developing any ubiquitous network infrastructure. In this multi-hop paradigm, the user's devices directly communicate in ad hoc mode not only to exchange their own data but also to forward/relay the traffic of other network devices that are not in the communication range of each other. To accomplish the task of multi-hop communication in different wireless scenarios, the researchers have made extensive efforts to build a set of standard protocols. A proliferation of routing protocols is found in MANETs' literature that represents Ad hoc On-demand Distance Vector (AODV) [1], Optimized Link State Routing (OLSR) [2], Dynamic Source Routing (DSR) [3], Topology Broadcast Based on Reverse Path Forwarding

(TBRPF) [4] etc., as the released standard protocols. The unique feature of these protocols is their ability to maintain stable end-to-end paths between the source-destination pairs in spite of a dynamic topology. These protocols are categorized into two main groups: reactive and proactive. The nodes in an ad hoc network are generally resource constrained, so, reactive routing protocols strive to save resources (i.e., energy, buffer etc.) by discovering routes only when they are required. In contrast, proactive routing protocols establish and maintain routes at all instants of time so as to avoid the latency that occurs during new route discoveries.

However, MANETs have not become widely accepted by the mass market due to its' lack of real world implementation and industrial deployment, integration, experimentation, simulation credibility, and socio-economic motivations [5]. So, a new class of networks called Wireless Mesh Networks (WMNs) [6], Delay/Disruption Tolerant Networks (DTNs) [7], and Vehicular Ad hoc Networks (VANETs) [8] have emerged fulfilling these requirements by following a more realistic development approach. These class of networks are characterized by resource constrained heterogeneous network nodes, and highly dynamic network topologies. The high node mobility causes intermittent connectivity among communicating nodes and frequent link disruption in the routing paths. These characteristics make routing challenging in this class of networks and may not be well served by the available conventional protocols developed for MANETs. The objective of this thesis is to study, analyze, and address the routing challenges of two multi-hop MANET-born networks (viz., heterogeneous WMNs and DTNs) in a congenial (i.e, all nodes are benign and follow the normal routing functionality) as well as in a hostile environment (i.e., in the presence of misbehaving nodes, both malicious and selfish). Finally, we have come with four major contributions viz., i) *Adaptive path selection scheme for high throughput heterogeneous wireless mesh networks*, ii) *Seasonality aware forwarder selection in social-based delay tolerant networks*, iii) *Trust-based forwarder selection framework for reliable and secure routing in hostile heterogeneous wireless mesh networks*, and iv) *A unified next-hop carrier selection framework based on Trust and MCDM for assuring reliability, security, and QoS in DTN Routing*

The rest of the chapter has been organized in following way. Section 1.1 provides a detail analysis of the forwarding/routing challenges in WMNs and DTNs in a congenial wireless environment. This section also discusses the existing forwarding/routing techniques available in the literature to address the routing challenges in WMNs and DTNs along with their strengths and weaknesses. Section 1.2 presents the detail analysis of the routing challenges that may arise due to the presence of misbehaving nodes (both malicious and

selfish) in WMNs and DTNs. A brief overview of various techniques/frameworks proposed in the literature to deal with the misbehaving nodes, their drawbacks and issues are also discussed here. In Section 1.3, we summarize the shortcomings of the existing techniques for addressing the forwarder/next-hop carrier selection issues in heterogeneous WMNs and DTNs. Finally, Section 1.4 presents the motivation and contributions of the thesis.

1.1 Routing challenges of wireless mesh networks and delay tolerant networks in a congenial environment

The conventional routing protocols available for multi-hop networks viz., AODV, OLSR, DSR, and TBRPF etc. are insufficient to address the unreliable nature (i.e., link failure, dynamic topology, intermittent connectivity etc.) of the wireless medium in heterogeneous WMNs and DTNs. These conventional protocols are based on their assumptions of stable routes from source to destinations and node homogeneity. Whereas, heterogeneous WMNs and DTNs are characterized by frequent node mobility, intermittent connectivity between the mobile clients, node heterogeneity, existence of static as well as mobile nodes, non-contemporaneous end-to-end link, energy and resource constrained devices. In such a class of network, generation of end-to-end paths is difficult due to node sparsity and mobility. Therefore, in such a diverse environment decision is taken in hop by hop manner for choosing a forwarder, rather than calculating and maintaining stable end-to-end paths in a reactive or in a proactive manner.

In the subsequent section (Section 1.1.1) of this chapter, we detail the routing challenges in WMNs with a special emphasis on heterogeneous WMNs. This section also includes the detail of various forwarding/routing approaches available in the literature of WMNs to deal with such challenges and their drawbacks are also discussed in the context of addressing the routing issues in heterogeneous WMNs. Section 1.1.2 details the routing challenges in DTNs followed by discussions on the existing techniques to address the challenges and issues therein.

1.1.1 Routing issues in wireless mesh networks

WMNs have gained popularity for providing a flexible and low cost extension of the Internet. The most prominent application scenario of WMNs is currently public wireless access. WMNs have demonstrated their potential in a variety of application domains viz., broad-

band home networking, community and neighborhood networking, enterprize networking, metropolitan area networks, transportation systems, building automation, health and medical systems, security surveillance systems and crisis management etc. [6]. WMNs have two types of nodes: mesh routers and mesh clients. Routers form a static backbone for providing connectivity and coverage to mobile mesh clients. Based on the nodes' functionality, the architecture of WMNs is classified into three categories, viz. *Infrastructure* WMNs, *Client* WMNs, and *Hybrid/Heterogeneous* WMNs or *HetMesh*. In this work we mainly address the issues in hybrid/heterogeneous WMNs and therefore, unless otherwise specified explicitly, the term HetMesh in the thesis refers to heterogeneous WMNs. HetMesh combines the benefits of Infrastructure and Client WMNs. In HetMesh, the mobile clients have the capacity to directly communicate to another client without intervening the mesh backbone and can act as an intermediate forwarder. Even during data transmission, a mesh router may offload the data traffic to a potential client if the router is overloaded. In such a scenario, several factors like capacity of individual nodes, interference near the node, traffic load across different parts of the network, client mobility pattern, energy consumption issues etc., influence the optimal decision for choosing an end-to-end path in the network. All these criterion make routing difficult in multi-hop heterogeneous WMNs. A detail discussion of the existing routing/forwarding protocols available for WMNs with a special emphasis on multi-hop heterogeneous WMNs is presented below. A discussion on their drawbacks is also incorporated here.

The path establishment in high throughput heterogeneous WMNs or HetMesh faces several challenges. In general, the existing routing/forwarding protocols available for general multi-hop and mesh networks are mainly categorized as *proactive* and *reactive*. The basic proactive and reactive path selection protocols, like AODV [1], OLSR [2] and their variants have been well studied in the literature [9, 10, 11, 12, 13, 14]. The proactive path selection mechanism finds out the optimum path before the actual forwarding requirements, and it may use the stale information for future decisions. Conversely, the reactive path selection introduces extra network overhead by flooding control packets every time a path is required to be established. Again, these existing proactive and reactive routing protocols have the common problem that they are suitable for a specific scenario, and are not generalized for real time application scenarios of heterogeneous WMNs. For instance, proactive routing protocols are suitable for an infrastructure fixed network whereas reactive protocols work better for mobile and dynamic time varying networks. Further, the WMN companies are developing a variety of routing protocols to satisfy their needs. Some of them are propri-

etary and held secret [15], while others use well-known ad hoc routing protocols. Firetide uses TBRPF [16], [17] and other companies rely on the IEEE 802.11 spanning tree protocol called MeshDynamics [18] for routing at layer 2. All these available general purpose, situation specific, and proprietary WMN routing protocols are unable to deal with the complexities (i.e., frequent link failure, high node dynamics, node heterogeneity and unstable end-to-end paths) of heterogeneous WMNs. Thus, to cope up with such problems, hybrid routing protocols have been proposed in the literature of multi-hop heterogeneous WMNs.

The authors in [19] have proposed Hybrid Wireless Mesh Protocol (HWMP) for IEEE 802.11s WLAN mesh networks. The protocol is based on a combination of both the proactive and the reactive approaches. IEEE 802.11s defines a new mesh data frame format and has an extensibility framework for routing. The protocol uses Media Access Control (MAC) addresses and a radio-aware routing metric for both mesh path selection and maintenance. In [20], a hybrid routing protocol, called Mesh Hybrid Routing Protocol (M-HRP) for WMNs, is presented that combines proactive and reactive components to achieve the mesh path selection objectives. The proactive component works at the static backbone, whereas route requests from clients are processed reactively. In an another approach, Hybrid Routing with Periodic Updates (HRPU) [21] is proposed for heterogeneous WMNs. In HRPU, all routes towards the gateway router are maintained in proactive manner, while all client nodes use reactive routing algorithm for path selection. However, the problem with these protocols is that, with high node mobility, link breakages in the network occur frequently, for which, the route towards the gateway router might become invalid causing network performance degradation. Further, mostly all these protocols are based on the assumption that an initial route towards the gateway router is maintained in a proactive/reactive fashion. In case of a link failure or new updates, the network acts in a reactive way, which involves a large amount of delay in path set-up time and the overhead also increases with increase in network size and mobility. Therefore the shortcomings of both the proactive path selection and the reactive path selection are inherent in these hybrid protocols for heterogeneous WMNs. Further, all these available hybrid protocols developed for heterogeneous WMNs improve some parameters, however compromise on the others [19, 20, 21].

Recently, more sophisticated forwarding/routing protocols have been proposed in the literature for heterogeneous WMNs. In [22], the authors present a mesh routing protocol that guarantees hop by hop bandwidth. A joint approach for routing and rate adaptation has been studied in [23] where the multi-rate environment has been explored in designing path selection metrics. Opportunistic routing/forwarding has been explored in the literature,

like [24] and the references therein, that exploits wireless broadcast environment to reduce path selection overhead. To cope up with the wireless channel dynamics, the authors in [25] propose a greedy path selection protocol for mesh networks. In [26], the authors have proposed a congestion aware opportunistic routing for multi-hop wireless networks. In a very recent work [27], the authors have proposed Multicast Opportunistic Routing (MOR) in multi-hop WMNs. The protocol is based on the broadcast transmissions and Learning Automata (LA) to explore the potential candidate node that can act as a forwarder and shall aid in the process of retransmission of the data. The basic assumptions of the protocol is that it learns from the past experience and the destination nodes are required to be in sync with one another in order to avoid broadcasting of duplicate data. However, in a HetMesh scenario, use of learning technique may not be accurate because of intermittent connectivity and highly dynamic topology.

To summarize, all of these routing, forwarding or path selection protocols proposed in the literature of multi hop WMNs inherently assume that nodes in the network are of equal capacity and therefore use a common routing metric to find out the path quality. Moreover, these protocols lack their credibility in terms of real world implementations and industrial deployments. In heterogeneous WMNs, a mesh router can be equipped with multiple interfaces, and can operate in multiple channels. Every mesh router forms a static mesh connectivity with the neighboring routers. With such a connectivity, multiple paths exist between any pairs of mesh routers separated by multiple hops. Further, the recent advances in high throughput technologies impose extra difficulties in the design of a good path selection metric. In a HetMesh scenario, the mobile clients are expected to support technology heterogeneity, where several technologies may coexist (like IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac etc.) with different sets of access technologies. For example, IEEE 802.11n/ac supports channel bonding for high throughput communication, whereas IEEE 802.11b/g does not. Therefore, these salient features of high throughput HetMesh differentiate it from general multi-hop mesh architecture, and therefore demands for a more sophisticated path selection mechanism.

1.1.2 Routing issues in delay tolerant networks

Delay/Disruption Tolerant Networks (DTNs) are the most interesting evolution of the multi-hop networking paradigm that depart from the Internet-oriented approach used in MANETs as it does not impose an end-to-end path from source to destination. DTNs are de-

ployed in extreme environments like battlefields, deep oceans, deep space, volcanic regions, developing regions (e.g. rural message delivery etc.), where they suffer challenging conditions like military wars and conflicts, terrorist attacks, earthquakes, volcanic eruptions, floods, storms, hurricanes, severe electromagnetic interferences, congested usage, etc. Under such extreme and challenged conditions, network connectivity becomes considerably intermittent and the existence of contemporaneous end-to-end path between any source-destination pair cannot be guaranteed. DTN gains its popularity in recent years as a means of addressing the issue of routing messages in partitioned networks [28]. In DTNs, generation of end-to-end paths are difficult due to node sparsity and mobility. Routing in DTNs is accomplished by exploiting mobility of wireless devices (called DTN nodes) for opportunistic message exchanges between them when they are in communication range of each other. Unlike traditional MANETs, where packets are forwarded along stable links, DTNs allow message forwarding along intermittent links usually caused by high mobility and low density of nodes. To attain reliability in presence of intermittent connectivity, routing in DTN is characterized by a message propagation scheme referred as "store-carry-forward" [29] where intermediate nodes (in the literature of DTN it is termed as "next-hop carriers") may need to store, carry, and wait for opportunities to forward in-transit message to another node along a path that eventually reaches the destination causing end-to-end latency. Under such a paradigm, each node independently makes forwarding decisions that take place when two nodes meet. DTN applications are expected to be delay tolerant, but minimizing delay lowers the time messages spend in the network and thus, reduces contention for resources. As such, selecting an intermediate node as a next-hop message carrier is a crucial issue in DTN for improving the routing performance by maximizing the message delivery ratio as well as to minimize the delay for a message to reach the destination. Now, we briefly discuss the various approaches that are used for selecting a next-hop carrier in DTN-based application scenarios. The shortcomings of these approaches are also addressed here.

The traditional routing protocols of wireless networks (e.g., AODV [1], OLSR [2], DSDV [30] etc.) are based on the assumption of existence of a stable path between the source-destination pair. Thus, these routing protocols are unable to cope with the intermittent connectivity, frequent and arbitrarily long-lived connectivity disruptions, existence of non-contemporaneous end-to-end path, node sparsity, long and variable communication latency of DTNs. Consequently, different routing approaches have been proposed in the literature of DTNs to support these features. These approaches can be broadly categorized as [29]:

- **Deterministic or Scheduled Routing:** In deterministic routing the contact information are known a priori. This makes design of routing protocols easy for DTNs.
- **Enforced Routing:** Enforced routing strategy is used for connecting an isolated network (e.g., island) with the Internet as well as connecting devices among themselves in that region. In such cases, special purpose mobile resources, like message ferries [31] and data mules [32] are deployed in the network to act as gateways (i.e., data messenger) between the isolated network and the rest of the Internet. These data messengers follow a predefined path to deliver the messages from source to destination.
- **Opportunistic Routing:** In opportunistic routing protocol, delivery is random, unexpected, and opportunity based. This approach of routing is used when mobility patterns of the nodes in the network are difficult to predict. Here, when two nodes come in contact of each other, they utilize this opportunity to transfer the messages. Thus, messages eventually get delivered to the destination.

In this thesis our interest lies in opportunistic routing, so rest of this section discusses about opportunistic message forwarding only. In DTNs, the contemporaneous path between the source-destination pair may not exist due to intermittent connectivity and frequent link disruptions. Thus, to cope with the prevailing uncertainty in DTN-based communication, routing is mobility assisted and nodes utilize their contact opportunities to make forwarding decisions. The opportunistic protocols designed to address the routing issues in DTNs are broadly classified into two categories viz., *flooding* and *forwarding* [33], which are detailed next.

In flooding based routing approach, a source node tries to send all its' messages to its' neighbors if they do not have the copy of the messages. This approach does not require to store any past information about the routing or mobility of the nodes. So, flooding is the obvious choice when no information is known in advance about the movement of the nodes or about the topology of the network. The protocols in this family induce multiple "replicas" of each message in the network without considering the potentiality of the candidate node for being selected as a next-hop carrier [34, 35, 36]. Though, these protocols in the flooding family achieve good delivery ratio with less delivery latency, however, flooding the network with duplicate messages cause high network overhead in term of storage and power spent on transmission and reception. These cause congestion leading to network performance

degradation. So, another class of routing approaches called "forwarding-based" has been explored to restrict the generation of bundle replicas in the network.

The protocols in the forwarding family calculate an utility metric based on "knowledge" to qualify the candidate node as the next-hop carrier on the routing path. A single copy of each message is forwarded to the qualified node. Most of these knowledge-based protocols select a suitable next-hop carrier based on contact history of potential carriers [37, 38], knowledge about traffic patterns in the network [39] or on probability of encountering the destination node [40]. However, the drawback is that, the protocols in this family maintain a single copy of the messages in the network causing poor delivery ratio leading to network performance degradation. So, some of them have used multi-copy spraying mechanisms to improve reliability amidst intermittent connectivity [41, 42].

Further, the increasing diffusion of smart hand-held devices in everyday life is generating a people-centric revolution in computing and communication. Therefore, researchers have started exploiting the social perspectives of human behavior in communication. In most of the terrestrial DTN applications (e.g., vehicular networks, mobile social networks, pocket switched networks etc.) the mobile nodes/devices are carried and used by people and thereby making forwarding decision based on peoples' social behavioral perspectives. So, a class of DTN forwarding algorithms, termed as "*social based DTN forwarding*" [43] have emerged, which exploits the social network properties in DTN forwarding. Popular social based DTN forwarding techniques [43] usually exploit three social network metrics: similarity between node-pairs [44], centrality of a node [45], and community of nodes [46].

The works in [47, 48, 49] have explored the usefulness of community detection algorithms in DTN forwarding. The shortcoming of these approaches is that they do not capture the dynamics of social relations among the nodes. In an another approach, SimBet [50] has exploited ego-betweenness centrality and similarity metric to forward messages in DTN. However, the shortcoming of SimBet is that, the authors model the relationship between the nodes as binary and does not consider the relative strength of its neighbors. Again, the proposed betweenness centrality of BubbleRap [51] requires the knowledge of the whole network, which in reality is not possible in DTN. Another set of social based forwarding techniques have exploited the concept of tie-strength [52]. Few of these can be found in [53, 54, 55, 56]. These techniques have modeled the change in contact patterns during time, and predicted strength of social relationships between node-pairs. However, in these approaches, the authors have failed to model the dynamic changes in contacts from human

behavioral perspectives. Therefore, the drawbacks of these existing state-of-the-art routing protocols of DTNs need to be addressed and demand for a more improved approach for selecting a next-hop carrier in the message forwarding path.

To summarize, the differences in network architecture, communication paradigm, and application scenarios of these two networks (i.e., HetMesh and DTNs) demand different approaches of forwarding/routing other than conventional protocols developed for traditional MANETs. The routing protocols of MANETs are based on their assumptions of continuous network availability, node homogeneity, and committed end-to-end path before transmission. These assumptions restrain the behavior of HetMesh and DTNs. Further, in these class of networks, a hop-by-hop forwarding decision looks more promising rather than computing a end-to-end path for data transmission between the source-destination pairs in the network. Moreover, the distributed and heterogeneous nature of these multi-hop networks, their infrastructure-less property coupled with the complexity of their underlying communication and application environment (i.e., unstable and unreliable nature of wireless medium, nodes' social behavior) have made the forwarding much more challenging than ever before. As such, selection of a suitable forwarder/next-hop carrier in the routing path of these multi-hop HetMesh and DTNs till remains an open research issue.

1.2 Routing challenges of heterogeneous wireless mesh networks and delay tolerant networks in a hostile wireless environment

The existing forwarding/routing protocols available in the literature of WMNs [10, 11, 19, 20] and DTNs [34, 37, 38, 43] look promising and work well in a friendly (i.e., all nodes are benign and follow the normal forwarding/routing functionalities) network environment for attaining their routing objectives, such as, maximizing packet/message delivery ratio while minimizing end-to-end delay and routing overhead. However, the task of forwarder/next-hop carrier selection in these protocols become much more challenging and they may not be accurate to address the routing challenges in a hostile scenario, (i.e., in the presence of "misbehaving" nodes), where behavior of nodes is unpredictable from the network as well as social perspectives [57], [58],. By misbehaving nodes, we mean both malicious and socially selfish nodes. A malicious node may either drop messages arbitrarily just to save energy or utilize them to launch more sophisticated attacks [57]. Again, a forwarding misbehavior can be caused by selfish nodes that are unwilling to spend resources (e.g., power and buffer) on forwarding messages of others with whom they do not have good social ties.

Further, a selfish node always tries to maximize its own benefits and may decide to forward a message if it has good social ties with the source, current forwarder/carrier or the destination node [58]. Thus, the misbehaving nodes have either negative or limited contributions to the network. The presence of misbehaving nodes in the forwarding/routing path may cause a serious threat and thus, routing becomes vulnerable to different kinds of attacks such as black hole, denial-of-service (DoS) and spoofing. Consequently, a communicating node has to be cautious when selecting a forwarder/next-hop carrier for routing packets in the network. These create new challenges for developing reliable and secure routing solutions in the hostile environment of HetMesh and DTNs. Moreover, to ascertain the intended network performance in a hostile scenario, each wireless node of HetMesh and DTN needs to rely on some sort of uncertainty about the goodness of other encountered nodes for forwarding/routing packets in the networks.

Use of traditional cryptographic primitives based techniques are insufficient to handle such uncongenial situations (e.g., node compromise, continuously changing nodes' behaviors to bypass traditional security walls etc.) because of their assumption of continuous network availability. Even though strong cryptography can provide integrity, confidentiality, and authentication, it fails in the face of insider attacks [59]. Moreover, in highly dynamic, delayed or disrupted network condition, key management and key distribution services are hard to implement. In addition, credit/reputataion based mechanisms are ineffective in dynamic network conditions as smooth propagation of credit/reputation values as well as end-to-end acknowledgements can not be guaranteed due to node sparsity, infrequent and intermittent node connectivity etc [60].

Therefore, to ensure a reliable and secure communication among wireless nodes in a hostile environment, a distributed collaboration among network entities is essential. Collaboration becomes productive only if all nodes in the network cooperate in a trustworthy manner [61]. Trust enables network entities to cope with the uncertainty and uncontrollability caused by independent movement and free intension of other network nodes. The concept of trust has originated from social sciences and is defined as the "subjective belief" about the behavior of an entity under consideration [62]. In general, "Trust" is the level of confidence or assurance in a node or network of nodes [63]. Thus, trust reflects the mutual relationship and maintains a reliable communication only with nodes which are trustworthy and avoids inclusion of misbehaving nodes (i.e., untrustworthy) in the routing path. An untrustworthy/misbehaving node can cause considerable packet loss and adversely affect quality and reliability of data. These situations motivate the application of trust-based

forwarder/next-hop carrier selection for secure and reliable communication in HetMesh and DTNs.

In Section1.2.1, we represent a brief outline about the available approaches to deal with misbehaving nodes in multi-hop wireless networks with a special focus on trust-based framework in WMNs. The shortcomings of these existing approaches are also analyzed in the context of reliable and secure forwarder selection process of HetMesh. Section1.2.2 details the existing trust-based approaches for detecting or avoiding malicious nodes from next-hop carrier selection in DTNs.

1.2.1 Trust-based forwarder selection in hostile multi-hop wireless networks

The available trust-based frameworks to deal with misbehaving/malicious nodes in a wireless environment mostly rely on cryptographic computations. One such protocol called "Ariande" [64] is a secure on-demand source routing based on authentication of source node. Another such protocol SAODV [65] is a secure variant of AODV which uses cryptographic extensions to provide authenticity and integrity of routing messages. It uses hash chains in order to prevent manipulation of the hop count field. The work in [66] presents a trusted routing named Trusted Computing Ad hoc On-demand Distance Vector (TCAODV), which extends the traditional AODV [1] routing protocol to ensure that only trustworthy nodes participate in route calculation and prevents selfish or malicious nodes from participating in the network. In TCAODV [66], a public key certificate as well as a per-route symmetric encryption key is established to ensure that only trusted nodes along the path can use the route. However, these approaches are insufficient as the key characteristics of HetMesh make it possible for attackers, including malicious users to add routers, establish links, and advertise routes. In addition, an attacker can steal the credentials of a legitimate user or a legitimate user can itself turn malicious, and thereby inject authenticated but incorrect routing information into the network. Moreover, these cryptographic computations generate high volume of security related traffic in the network and can easily cause congestion and prevent the flow of normal data traffic in a resource constrained network. Therefore, all these existing solutions imply a reduction of performance due to additional cryptographic computations.

In addition, a few non-cryptographic solutions are also made available in the literature of multi-hop heterogeneous network to address the issues of misbehaving nodes in a hostile wireless environment. The authors in [67] evaluated trust evidence in ad hoc networks

and have shown that two nodes having no previous interaction are able to establish indirect trust. However, in reality, direct observations are more significant than the indirect one. The trust model in [68] is based on reputation value which is evaluated on the basis of aggregation of collected feedbacks from the neighboring nodes. However the feedback collection may not be a feasible approach in a highly dynamic network condition where maintaining a reverse path between the source-destination pair is not possible. The authors in [69] presented an information theoretic framework for trust quantification in ad hoc networks and simulated the framework for malicious node detection. A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks is proposed in [70]. The work presents a mechanism based on node monitoring complemented by a reputation functionality. Further, to mitigate routing misbehavior in ad hoc networks, the authors in [71] proposed a reputation-based trust management scheme that incorporates the concept of "watchdog" for monitoring node behavior and a "pathrater" for collecting reputation values of other nodes in the network. However, the secure routing frameworks that require persistent monitoring operations to observe nodes' packet forwarding behavior may result in low network performance in heterogeneous WMNs due to their lack of stable common multi-hop path from source to destination. This is due to frequent link disruption and intermittent connectivity pattern that causes a node to lose connectivity with the node which it desires to monitor. A trust measurement scheme for WMNs has been reported in [72], where the Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) [73, 74] approach is used for quantification of trust relationship. The scheme derives the trust level of each node in the WMN, however, no implementation and evaluation are carried out to test its effectiveness.

Although a variety of trust models have been proposed and developed by research community for ad hoc and WMNs, however, to the best of our knowledge, these schemes have not yet been extended for heterogeneous WMNs. The architectures and routing nature of HetMesh are different from that of ad hoc and general purpose mesh networks. HetMesh follow a hierarchical architecture where clients communicate in a multi-hop fashion with their nearby routers. Again multiple paths are available in mesh backbone allowing multiple alternative routers to route the traffic between the source destination pair. Therefore, the methods used for quantification of node behavior in ad hoc and mesh networks are not applicable for HetMesh. Hence, trust-based frameworks designed for conventional ad hoc and mesh networks need to be tailored to meet the prevailing constraints of heterogeneous WMNs.

1.2.2 Trust-based next-hop carrier selection in hostile delay tolerant networks

The available trust-based approaches [75, 76, 77, 78] to deal with misbehaving nodes basically rely on recommendations or feedback mechanisms to build trust among participating nodes. This trust value is then used to identify misbehaving nodes and avoid selecting such nodes as message carriers in DTN routing. In [79], a Secure Reputation-based Dynamic (SReD) window scheme has been proposed to estimate the trust in DTNs. The trust estimation is based on cryptographic operation, node's behavior, and reputation. A limitation of their work is that no consideration is taken to tackle inside attackers which are malicious and selfish in nature. The authors in [80] have addressed the problem of misbehaving carriers and propose a solution based on reputation. The shortcoming of the proposed method is that the reputation building mechanism is based on the assumption that the system is capable of keeping track of intermediate carriers as a whole for message delivery, which is infeasible in an opportunistic environment. The work in [75] proposed an Iterative Trust and Reputation Mechanism (ITRM) to detect and isolate malicious nodes from the network iteratively. However, this scheme is solely aimed at preventing Byzantine type of attack in DTNs. The work in [78] has proposed a weighted average of social trust and quality of service trust to analyze the trust level of each node in DTNs. The trust evaluation protocol relies on the use of direct trust evidence and indirect recommendations to estimate the trust value of each node in DTNs. However, the work does not focus on the prevailing uncertainty in DTNs' message propagation scheme, and the functionality offered by mobile devices in a people-centric opportunistic communication scenario is not explored from social networking perspective. In an another approach [76], the authors have proposed a reputation assisted framework to evaluate an encounter's competency of delivering data in DTNs. The working principal of the framework is based on collected evidences of nodes' packet-forwarding behavior. However, the framework is solely aimed at preventing black hole attack in opportunistic DTNs. In [77], a probabilistic misbehavior detection scheme (iTrust) has been presented that adopts the concept of "Inspection Game" to stimulate cooperation of misbehaving nodes and consider a periodically-available central Trusted Authority (TA) to judge the nodes' packet forwarding behavior. However, if misbehaving nodes do not follow the game strategies, a low message delivery ratio would still result. In addition, most of these approaches did not asses the nodes' behavior from a social networking perspective to address the issues arising from socially selfish nodes, which is of primary importance of communication in people-centric networking scenario. Furthermore, some

of these approaches are based on the assumptions of i) use of network monitoring system such as, "Watchdog" to observe nodes' packet forwarding behavior [76], ii) feedback mechanisms to built reputation [75] and iii) centralized trusted authority [77] to judge nodes' behavior. These assumptions, however, restrain the behavior of DTNs where connectivity is intermittent and communication is opportunistic in nature.

Recently, some social-aware routing protocols have been made available in the literature for reliable message forwarding in opportunistic DTNs. The work in [81] has provided an overview of routing and data dissemination issues in opportunistic DTNs with a special attention on characteristics of Mobile Social Networks (MSNs) and analysis metrics, human mobility models, dynamic community detection methods, routing and data dissemination protocols. However, none of these protocols have considered routing trade-offs between conflicting requirements and goals in the protocol design. Further, sufficient attempts have not been made to study the impact of social selfishness on the performance of routing and data dissemination protocols. In an another social-based approach [82], the authors have proposed a distributed optimal Community Aware Opportunistic Routing (CAOR) algorithm for DTN-based MSNs. However, in their work, no attempt has been made to address the uncertainty issues that might arise due to the presence of selfish nodes in a hostile DTN scenario. In [83], a Trust Based Intelligent Routing (TBIR) using Artificial Neural Network (ANN) is proposed for DTNs which exploits the "Call Data Record" from "Call Detail Record" in socially active communities. However, information regarding community formation and detection have not been provided in TBIR. Moreover, the work has not addressed the reliability and Quality-of-Service (QoS) issues in DTN-based communication. In a very recent work [84], the authors have proposed a trust and reputation management mechanism entitled "Socially-Aware Reputation mechanism for Opportunistic diSsemination" (SAROS), for opportunistic networks. The experimental results exhibit the efficiency of SAROS in terms of the routing metric called "correct message hit rate", but reported with high delivery latency. Further, the protocol's resiliency against the security attacks is not reported in the current work. Moreover, SAROS may require modifications to be directly applied to pure opportunistic-DTNs. It may be noted that SAROS mainly works by keeping track of intermediate carriers responsible for forming correct and incorrect *paths as a whole* for message delivery. In DTNs, however, contemporaneous end-to-end paths between source-destination pairs are hard to achieve due to the existence of frequent link disruptions, intermittent connectivity etc. In addition, the protocols available in [85, 86, 87, 88] have been developed from a social networking perspective and try to optimize the social characteristics of mobile

users for message forwarding. However, they did not focus on the issues (viz., uncertainty, delay, mobility etc.) that arise from DTN perspective as well as from nodes' abnormal behavioral perspective.

In the next section (Section 1.3), we summarize the shortcomings/research challenges of these existing trust-based and social-aware approaches for their applicability in HetMesh and DTNs scenarios, which is further followed by (Section 1.3.1) listing of design objectives/key properties that any secure forwarder/next-hop carrier selection framework proposed for hostile HetMesh and DTNs must possess.

1.3 Shortcomings/research challenges of the existing trust-based approaches for their adaptability in HetMesh and DTNs

To summarize, all these available trust-based and social aware routings appearing in the literature are best effort protocols in their respective domain, but we found the following drawbacks/research challenges associated with them for addressing the forwarder/next-hop carrier selection in HetMesh and DTNs:

1. Most of the trust-based frameworks proposed for ad hoc wireless networks assume that nodes are having equal capacity and competency, wherein each node in HetMesh and DTNs could be highly heterogeneous. The heterogeneity could be in terms of the roles (i.e., router or client) of the nodes, their inherent technical capability (in terms of buffer, energy, mobility) and security (i.e., malicious, selfish). This implies that not all nodes or their contents can be treated equally and thus, require a different approach for trust evaluation. Therefore, how to evaluate trust in a heterogeneous environment has become an open research challenge.

2. The trust-based frameworks available in the literature have not considered the nodes' malicious and social behavior together to judge the competency of a node for being selected as a forwarder/next-hop carrier in the routing path. In a people-centric social environment a non-malicious node may exhibit selfish behavior in data forwarding and this will lead packets to drop either due to buffer overflow or Time-to-Live (TTL) expiration. Again, a socially good node may behave maliciously by providing false recommendations about other peer nodes to increase their individual gain. Therefore, how to deal with such conflicting node behaviors (i.e., the act of maliciousness and social selfishness) together to cope with misbehaving nodes in a hostile HetMesh and

DTN environment has become an important issue to address.

3. Furthermore, none of these techniques could focus on the inherent risk involved in the packet/message propagation scheme as well as the QoS requirement of the underlying secure routing protocols amidst uncertainty. In a hostile scenario, an intermediate honest forwarder/carrier may misbehave either by dropping packets/messages or by not forwarding them to the intended recipients. So, a measure of risk/uncertainty in communication is an important issue to address. Again, the trusted forwarder/carrier selection process incurs an additional amount of end-to-end delay during the filtering process of misbehaving nodes in the routing path. Thus, delay minimization is an important issue for ensuring the QoS requirement of reliable and secure routing in HetMesh as well as in DTNs.

4. Moreover, the performance of these available frameworks have not been evaluated simultaneously against the routing metrics (viz., throughput, packet delivery ratio, routing overhead, end-to-end delay etc.) as well as the security metrics (viz., attack detection rate, false positive, false negative etc.) in the application oriented wireless networking domain.

5. Again, none of these frameworks are capable of reflecting mission difficulty (i.e., risk upon task failure), changing network environments (e.g., increasingly hostile environment as attackers' strength increases, high communication load, changing node speed and node density etc.), and conditions of participating nodes (e.g., low energy, buffer availability, link status, selfishness etc.). These situations pose severe limitations on the functionality of the trust-based frameworks in detecting misbehaving nodes and in result the overall network performance degrades.

6. Nonetheless, the trust evaluation process of these available frameworks are mostly based on single trust evaluation metric (in general nodes' packet forwarding behavior), however in reality, the functionality and evaluation of trust depends on multiple criteria (viz., mobility, link and buffer capacity, social aspects etc.). Thus, how to correlate and consider these multiple trust measuring criteria while designing a reliable and secure routing in HetMesh and DTNs has become a challenging aspect to the research community.

1.3.1 Design objectives and key properties of reliable forwarder selection framework for hostile HetMesh and DTNs

The research challenges discussed in Section 1.3 reveals the fact that any reliable and secure forwarder/next-hop carrier selection framework proposed for hostile HetMesh and DTN scenarios must address and possess the following design objectives and key properties:

1. *Adaptability to changing network conditions*: The framework must incorporate adequate functionality for each node to reflect the changing network environments (e.g., increasingly hostile environment as attackers' strength increases, link capacity, high communication load etc.) as well as technical competency and behavioral conditions of the participating nodes (e.g., low energy, buffer capacity, compromised status, social aspects of node behavior etc.).

2. *Misbehaving node detection capability*: The open and dynamic nature of HetMesh and DTNs make them extremely vulnerable to different type of attacks like black hole attack, wormhole attack, sybil attack, DoS attack etc. Due to high cost and overhead involved in encryption process, data packets in these networks are usually transmitted in plain text form, without encrypting them. The attacker can easily intercept these plain text data packets and forge them before reintroducing them back into the network. This can have an adverse ramification on the integrity and confidentiality of these networks. Therefore, due to high stakes involved in their security, any trust-based framework proposed for HetMesh and DTNs must be capable of detecting such attacks with high detection rate.

3. *Reduced computational overhead*: Wireless networks like HetMesh and DTNs are characterized by energy and resource constrained nodes. Therefore, any security framework that requires substantial amount of computational overhead may degrade the network performance in terms of throughput, packet delivery ratio and delay. Moreover, computation intensive monitoring operation drains out the energy level of the nodes which effectively shortens the life span of these networks. Therefore, any security framework proposed for energy constrained wireless networks must adopt appropriate measures to reduce the computational overhead and delay required for efficient functioning of the framework.

4. *Consideration of uncertainty in nodes' behavior*: The traditional cryptographic-based

security frameworks developed for multi-hop wireless networks are insufficient to handle the prevailing uncertainty (e.g., node compromise, continuously changing nodes' behaviors to bypass traditional security walls etc.) in HetMesh and DTN scenarios because of their assumption of continuous network availability. Therefore, the trust-based frameworks proposed for heterogeneous networks must consider these uncongenial situations and adopt appropriate measures to tackle the uncertainties of such networks.

5. *Absence of any centralized authority for node monitoring*: The consideration of centralized trusted authority to judge nodes' behavior may not be appropriate in HetMesh and DTN scenarios where connectivity is intermittent and communication is opportunistic in nature. Further, the use of node monitoring system to observe nodes' packet forwarding behavior may result in low network performance. This is due to frequent link disruption and intermittent connectivity pattern that cause a node to lose connectivity with the intermediate node which it desires to monitor. Therefore, any secure framework proposed for HetMesh and DTNs must consider these constraints and adopt appropriate measures to observe and collect information about nodes in the networks.

6. *Distributed collaborations*: In highly dynamic network conditions, the key distribution and key management services available for wireless networks are infeasible to implement. Further, the credit/reputataion based mechanisms are ineffective in such networks as smooth propagation of credit/reputation values as well as end-to-end acknowledgements can not be guaranteed due to node sparsity, infrequent and intermittent node connectivity etc. Therefore, ensuring secure and reliable communication among wireless nodes under such a hostile environment, a distributed collaboration among network entities is essential.

1.4 Motivation and Contributions of the Thesis

1.4.1 Adaptive path selection scheme for high throughput heterogeneous wireless mesh networks

Heterogeneous Wireless Mesh Network (HetMesh) is a promising high throughput technology for multi-hop data forwarding by mobile clients and backbone routers in a dynamic

environment. HetMesh shows a hierarchical architecture, where the backbone comprises of fixed infrastructure mesh routers, and the clients are of ad hoc and dynamic in nature. Both the mesh routers and mesh clients may exploit multi-channel and multi-interface capabilities for connecting with the backbone and outside Internet. Although hybrid routing protocols have been proposed for such hierarchical environments, however the main challenge lies in deciding when the nodes should use proactive component and when the reactive one. In most of the existing hybrid protocols, this decision is kept to network administrator that makes the protocols non-adaptive and configuration dependent. Moreover, HetMesh supports Wifi-Direct facility and other separate access technologies in its mobile clients, which make the selection of a suitable forwarder for data transmission challenging. Towards this end, a unified path determination scheme for high throughput HetMesh is proposed as the first contribution of the thesis.

The proposed method of forwarder selection uses a unified scheme for high throughput HetMesh, where clients can leverage their full capacities and may act as a potential forwarder if they have sufficient available resources. In this work, enhancements for path selection quality in a high throughput HetMesh are proposed, where the technical competency (in terms of link capacity, residue energy and buffer) of each willing node (i.e., mesh routers and clients) in the forwarding path has been taken into consideration for deciding their potentiality for being selected a forwarder. The proposed enhancements not only improve path selection quality in a high throughput HetMesh, but also take robust decisions to make the path selection process adaptive. In the proposed scheme, we define a resilient metric to decide the potentiality of mesh clients to act as a forwarder. Apart from that, a novel routing metric is designed by combining multiple path selection criteria. The existing hybrid path selection protocol is tuned to augment the proposed metrics. The performance of the proposed scheme is evaluated through testbed as well as large scale simulation results. The performances have been found to get enhanced compared to the existing routing protocols of mesh networks, and has shown more resilience to increased traffic load and client mobility rate. Moreover, the performance results also inferred the scalable nature of the proposed scheme.

1.4.2 Seasonality aware forwarder selection in social-based delay tolerant networks

Delay/Disruption Tolerant networks (DTNs) are a class of intermittently connected multihop wireless networks in which contemporaneous end-to-end paths from source to desti-

nation do not exist. These networks are highly dynamic and are characterized by frequent partitions due to disruptions, large delays, asymmetric data rate and high packet loss rate. These make routing in DTN a very challenging problem. Traditional routing protocols developed for MANETs are based on the assumption of continuous end to end path from source to destination and thus, are unable to function efficiently in DTNs resulting low network performance. The communication in DTN is mostly opportunistic, taking advantage of opportunistic contacts among nodes to exchange data. Due to intermittent connectivity, the contact duration between communicating nodes are very limited. Therefore, it is essential that this duration has to be used very smartly for forwarding the message to the best possible next-hop carrier for eventual delivery of that message. In literature, various approaches have been proposed for routing in DTNs. These approaches are categorized as flooding based, forwarding based and social metric based. Social-based routing is a relatively new approach for addressing the routing problem in DTNs. It is based on the observation that in most of the terrestrial DTN applications (such as mobile social networks, pocket switched networks etc.), people carrying the hand-held mobile devices exchange information. The inherent social property of these people-centric DTN applications have encouraged contemporary researchers in exploiting social metrics to devise forwarding techniques for efficient path selection.

The second contribution of this thesis proposes a novel social metric based forwarding technique for efficient routing and thus ensuring reliability in people-centric DTNs. This work observes evidence of seasonal behavior in contacts between node-pairs in real mobility traces, and exploits it to devise a novel seasonality aware similarity measure. We incorporate seasonality information into tie-strength, and then use it as link weight in a weighted similarity measure which we extend from Katz similarity index. Our proposed technique called *Seasonality Aware Social-based* (SAS) forwarding is based on the newly designed similarity measure and ego-betweenness centrality. Finally we perform real trace driven simulations and the results exhibit that SAS outperforms baseline social based DTN forwarding methods in terms of delivery ratio, delivery latency, and delivery overhead.

1.4.3 Trust-based forwarder selection framework for reliable and secure routing in hostile heterogeneous wireless mesh networks

Heterogeneous Wireless Mesh Networks (HetMesh) do not rely on any centralized administration and they are built by the connection of various static and mobile entities (i.e.

nodes). The presence of misbehaving nodes (both malicious and selfish) within the network may disrupt the normal routing activities either by dropping or spoofing data packets. To ensure a reliable and secure communication among wireless nodes under hostile environment, a distributed collaboration between these network entities is essential. Collaboration becomes productive only if all nodes in the network co-operate in a trustworthy manner. Therefore, to ensure a reliable and secure route discovery in a hostile environment, it is necessary to compute trustworthiness of individual nodes in a cooperative manner for discovering neighbors, selecting routers and announcing topology information in HetMesh. To address these issues, a novel trust-based forwarder selection framework for HetMesh is proposed as the third contribution of the thesis.

In our proposed framework, "trust" has evolved form individual observations and collected recommendations, where, each individual node in the network effectively assigns a trust called individual trust to each of its neighboring nodes depending on node behavior. Again, depending on these assignments, each node selects its neighbor whose trust value is greater than a particular threshold value and subsequently advertises these neighboring trustworthy nodes in the network with their respective trust values. From these broadcasted trust information, recommended trust for neighboring nodes are calculated. Combination of both individual trust and recommendation trust gives actual trust value. Trust value thus calculated is a continuous real number lying in the closed interval [-1,1]. Nodes with trust value above zero are considered as trustworthy and are included in the routing process whereas nodes having trust value lower than zero are recognized as misbehaving or malicious nodes and are excluded from routing. In this work, "trust" is interpreted as a level of uncertainty as described in [69]. In our proposed trust-based forwarder selection framework, a "Multiple Criteria Decision Making" (MCDM) technique called "Technique for Order Preference by Similarity to Ideal Solution" (TOPSIS) [73, 74] is used for quantification of trust relationship into discrete quantities. The proposed framework is then integrated with our enhanced routing protocols for HetMesh for reliable and secure route calculation. The performance of the framework is evaluated through extensive simulation study under hostile networking scenarios with varying number of malicious nodes, node density, node speed, and traffic load. The experimental results exhibit the resiliency of the framework against attacks and thus reliability and security of the corresponding routing protocol get enhanced in terms of Throughput, Packet Delivery Ratio (PDR), Normalized Routing Overhead (NRO), End-to-End Delay, Attack Detection Rate (ADR), False Positive Rate (FPR), False Negative Rate (FNR) etc., in dense as well as in dynamic networks. The proposed

trust-based forwarder selection framework ensures detection of malicious and misbehaving nodes in the network.

1.4.4 A unified next-hop carrier selection framework based on trust and MCDM for assuring reliability, security and QoS in DTN routing

The commonly used metric to select a potential next-hop carrier in DTN routing is the ability of delivering data to the destination, which is estimated as the probability of encountering the destination node or is guided by any other utility parameter derived from social networks in general. The higher the probability or utility of encountering the destination, the more is the competency of the node for delivering data successfully. Although these estimation of delivery probability or utility parameters are reasonable in a congenial (i.e., friendly) wireless environment, however it may not be accurate in a hostile scenario (i.e., in presence of misbehaving nodes). This may even lead a node to select a misbehaving node (both malicious and selfish) as the next-hop forwarder. Misbehaving nodes consume network resources, reduce network performance and availability. Therefore, selection of a next-hop carrier is crucial in a hostile environment for ensuring the reliability and security of the underlaying communication paradigm of DTNs.

The fourth contribution of this thesis proposes a novel trust-based unified framework, called *Multi-Attribute Trust Evaluation and Management* (MATEM) for choosing a reliable next-hop carrier in DTNs. This framework can be flexibly integrated with a large family of existing data forwarding protocols designed for DTN-based communication. MATEM is decentralized in nature, and allows a node to periodically estimate trust value of other nodes based on specific trust measuring criteria and "Multi Criteria Decision Making" (MCDM) technique, known as "Technique for Ordered Priority with Similarity to Ideal Solution" (TOPSIS). The proposed framework also improves network performance, when incorporated with existing routing protocols for DTNs, because honest nodes can avoid working with misbehaving nodes and thus avoid inclusion of them into the forwarding path. Extensive simulations are carried out to demonstrate the suitability and efficiency of the proposed scheme. As per the knowledge goes, the proposed work is the first of its kind that integrates multiple conflicting trust measuring criteria and uses an interdisciplinary technique to learn and compute absolute trust value of each node in DTNs.

The effectiveness and robustness of MATEM against different security metrics, viz., *attack detection*, *false positive* and *false negative* rates are assessed in the presence of bad-mouthing,

good-mouthing, and selfish attacks. The framework efficiency is also evaluated through extensive simulation study and a comparative analysis with other existing frameworks are carried out in terms of different routing metrics, viz., *message delivery ratio*, *delivery latency*, and *delivery cost*. Furthermore, a user experiment is conducted to investigate the impact of MATEM on a real testbed forming a DTN environment. Results generated from simulations and the real testbed verified the usability and user acceptance of MATEM in DTN.

1.5 Organization of Thesis

The thesis work has been documented in the following six chapters:

Chapter 2 presents the adaptive path selection scheme for high throughput heterogeneous wireless mesh networks (HetMesh).

Chapter 3 presents a social metric aware forwarding scheme for delay tolerant networks (DTNs).

Chapter 4 provides a trust-based forwarder selection framework for reliable and secure routing in heterogeneous wireless mesh networks using Multi Criteria Decision Making Techniques (MCDM).

Chapter 5 presents a unified next-hop carrier selection framework based on Trust and MCDM for assuring reliability, security, and QoS in DTN Routing.

Chapter 6 concludes the thesis with summarization of the works done, and suggests the direction for possible future works over the HetMesh and DTNs routings as well as the possible amendments over trust-based frameworks are also conveyed.

2

Adaptive Path Selection for High Throughput Heterogeneous Wireless Mesh Networks

2.1 Introduction

Wireless Mesh Networks (WMNs) are self-organizing, self-configuring, self-healing, self-optimizing, and fault tolerant packet-switched networks [6, 89, 90] that provide last mile broadband Internet connectivity through multi-hop data forwarding. WMNs have two types of nodes: mesh routers and mesh clients. Routers form a static backbone for providing connectivity and coverage to mobile mesh clients. Based on the nodes' functionality, the architecture of WMNs is classified into three categories, viz. *Infrastructure* WMNs, *Client* WMNs, and *hybrid/Heterogeneous* WMNs or *HetMesh*. Heterogeneous WMNs combine the benefits of Infrastructure and Client WMNs, as well as provide simultaneous support for multi-hop access of routers by diverse mobile clients. Though these advantages together favor for high throughput in a HetMesh architecture, but the routing/forwarding capability of resource-constrained mobile clients make the path selection process challenging in heterogeneous and dynamic environments. As such, selection of a suitable next-hop forwarder for improving path selection quality in a HetMesh still remains an open research issue.

Recently, some sophisticated routing protocols have been proposed in the literature for heterogeneous WMNs. In [22], the authors present a mesh routing protocol that guarantees hop by hop bandwidth. A joint approach for routing and rate adaptation has been studied

in [23] where the multi-rate environment has been explored in designing path selection metrics. Opportunistic routing/forwarding has been explored in the literature, like [24] and the references therein, that exploits wireless broadcast environment to reduce path selection overhead. To cope up with the wireless channel dynamics, the authors in [25] propose a greedy path selection protocol for mesh networks.

Almost all the routing schemes, forwarding or path selection protocols proposed in literature inherently assume that nodes in the network are of equal capacity and therefore use a common routing metric to find out the path quality. However, high throughput HetMesh has some salient features that differentiate it from general mesh architecture, and therefore demands for a more sophisticated path selection mechanism.

The objective of this work is to design a unified scheme for high throughput HetMesh, where clients can leverage their full capacities and may act as a potential forwarder if they have sufficient available resources. In this work, enhancements for path selection quality in a high throughput HetMesh are proposed, which can be applied to any existing hybrid routing protocol. The proposed enhancements not only improve path selection quality in a high throughput HetMesh, but also take robust decisions to make the path selection process adaptive. In the proposed scheme, we define a resilient metric to decide the potentiality of mesh clients to act as forwarders. Apart from that, a novel routing metric is designed by combining multiple path selection criteria. The existing hybrid path selection protocol is tuned to augment the proposed metrics. The performance of the proposed scheme is evaluated through testbed as well as large scale simulation results.

The rest of the chapter has been structured in following way. Section 2.2 presents the background study and literature review on mesh routing protocols. The drawbacks associated with these works are listed out, which provide the motivation for the work carried out in this chapter. Our proposed scheme for adaptive path selection for high throughput heterogeneous WMNs has been presented in Section 2.3. Section 2.4 presents the performance evaluation and the comparative analysis of the proposed path selection scheme with Modified Optimized Link State Routing (M-OLSR) [10], Extended Ad hoc On-demand Distance Vector (E-AODV) [11], and Mesh Hybrid Routing Protocol (M-HRP) [20] for it's applicability in HetMesh architecture. The implementation details of the proposed scheme in a real testbed scenario are presented in Section 2.5 followed by the conclusion in Section 2.6.

2.2 Background and Literature Review

The existing routing/forwarding protocols available for general multi-hop and mesh networks can be grouped into three categories: proactive, reactive and hybrid. The basic proactive and reactive path selection protocols for multi-hop and mesh networks, like Ad hoc On-demand Distance Vector (AODV) [1], Optimized Link State Routing (OLSR) [2] and their variants have been well studied in the literature [9, 10, 11].

The work in [10], reported a variation of a link state routing protocol called Modified Optimized Link State Routing (M-OLSR) that has been developed for adaptability in infrastructure based WMN scenarios. M-OLSR is proactive in nature and uses the concept of multipoint relays (MPRs) [91] for overhead optimization. The authors modify traditional OLSR [2] for WMNs that adaptively supports static mesh routers and mobile mesh clients for communication. In M-OLSR, the static backbone routers route the data packets to the destination gateway nodes where mobile clients act as source nodes. M-OLSR optimizes the high overhead issue related to the proactive routing approach but reported with high end-to-end delay in dense and dynamic scenarios.

In another approach [11], traditional AODV protocol has been modified for WMNs and the modified protocol is named as Extended-AODV (E-AODV). E-AODV is reactive in nature and during routing, paths that comprise mobile clients are discarded. A new routing metric called Mesh Router Count (MRC) has been introduced apart from hop count. To evaluate E-AODV's performance and suitability in WMNs, a comparison of the protocol has been carried out with traditional AODV (applied to WMNs) [92] and M-OLSR [10], in terms of throughput, Packet Delivery Ratio (PDR), Normalized Routing Overhead (NRO) and packet end-to-end delay. Simulation results as reported in [11] justify that, though E-AODV attains a satisfactory Constant Bit Rate (CBR) throughput, PDR, and end-to-end Delay, its NRO rises very sharply in comparison to M-OLSR in a sparse network. Whereas, in case of dynamic networks, with increase in node density, M-OLSR performs much better than E-AODV and AODV in terms of throughput, PDR, NRO, but its end-to-end delay is high as compared to E-AODV and AODV. Being a proactive protocol M-OLSR is expected to have less delay time, but the simulation results presented in [11] show a contrast result. This is due to the existence of mobile clients for which the topology changes frequently.

The work in [12], reported with a reactive routing protocol called Mesh Routing Protocol (MRP) that tries to maintain a routing tree between the clients and the gateways of WMNs.

The maintained tree is then used for mirroring the flow of data in the network and tries to eliminate the overhead associated with maintaining direct routes between the clients. According to this scheme, any node in a WMN will only know how to reach one gateway and is reachable only from a gateway node. Any small amount of client-to-client traffic can be routed through the common parent of the clients. The multi-hop communication between the mesh clients are not allowed in this scheme.

In [13], the authors propose extensions to existing ad hoc routing protocols like AODV [1], Dynamic Source Routing (DSR) [3] and SOAR [14], for optimized access to a set of nodes called "net-marks" similar to gateways in WMNs. They evaluated performance of the extended SOAR [14] routing protocol which follows a link state routing approach (i.e., proactive) and showed via simulations that it outperforms both DSR and AODV.

Further, the WMN companies are developing a variety of routing protocols to satisfy their needs. Some of them are proprietary and are held secret [15], while others use well-known ad hoc routing protocols. Firetide uses Topology Broadcast based on Reverse-Path Forwarding (TBRPF) [16], [17]. Other companies rely on the IEEE 802.11 spanning tree protocol for routing at layer 2 which is known as MeshDynamics [18].

However, the existing proactive and reactive routing protocols have the common problem that they are suitable for a specific scenario, and are not generalized for real time application scenarios of WMNs. For instance, proactive routing protocols are suitable for an infrastructure fixed network whereas, reactive protocols works better for mobile and dynamic time varying networks. To cope up with such problems, hybrid routing protocols have been proposed in the literature. Here, we detail some of the existing and recently proposed hybrid routing protocols available in the literature of WMNs.

The IEEE 802.11s standard for WMN proposes Hybrid Wireless Mesh Protocol (HWMP) along with airtime link metric [93] that combines both the proactive and reactive path selection components. IEEE 802.11s defines a new mesh data frame format and has an extensibility framework for routing. The protocol is based on AODV [1] and has a configurable extension for proactive routing towards mesh portals. The HWMP uses MAC addresses and a radio-aware routing metric for the calculation of paths. In [20], a hybrid routing protocol, called Mesh Hybrid Routing Protocol (M-HRP) for WMNs, is presented that combines proactive and reactive components to achieve mesh path selection objectives. The proactive component works at the static backbone, whereas route requests from clients are processed reactively.

In an another approach, Hybrid Routing with Periodic Updates (HRPU) [21] is proposed for WMNs. In HRPU, the mesh portal periodically broadcasts a mesh update message (similar to the route reply message of a reactive protocol like AODV), which allows all nodes to have a route towards the mesh portal. Thus all the nodes proactively maintain the route towards the mesh portal while for the nodes within the mesh network, reactive routing algorithm is used. However, with high node mobility, link breakages occur frequently. Thus on link breakages, the route towards the mesh portal might become invalid causing network performance degradation. In HRPU, proactiveness is provided by the semi permanent maintenance of routes, whereas reactiveness comes when data is to be transmitted within the network.

To summarize, all these available hybrid protocols developed for WMNs improve some parameters however compromise on others. Further, almost all of the routing, forwarding or path selection protocols proposed in literature inherently assume that nodes in the network are of equal capacity and therefore uses a common routing metric to find out the path quality. However, high throughput HetMesh has some salient features that differentiates it from general mesh architecture, and therefore demands for a more sophisticated path selection mechanism.

The salient features of a HetMesh are summarized below;

1. HetMesh shows a hierarchical architecture, where the backbone comprises of fixed infrastructure mesh routers, and the clients are of ad hoc and dynamic in nature. Both the mesh routers and mesh clients may exploit multi-channel and multi-interface capabilities for connecting with the backbone and the outside Internet. Although hybrid routing protocols have been proposed for such hierarchical environments, however the main challenge lies in deciding when the nodes should use proactive component and when reactive one. In most of the existing hybrid protocols, this decision is kept for the network administrator that makes the protocols non-adaptive and configuration dependent.

2. With the advanced direct wireless communication technologies, like Wi-Fi Direct [94], the mobile clients have the capacity to directly communicate to another client without intervening the mesh backbone. Further, many mobile clients with such advanced technologies can act as intermediate forwarders. In such a diverse environment it is challenging to figure out the next-hop forwarder. Several scenarios may exist, like

(a) A mobile client has both a backbone router and another mobile client as potential next-hop. In such a scenario, several issues play around the optimal decision–like capacity of individual nodes, interference near the node, traffic load across different parts of the network, client mobility pattern, energy consumption issues etc.

(b) A router may offload the data traffic to a potential client forwarder if the router is overloaded. Such offloading techniques play an important role in balancing network traffic across the complete service domain.

3. Further, the recent advances in high throughput technologies impose extra difficulties in the design of a good path selection metric. Several technologies may coexist (like IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac etc.) with different sets of access technologies. For example, IEEE 802.11n/ac supports channel bonding for high throughput communication, whereas IEEE 802.11b/g does not. In a HetMesh scenario, it is challenging to handle such technology heterogeneity, and the mobile clients are expected to have such kind of heterogeneity.

Therefore, the research work presented in this chapter addresses these issues of high throughput HetMesh for multi-hop data forwarding by mobile clients and backbone routers in a dynamic environment. The proposed forwarding scheme has combined the multiple path selection criteria (i.e., the technical competency of node in terms of reserve energy, buffer capacity, link capacity etc.) for defining a novel resilient path metric that makes the path selection adaptive in HetMesh environments.

2.3 Proposed Scheme for Adaptive Path Selection in HetMesh

This section proposes a new *Adaptive Path Selection Scheme* (Adapt-PSS), that uses both proactive and reactive approaches for improving path selection quality in a high throughput HetMesh network. The backbone routers in Adapt-PSS use an improved version of OLSR, called M-OLSR [10], for maintaining their routing table in a proactive manner, which is updated during each refresh interval. Whenever a mobile client has packets to transmit, it broadcasts a probe packet to its neighbor nodes requesting their willingness in packet forwarding. The neighbors then reply back with feedback packets informing their willingness to forward traffic in the network. Depending on the received feedback packets, the source node performs additional computation to estimate link quality of willing neighbors. From

the acquired feedback and estimated information, the source node in Adapt-PSS computes path metric adaptively that leads to the selection of a better path in a HetMesh network. The main functionalities of Adapt-PSS are *Neighbor Detection*, *Topology Dissemination* and *Path Determination*, which are detailed below.

2.3.1 Neighbor Detection

In Adapt-PSS, each backbone router detects its one-hop neighbors through periodic exchange of `HELLO` packets. A `HELLO` packet contains the emitting node's own address, link status, willingness to carry traffic, and information about its neighbors in the network. The link status can be `symmetric`, `asymmetric`, or `lost`. Willingness of all routers are set to `TRUE` indicating their willingness to forward traffic in the network. During `HELLO` packet exchange, each router updates its neighbor list with an objective to select some routers as *Multi Point Relays (MPRs)* based on following criteria:

1. The router's link status should be `symmetric`.
2. Its willingness is set to `TRUE`.
3. It covers all its two-hop neighbor set.

MPRs are selected for optimized flooding of control traffic in the network. Each router also maintains an "MPR selector set" of other nodes, which have chosen the designated router as an MPR. An MPR may choose to report only links between itself and its MPR selector set.

2.3.2 Topology Dissemination

An MPR periodically broadcasts `TOPOLOGY_CONTROL` (`TC`) messages, containing own identity and its MPR selector set. Through `TC` messages, each router maintains a *Topology Table*, which records identity of the destination node, identity of the immediate MPR for the destination, a sequence number indicating freshness of information, recording time stamp and a validity time. For each destination, a router maintains at least one entry in the Topology Table. `TC` messages provide link-state information to backbone routers for maintaining partial topology graph of the network. Using this partial topology graph, optimal paths from a node to any reachable destination in the network are computed.

The outcome of neighbor discovery and topology dissemination functionalities of Adapt-

PSS enables each backbone router to maintain a *Routing Table* describing destination node address, next-hop node address and path quality to reach the destination, which allows it to route data to destination node in the network. The calculation of path quality is described in the subsequent discussions.

2.3.3 Path Determination

A mobile client in Adapt-PSS broadcasts a `PROBE_REQUEST` packet to gather information about its neighbors and adaptively establishes a path on demand whenever it has data packets to transmit. Upon receiving the `PROBE_REQUEST` packet, each neighbor replies back with a `PROBE_RESPONSE` packet. The `PROBE_RESPONSE` packet contains a forward willingness (viz. `FWD_WLNG`) field, which the sender adaptively computes based on its own present load and energy conditions, as in Equation (2.1):

$$\texttt{FWD\_WLNG}_j \;=\; \alpha \times \frac{\mathcal{L}_{\text{max}}}{\mathcal{L}_j} + (1-\alpha) \times \frac{\mathcal{E}_j}{\mathcal{E}_{\text{max}}} \tag{2.1}$$

where, node j is a neighbor of the mobile client, and α is a balancing factor $(0 < \alpha < 1)$ that balances weight of load and energy. $\mathcal{L}_j$ is the traffic load of node j whereas $\mathcal{L}_{\text{max}}$ is the maximum load. Similarly, $\mathcal{E}_j$ is the energy consumption factor of node j and $\mathcal{E}_{\text{max}}$ is the maximum (initial) energy consumption factor (in general, it is 1 when battery is fully charged). The target is to minimize $\mathcal{L}_j$ while maximize $\mathcal{E}_j$ constraint to their respective normalization through the maximum possible values. The calculations of $\mathcal{L}_j$ and $\mathcal{E}_j$ are as follows.

$$\mathcal{L}_j \;=\; \frac{\text{No. of Buffered Packets}}{\text{Buffer Size}} \tag{2.2}$$

and,

$$\mathcal{E}_j \;=\; \begin{cases} \mathcal{B}_{\text{init}} & \text{when } \mathcal{B}_t = \mathcal{B}_{\text{init}}; \\ \dfrac{\mathcal{B}_t}{\mathcal{B}_{\text{init}} - \mathcal{B}_t} & \text{when } \mathcal{B}_t \neq \mathcal{B}_{\text{init}}; \end{cases} \tag{2.3}$$

where $\mathcal{B}_{\text{init}}$ is the initial battery power and $\mathcal{B}_t$ is the battery power at time t after the battery is last recharged.

On receipt of the `PROBE_RESPONSE` packets, the client checks the `FWD_WLNG` field of the received packets. The packets having `FWD_WLNG` field values above the pre-defined thresh-

old are further processed for next-hop forwarder selection and others are immediately discarded. The selection is based on a new parameter computed from two attribute-components; node willingness to participate in the forwarding procedure (viz. FWD_WLNG) and the link quality estimates (viz. LINK_EST). This proposed parameter for path selection quality is termed as *Multi-Attribute Adaptive Path Metric* (MAAPM), which is defined as follows:

$$\texttt{MAAPM}_j \;=\; \beta \times \texttt{FWD\_WLNG} + (1-\beta) \times \texttt{LINK\_EST} \tag{2.4}$$

where β is a balancing factor $(0 < \beta < 1)$ that balances weight of FWD_WLNG and LINK_EST.

The calculation of link estimate is based on two parameters - the standard IEEE 802.11s HWMP airtime link metric [95] and the estimated link capacity. Airtime link metric computes the propagation and transmission time for a test packet considering the channel error rate. To handle the heterogeneity introduced by high throughput wireless networking standard, we use the link capacity. The link capacity of a link l, $\mathcal{C}_l$, is computed using Equation (2.5):

$$\mathcal{C}_l \;=\; \frac{Q \times C_Q}{L_l} \tag{2.5}$$

where, Q is the number of available channels, C_Q is the capacity per channel, and L_l is the number of virtual links in transmission range of l. The number of virtual links can be computed by overhearing the channel in promiscuous mode.

Let $\mathcal{A}$ be the airtime link value computed by a mesh node. Then LINK_EST is calculated as follows:

$$\texttt{LINK\_EST} = \mathcal{C}_l \times \mathcal{A} \tag{2.6}$$

Intuitively, LINK_EST provides the volume of data that can be transferred over a link in a single shot.

After computing MAAPM for all compatible neighbors, the node having maximum MAAPM value is chosen as the next hop forwarder of data packets. This process continues until a router is selected as the next-hop forwarder, which decides the path to destination based on its proactive routing table, as already detailed in Section 2.3.1 and Section 2.3.2.

The processes of forwarder selection and path determination in Adapt-PSS are shown as Algorithm 1, which are evaluated in next section through extensive simulations.

Algorithm 1: Forwarder selection and path determination in Adapt-PSS

1. Each source node (mobile client) broadcasts a `PROBE_REQUEST` packet if it has data packets to transmit
2. On receipts of `PROBE_REQUEST`; each neighbor adaptively computes `FWD_WLNG` based on its own present load and energy conditions
3. Each neighbor replies back with a `PROBE_RESPONSE` packet containing `FWD_WLNG` field
4. On receipt of `PROBE_RESPONSE`, the source checks the `FWD_WLNG` field of the received packets
5. The neighbors whose `FWD_WLNG` field is above the pre-defined threshold are considered compatible for next-hop forwarder selection and others are immediately discarded
6. The *Multi-Attribute Adaptive Path Metric* (`MAAPM`) is computed for all compatible neighbors based on their `FWD_WLNG` and link quality estimates viz., `LINK_EST`
7. The neighbor node having maximum `MAAPM` value is chosen as the next-hop forwarder of data packets
8. This process continues until a forwarder is selected whose next-hop address is the destination of the data packets
9. End

2.4 Simulation of Adapt-PSS and Performance Evaluation

This section presents the simulation study of the proposed path selection scheme along with a detail analysis of the experimental results. Section 2.4.1 presents the set of parameters used for the simulation study and the results are illustrated in Section 2.4.2.

The performance evaluation of Adapt-PSS is carried out with ns-2 simulator [96] and a comparative analysis with M-OLSR [10], E-AODV [11], and M-HRP [20] have been studied to find it's applicability in HetMesh architecture. The protocols available in [10], [11], and [20] are re-simulated in this work to enable comparisons with Adapt-PSS in ns-2 and comparative results have been illustrated. Extensive simulations are carried out to evaluate

Adapt-PSS's performance in terms of throughput, Packet Delivery Ratio (PDR), Normalized Routing Overhead (NRO), and end-to-end delay in a dense and dynamic network with varying traffic load and mobility rate.

Table 2.1: Parameters for Simulation Model

Simulation Parameters	**Value**	**Simulation Parameters**	**Value**
Simulator	ns-2 (version 2.35)	Mobility Speed	1 m/s - 5 m/s
Operating System	Ubuntu 13.10	Pause Time	5 s
Simulation Time	100 s	Traffic Type	CBR
Simulation Area	1000 m×1000 m	Total CBR Flows	25
No. of Nodes	50	Data Payload	512 bytes
Transmission Range	250 m/s	Packet Rate	20 pkt/s-60 pkt/s
Interference Range	550 m	Mac Layer	802.11 DCF with RTS/CTS
Node Placement Dist.	200 m	Radio Frequency	2.4 GHz
Movement Mode	Random-Waypoint	Radio Channel Rate	2 Mbps
RF Propagation Model	Two-RayGround	Antenna	Omni-directional

2.4.1 Simulation Environment

Adapt-PSS, M-HRP, E-AODV and M-OLSR are built on top of IEEE 802.11 MAC model of ns-2 and random waypoint model is adopted for driving mobile clients. In order to gain good confidence in the results, we run simulations 10 times with different seed values to obtain mean value of the above mentioned parameters. Table 2.1 depicts the value set for all simulations. The topology of a dense network is generated by placing 16 static routers at 200 meters interval to form a rectangular grid, where 34 mobile clients are allowed to move within the topology area. The 4 routers at the border position of the grid are selected as gateway routers. To analyze the protocols' scalability with network dynamics and traffic load, simulations are performed by varying mobility rate from 1 m/sec to 5 m/sec, and varying traffic load from 15 packets/sec to 30 packets/sec respectively, while keeping the number of Constant Bit Rate (CBR) flows as 25.

2.4.2 Results and Analysis

From Figure 2.1, Figure 2.2 and Figure 2.3, it has been observed that the aggregate throughput of Adapt-PSS, M-HRP, M-OLSR, and E-AODV show resilience to increasing traffic load with low mobility. This is due to closer association and availability of nodes in the network causing minimal chances of link breakages. With increase in mobility, throughput

of all protocols degrades, but in Adapt-PSS, it degrades gracefully than others. This is due to the consideration of multiple attribute quality for next-hop forwarder selection in Adapt-PSS, where a node having better energy and channel capacity is chosen as a forwarder. The other protocols mostly aim for finding a static router as their next-hop.

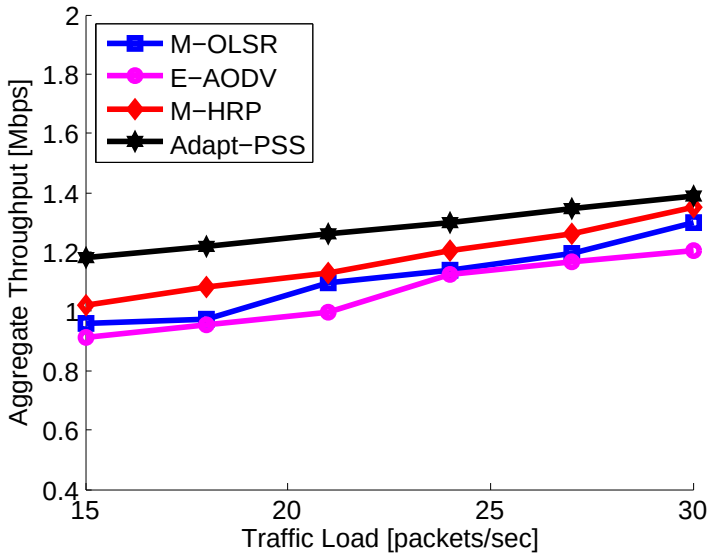


Figure 2.1: Aggregate throughput Vs Traffic Load in 1 m/s mobility rate

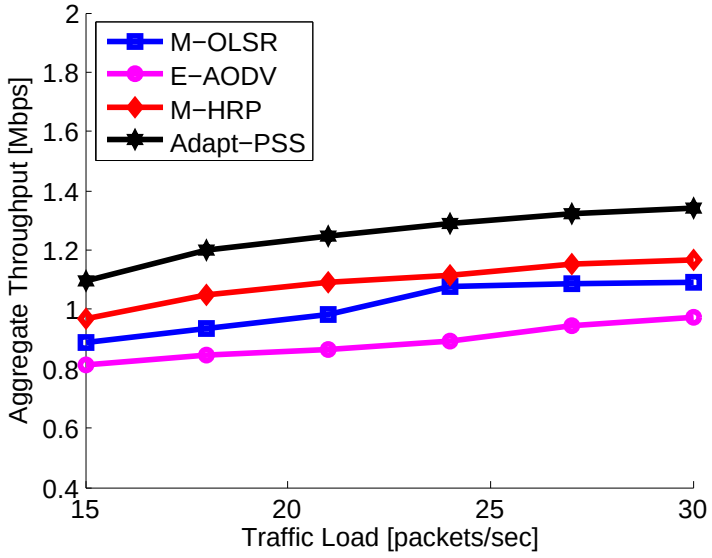


Figure 2.2: Aggregate throughput Vs Traffic Load in 3 m/s mobility rate

Figure 2.4, Figure 2.5 and Figure 2.6 show that as traffic load intensifies, PDR decreases for all protocols because of increased intra-flow and inter-flow interference and contention. Moreover, with increase in mobility rate, PDR drops for all protocols because clients lose connectivity with their next-hop forwarders/routers more, often leading to frequent link

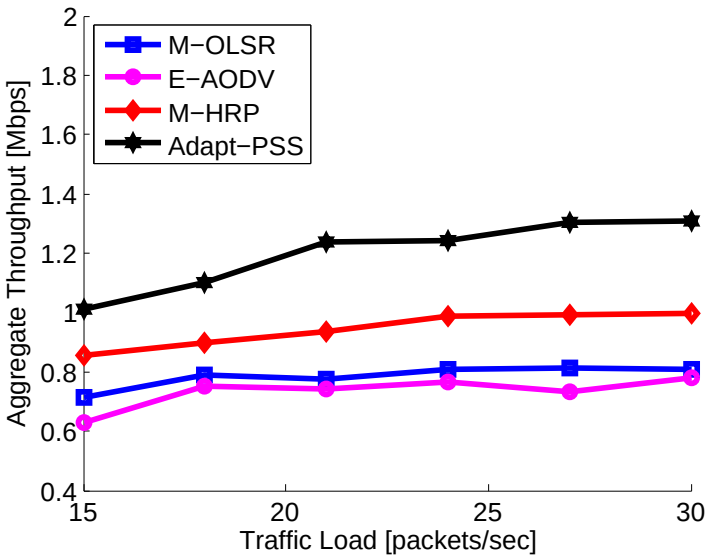


Figure 2.3: Aggregate throughput Vs Traffic Load in 5 m/s mobility rate

breaks and data loss. However, there is an insignificant degradation of PDR for Adapt-PSS, as its path computation involves link capacity. So chances of packet drops due to link breakage, buffer overflow and low energy are minimized. The decrease in PDR for M-HRP with increase in mobility rate is due to the increase in hop count, which, in turn, increases forwarding overhead and delay resulting in packet drops. The decrease in PDR of M-OLSR and E-AODV is due to the possibility of transmission via a non-refreshed path from its one-hop router.

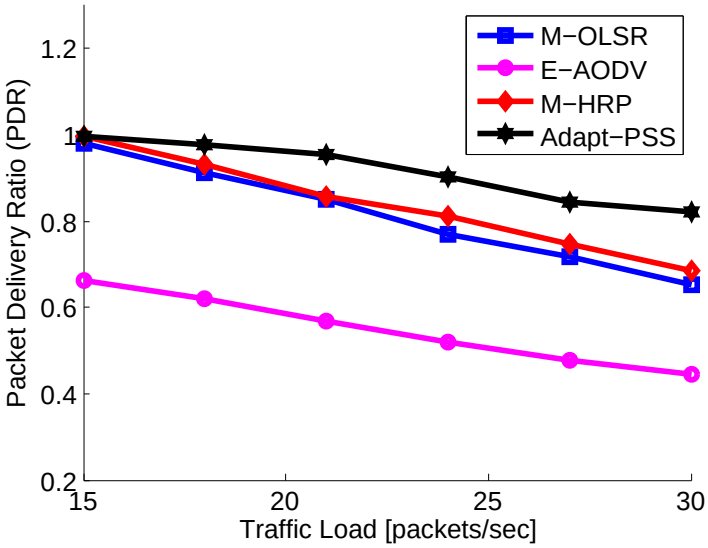


Figure 2.4: PDR Vs Traffic Load in 1 m/s mobility rate

Figure 2.7, Figure 2.8 and Figure 2.9 depict NRO as a function of traffic load and mobility

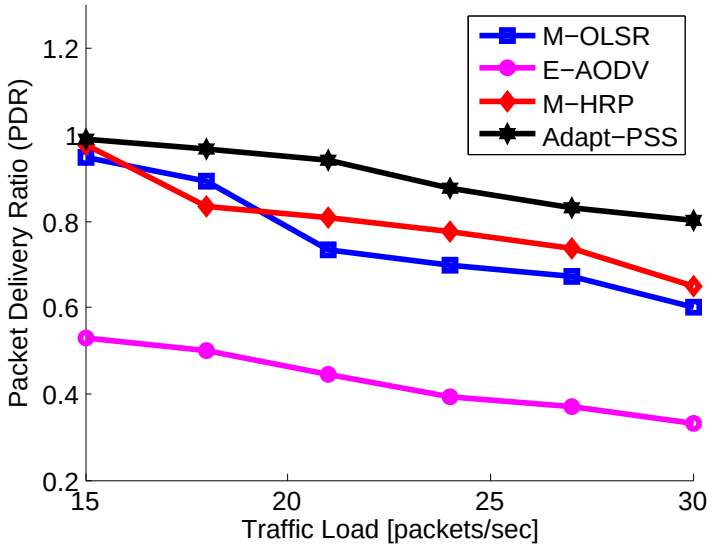


Figure 2.5: PDR Vs Traffic Load in 3 m/s mobility rate

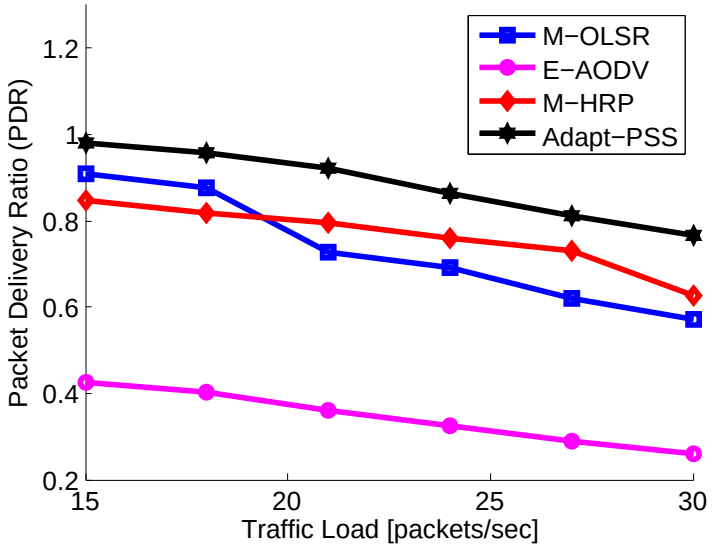


Figure 2.6: PDR Vs Traffic Load in 5 m/s mobility rate

rate for the four protocols. It has been observed that NRO of M-HRP and E-AODV rises with increase in mobility rate. The main reason behind this increase is the corresponding increase in loss of packets that triggers path discovery. In E-AODV and M-HRP, destination node generally replies with a single `RREP` packet per route discovery. However, if `RREP` is not received, `RREQ` packet is retransmitted for pre-defined times. In this process, packets are dropped due to limited buffer capacity of clients. The situation worsens with increasing traffic load, because congestion forces nodes to declare link failure although the links still exist causing generation of `RERR` packets. This leads to more routing overhead for repairing

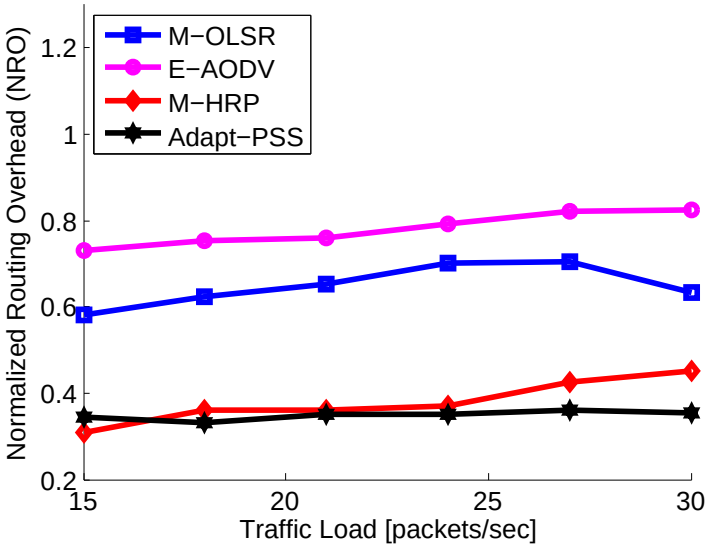


Figure 2.7: NRO Vs Traffic Load in 1 m/s mobility rate

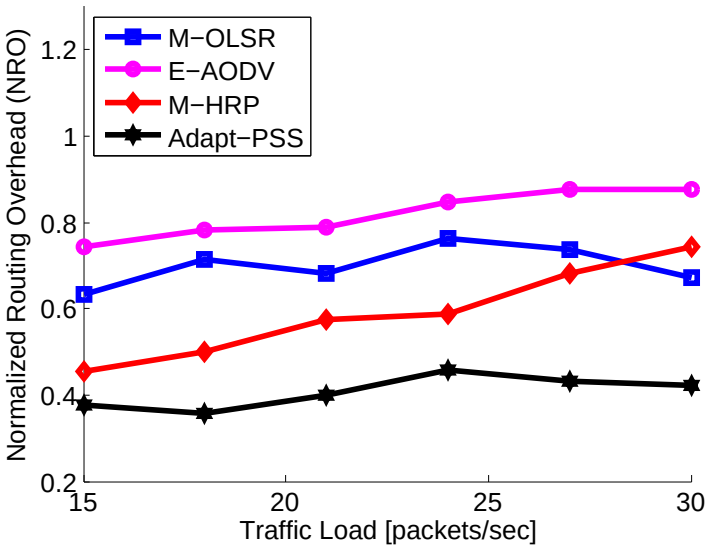


Figure 2.8: NRO Vs Traffic Load in 3 m/s mobility rate

broken links in both M-HRP and E-AODV. However, NRO of Adapt-PSS does not increase significantly due to its adaptiveness in link quality estimation and availability of multi-hop capability of clients, which further reduces the chances of packet drops and repeated estimation process. NRO of M-OLSR shows immunity to increased traffic load because of its proactive nature.

The end-to-end delay increases linearly with increase in traffic load and mobility rate for both Adapt-PSS and M-HRP, which is evident from Figure 2.10, Figure 2.11 and Figure 2.12. Increase in end-to-end delay in M-HRP is due to the queuing delays. Whereas, the reason

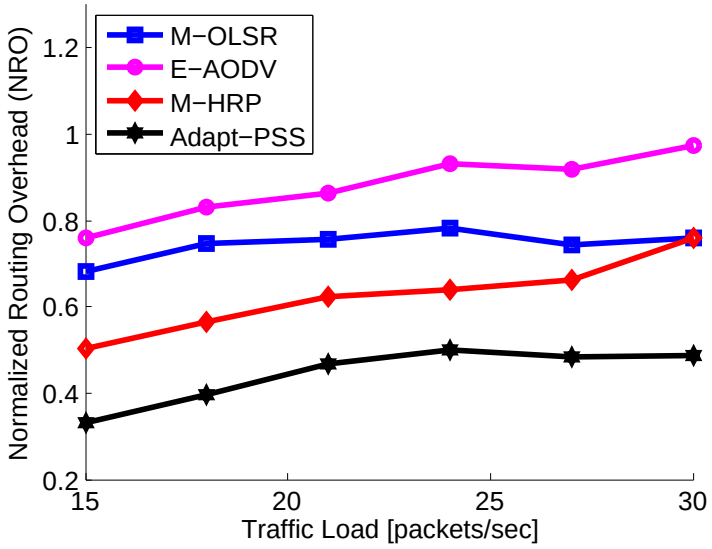


Figure 2.9: NRO Vs Traffic Load in 5 m/s mobility rate

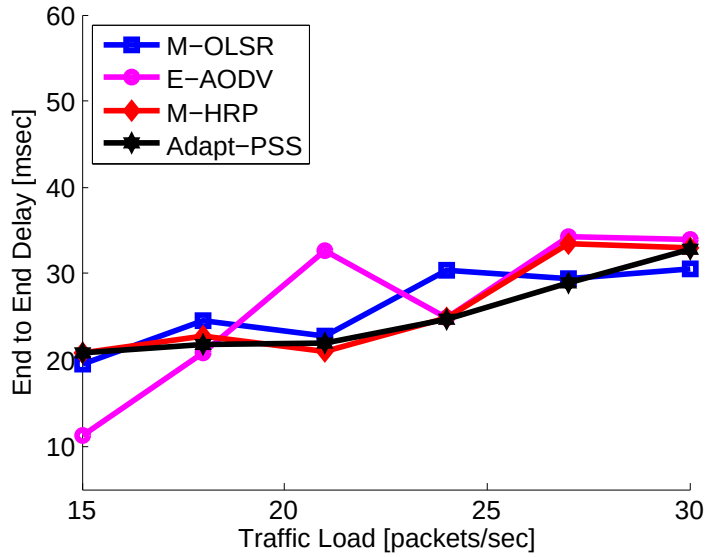


Figure 2.10: End-to-end delay Vs Traffic Load in 1 m/s mobility rate

for increase in delay in Adopt-PSS is that, it selects a next-hop forwarder on the basis of feedback and estimated components in a hop-by-hop manner for path determination. End-to-end delay of M-OLSR is minimum due to its proactive route maintenance. Contrasting result by E-AODV is due to its on-demand path determination.

The simulation results of Adapt-PSS are further validated through its testbed implementation as discussed in the next section.

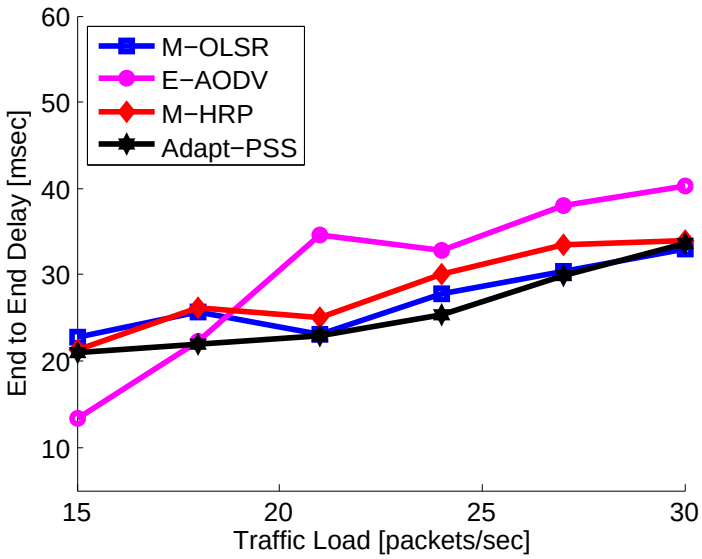


Figure 2.11: End-to-end delay Vs Traffic Load in 3 m/s mobility rate

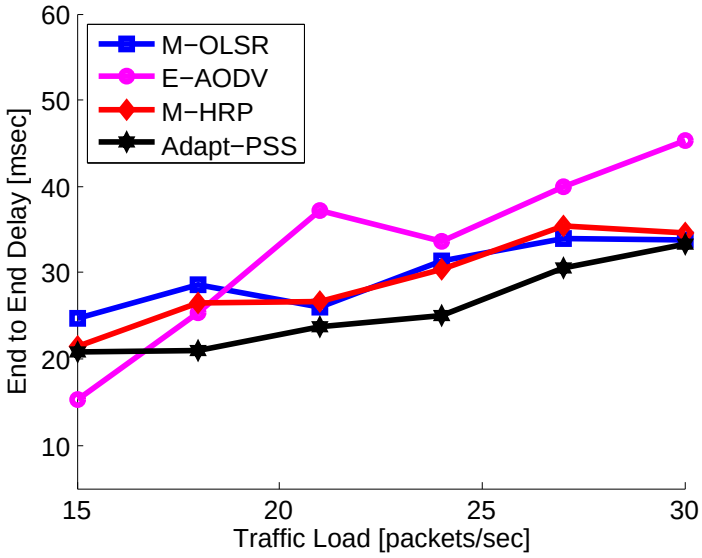


Figure 2.12: End-to-end delay Vs Traffic Load in 5 m/s mobility rate

2.5 Implementation of the Proposed Scheme in a Testbed and Performance Analysis

This section details the underlaying system model for testbed implementation of Adapt-PSS and it's implementation details. Further, a comparative performance analysis of the proposed scheme with M-HRP [20], M-OLSR [10], E-AODV [11] and HWMP [93] is also presented in Section 2.5.2.

2.5.1 System Model

The proposed work focuses on next-hop forwarder selection and subsequent path determination in a high throughput HetMesh architecture, where clients can communicate among themselves in a multi-hop fashion without involving backbone routers. The backbone routers are static, non power-constrained, and maintain their own routing Tables proactively. On the other hand, the clients are mobile, energy-constrained and are enabled with Wi-Fi Direct mode to connect in a peer-to-peer manner. The Wi-Fi Direct mode has the ability to connect heterogeneous clients, and allows direct data transmission among themselves with minimal setup. Such feature enables multi-hop communication between the clients, which improves connectivity and coverage of a high throughput HetMesh.

We implement Adapt-PSS in a small scale testbed, comprising of 6 wireless access points configured in a mesh router scenario, and 12 clients nodes. The network is a heterogeneous one, where the access points are Asus RT-AC3200 high throughput wireless routers, and the client nodes are of two categories - 8 nodes are Asus USB-AC56 IEEE 802.11ac client adapters, and 4 nodes are mobile phones (Moto X) supported with IEEE 802.11ac communication. The access points are equipped with standard Linux kernel with open source `asuswrt-merlin` [97] device drivers. The IEEE 802.11ac USB client adapters also work in standard linux platform (Ubuntu 14.04.2). The mobiles phones are equipped with android 4.4 (kitkat) with high throughput wireless supports. The 802.11ac routers form a high speed wireless mesh backbone through open source `open80211s` [98] supports.

The proposed path selection protocol, along with M-HRP [20], M-OLSR [10], E-AODV [11] and HWMP [93] are implemented in the Linux kernel. In our set-up, the mobile phones are only traffic producers or traffic consumers and they do not forward any data traffic. However, the USB client boards can participate in the forwarding procedure if they have sufficient amount of resources, as discussed in the proposed Adapt-PSS mechanism. Both the USB clients and the phones are mobile devices. One of the mesh routers in the backbone is connected with the outside Internet through Gbps Ethernet.

2.5.2 Results and Analysis

We generate two types of traffic through `Seagull` multi-protocol traffic generator - traffic between two clients, and traffic between clients to the mesh gateway. The mean traffic generation rate for every client is 3 Mbps on average (when they are using a video streaming

application) or they utilize the full bandwidth by elastic traffic application (large FTP file transfer). The streaming and the elastic application has been distributed among the client nodes in $20\% - 80\%$ ratio. We measure aggregate throughput, PDR, NRO and end-to-end delay with varying mobility.

Table 2.2: Testbed Results (Mobility = 3 m/s)

Protocol	Throughput (Mbps)	PDR	NRO	Delay (ms)
E-AODV	75	0.51	0.72	6.1
M-OLSR	91	0.73	0.546	5.4
M-HRP	123	0.82	0.612	3.5
HWMP	128	0.81	0.581	3.8
Adapt-PSS	156	0.92	0.312	1.9

Table 2.3: Testbed Results (Mobility = 6 m/s)

Protocol	Throughput (Mbps)	PDR	NRO	Delay (ms)
E-AODV	35	0.31	0.78	8.4
M-OLSR	41	0.53	0.59	7.37
M-HRP	73	0.72	0.63	4.18
HWMP	78	0.71	0.57	3.9
Adapt-PSS	96	0.82	0.38	2.14

The results, shown in Table 2.2 and Table 2.3, indicate that Adapt-PSS efficiently uses `MAAPM` to increase the throughput significantly in different mobility rates. The end-to-end delay also confirms minimal contention for physical wireless media due to its consideration of optimal link capacity in `MAAPM`. The testbed results are in accordance with the simulation results, in which Adapt-PSS shows notable improvements in its NRO as compared to other existing protocols. However, due to the absence of any inter-flow interference in the testbed, the improvement in PDR and end-to-end delay is notably higher in the testbed than in the simulation results.

2.6 Conclusion

HetMesh is a hierarchical architecture supporting heterogeneous and dynamic environment, where the path selection process is expected to be adaptive to provide high throughput. This work of this chapter proposed Adapt-PSS, a unified path determination scheme, which has incorporated the novel resilient path metric `MAAPM` to take robust decisions for

improving path selection quality in high throughput HetMesh. The novel path metric is defined by combining multiple path selection criteria to leverage the resource availability of clients for acting as potential forwarders. Adapt-PSS has been evaluated through testbed and extensive set of simulations. The performances of Adapt-PSS have been found to get enhanced compared to the existing routing protocols of mesh networks, and have shown more resilience to increased traffic load and client mobility rate. The performance analysis of the proposed path selection mechanism shows on the average $30\% - 50\%$ improvement in average throughput, while also improving other performance metrics. Moreover, the performance results also inferred the scalable nature of Adapt-PSS. Excellency in these qualities of Adapt-PSS makes it a worthy path selection scheme for public wireless access scenarios of high throughput HetMesh, supporting hundreds of mobile users. In the next chapter, we have addressed the issues of forwarder selection in Delay/Disruption Tolerant Networks (DTNs) and have proposed a novel seasonality aware next-hop carrier selection in social-based DTNs.

3

Seasonality aware forwarder selection in social-based delay tolerant networks

3.1 Introduction

Intermittently connected Mobile Ad hoc Networks (MANETs) lack contemporaneous end-to-end paths from source to destination. Message delivery in these networks must be delay tolerant, and so these networks are often called as Delay Tolerant Networks (DTNs). DTN was originally developed for Inter Planetary Networks (IPNs), but later its applications have been realized in terrestrial mobile networks such as Vehicular Ad hoc Networks (VANETs) [99], Pocket Switched Networks (PSNs) [100], Mobile Social Networks (MSNs) [101], which are characterized by intermittent connectivity, frequent link disruption, existence of non-contemporaneous end-to-end path, long and unpredictable communication latency, etc. To deal with intermittent connectivity, DTNs follow a message propagation scheme referred as *store-carry-and-forward* [102], where intermediate nodes (known as carriers) store and physically carry buffered messages until they get in contact with the destination or a suitable next-hop carrier. In this scheme, each node independently makes forwarding decisions for opportunistic message exchange between them when they are in communication range of each other. In most of the terrestrial DTN applications, the mobile nodes/devices are carried and used by people and thereby making forwarding decision based on peoples' social behavioral perspectives. So, a class of DTN forwarding, namely

social based DTN forwarding algorithms [43] have emerged, which exploit social network properties in DTN forwarding. Our work in this chapter proposes a **S***easonality* **A***ware* **S***ocial Based DTN Forwarding (SAS)* mechanism, which capitalizes on seasonal behavior in human contacts.

Popular social based DTN forwarding techniques [43] usually exploit three social network metrics: similarity between node-pairs [44], centrality of a node [45], and community of nodes [46]. Intuition behind use of these three metrics are: (i) similar nodes meet each other frequently, so a node similar to the destination node has better delivery probability of the message; (ii) central nodes act as hub, and are reachable to other nodes; and (iii) nodes inside a community meet frequently, so forwarding the message to a node that resides within the destination's community increases the chances of message delivery. SimBet [50] is a social based DTN forwarding technique which has utilized similarity and centrality metric, whereas BubbleRap [51] has exploited centrality metric and community structure. Lack of infrastructure in DTN forces individual nodes to take forwarding decisions independently through message exchange. Unavailability of a centralized view of the network limits the social based DTN forwarding techniques to use only locally calculable social network metrics. However, advanced social network metrics, such as random walk similarity measure [44], betweenness centrality measure [45], community detection algorithms [46] are global in nature, and can not be directly applied to DTN forwarding. So, approximated versions of the global metrics have been devised for forwarding in DTNs. The authors in SimBet [50] have used an approximated version of betweenness centrality called ego-betweenness centrality [103], that calculates the betweenness centrality of each node in their respective ego networks. BubbleRap [51] 's approximation of betweenness centrality has been a modified version of degree centrality and has used a distributed community detection algorithm for DTNs [104]. Further, it has been observed that, SimBet and BubbleRap dynamically calculate the social relationship between the nodes to choose the best relay node. SimBet models the relationship between the nodes as binary and does not consider the relative strength of its neighbors. To justify the reason, the authors of SimBet argue that ego betweenness has high correlation with sociocentric betweenness . However, by analyzing the different mobility traces [105, 106] we found that the correlation of ego betweenness and social betweenness is not that high but correlation of ego betweenness and sociocentric betweenness of a node inside a community has very high correlation as shown in Table 3.1. Moreover, in their work, the small world created by the network of mobility traces also have very less diameter (< 2)). Again, BubbleRap uses the concept of sociocentric betweenness

centrality which requires the knowledge of the whole network, which in reality is not possible in DTN. Therefore, these issues of the existing state-of-the-art routing protocols of social based DTNs motivate us to observe evidences of seasonal behavior in node contacts in real mobility traces and exploit it to devise a novel seasonality aware similarity measure.

Table 3.1: Characteristics of the mobility traces

Trace	#Nodes	#Edges	Average Degree	Average Clustering Co-efficient	Average Shortest Path Length	Co-relation of Sociocentric Betweenness and Ego Betweenness	
						Whole Network	Within Community
Reality	96	3085	64	.816	1.324	.75	.984
Sassy	25	155	12	.712	1.503	.88	.987
Cambridge	36	541	30	.892	1.141	.608	.990

In our work, we model the contact history between node-pairs to formulate tie-strength which preserves seasonality of human contacts. Traditional approaches to model tie-strength [53, 54, 55, 56] use variants of average separation duration between node-pairs. We observe strong seasonality, i.e., repetitive contact pattern in real mobility traces and exploit it to formulate tie-strength. Our model measures the tie-strength as weighted average of separation duration and a seasonality aware contact strength. Based on Katz [107] similarity index we define a weighted similarity index between two nodes. Our motivation of using Katz similarity metric has been its inherent property of giving more importance to the direct contacts over the indirect ones. By analyzing real mobility traces, we find that although ego-betweenness centrality is not a good substitute for sociocentric/global betweenness, but it can accurately approximate global betweenness within communities. Our proposed DTN forwarding technique SAS exploits the proposed weighted Katz based seasonality aware similarity measure and ego-betweenness centrality, where the similarity value effectively deals with intra-cluster forwarding and ego-betweenness drives the inter-cluster forwarding. We adapt the utility proposed in SimBet, which exploits similarity and centrality, and propose the Seasonality aware DTN forwarding algorithm SAS. Finally, we simulate our work on real mobility traces to demonstrate the effectiveness of SAS over state-of-the-art social based DTN forwarding algorithms: SimBet and BubbleRap.

The rest of the chapter has been structured as follows. Section 3.2 discusses related works on social based forwarding in DTNs. The drawbacks associated with these works are listed out, which provide the motivation for the work carried out in this chapter. Our proposed seasonality aware social based forwarding in DTNs has been presented in Section 3.3. Section 3.4 presents the performance evaluation and analysis of the proposed social based forwarding scheme with the benchmark SimBet [50] and BubbleRap [51] to validate its effectiveness in attaining routing objectives. Finally, in Section 3.5 we conclude our work.

3.2 Background and Literature Review

This section introduces the different approaches of routing techniques available in the literature of DTNs with a special focus on the social based forwarding techniques.

The routing protocols in DTNs can be broadly classified into two categories: *flooding* and *forwarding* [33]. The protocols in the flooding family induce multiple "replicas" of each message in the network without considering the potentiality of the candidate node for being selected as a next-hop carrier [108, 35, 36, 109]. In this routing approach, a source node tries to send all its' messages to its' neighbors if they do not have the copy of the messages. This approach does not require to store any past information about the routing or mobility of the nodes. So, flooding is the obvious choice when no information is known in advance about the movement of the nodes or about the topology of the network.

In [108], the authors have proposed "Epidemic routing" as one of the basic flooding based routing protocol in DTNs. In Epidemic, a node floods the messages to it's neighbor nodes who does not have a copy of the message. In this protocol, whenever two nodes have an encounter, they exchange their summary vector which contains the IDs of the messages they are carrying. After comparing the summary vector, each node determines the messages they are not carrying which the other nodes have and requests for those messages. Depending on this request message transfer is done between the nodes. Random pairwise exchange of messages are used to ensure eventual message delivery. This process of continuous replication flood the network with same copy of messages to guarantee maximum delivery ratio in presence of infinite storage availability for all the nodes in the network. However in reality, nodes have limited storage capacity, and a limited number of messages can be stored. Flooding the network with messages causes high overhead in term of storage and power spent on transmission and reception. This causes the degradation of network performances. In an another approach called "Two-Hop Forwarding" [110], each node is assumed to encounter every other node for some short duration of time. Within this duration, the source node replicates each message to the first encountered node and the messages are stored until they come in contact with the destination. In this protocol, routing overhead is reduced at the cost of increased message delivery latency. In addition, "Spray and Wait" [109] is a controlled flooding based routing protocol that requires no knowledge about the network. Unlike epidemic it limits the number of message copies to be forwarded in the network. The protocol works in two phases i) *spray* and ii) *wait*. In spray phase the source spreads $\mathcal{M}$ copies of the messages in the network. If the destination is not found in spray phase,

then the relay nodes having message copies will enter into a wait phase in which they wait until the messages are delivered to the destinations directly. Relay nodes do not make any additional copies of the message, in turn reducing the resource usage.

Though, these protocols in the flooding family achieve good delivery ratio and less delivery latency, but flooding the network with duplicate messages cause high network overhead in term of storage and power spent on transmission and reception. These cause congestion leading to network performance degradation. So, another class of routing approaches called "forwarding-based" have been explored to restrict the generation of bundle replicas in the network.

The protocols in the forwarding family calculate an utility metric based on "knowledge" to qualify the candidate node as the next hop carrier on the routing path. A single copy of each message is forwarded to the qualified node. Most of these knowledge-based protocols select a suitable next-hop carrier based on contact history of potential carriers [37, 38], knowledge about traffic patterns in the network [39] or on probability of encountering the destination node [40]. Furthermore, some of them have used multi-copy spraying mechanisms to improve reliability amidst intermittent connectivity [41, 42].

In the basic forwarding based protocol called "First Contact" (FC) [36], the source node tries to forward the message to one of the randomly selected link among all the current contacts. The authors have tried to improve the performance of the protocol by forwarding the message in a direction closer to the intended destination node. To avoid the routing loop, a path vector has been proposed. In this scheme a single copy of each message is maintained in the network.

In an another approach, the Probabilistic Routing Protocol using History of Encounters and Transitivity (PRoPHET) [35] uses utility based replication for delivery of messages. PRoPHET uses history of encounter information to calculate the utility metric of a node. In this protocol, each source node calculates its delivery probability to every other node in the network. These probability values are updated on every contact for each known destination. The delivery probability is aged by a factor over time. It also uses, transitive relation to update the delivery predictability of a node, with whom it is not directly connected. In Rapid [111], a node calculates the utility value of each message that is present in its buffer and this utility value decides in which order it should be relayed to the next node. RAPID derives a per-packet utility function from the routing metric. At a transfer opportunity, it replicates a packet that locally results in the highest increase in utility. To calculate this

utility value, it first estimates the delivery delay of the message. This estimation is based on the two or three hop's information. This limits the estimation because the destination may be present beyond two or three hops.

Recently, social based routing is relatively a new approach and has become popular for addressing the routing problem in DTNs. It is based on the observation that in most of the terrestrial DTN applications people are carrying mobile devices (like Pocket Switched Networks, Mobile Social Networks etc.) and thereby making forwarding decision based on peoples' social behavioral perspectives. In social based DTN applications, hand-held mobile devices exchange information. The inherent social property of DTN has encouraged contemporary researchers in exploiting social metrics to devise forwarding techniques for efficient routing. So, a class of DTN forwarding, namely *social based DTN forwarding* algorithms [43] have emerged, which exploits social network properties in DTN forwarding. Social based DTN forwarding has been popular in DTN specific applications like vehicular networks, mobile social networks, pocket switched networks etc. In such application domains, people carry mobile devices, whose behaviors are unpredictable from social aspects as well as from ad hoc networking aspects. Zhu et. al. [43] and Wei et. al. [112] have provided two recent surveys on social based DTN forwarding techniques. "Centrality", "Similarity" and "Community" have been the most effective social network metrics used for DTN forwarding.

Authors in [47, 48, 49] explored the usefulness of community detection algorithms in DTN forwarding. The motivation of using communities has been: if the carrier encounters a node which belongs to the destination's community, the message will be delivered with high probability. The authors in [47, 48, 49] explored the possibility of community detection and interest profile based forwarding algorithms in DTNs. In these approaches, messages are forwarded to the encountered node if it belongs to the same community as the destination node or if it's interest profile matches with the destination node's interest profile. The shortcoming of these approaches is that they do not capture the dynamics of social relations among the nodes.

In an another approach, SimBet [50] has exploited ego-betweenness centrality and similarity to forward messages in DTN. Central nodes work as hubs and are reachable to all other nodes in the network, and nodes similar to the destination contacts with it frequently. However, the shortcoming of SimBet is that, the authors model the relationship between the nodes as binary and does not consider the relative strength of its neighbors.

Again, BubbleRap [51]'s approximation of betweenness centrality has been a modified version of degree centrality and it has used a distributed community detection algorithm for DTNs [104]. The proposed betweenness centrality of BubbleRap requires the knowledge of the whole network, which in reality is not possible in DTN.

Another set of social based forwarding techniques have exploited the concept of tie-strength [52]. Few of these can be found in [53, 54, 55, 56]. These techniques have modeled the change in contact patterns during time, and predicted strength of social relationships between node-pairs. The authors in [53, 54, 55, 56] have failed to model the dynamic changes in contacts from human behavioral perspectives.

Therefore, these issues of the existing state-of-the-art routing protocols of social based DTNs motivate us to observe evidences of seasonal behavior in node contacts in real mobility traces and exploit them to devise a novel seasonality aware similarity measure. Our work has incorporated seasonality behavior of human contacts into tie-strength towards DTN forwarding. To the best of our knowledge, our work is the first one to exploit seasonality behavior of human contacts in DTN forwarding.

3.3 Proposed Seasonality-aware Forwarding Scheme

Here we present our **S**easonality **A**ware **S**ocial Based DTN Forwarding (SAS), a DTN forwarding algorithm which exploits seasonal behavior of human contacts. Our proposed measures of seasonality aware "tie-strength" is detailed in Section 3.3.1. The modified version of "similarity", and "centrality" measure with incorporation of seasonal behavior of node contacts are detailed in Section 3.3.2 and Section 3.3.3, respectively. The newly formed "utility" function to determine the node's potentiality as a next-hop forwarder in DTN routing is presented in Sections 3.3.4. Finally Section 3.3.5 represents the proposed seasonality aware forwarding algorithm in social based DTNs.

We consider a category of DTN like Pocket Switched Networks [100] or Mobile Social Networks [101], which consists of cellular devices carried by human beings. They use Bluetooth interface to exchange data among themselves. Each device can act as a source, destination, or forwarder of a message. Due to mobility of these devices, a continuous source-to-destination path may not exist. These devices communicate in *opportunistic* manner during contacts, when a sender and a receiver comes into contact at a time which is unknown beforehand. During this contact, these devices make the forwarding decision of

data. In DTN the network topology changes rapidly and the nodes do not have any knowledge of future connections. The inter-node contact duration is often limited. During this duration only a limited number of messages can be transferred. Also, DTN uses multihop forwarding for messages. A large number of hops increases the probability of delivery of message, but also increases the delivery cost. So it is needed to have an efficient strategy to select the best relay nodes.

Use of social network metrics have been prominent [43] in DTNs where the network is formed with hand held mobile devices carried by humans. The reason for this is that mobility in such networks is driven by the social network properties, which are less volatile than the traditional metrics. In this work, we exploit the seasonality/repetitive pattern in human contacts and have incorporated it with the other state-of-the-art social network metrics towards proposing a **S**easonality **A**ware **S**ocial Based DTN Forwarding called SAS. Similar to SimBet [50], we select the best relay node based on a utility metric which exploits two social network metrics: centrality and similarity. We model the seasonality in human contact to propose a novel formulation for calculating tie-strength, and incorporate it as link weight into the proposed weighted similarity metric based on Katz similarity index [107]. By analyzing real mobility traces, we find that ego-betweenness [103] can be a good approximation for sociocentric betweenness [45] inside communities. We combine the proposed seasonality aware similarity and ego-betweenness in a utility function and propose the forwarding mechanism SAS.

3.3.1 Strength of tie

Strength of tie [52] measures the strength of social relationship between two individuals. A simple way to measure the tie-strength may be the total number of contact or the total duration of contact. Motivation of using tie-strength in DTN forwarding has been: if a node carrying the message gets into contact with a node which is strongly connected to the destination (i.e., has met with the destination many times or for long time in the past), they may meet again and may deliver the message with high probability. Tie-strength can be regarded as a similarity measure for directly connected node-pairs. However, the destination may not be directly connected to every node the carrier meet, so multi-hop similarity measure is required. We discuss the multi-hop similarity in the next subsection.

Traditional approaches to model node-pair's tie-strength use variants of average separation duration [53, 54, 55, 56]. In general, the average separation duration between two

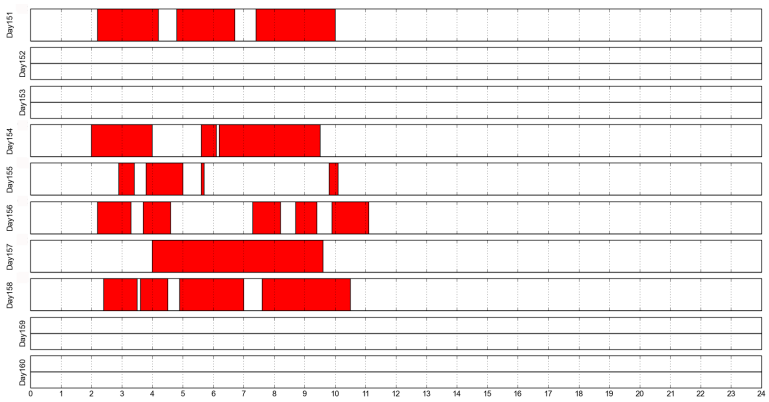


Figure 3.1: Seasonality pattern in `Reality` trace

nodes x and y during the time interval $[0, T]$ is given as:

$$S_{avg}^{[0,T]}(x, y) = \frac{\int_{t=0}^{T} f(t)dt}{T} \tag{3.1}$$

where $f(t)$ represents the estimated time remaining for the next encounter between the nodes x and y at time t. Strength of tie is usually formulated as a function which is inversely proportional to the average separation duration. This approach assumes that the node-pairs which have come into contact for longer duration in past are tied with stronger relationship, and are likely to come into contact in future.

Our proposed measure of tie-strength has been encouraged by observed seasonality pattern in node-pairs' contact history. Figure 3.1 shows the contact pattern of two nodes in the `Reality` trace during 10 days. Each rectangle in the vertical dimension represents a day, and each day is divided into 24 parts which represent hours. The duration of a day filled with red is the contact duration between the two nodes. The figure shows that the six days which have some contacts, follow similar contact pattern. The bursts of contacts happen during the same 9 hour period of these days. It might be explained as, the two persons workplace may be same and this nine hour duration might be their working hours. The days which observe no contact may be holidays, which repeat in every seven days. It is also observable that the contact pattern of the day at the top of the figure is very similar to the eighth day from top. It indicates that the contact pattern repeats every week. We exploit this seasonality pattern of human contact to measure of link strength, which is a weighted average of the traditional average separation duration and seasonality aware tie-strength. We describe below how each node calculates their tie-strength with its' neighbors. For simplicity and as per the requirement for the mobility traces in hand, we explain this method

with two granularities of seasonality, daily and weekly. However, this method is trivially extendable for more levels of seasonality, such as monthly, quarterly, yearly, etc.

We divide the duration of a day into equal size time-window Δ_0, say an hour. $\Delta_1 = a \times \Delta_0$ = duration of a day, $\Delta_2 = b \times \Delta_1 = a \times b \times \Delta_0$ = duration of a week. Note that, in our case $a = 24$ and $b = 7$, but for maintaining generality we use the variables a and b. $f(t)$ represents the time remaining to the next encounter between two nodes (x, y) at time t. Each node x maintains a seasonality matrix $m^{(x,y)}$ for each of its contacts y, $m^{(x,y)}[i, j]$ be the elements of the seasonality matrix $m^{(x,y)}$. The dimension of $m^{(x,y)}$ is $b \times a$. When two nodes x and y come to contact for the first time, both of the nodes initialize $m^{(x,y)}$, and all of its elements are initialized as 0. The nodes keep a variable p which stores the total number of time-windows elapsed, and is initialized as 0. They also keep the variables q and s, initialized as 0, which keep track of the offset of the current time window in the seasonality matrix for row and column, respectively. The variable $\mathbb{T}$ representing non-seasonal strength of the link (x, y) is initialized as 0. After each Δ_0 amount of time, both of the nodes trigger the following steps, which update an matrix element, the variables, and calculate the tie-strength of (x, y) for the next time window.

$$m^{(x,y)}[q, s] = \frac{m^{(x,y)}[q, s] + \Delta_0 / \int_{t=p\times\Delta_0}^{p\times\Delta_0+\Delta_0} f(t)dt}{p \times \Delta_0 + \Delta_0} \tag{3.2}$$

$$\mathbb{T} = \frac{p \times \Delta_0 + \Delta_0}{\mathbb{T} + \int_{t=p\times\Delta_0}^{p\times\Delta_0+\Delta_0} f(t)dt} \tag{3.3}$$

where p is incremented as $p = p + 1$ and the offsets of the next time window in the seasonality matrix for row and column are updated as $q = (p - p \mod (a \times b)) \mod b$ and $s = p \mod b$, respectively.

Finally, the seasonality aware tie-strength of the link (x, y) for the next time-window is calculated as the weighted average of average separation duration and seasonality components:

$$w^p(x, y) = \alpha \times m^{(x,y)}[q, s] + (1 - \alpha) \times \frac{1}{\mathbb{T}} \tag{3.4}$$

where the parameter $0 \leq \alpha \leq 1$ regulates the weight of the seasonality aware component in the tie-strength formulation.

3.3.2 Similarity

The motivation of using similarity measure in DTN forwarding is that similar nodes meet frequently, and a node similar to the destination node is highly likely to deliver the message to the destination node. In SimBet, similarity between two nodes is calculated as the number of common neighbors between them. It treats direct and indirect contacts in a similar manner. We argue that the nodes which have met the destination at past, are more similar to the destination than those which are two hop away. We adopt Katz index [107] to define the similarity metric. Katz similarity index between the nodes x and y is given as:

$$Katz(x,y) := \sum_{l=1}^{\infty} \beta^l \times |paths_{x,y}^{<l>}|, \tag{3.5}$$

where $paths_{x,y}^{<l>}$ represents the set of all paths of length l between nodes x and y. $\beta > 0$ is a constant that regulates the amount of importance given to higher length paths. As $\beta \to 0$, Katz index starts behaving like common neighbor.

We modify Katz index to accommodate tie-strength. We consider upto 2 length paths to make it locally calculable. The Similarity measure between nodes x and y is given as:

$$Sim(x,y) = \beta \times w(x,y) + \beta^2 \times \sum_{k \in N(x) \cap N(y)} w(x,k) + w(k,y), \tag{3.6}$$

where $N(x)$ is the set of neighbors of a node x, and $w(x,y)$ is the weight of a link (x,y) for the current time window, given by Equation (3.4).

3.3.3 Centrality

Centrality measures the importance/accessibility of a node in the network. Central nodes are considered as highly reachable to the other nodes in the network. Betweenness [45] is one of the widely used centrality measure used in social based DTN forwarding techniques [43]. Nodes with high betweenness centrality fall into large number of shortest paths linking to other node-pairs in the network. Thus, these nodes act as bridges to reach to all other nodes in the networks. Betweenness Centrality is calculated as:

$$Bet_C(x) = \sum_{y \neq z \neq x, (y,z) \in \text{Nodes}} \frac{g_{y,z}(x)}{g_{y,z}} \tag{3.7}$$

where $Bet_C(x)$ is the global/socio centric betweenness centrality of node x, $g_{y,z}$ is the total number of geodesics (shortest paths) between nodes y and z, and $g_{y,z}(x)$ is the number of shortest paths between node y and z passing through x.

Socio centric betweenness is a global measure, and is difficult to measure in DTN forwarding because the nodes in DTN have access to the local information only. Flooding may be one solution, but it will increase the message cost exponentially. Moreover, due to sparse and dynamic nature of DTN, message may take long to reach the destination. Consequently, in DTN it is impossible to achieve consistent values of the global measures like socio centric betweenness throughout the network. SimBet [50] has capitalized the concept of Ego networks [103] in DTN forwarding, which approximates socio centric betweenness by calculating betweenness centrality locally, within the node's ego network. Ego network of a node is defined as a network which consists of the node, its neighbors, the links of the node with its neighbor, and the connections among its neighbors. The ego-betweenness of a node x is calculated as:

$$Bet_E(x) = \sum_{y \neq z \neq x, (y,z) \in N(x)} \frac{g_{y,z}(x)}{g_{y,z}} \tag{3.8}$$

Where $Bet_E(x)$ is the ego-betweenness centrality of x, $g_{y,z}$ is the total number of geodesics (shortest paths) between nodes y and z, and $g_{y,z}(x)$ is the number of shortest paths between node y and z passing through x. $N(x)$ is the set of neighbors of x.

Marsden [113] has observed that ego-betweenness and socio centric betweenness are highly correlated in social networks. We investigate the relationship between socio centric and ego-betweenness in the real mobility traces discussed in Section 3.1. Table 3.1 shows that correlation between ego-betweenness and socio centric betweenness in the whole network is insignificant. However, when the network is partitioned into communities, ego-betweenness and socio centric betweenness correlate highly. So, we argue that a node with high ego-betweenness acts as a good hub inside its community, and can be useful in forwarding the message when the destination is inside its community.

3.3.4 Utility

A carrier having a message must choose another node to forward it, so that the message reaches the destination with high probability. When a carrier comes into contact with a

node, it calculates an utility function of the node with respect to the destination. The carrier forwards the message to the node based on this utility function. Like SimBet [50], we define the utility as a combination of two utilities: similarity and centrality.

Utility of a node y (which comes into contact with the carrier x) for delivering a message to node d is calculated as:

$$Utility(y,d) = \gamma \times SimUtility(y,d) + (1-\gamma) \times BCUtility(y) \tag{3.9}$$

Where,

- $SimUtility(y,d) = \frac{Sim(y,d)}{Sim(x,d)+Sim(y,d)}$ is the similarity utility of the node y with the destination d with respect to the career x,
- $BCUtility(y) = \frac{Bet_E(y)}{Bet_E(x)+Bet_E(y)}$ is the betweenness utility of the node y with the destination d with respect to the career x,
- $\gamma \in [0,1]$ is a balancing parameter, which allows for setting the relative importance of Betweenness utility and Similarity utility,
- $Sim(-,-)$ and $Bet_E(-)$ are calculated using Equation (3.6) and Equation (3.8) respectively.

3.3.5 Forwarding algorithm

Here we present our proposed forwarding algorithm based on ego-betweenness centrality and seasonality aware similarity index, which extends the forwarding algorithm of SimBet [50]. It evaluates a nodes' utility for being chosen as a potential forwarder. This algorithm makes no pre-assumption of global knowledge of the network, and makes the forwarding decisions on the fly based on locally exchanged information. For this to happen, on encountering a node y, node x verifies whether it is carrying any messages destined to y. If this is found to be true, then all messages destined for y are delivered. Subsequently, the encounter vectors are received from node y. The encounter vector contains information (list of contacts and tie-strength of the links with their contacts) about the nodes that each of them have encountered. This encounter information is then used to update the ego-betweenness value on node x and similarity value as described in Equations (3.8) and (3.6) respectively. Further, the two nodes x and y exchange a summery vector that contains a list of destination nodes for whom they are carrying messages, and their betweenness and

similarity values. Thereafter, node x calculates the Utility value of its own and of node y for each destination in the received summery vector following Equation (3.9). If the node y's utility is higher than x's, x forwards the message to y in greedy fashion. We summarize the algorithm as follows.

1. On encountering y, if node x has messages destined for y, it delivers them to y.
2. x receives the encounter vector of node y, which contains y's contacts and $w^p(y,k)$'s where $k \in N(y)$.
3. Node x and y exchange the summery vector information containing list of messages carried by them for each destination node.
4. For each message in the Message list calculate $Utility(x,d)$ and $Utility(y,d)$ for each destination d.
5. If $Utility(y,d) > Utility(x,d)$, node y becomes the forwarder and receives messages from x.

3.4 Performance Evaluation of SAS

This section detail the performance evaluation and analysis of the proposed social based forwarding scheme (SAS) with the benchmark SimBet [50] and BubbleRap [51] to validate its' effectiveness in attaining routing objectives. The different evaluation metrics under consideration are described in Section 3.4.1. Section 3.4.2 provides a brief description of the data traces used in the experiments and summarizes characteristics of the social network induced by the contacts in the mobility traces. The experimental setup used for generation of mobility traces through trace-driven test with dataset from the `Reality` [114] and `Cambridge` [115] datasets are represented in Section 3.4.3. Finally, the experimental results and their analysis are summarized in Section 3.4.4.

3.4.1 Routing Objective and Evaluation Metrics

Routing Objective of DTN routing protocol depends on application. Generally the objective is to increase the delivery ratio while not increasing the cost of delivery much. Generally, DTN routing protocols are evaluated based on the following metrics, which we follow in this work:

- **Delivery Ratio:** It is the ratio between the number of messages delivered and the total number of messages generated.
- **Delivery Cost:** It is the ratio between the number of message transmission required for delivery to the total number of messages delivered.
- **Average Latency:** It is the time duration between the message generation and its delivery, averaged over all messages.

3.4.2 Data sets

We perform our experiments on three real mobility traces, namely `Cambridge`, `Reality` and `Sassy`. A brief description of the three traces are given next. The characteristics of the social network induced by the contacts in the mobility traces are already summarized and discussed in Table 3.1 of Section 3.1.

- `Cambridge`: This dataset [105] includes the traces of Bluetooth sightings by groups of users carrying iMotes for 11 number of days. The iMotes devices were distributed among the doctoral students and faculty comprising a research group at the University of Cambridge Computer Laboratory.
- `Reality`: The MIT's Reality Mining experiment [106] conducted in 2004 was aimed at studying community dynamics. The study consist of one hundred Nokia 6600 smart phones having Bluetooth network connectivity and were distributed among the students and staff at MIT. The study generated data, collected by these 100 human carried devices over the course of nine months, include call logs, Bluetooth devices in proximity (i.e. contact logs), cell tower IDs, application usage, and phone status. The study resulted in the first mobile data set with rich personal behavior and interpersonal interactions.
- `Sassy`: This dataset [116] is an outcome of the experiments carried out by a group of participants (22 undergraduate students, 3 postgraduate students, and 2 members of staff) forming a mobile sensor network at University of St Andrews. The experimental set up was made of 27 T-mote invent devices (mobile IEEE 802.15.4 sensors) carried by human users and Linux-based base stations for bridging the 802.15.4 sensors to the wired network. The participants were asked to carry the devices whenever possible

over a period of 79 days. The data set contains information about the participants' encounter records as well as their social network data generated from Facebook data.

3.4.3 Experiment Setup

We have used Opportunistic Networking Environment (ONE) simulator [117] for simulation purpose. It is specifically designed for evaluation of DTN routing and application protocols. We have evaluated our simulation through trace-driven test with dataset from the `Reality` [114] and `Cambridge` [115] datasets, described in Section 3.4.2. `Reality` dataset spans for about six months. During the simulations for reality datasets 1000 messages were generated during $5 - 6$ month period by randomly choosing the source and destination nodes. `Cambridge` dataset spans for about 11 days. During the simulations with `Cambridge` dataset, 1000 messages were generated after $9 - 11$ day period by randomly choosing the source and destination nodes. Each simulation is repeated 10 times with different random seeds, and the average evaluation results are reported. The parameters for the simulations for the datasets are summarized in Table 3.2.

Table 3.2: Parameters for Simulation Setup

Dataset	`Reality`	`Cambridge`
Number Nodes	97	36
Transmission Range	10 m	10 m
Transmission Speed	250 kBps	250 kBps
Message size	$10 - 100$ kb	$10 - 100$ kb
Time To Live (TTL)	$1 - 12$ days	2 min - 24 hrs

3.4.4 Results and Discussion

We compare the performance of the proposed DTN forwarding algorithm SAS with the state-of-the-art social based DTN forwarding algorithms: SimBet [50] and BubbleRap [51]. We vary the parameter α to tune the effect of seasonality in SAS. We set β, the parameter of the Katz similarity measure to a typical value $.05$ [44].

Figures 3.2, 3.3, 3.4, 3.5, 3.6, 3.7 summarize the comparative performance of SAS with BubbleRap and SimBet for the three evaluation metrics viz., "delivery ratio", "delivery cost" and "average latency". Further, to evaluate the effects of the seasonality component on the performance of SAS, we set three different values for the parameter α (i.e., $\alpha = 0$, $\alpha = 1$,

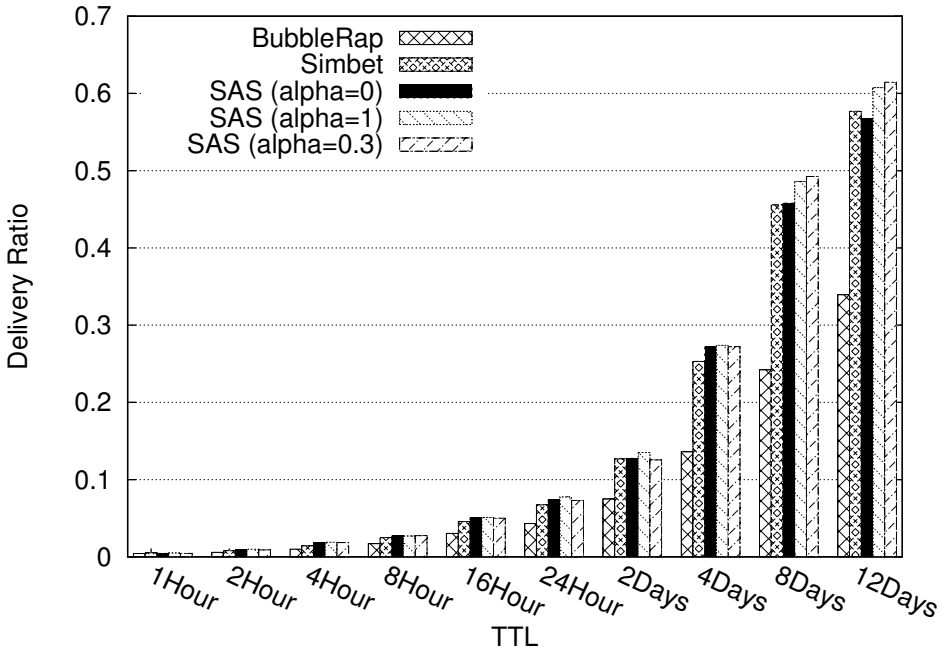


Figure 3.2: Message delivery ratio Vs TTL in Reality data set

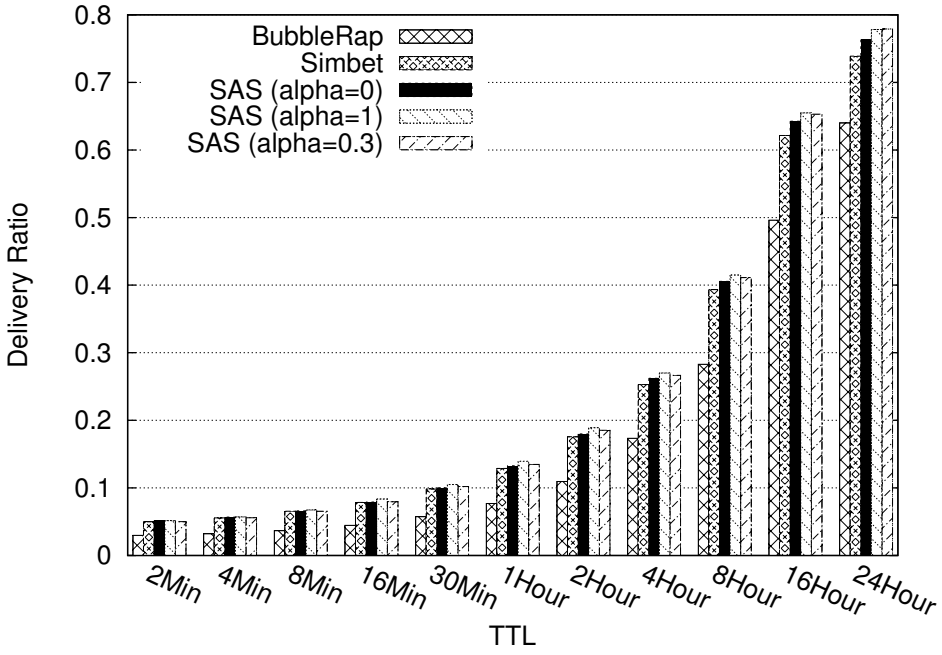


Figure 3.3: Message delivery ratio Vs TTL in Cambridge data set

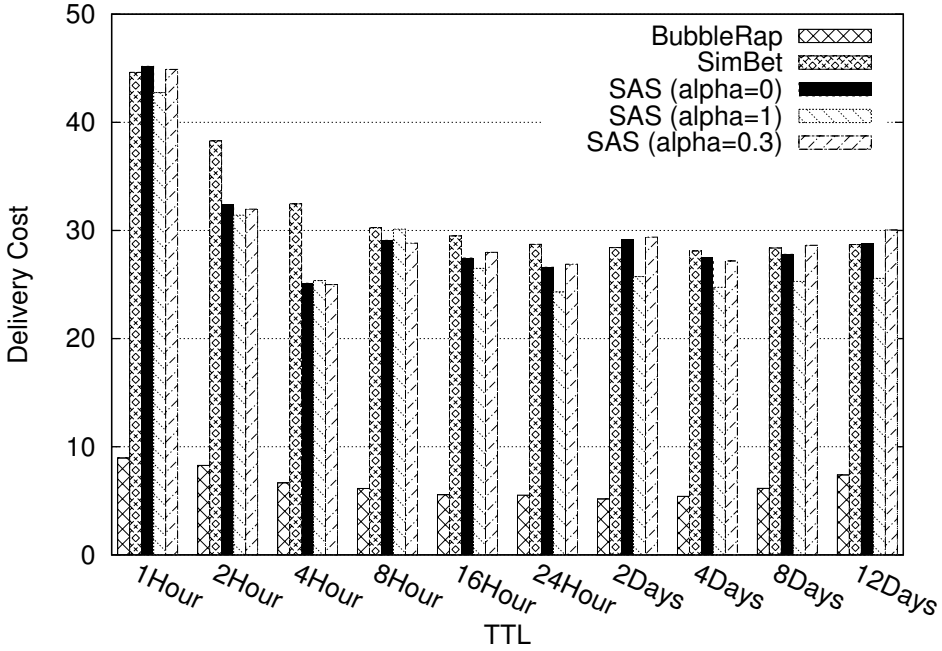


Figure 3.4: Message overhead ratio Vs TTL in Reality data set

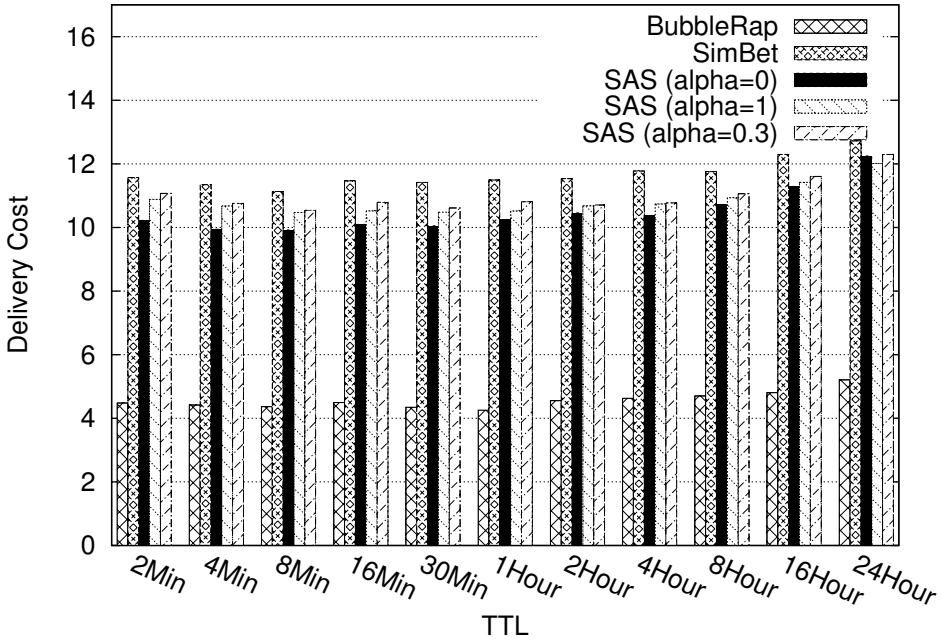


Figure 3.5: Message overhead ratio Vs TTL in Cambridge data set

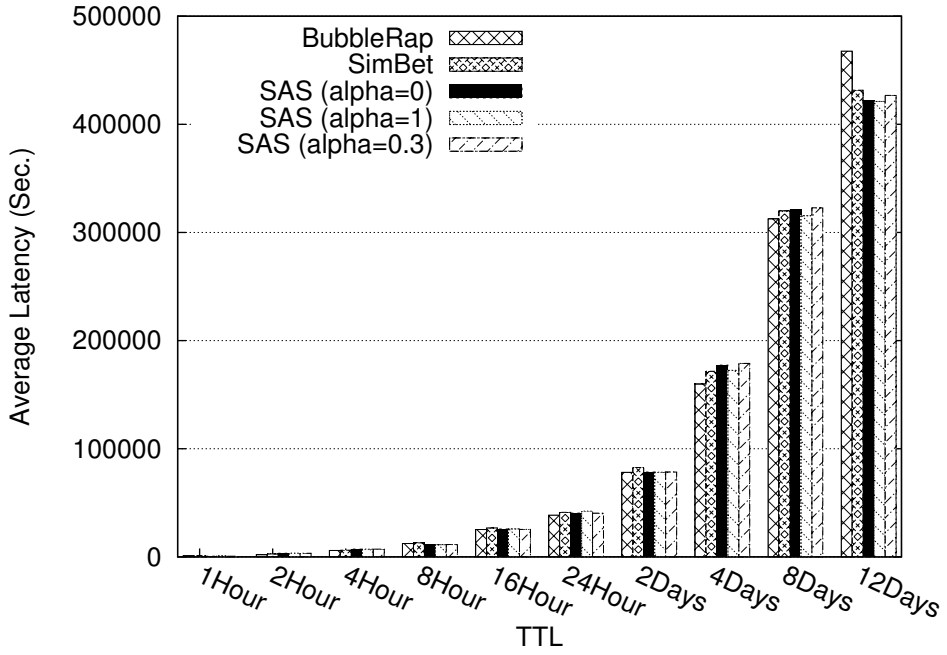


Figure 3.6: Message average latency Vs TTL in Reality data set

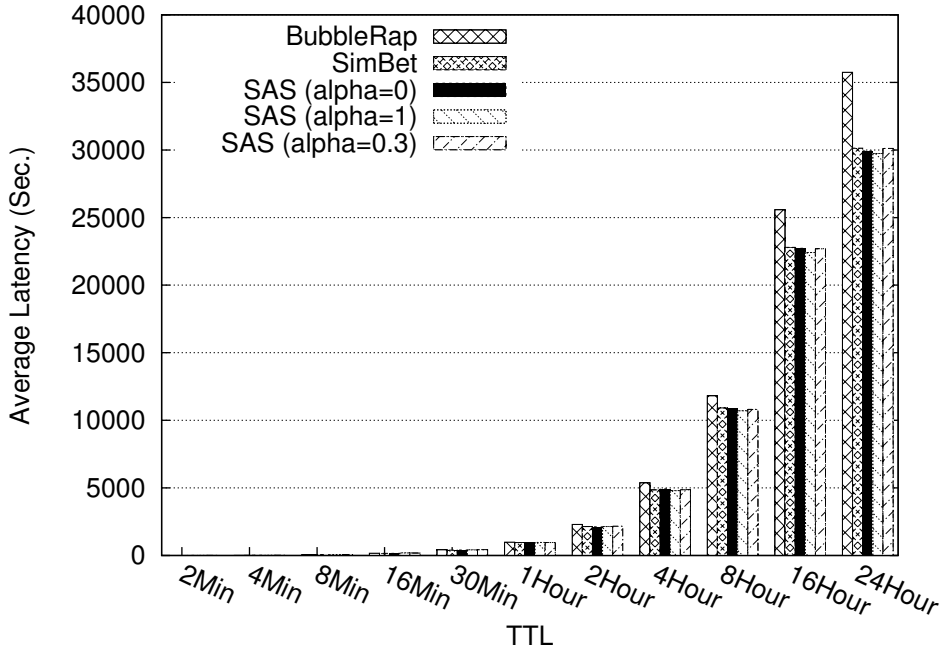


Figure 3.7: Message average latency Vs TTL in Cambridge data set

$\alpha = 0.3$) and have obtained the simulation results for three different performing versions of SAS. Results for SAS (alpha=0) measure the performance of SAS when the tie-strength does not contain the seasonality component, SAS (alpha=1) represents SAS when the tie-strength is calculated with a high weighted value set for the seasonality component, and SAS (alpha=0.3) represents SAS where the tie-strength is calculated with a low weighted seasonality component. Here we detail the results of these three performing versions of SAS with varying TTL values (as represented in Table 3.2). We also varied the utility parameter γ for SAS and SimBet, but found that $\gamma = 0.5$ gives best performance in general.

Figure 3.2 and Figure 3.3 show that all the three different versions of SAS (i.e., SAS (alpha=0), SAS (alpha=1), SAS (alpha=0.3)) outperform SimBet and BubbleRap significantly with respect to delivery ratio over the two traces (i.e., "reality" and "cambridge") and the TTL values. SAS(alpha=0.3) outperforms SimBet by 6.50% and BubbleRap by 81.10% for TTL=12Days in `Reality` trace. SAS(alpha=0.3) outperforms SimBet by 5.41% and BubbleRap by 21.70% for TTL=12Days in `Cambridge` trace. SAS (alpha=1) always outperforms SAS (alpha=0), which indicates the usefulness of the seasonality component of tie-strength. Again, it is also notable from Figure 3.4 and Figure 3.5 that all the performing versions of SAS (i.e., SAS (alpha=0), SAS (alpha=1), SAS (alpha=0.3)) do not incur much delivery cost as compared to SimBet to achieve the gain in delivery ratio in `Reality`, and achieves better delivery cost than SimBet in `Cambridge`. From Figure 3.6 and Figure 3.7, it has been observed that for all of the forwarding techniques under consideration in the simulation study (except BubbleRap), average latency values are almost same for all the protocols.

3.5 Conclusion

This chapter of the thesis has proposed SAS, a novel seasonality aware adaptive forwarding technique in social DTNs. The work is based on the observation of existence of seasonal behavioral pattern in node contacts in real mobility traces. SAS invoked a weighted Katz based similarity measure and ego-betweenness centrality to evaluate a utility value of an encountered node. Based on this utility, it decides the competency of a candidate node for being selected as a next hop message forwarder in DTN routing. The proposed method has been evaluated against different routing metrics through extensive set of simulation study with real mobility trace data sets. The performances of SAS has been found to get enhanced compared to the existing baseline social based forwarding schemes available for DTNs.

In the next chapter, we have addressed the issues of routing vulnerabilities in HetMesh

that may arise due to the existence of “misbehaving nodes” (both malicious and selfish) in the forwarding path. Although the different categories of routing protocols available in the literature of HetMesh look promising and work well in a friendly (i.e., congenial) environment, they may not be accurate in a hostile scenario, (i.e., in the presence of “malicious” and “selfish” nodes), where behavior of nodes is unpredictable from the network as well as social perspectives [118], [57]. In a hostile scenario, an intermediate honest node may misbehave either by dropping messages or by not forwarding them to the intended recipients. Thus the presence of misbehaving nodes in the forwarding path may cause a serious threat and thus routing becomes vulnerable to different kinds of attacks. Hence, in order to avoid misbehaving nodes in the forwarding path of HetMesh, we have proposed a novel unified framework based on trust and “Multiple Criteria Decision Making” (MCDM) technique, which can be flexibly integrated with a large family of existing routing protocols to ensure reliable and secure communication over HetMesh.

4

Trust-based forwarder selection framework for reliable and secure routing in hostile heterogeneous wireless mesh networks

4.1 Introduction

The concept of Heterogeneous Wireless Mesh Networks (HetMesh) has evolved recently and several research groups are working on its various aspects [119]. By definition, HetMesh is a multi-hop wireless access network and shows hierarchical architecture, where the backbone comprises of fixed infrastructure mesh routers, and the clients are of ad hoc and dynamic nature. Both the mesh routers and mesh clients may exploit multi-channel and multi-interface capabilities for connecting with the backbone and outside Internet. HetMesh combines the benefits of Infrastructure and Client WMNs, as well as provide simultaneous support for multi-hop access of routers by diverse mobile clients. Further, with the advanced direct wireless communication technologies, like WiFi-direct [94], the mobile clients in HetMesh have the capacity to directly communicate to another client without intervening the mesh backbone. Moreover, many mobile clients with such advanced technologies can also act as intermediate forwarder. In such a diverse environment, selection of next-hop forwarder is the prime routing issue in HetMesh. Recently, some hybrid routing schemes available in the literature have addressed the forwarder selection problem in HetMesh [119, 24]. Although these routing schemes look promising and work well in a

friendly (i.e., congenial) environment, but they may not be accurate in a hostile scenario, (i.e., in the presence of "misbehaving" nodes), where behavior of nodes is unpredictable from the network as well as social perspectives. A misbehaving node can attract packets from a legitimate node and drop those packets which in turn degrades the HetMesh's performance. The misbehaving nodes have either negative or limited contributions to the network. The presence of misbehaving nodes in the forwarding path may cause a serious threat to HetMesh-based communication and thus routing becomes vulnerable to different kinds of attacks such as black hole, DoS, and spoofing attacks. Consequently, a communicating node has to be cautious when selecting a next-hop forwarder for routing packets in the network. Therefore, it is essential to design a secure routing framework that associates misbehavior detection scheme (i.e., detection of malicious and compromised nodes) for secure route calculation in HetMesh.

There is a traditional way of securing routing protocols [64, 65, 66] by transmitting authenticated routing messages among the wireless network entities. However, this approach is insufficient as the key characteristics of HetMesh make it possible for attackers, including malicious users, to add routers, establish links, and advertise routes. In addition, an attacker can steal the credentials of a legitimate user or a legitimate user can itself turn malicious, and thereby inject authenticated but incorrect routing information into the network. All these existing solutions [64, 65, 66] imply a reduction of performance due to additional cryptographic computations. These situations motivate the application of trust-based strategy for ensuring routing security in HetMesh. Since, routing process in HetMesh relies on participation and cooperation of nodes within the network, therefore, trusted routing is beneficial for discovering neighbors, selecting routers and announcing topology information for secure route discovery and its maintenance [120]. Hence, a cooperative mechanism is required to built trust among the nodes to classify them as trustworthy (honest) or untrustworthy (misbehaving). This mechanism is to be integrated with the routing protocols for a reliable and secure route calculation in the hostile HetMesh scenarios.

The subject of this chapter is the introduction of a novel unified forwarder selection framework for secure routing in HetMesh which is based on trust and Multiple Criteria Decision Making (MCDM) technique [121]. The proposed framework is called *Trust-Based Multiple Criteria Decision Making* (TB-MCDM) and takes into account multiple trust measuring criteria for trust quantification and addresses the different issues of misbehaving nodes in a hostile HetMesh scenario.

The rest of the chapter is organized as follows. Section 4.2 provides a brief summary of different available approaches for secure routing with a special emphasis on trust-based framework in Mobile Ad hoc Networks (MANETs), Wireless Sensor Networks (WSNs) and Wireless Mesh Networks (WMNs). The issues with these available approaches and the motivation for the work in this chapter are also presented here. The proposed TB-MCDM framework and it's different components are detailed in Section 4.3. The framework resiliency against different attack conditions is verified in Section 4.4. This section also presents the evaluation of TB-MCDM against different security metrics viz., attack detection rate, false positive, false negative rate etc., in presence of bad-mouthing, good-mouthing, and selfish attacks. Section 4.6 presents the simulation results of TB-MCDM against different routing metrics viz., throughput, packet delivery ratio, normalized routing overhead, and end-to-end delay. This section also includes the comparative analysis of TB-MCDM with other recently proposed trust-based frameworks available in the literature for WMNs. Section 4.7 summarizes our work in this chapter.

4.2 Background and Existing Works, Issues and Motivation

This section presents the different available approaches for secure routing with a special focus on trust-based framework in Mobile Ad hoc Networks (MANETs), Wireless Sensor Networks (WSNs) and Wireless Mesh Networks (WMNs). It also discusses the irrelevancy of the traditional approaches for ensuring routing security in HetMesh and the motivation behind the application of trust-based framework for addressing the issue of misbehaving nodes in a hostile environment.

The work in [67] interpreted trust as a relation among entities that participate in various protocols. They have evaluated trust evidence in ad hoc networks without considering pre-established infrastructure. Using the concept of directed graphs, they distinguished entities as nodes and trust relation between nodes as edges to model the trust evaluation process. Again they emphasized on design issues related to trust evaluation algorithms and provided intuitive requirements for it. Applying theory of semirings they showed that two nodes having no previous direct interaction are able to establish indirect trust.

A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks is proposed in [70]. The work presents a mechanism based on node monitoring complemented by a reputation functionality. The proposed mechanism is able to differentiate between cooperative and non-cooperative nodes in the network. The limitations of the

mechanism is that it relies only on positive reputation information without the facility to submit negative feedback.

To mitigate routing misbehavior in MANETs, the authors in [71] proposed a reputation-based trust management scheme that incorporates the concept of "watchdog" for monitoring node behavior and a "pathrater" for collecting reputation values of other nodes in the network. The drawback of the proposed method is that it is based only on direct observations.

In an another approach, the authors in [122] designed a trust based secure routing framework for WSNs. They have analyzed the secure framework theoretically for assessment of involved cost in the proposed model. Again, validation of the framework has been done by various routing protocols and experimental evidences have been provided to defend various attacks in WSNs.

The authors in [123] have proposed a service trust based routing which is based on the subjective trust model. In their design they have involved passive trust of objects and combined direct trust and recommended trust. They have presented passive trust feedback method which avoids malicious nodes' deception. Extensive simulation experiments are provided to prove the feasibility and rationality of their trust model.

The work in [68] presents a comprehensive and robust reputation evaluation framework for wireless mesh networks. The reputation value have been evaluated on the basis of aggregation of collected feedbacks. The authors have used Kalman filtering method for feedback aggregation. Further, to mitigate malicious feedback aggregation, they have designed an expectation maximization algorithm. The authors have provided a theoretical analysis for demonstrating the robustness of their proposed framework.

The authors in [69] have presented an information theoretic framework for quantitative trust measurement. They modeled trust propagation in ad hoc networks. According to them, trust is a measurement of uncertainty with its value represented as entropy. For basic understanding of trust propagation they have developed four axioms. On the basis of these axioms two trust models have been presented: i) *entropy-based model* and ii) *probability-based mode*l. For secure ad hoc routing and malicious node detection they employed the proposed trust evaluation method and trust models in ad hoc networks. Furthermore, simulation results show that their trust evaluation system can significantly improve network throughput as well as effectively detect malicious behaviors in ad hoc networks.

There are few research approaches on secure routing in WMNs and they are based on

cryptographic computations. Most of them are adopted from existing solutions available for Mobile Ad hoc Networks (MANETs). One such protocol called Ariande [64] is a secure on-demand source routing based on authentication of source node. Another such protocol SAODV [65] is a secure variant of AODV which uses cryptographic extensions to provide authenticity and integrity of routing messages. It uses hash chains in order to prevent manipulation of hop count field. The work in [66] presents a trusted routing named Trusted Computing Ad hoc On-demand Distance Vector (TCAODV), which extends the traditional Ad hoc On-demand Distance Vector (AODV) [1] routing protocol to ensure that only trustworthy nodes participate in route calculation and prevents selfish or malicious nodes from participating in the network. In TCAODV [66], a public key certificate as well as a per-route symmetric encryption key is established to ensure that only trusted nodes along the path can use the route. All these existing solutions imply a reduction of performance due to all additional cryptographic computations.

A non-cryptographic based trust measurement scheme for WMNs has been reported in [72]. The authors have used "Technique for Order Preference by Similarity to Ideal Solution" (TOPSIS) [73, 74] for quantification of trust relationship. The proposed scheme only derives the trust for each individual node through direct observations and recommendations collection, but no implementation and evaluation is carried out to test its effectiveness in HetMesh scenario.

To summarize, although a variety of trust models have been proposed and developed by research community for MANETs, WSNs, and WMNs, but to the best of our knowledge, these schemes have not yet been extended for HetMesh. In HetMesh architecture, simultaneous support for multi-hop and multi-path access of routers by diverse mobile clients are allowed. Further, clients can communicate among themselves in a multi-hop fashion without involving backbone routers. Thus, the architecture and routing nature of HetMesh is different from that of MANETs, WSNs, and general purpose WMNs, and therefore demands for a different approach to combat the prevailing uncertainties in hostile networking scenarios.

Therefore, it is essential to design a misbehavior detection framework (i.e. detection of malicious and selfish nodes) in HetMesh with minimal computational overhead. Further, this framework can be used by any suitable routing protocol for secure route calculation in the presence of misbehaving nodes. Thus, the objective of this work is to design a trust-based forwarder selection framework that ensures a self organized collaboration and helps

routing protocols to detect misbehaving nodes in the network. The proposed framework allows only trusted nodes to participate in route establishment and hence enhances security features of the corresponding protocol.

4.3 Proposed trust-based forwarder selection in HetMesh

This section details the proposed trust-based forwarder selection framework for ensuring routing security in a hostile HetMesh environment. Section 4.3.1 presents the definition of "trust" and the axioms [69] that are being considered for building trust relationship in HetMesh are detailed here. The Multiple Criteria Decision Making (MCDM) technique called Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) [73] that we have considered for quantification of trust relationship in HetMesh is detailed in Section 4.3.2. Section 4.3.3 details the trust evaluation process of TB-MCDM. The different components of the proposed trust evaluation process along with their functionalities that are used for avoiding misbehaving nodes in a hostile HetMesh environment are also detailed in this section. An illustrative example to explain the proposed trust derivation system of TB-MCDM is provided in Section 4.3.4

4.3.1 Modeling Trust in HetMesh

In our proposed trust-based framework, we describe "trust" as a relationship established between two entities (i.e. nodes) for a specific action. In particular, one entity trusts the other entity to perform an action. Here, the first entity is referred as "Subject" and the second entity is called an "Agent" and both of them are neighbors to each other. The axioms [69] that are being considered for describing trust relationship in HetMesh are listed below. The trust building process of our proposed framework is guided by these axioms.

Axiom 1: *Uncertainty is a measure of trust.* From a subject's point of view certainty of performing an action by an Agent is described as trust. Thus trust value between these two entities is represented by T(*Subject : Agent, Action*) and is defined as

$$T\{Subject : Agent, Action\} = \begin{cases} 1 - H(p), & for\ 0.5 \leq p < 1 \\ H(p) - 1, & for\ 0 \leq p < 0.5 \end{cases} \tag{4.1}$$

where $H(p) = -plog_2(p) - (1-p)log_2(1-p)$ and p = P(*Subject : Agent, Action*). Here "Sub-

ject" is the entity assigning trust and "Agent" is the entity whose trustworthiness of performing an Action is assigned. P(*Subject : Agent, Action*) denotes the probability that Agent will perform an Action in the subject's point of view. When $p = 1$, Subject trusts the Agent most and the trust value is 1. When $p = 0$, the "Subject" distrusts the "Agent" most and the trust value is -1. When $p = 0.5$, the "Subject" has no trust for the "Agent" and the trust value is 0. Trust value is an increasing function with p.

Axiom 2: *Concatenation Propagation of Trust Does Not Increase Trust.* This axiom for defining trust relationship states that when a "Subject" establishes a trust relationship with an "Agent" through recommendation collection, the trust value between "Subject" and "Agent" should not be more than the trust value between the "Subject" and the "Recommender" as well as the trust value between the "Recommender" and the "Agent". Say, $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$ are three different entities, where $\mathcal{A}$ is the "Subject", $\mathcal{B}$ is the "Recommender", $\mathcal{C}$ is the "Agent". Let us consider that $\mathcal{A}$ has trust relationship with $\mathcal{B}$ which is represented as T_{AB} and $\mathcal{B}$'s recommendation for $\mathcal{C}$ to $\mathcal{A}$ is represented as R_{BC}. Then if agent $\mathcal{A}$ wants to establish trust relation with $\mathcal{C}$ through recommendation then according to Axiom 2, its mathematical representation is as given below:

$$T_{AC} \leq min\,(T_{AB}, R_{BC}) \tag{4.2}$$

Axiom 3: *Multi-path Propagation of Trust Does Not Reduce Trust.* This axiom states that if a "Subject" receives the same recommendation values for the "Agent" from multiple sources, then the computed trust value for the "Agent" should be no less than in the case where the "Subject" receives less number of recommendations.

Axiom 4: *Trust Based on Multiple Recommendations from a Single Source Should Not Be Higher Than That From Independent Sources.* It is possible to have multiple recommendations from a single source if the trust relationship is established jointly through concatenation and multi-path trust propagation. Since the recommendations from a single source are highly correlated, then the trust built on these correlated recommendations should not be higher than the trust built upon recommendations from independent sources.

4.3.2 Technique for Ordered Priority with Similarity to Ideal Solution (TOPSIS)

A variety of multiple criteria decision making (MCDM) techniques are available which help in ranking alternatives with respect to the different attributes and selection of the best

alternative. TOPSIS is abbreviated for Technique for Order Preference by Similarity to the Ideal Solution. TOPSIS was developed by Hwang and Yoon [121], based on the concept that the chosen alternative should have the shortest distance from the positive ideal solution (PIS) and the farthest from the negative ideal solution (NIS) for solving a multiple criteria decision making problem. Briefly, the PIS is made up of all best values attainable for a criteria, whereas the NIS is composed of all worst values attainable for a criteria. In our proposed TB-MCDM framework TOPSIS is used for quantification of trust relationship. The TOPSIS method involves following seven different steps for selection of best alternative among all available alternatives depending upon multiple criteria. The variations required to fit TOPSIS in our proposed TB-MCDM are described next.

1. Construction of the decision matrix: The decision matrix is the relational matrix between the attributes and the alternatives.

2. Construction of the normalized decision matrix: The normalized value in the normalized decision matrix can be any transformation of the column of the decision matrix with the value being in between 0 and 1.

3. Assignment of weights to the criteria: Assign a weight vector w_j to each criterion. The weight criteria can be obtained from various techniques, e.g., analytic hierarchy process [124]. In our work we considered each of the criteria having similar priority, so assigned weights are equal for each of the criteria.

4. Construction of the weighted normalized decision matrix: Each column of the normalized decision matrix is multiplied by its associated weight and a new matrix is obtained; the new matrix thus formed is called the weighted normalized decision matrix.

5. Determination of the ideal and non-ideal solution: The ideal (A*) and the non-ideal A^{-} solutions are defined as follows:

   $A^{*} = (v_0^{*}, ..., v_m^{*})$,where

$$v_j^{*} = \left\{ max\left(v_{ij}\right),\ if\ j > J;\ min\left(v_{ij}\right),\ if\ j < J^{'} \right\} \tag{4.3}$$

   $A^{-} = \left(v_0^{'}, ..., v_m^{'}\right)$,where

$$v_j^{'} = \left\{ min\left(v_{ij}\right),\ if\ j > J;\ max\left(v_{ij}\right),\ if\ j < J^{'} \right\} \tag{4.4}$$

6. Calculation of the separation measures for each alternative: The separation from the ideal alternative is:

$$S_i^* = \left[\left(v_j^* - v_{ij}\right)^2\right]^{1/2}, \; where\, i = 1, ..., m \tag{4.5}$$

Similarly, the separation from the negative ideal alternative is:

$$S_i^- = \left[\left(v_j^{'} - v_{ij}\right)^2\right]^{1/2}, \; where\, i = 1, ..., m \tag{4.6}$$

7. Calculation of the relative closeness to the ideal solution is:

$$C_i^* = \frac{S_i^-}{\left(S_i^* + S_i^-\right)} \tag{4.7}$$

4.3.3 Trust evaluation in TB-MCDM

In the proposed trust evaluation process of TB-MCDM, four different trust measuring criteria have been considered. Based on these criteria and interaction between nodes, a behavioral relationship is established among the network entities. This behavioral relationship is then transformed into discrete quantity. This transformation process is known as the quantification of trust relationship. In HetMesh, there exists multiple alternative routes between a source-destination pair. Therefore, the process of trust quantification in HetMesh can be compared to a multiple criteria decision making (MCDM) problem where the objective of the technique is to select best source-destination path among the available choices depending on some criteria. The criteria that have taken under consideration for quantification of trust relationship in TB-MCDM are *i*) probability (*p*) that an Agent will perform a particular action, *ii*) number of packets to be forwarded on behalf of a Subject, *iii*) number of packets successfully forwarded by the Agent, and *iv*) Delivery Ratio Efficiency (DRE). The steps required to calculate and assign trust to each individual node in TB-MCDM framework are detailed next.

Assumptions:

The proposed framework considers the following assumptions:

- Heterogeneity of nodes is being considered for HetMesh.
- Every node in the network authenticates each other before any interaction.

Components of TB-MCDM:

Here we detail the different components and the trust evaluation process of the proposed forwarder selection framework.

- Defining Action: Packet Forwarding and Recommendation Exchange are considered as "Actions" depending upon which the trust relationship will be established.
- Trust values are considered to be of two different types as described:
  - *Individual Trust:* It is the value which is assigned by the "Subject" depending upon the behavioral activity of the "Agent". This value is specifically allotted depending upon the performance of an Agent on a particular task that the Subject assigns it. The individual trust value is independent from the influence of any third party.
  - *Recommended Trust:* This value is provided by a third party i.e., "Recommender" who trusts or distrusts an "Agent". The subject considers this value and builds up a recommended trust value of an agent. This process of trust building is governed by the axioms as described in Section 4.3.1.

  The above mentioned two different trust values are taken into account while computing the total trust value i.e., T of a particular "Agent" by the "Subject".

$$T_x = T_{Individual} + T_{Recommended} \tag{4.8}$$

Considering the above factors, the trust evaluation system of TB-MCDM is divided into two disjoint modules. They are *Individual Trust Building System* and *Recommended Trust Building System*. A "Subject" (initially a client and subsequently intermediate router in HetMesh) uses a combination of these two modules to derive the trust value of each node in TB-MCDM. The different components of TB-MCDM are depicted in Figure 4.1 and are described next.

- **Behavior Monitor:** This component of the proposed framework collects the information about the "Agents" (i.e. neighbor nodes) and is responsible for deriving individual trust of HetMesh nodes by a "Subject". These information are precisely the facts which are related with Subject and Agent relationship (i.e., Action). The four criteria that are being considered for deriving individual trust are:

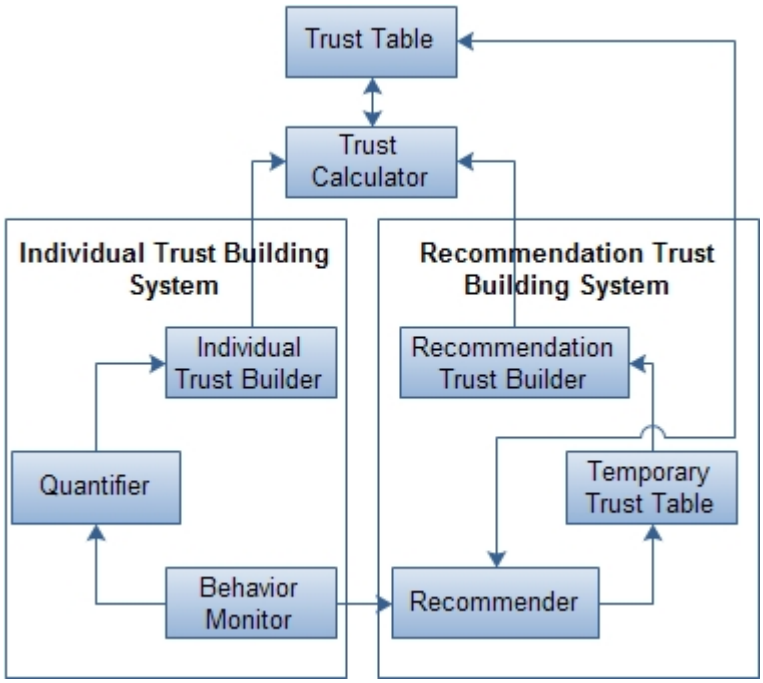


Figure 4.1: Trust-Based Multiple Criteria Decision Making Framework for next-hop carrier selection in hostile HetMesh

1. Probability (p) that an agent will perform a particular action. This value is calculated from Equation (4.1). T and p have one to one relation.
2. Number of packets to forward by the "Agent" on behalf of a "Subject".
3. Number of packets successfully forwarded by the "Agent".
4. Delivery Ratio Efficiency (DRE).

At the initial stage of the trust building process, a default trust value is assigned to every "Agent" when they are going to start working for the "Subject" for the first time. The assigned value signifies that the node neither trusts nor distrusts the agent. So maximum uncertainty is observed when such condition arises.

$$T_x(a_i) = 0,\ where\ a_i = Set\ of\ 1\ and\ 2\ Hop\ Neighbors. \tag{4.9}$$

- **Quantifier:** This component of TB-MCDM works with the behavior monitor. This helps in quantifying the observations made by the "Subject" into discrete values. Say, an "Agent" performs k number of events either successfully or unsuccessfully out of n

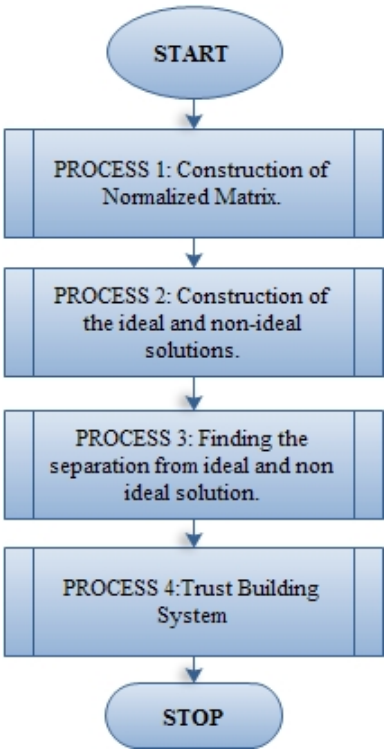


Figure 4.2: MCDM Machine

trials. Then its DRE is calculated with the following formula:

$$DRE = \frac{k+1}{n+2} \tag{4.10}$$

where k = no. of packets delivered successfully and n = no. of packets required to deliver.

- **Individual Trust Builder:** This component of TB-MCDM is the MCDM machine that resides in every "Subject" which actually uses the information provided by the *Quantifier* to calculate the individual trust of an "Agent". The MCDM machine is explained with the help of control flow charts depicted in Figure 4.2 and its different phases are subsequently elaborated in Algorithm 1, Algorithm 2, Algorithm 3, and Algorithm 4 respectively.

  It is to be noted although the technique of TOPSIS is used in the proposed MCDM machine, but the first two steps of TOPSIS [73] are not present in the proposed MCDM machine as depicted in Figure 4.2; these two steps are assigned to the *Quantifier*.

Algorithm 1: Normalized Matrix Construction

Input: Trust measuring criteria as column element, neighbors as row element and trust scores associated with trust measuring criteria are matrix element

Output: Normalized Matrix of Alternatives and Criteria

1. $j \leftarrow 0$ (Initializing counter to 0).
2. If $j <$ No. of Criteria
   (a) $i \leftarrow 0$
   (b) If $i <$ No. of Alternatives
       Input for each node w.r.t. criteria a[i][j]
       i ++, Goto Step (a)
   (c) Else
       j ++, Goto Step 2
3. Else
   (a) x [j]$\leftarrow$ Column wise square root of the sum of square of the scores
   (b) $j \leftarrow 0$
   (c) If $j <$ No. of Criteria
       i. $i \leftarrow 0$
       ii. If $i <$ No. of Alternatives
           a[i][j] $\leftarrow$ a[i][j] $\div$ x[j]
           i ++, Goto Step (ii)
       iii. Else
           j ++, Goto Step (c)
   (d) Else End.

Algorithm 2: Construction of Ideal and Negative-Ideal Solutions

Input: Elements of the normalized matrix

Output: Maximum and minimum elements of each row as +ve ideal and -ve ideal solution of each alternatives

1. $i, j \leftarrow 0$ (Initialize Counters)
2. If $j <$ No. of Criteria
   (a) pos_ideal[j] $\leftarrow$ Max(a[i][j]) and

neg_ideal[j] $\leftarrow$ Min($a[i][j]$),
where 0 $< i <$ No. of Alternatives(nodes)

(b) j++, Goto Step 2

3. Else End

Algorithm 3: Separation measures for each alternatives

Input: Ideal and non-ideal solution sets for all alternatives

Output: Alternative having shortest distance from the +ve ideal solution and longest distance from the -ve Ideal solution

1. i,j $\leftarrow$ 0 (Initialization)
2. If $i <$ No. of Alternative
   (a) $b[i][j]\leftarrow(pos\_ideal[j] - a[i][j])^2$ and
   $c[i][j]\leftarrow(a[i][j] - neg\_ideal[j])^2$
   where 0 $< j <$ No. of Criteria
   (b) i++, Goto Step 2
3. tempB[i], tempC[i], $i\leftarrow$0
4. If $i <$ No. of Alternative and
   0 $< j <$ No. of Criteria
   (a) $j\leftarrow$0
   (b) tempB[i]$\leftarrow$tempB[i] + $b[i][j]$
   tempC[i]$\leftarrow$tempC[i]+$c[i][j]$
5. while $i <$ No. of Alternative do
   (a) tempB[i]$\leftarrow(tempB[i])^{1/2}$
   (b) tempC[i]$\leftarrow(tempC[i])^{1/2}$
   (c) i++
6. end while
7. End

Algorithm 4: Calculation of relative closeness to the ideal solution

Input: +ve and -ve ideal solution sets

Output: Closeness measure of each alternative

1. $i\leftarrow$0
2. while $i <$ No. of Alternative do
   (a) rank[i]=$\frac{tempC[i]}{(tempB[i]+tempC[i])}$

(b) i++

3. $i \leftarrow 0$
4. while $i <$ No. of Alternative do
   (a) If rank[i] ≥ 0.5 and rank[i] < 1 Then
   rank[i]$=1 - H($rank[i]$)$
   (b) Else
   rank[i]$=H($rank[i]$) - 1$
5. end while
6. End

- **Temporary Trust Table:**

  This temporary trust table is a component of the "Recommendation Trust Building System" and stores the information regarding each of the "Agent" which exchanges recommendation with the "Subject". This trust table format is shown in Figure 4.3 and its different components are described below.

Recommender_id	Agent_id	Recommendation_Trust_Value

Figure 4.3: Temporary Trust Table

1. $Recommender\_id$ is the field which shows the identity of the node which sends the recommendation message.
2. $Agent\_id$ field denotes the identification of node whose recommendation is provided by a node with $Node\_id = Recommender\_id$
3. $Recommendation\_Trust\_Value$ field stores the trust value of an "Agent" which is obtained by the "Subject" by considering Equation (4.11).

$$R_{a_i} = \{RecommenderNode : AgentNode, Action\} \tag{4.11}$$

- **Recommender:** This component of the proposed TB-MCDM framework is responsible for broadcast of recommendation message. The recommendations are for those nodes whose trust value is greater than a predefined threshold at present as well as in the past. The threshold value that has been considered in our system is 0. So any "Agent"

having history of trust value greater than 0 will be considered for recommendation as well as trustworthy node with a certain trust value that the "Subject" assigns to that agent. This is to guarantee the fact that a trustworthy agent must not have a past history of being malicious and misbehaving.

- **Recommendation Trust Builder:** This component of Figure 4.1 helps in processing the temporary trust table for assigning a recommendation trust value. Subject activates this component while assessing an agent to find whether the agent is recommended by any other node, and if recommended then by whom and with what trust level. On getting these information, "Recommendation Trust Builder" then searches the "Trust Table" of the Subject to find out the trust level of the Recommender node. If the Trust value is positive then new recommended value is derived by considering the trust of recommender and recommended trust value as considered in Axiom 2 of Section 4.3.1. In this case, there exists no possibility of negative trust value or unavailable trust value because recommendation message only from trustworthy nodes is accepted, others are discarded. Further, on receiving recommendations, the Subject computes the offset value (λ) between the received recommended trust and the individual trust of the Agent stored in Subject's own trust table. If the value of the offset is ≥ 0.2 (i.e., $\lambda \geq 0.2$), the trustor considers it as a malicious activity and updates the recommended trust value of the Agent by the stored individual trust value.

- **Trust Calculator**: This component of TB-MCDM is the simplest of all modules of the proposed system and it only adds the value supplied by the *Individual Trust Building* and *Recommendation Trust Building* subsystems and prepares a list to be supplied to the *Trust Table* component.

- **Trust Table:** This table contains the information regarding the trust value assigned to different "Agents" by the "Subject". The format of this trust table is depicted in Figure 4.4 and described subsequently.

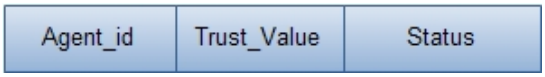


Figure 4.4: Trust Table Format in a Node

Here $agent\_id$ and $Trust\_value$ are the Agent's identity and Subject's trust on the agent, respectively. The status field is set to 1 when the node is trustworthy and is be-

having normally. But whenever Agent's behavior becomes suspicious and trust value becomes negative then this status field value becomes 0. It is to be noted that this status field once changed to 0 can never be changed to 1 irrespective of the fact that the Agent stops misbehaving. The status field plays an important role for recommendation decision process because the ultimate objective is to avoid an Agent having misbehaving and malicious history.

The proposed trust evaluation process is summarized in an algorithmic format named as Trust Building Process, Trust Calculator and Recommendation Broadcast process which are described next.

Algorithm 5: Trust Building Process
Input: Neighbor list
Output: Initial Trust

1. Subject considers each neighbor from neighbor list as an agent
2. While every agent is not processed
3. Subject select each agent
4. If Agent not perform action for Subject then
   T(a_i)=0
5. Else
   Call to Trust Calculator and Recommendation Broadcast Processing
6. End

Algorithm 6: Trust Calculator

- Module 1: Individual Trust Building
  Input:
  - Agent List a_i, where $1<i<n$ and n is the number of agents
  - No. of packets needed to be delivered for each a_i
  - No. of packets successfully delivered for each a_i
  - Initial Trust Value
  - Delivery Ratio Efficiency (DRE)

Output: Individual Trust and Recommendation Trust

1. Prepare above information in form of a decision matrix
2. Apply the MCDM strategy to recalculate individual trust value

- Module 2: Recommendation Trust Building
  1. Search the Temporary Trust Table for a_i
  2. Get the T Recommended for a_i
  3. T(a_i)=$T_{Individual}$+$T_{Recommended}$
  4. Update the Trust Table against each agent with new calculated value
  5. If T(a_i) $>$ Threshold then
     Broadcast this T(a_i) with the $Agent_{id}$

Algorithm 7: Recommendation Broadcast Processing
Input: Recommendation message from each trustee node
Output: Updated recommendation table

1. Collect each Recommendation Message if the recommender is trusty otherwise discard message
2. Extract $recommender_{id}$, $agent_{id}$ and $trust_{value}$ from Recommended Messages and transform it into a tuple r_i,a_i,R(a_i)
3. $T_{Recommended}$ = min (T_{ai},R_{ai}) , where T_{ai} is the calculated trust of the agent
4. If a_i is present in Temporary Trust Table then
   Update the $T_{Recommended}$ Field
5. Else
   Insert r_i,a_i,$T_{Recommended}$ tuple into Temporary Trust Table
6. Repeat 1-5 for all Different Recommendation Messages

4.3.4 An Illustrative Example

The proposed unified trust-based next-hop carrier selection framework called TB-MCDM is validated using C++ code simulation. The example given below illustrates the same.

Let a "Subject" say $\mathcal{S}$ is considered which has five neighbors called "Agents" (a_i) say (*a1,a2,a3,a4,a5*). It is required to construct the trust table of the Subject $\mathcal{S}$.

1. If there is no information about the Agents with the subject, it indicates there is no previous interaction between the Subject and the Agents. Also there is no recommendation from any other nodes. At this time an intermediate trust value ($T_{val} = 0$) will be assigned to the Agents. So the trust table of Subject $\mathcal{S}$ is as follows.

$$S_{TrustTableEntries=} \begin{array}{ccc} Agt_{id} & T_{Val} & Status \\ a1 & 0 & 1 \\ a2 & 0 & 1 \\ a3 & 0 & 1 \\ a4 & 0 & 1 \\ a5 & 0 & 1 \end{array}$$

2. Let after an interval of *t* time the trust building process is again invoked. At that time the Subject $\mathcal{S}$ will collect the information regarding its multiple trust measuring criteria i.e., i) *probability of successful completion of an Action by the Agent*, ii)*number of packets needed to be forwarded*, iii) *packets actually delivered successfully*, and iv) *delivery ratio efficiency* (DRE). These values are then fed into the MCDM machine. The Agents are considered as the different "alternatives" and information regarding different trust measuring components about the Agents are considered as "criteria". They are represented in matrix form as follows:

$Agnts$	p	$Pck_{toForward}$	$Pck_{Delivered}$	DRE
$a1$	0.5	120	110	0.92
$a2$	0.5	150	140	0.96
$a3$	0.5	100	25	0.25
$a4$	0.5	80	15	0.19
$a5$	0.5	120	50	0.41

3. The "Subject" uses the different values obtained from multiple trust measuring criteria and invokes the MCDM machine to calculate a new probability value *(p)* for each of its Agents. It is calculated following TOPSIS method as described in Subsectiontopsis.

$Agents$	p
$a1$	0.78704
$a2$	1
$a3$	0.111999
$a4$	0
$a5$	0.314025

4. The "Subject" uses Equation 4.1, to calculate the trust value $\mathcal{T}$ for each of its "Agent". The calculated trust values for the "Agents" by the "Subject" are as follows.

$Agents$	"T"	$Remarks$
$a1$	0.25	$(TrustworthyNode)$
$a2$	1	$(MostTrustworthyNode)$
$a3$	-0.49	$(UntrustworthyNode)$
$a4$	-1	$(MostUntrustworthyNode$
$a5$	-0.10	$(UntrustworthyNode)$

5. Recommendation will be advertised for Agents *a1* and *a2*. The trust building process of TB-MCDM will be executed whenever the Subject invokes it.

4.4 Attacks on TB-MCDM

In TB-MCDM, the evaluation of trustworthiness of each participating node ensures an effective method to simulate nodes misbehavior and thus to improve routing security in hostile HetMesh. However, generally any trust evaluation system itself is an attractive target for attackers. This section details the probable attacks that may hinder TB-MCDM's efficiency and the preventive measures that have been considered while designing the proposed secure framework. Detailed simulation based results and their analysis are also provided in Section 4.5 to claim the resiliency of the TB-MCDM framework against attacks.

The trust building process of TB-MCDM is based on individual trust building system module (i.e formation of individual trust) and recommendation trust building system module (i.e., recommended trust). The individual trust is assigned by the "Subject" depending upon the behavioral activity of the "Agent". This value is specifically allotted depending upon the performance of an Agent on a particular task that the Subject assigns it. The individual trust value is independent from the influence of any third party. The recommended trust is accumulated through collective recommendations from neighboring nodes. In a hostile

scenario, an honest node may turn dishonest and behave maliciously by providing false recommendations about other nodes in the network. Thus, a malicious node can undermine the trust building system by boosting trust values for malicious parties or framing up good nodes to launch *bad-mouthing* and *good-mouthing* attacks. These types of activities by misbehaving nodes lead a "Subject" to make unreliable decisions and thus undermine the effectiveness and performance of TB-MCDM in a hostile HetMesh scenario. Moreover, the consideration of nodes' selfish behavior is also another important issue to be addressed in TB-MCDM's resiliency against *Selfish* attacks. Here, we detail the prominent attacks that may be launched by misbehaving nodes in TB-MCDM.

- *Bad-mouthing attacks*: A malicious node can launch this attack on the recommendation trust building system module of TB-MCDM. In this attack, the malicious nodes provide unfairly low recommendations related to different trust measuring criteria for good nodes. This attack is launched with an ill intent to tarnish the trust value of good nodes and so as to reduce their chances of being selected as the packet forwarder in the routing path. This situation may reduce the presence of good nodes in the network and may confuse a "Subject" to select a next-hop forwarder in the routing path formation.

- *Good-mouthing attacks*: In this attack, the malicious nodes provide unfairly positive recommendations for some colluding nodes and boost their trust values in the network. The intention of such an attacker is to increase the chance of packet routing through malicious nodes and thus dropping those packets from the network leading to performance degradation of the TB-MCDM framework.

- *Selfish attacks*: The selfish nodes are those who are unwilling to spend their resources on forwarding packets of other nodes with whom they do not have good social relationships. Thus, they may launch selfish attacks by dropping those packets for which they are not interested to forward. This act of selfish nodes degrades the intended network performance.

4.5 Performance Evaluation of TB-MCDM against Attacks

This section presents the experimental study that has been carried out to confirm the TB-MCDM's resiliency against *Bad-mouthing*, *Good-mouthing*, and *Selfish* attacks. The experimental environment is created with the NS 2 simulator [125], which is designed to

evaluate routing protocols of wireless networks. Extensive simulations are carried out to evaluate TB-MCDM's resiliency in terms of standard security metrics viz., *Attack Detection Rate* (ADR), *False Negative Rate* (FNR), and *False Positive Rate* (FPR) in the presence of bad-mouthing, good-mouthing and selfish attacks. The metric ADR represents the number of misbehaving nodes providing dishonest recommendations identified by TB-MCDM, while FNR indicates the number of dishonest recommendations identified as honest, and FPR represents the number of honest recommendations identified as dishonest by the TB-MCDM framework. The percentage of misbehaving nodes are varied to evaluate the TB-MCDM's resiliency under different attack conditions. Further, the same set of experiments are also carried out with different trust threshold settings to get the best achievable performance of the TB-MCDM under dynamically changing network conditions in a hostile HetMesh scenario.

Table 4.1: Parameters For Attacks Scenario Simulation Model

Simulation Parameters	**Value**
Simulator	ns-2 (version 2.35)
Operating System	Linux (Ubuntu 10.04)
Simulation Time	100 sec
Simulation Area	[1000m X 1000m]
Number of Nodes	50
Percentage of Misbehaving Nodes	[5% - 45%]
Transmission Range	250 meters/sec
Interference Range	550 meters
Node Placement Distance	200 meters
Movement Mode	Random-Waypoint
Speed of Mobile Nodes	[1 meter/sec-5 meter/sec]
Pause Time	5 sec
Traffic Type	CBR
Total CBR Flows	25
Data Payload	512 bytes
Packet Rate	[20p/sec-60p/sec]
Mac Layer	802.11 DCF with RTS/CTS
Radio Frequency	2.4 GHz
Radio Channel Rate	2Mbps
RF Propagation Model	Two-RayGround
Antenna	Omni-directional

4.5.1 Simulation Environment

The resiliency of TB-MCDM against different attack scenarios is evaluated on top of the Adaptive Path Selection Scheme (Adapt-PSS) [119] routing protocol developed for HetMesh. In the experimental setup, we have considered both honest and misbehaving nodes

moving in the network area. The node mobility is created with RandomWayPoint mobility model. The source-destination pairs are selected at random from the honest nodes. The parameter settings for all our experiments are listed in Table 4.1.

4.5.2 Results and Analysis

Here we analyze the set of results that have been obtained from the simulation study to confirm the resiliency of TB-MCDM under different attack scenarios. The effects of such attacks are also analyzed with different trust threshold settings.

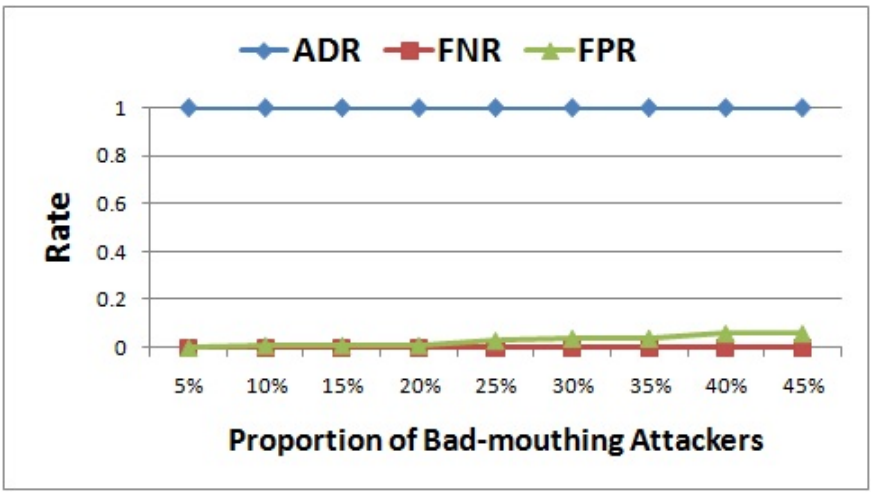


Figure 4.5: ADR, FPR, FNR against Trust Threshold 0.3

Figures 4.5, 4.6, and 4.7 exhibit the effects of *Bad-mouthing* attack on TB-MCDM's ADR, FNR, and FPR metrics. The simulations have been carried out by varying the proportion of attackers from 5% to 45% in the network. It has been observed that TB-MCDM can effectively mitigate the dishonest recommendations propagated by the bad-mouthing attackers. The ADR and FNR metrics show optimal results in the presence of bad-mouthing attackers, while keeping the FPR at a very low level (3%). The results of the simulation study are obvious due to the consideration of different set of axioms for recommendation collection and aggregation in TB-MCDM. The TB-MCDM framework allows a "Subject" to receive recommendations from trustworthy nodes only. Moreover, it has the capability of avoiding dishonest recommendations through the offset evaluation procedure that can segregate an honest recommendation from a dishonest one. Thus, the recommendations from the misbehaving nodes could be avoided in recommendation trust building system of TB-MCDM.

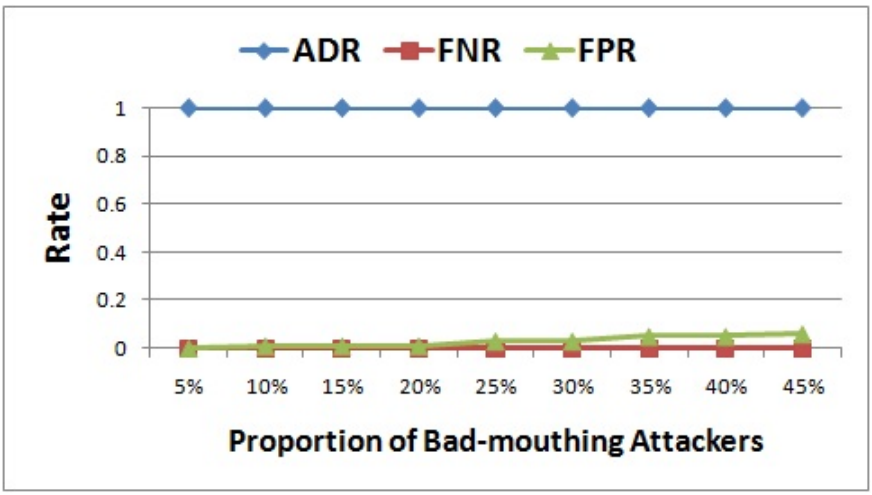


Figure 4.6: ADR, FPR, FNR against Trust Threshold 0.5

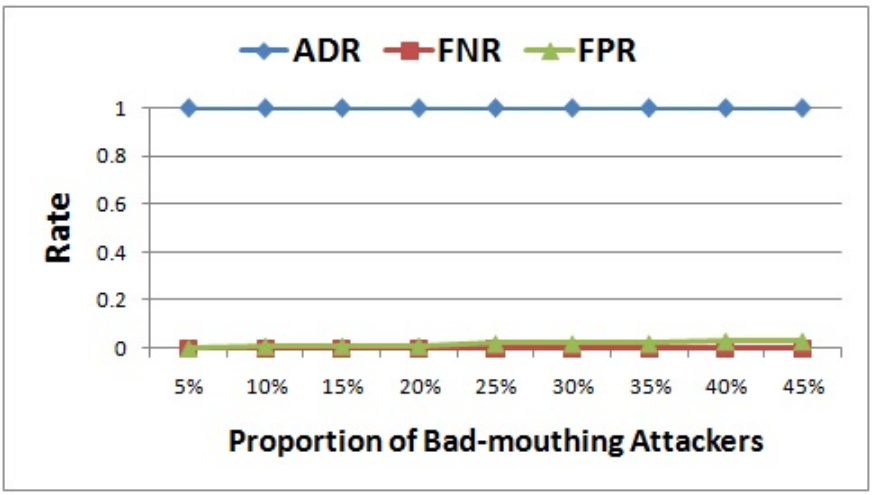


Figure 4.7: ADR, FPR, FNR against Trust Threshold 0.7

The reason for existence of low FPR is the consideration of the *offset* threshold value due to which some honest recommenders are treated as dishonest. Further, with different trust threshold settings, the simulation results of TB-MCDM represent a similar trend in terms of ADR, and FNR metrics. Whereas, the existence of FPR (with trust threshold 0.3 and 0.5) has been nullified with trust threshold 0.7, because this setting has allowed only high trust valued nodes to participate in trust building process and thereby minimizing the effects of recommendation offset.

Figures 4.8, 4.9, and 4.10 depict the effect of *Good-mouthing* attack on TB-MCDM's

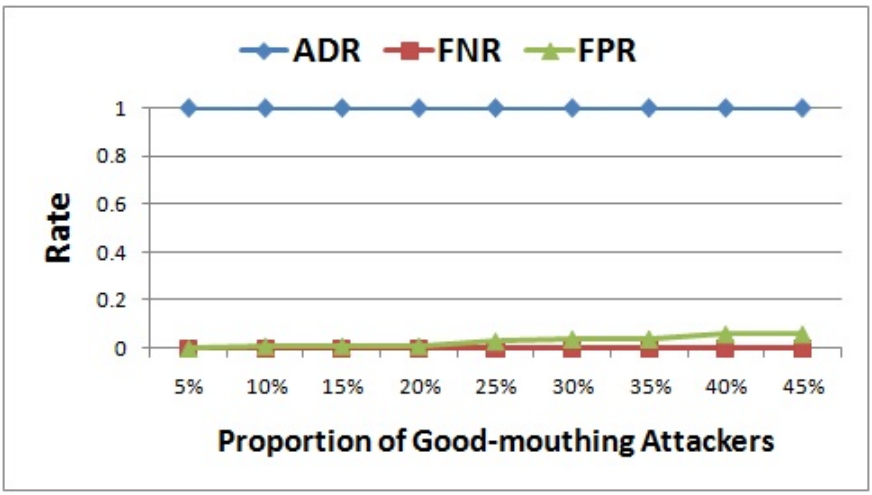


Figure 4.8: ADR, FPR, FNR against Trust Threshold 0.3

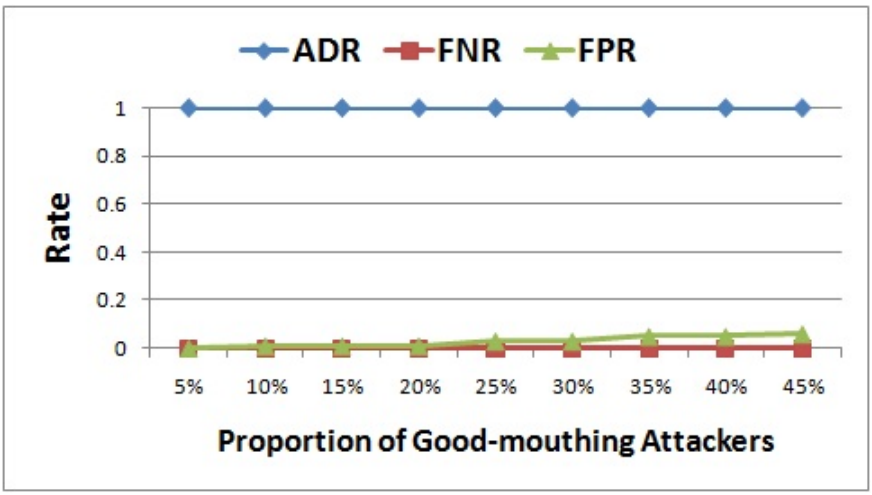


Figure 4.9: ADR, FPR, FNR against Trust Threshold 0.5

ADR, FNR, and FPR metrics. Similar, to bad-mouthing attack, in this set of simulations, the percentage of good mouthing attackers are varied from 5% to 45% to evaluate the resiliency of the TB-MCDM framework in terms of ADR, FNR, FPR. The proposed framework is seen to be identifying the dishonest recommendations and eliminating false negatives effectively. The proportion of false positives is maintained at a reasonable low level. The justification for such results is similar to what was explained in the case of *Bad-mouthing* attack.

Figures 4.11, 4.12, and 4.13 show the performance of TB-MCDM in the presence of *Selfish* attacks. In a social environment, selfish nodes launch such attacks by dropping

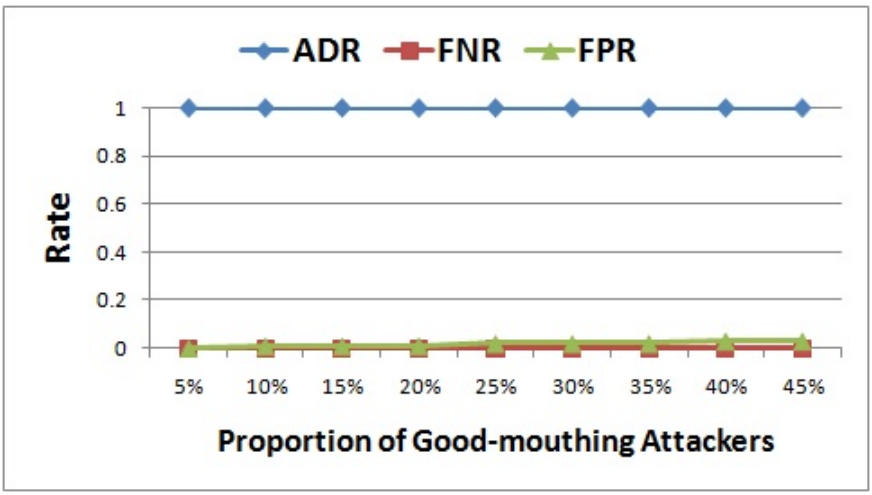


Figure 4.10: ADR, FPR, FNR against Trust Threshold 0.7

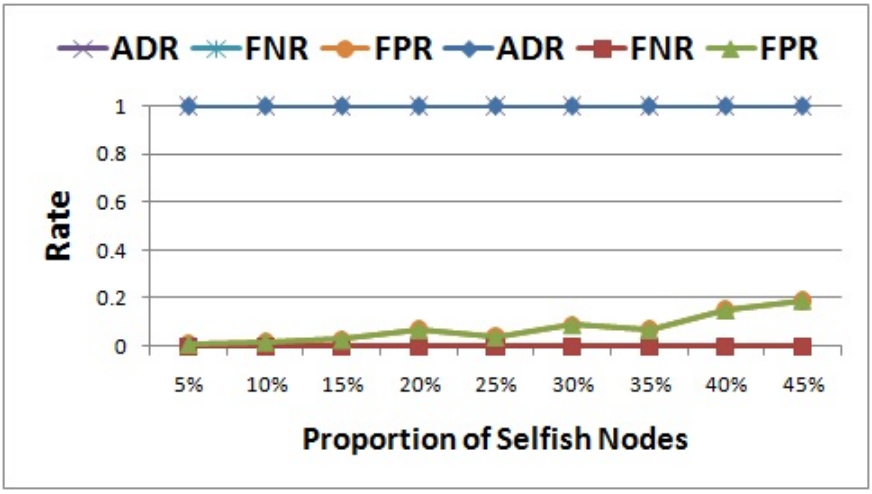


Figure 4.11: ADR, FPR, FNR against Trust Threshold 0.3

packets to save their resources if those packets are meant for the recipients with whom the attacker does not have good social ties. In our experimental study, we simulate this attack with node's packet dropping behavior. The results generated from the simulation study exhibit the efficiency of TB-MCDM in terms of ADR and FNR. This was achievable due to the consideration of the trust measuring criteria i) *number of packets to be forwarded on behalf of a Subject* and ii) *number of packets successfully forwarded by the Agent* to simulate the selfish behavioral pattern of HetMesh nodes and thus can avoid *Social attacks* in the routing path.

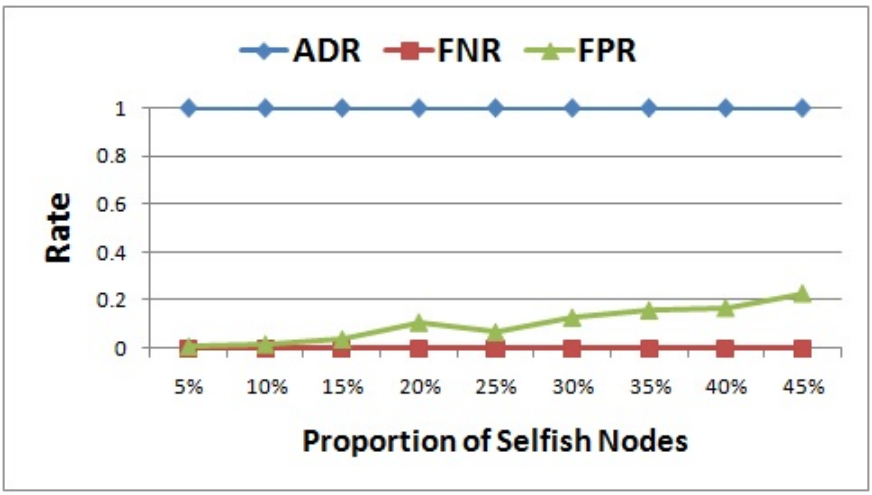


Figure 4.12: ADR, FPR, FNR against Trust Threshold 0.5

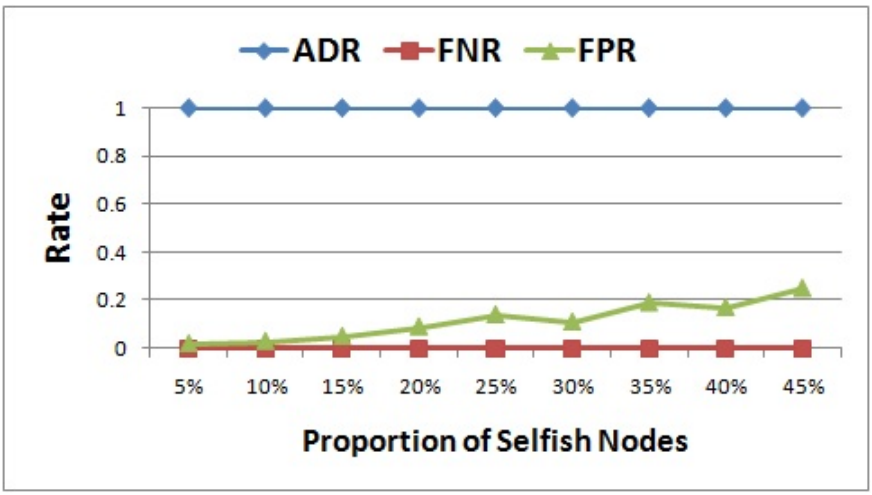


Figure 4.13: ADR, FPR, FNR against Trust Threshold 0.7

The increasing trend in the FPR with an increase in selfish attackers is an effect of nodes' packet dropping due to non availability of suitable next hop forwarder. Further, with high trust threshold settings, the chances of availability of competent forwarders get reduced and thus the scope of packet forwarding in HetMesh is lowered. These factors cause buffer overflow at the participating nodes leading to rise in FPR.

It has been observed from the simulation study that consideration of different trust axioms for recommendation collection have a varied level of positive impacts on the performance of TB-MCDM against different security attacks. The simulation results demonstrate

that with different trust threshold settings (i.e., 0.3, 0.5, 0.7), the ADR and FNR remain stable in the presence of "Bad-mouthing", "Good-mouthing", and "Selfish" attacks. But the amount of FPR decreases by 3% with changes in threshold (i.e., from 0.5 to 0.7) for "Bad-mouthing" and "Good-mouthing" attacks, whereas it increases by 5% for "Selfish" attacks. The reason for low FPR with increasing trust threshold (i.e., 0.7) setting in case of "Bad-mouthing" and "Good-mouthing" attacks is that this threshold has allowed only high trust valued nodes to provide recommendations and thereby the effects of recommendation offset gets minimized. Whereas an increase in FPR with trust threshold 0.7 in case of "Selfish" attacks is due to the non-availability of competent forwarders in the routing paths. This causes honest nodes to drop messages due to buffer overflow leading to rise in false positive proportions. Therefore, it can be concluded that consideration of threshold setting as 0.5 enhances the performance of TB-MCDM by eliminating nodes' misbehaving activities (i.e., dishonest recommendations and nodes' selfish behaviors) even though it could result in a small proportion of FPR (3% only) in all the attack scenarios under consideration.

4.6 Simulation of TB-MCDM and Performance Evaluation

This section introduces the different sets of simulation study that have been carried out to test the adaptability and suitability of the TB-MCDM framework for ensuring routing security in hostile HetMesh environment. To validate the useability and adaptability of the proposed framework, we have integrated it with a unified path selection scheme [119] available in HetMesh. Thus, TB-MCDM framework has not only been integrated with non-trust based forwarding algorithm [119] available in HetMesh, but also been compared with a trust based routing protocol, as available in [126] to evaluate a node's ability for secure route formation and therefore reliable delivery of data to the destination. The protocols under study are *Adaptive Path Selection Scheme* (Adapt-PSS) [119] and *Trusted Modified Optimized Link State Routing* (TM-OLSR) [126].

TB-MCDM has been implemented with Network Simulator NS-2 [125]. The protocols available in [119], [126] are re-simulated in this work to enable comparisons in the same scenarios with NS-2 [125] simulator. Extensive simulations are carried out to evaluate TB-MCDM's performance in terms of throughput, Packet Delivery Ratio (PDR), Normalized Routing Overhead (NRO) and end-to-end delay under various networking scenarios with varying number of misbehaving nodes, traffic load, and node speed. A comparative analysis of TB-MCDM with TM-OLSR [126] and Adapt-PSS [119] has been studied to evaluate its

adaptability and suitability in hostile HetMesh environment.

The Trusted Modified Optimized Link State Routing (TM-OLSR) Protocol integrates a multiple criteria decision making technique based trust model with M-OLSR (Modified OLSR) [10] for trust evaluation and detection of malicious and misbehaving nodes in Wireless Mesh Networks (WMNs). The three main functionalities of the TM-OLSR protocol are *HELLO Exchange*, *Topology Dissemination*, and *Routing Table Calculation*. Each node in TM-OLSR detects its trustworthy, static, and symmetric neighbor nodes with which it has a direct link through periodic exchange of "HELLO" messages." HELLO" message serves three independent tasks: *i)* Link sensing, *ii)* Neighbor detection, *iii)* MPR Selection signaling. The outcome of link sensing is a link Set and is used when declaring neighbor information in HELLO messages. The outcome of HELLO exchange is neighbor table for each node in TM-OLSR. The table records information about its one hop neighbors, link status with these neighbors, neighbor type, neighbor trust value, neighbor status and a list of two-hop neighbors. On the basis of collected information, each node in TM-OLSR calculates its routing table containing destination node address, Next-hop node address and hop required to reach the destination, which allows it to route data to destination node in the network. Route is through its trusted static router nodes. Client nodes communicate with the destination through trusted static routers. Any amount of client-to-client communication is through static trusted routers only.

The Adapt-PSS is a unified path determination scheme for high throughput HetMesh, where a novel resilient path metric has been defined by combining multiple path selection criteria to leverage the resource availability of clients for acting as potential forwarders. The protocol uses both proactive and reactive approaches for improving path selection quality in a high throughput HetMesh network. The backbone routers in Adapt-PSS use an improved version of Optimized Link State Routing (OLSR), called M-OLSR (Modified OLSR) [10], for maintaining their routing table in a proactive manner, which is updated during each refresh interval. Whenever a mobile client has packets to transmit, it broadcasts a probe packet to its neighbor nodes requesting their willingness in packet forwarding. The neighbors then replies back with feedback packets informing their willingness to forward traffic in the network. Depending on the received feedback packets, the source node performs additional computation to estimate link quality of willing neighbors. From the acquired feedback and estimated information, the source node in Adapt-PSS computes path metric adaptively that leads to the selection of a better path in a congenial HetMesh environment. The routing performance of Adapt-PSS has been simulated and evaluated with and without integrating

the TB-MCDM framework in a hostile HetMesh environment. The Adapt-PSS protocol with TB-MCDM is renamed as Adaptive-TB-MCDM. From now onwards, we address TB-MCDM as Adaptive-TB-MCDM in the rest of our work in this chapter.

4.6.1 Assumptions

Our simulation model is based on a hierarchical network architecture called HetMesh, where two types of nodes exists, viz., routers and clients. Routers are static forming a infrastructure backbone and clients has the mobility. Clients of HetMesh have got a spontaneous and dynamic character where they can communicate among themselves in a multi-hop fashion without involving backbone routers. The backbone routers are static, non power-constrained, and maintain their own routing Tables proactively. On the other hand, the clients are mobile, energy-constrained and are enabled with Wi-Fi Direct mode to connect in a peer-to-peer manner. The Wi-Fi Direct mode has the ability to connect heterogeneous clients, and allows direct data transmission among themselves with minimal setup. For simplicity we assume that misbehaving nodes drop the packets they receive.

4.6.2 Simulation Environment

We first investigate the establishment of trust table in each individual node of HetMesh through proposed trust building model. Initially the Trust value of each nodes is 0. TB-MCDM based routing protocol and the trust model works in association to each other. Trust is calculated in each time interval and remain valid for a small time duration. Our Adaptive-TB-MCDM, Adapt-PSS and TM-OLSR routing models are built on the top of IEEE 802.11 MAC model of NS-2 and random waypoint model is adopted for driving mobile clients. A node in motion updates its position after every fixed interval of time. In order to gain good confidence in the measurement results, we run simulations 10 times with different seed values to obtain mean value of different matrices. Table 4.2 depicts the parameters set for simulation model that is common for all our simulation scenarios. The other attributes of our simulations viz., number of misbehaving nodes, node speed, and traffic load are varied from scenario to scenario.

Table 4.2: Parameters for Simulation Model

Simulation Parameters	**Value**
Simulator	ns-2
Operating System	Linux (Ubuntu 10.04)
Simulation Time	100 sec
Simulation Area	1000m X 1000m
Number of Nodes	50
Transmission Range	250 meters/sec
Interference Range	550 meters
Node Placement Distance	200 meters
Movement Mode	Random-Waypoint
Speed of Mobile Nodes	1 meter/sec-5 meter/sec
Pause Time	5 sec
Traffic Type	CBR
Total CBR Flows	25
Data Payload	512 bytes
Packet Rate	20p/sec-60p/sec
Mac Layer	802.11 DCF with RTS/CTS
Radio Frequency	2.4 GHz
Radio Channel Rate	2Mbps
RF Propagation Model	Two-RayGround
Antenna	Omni-directional

4.6.3 Performance Metrics

The performance of Adaptive-TB-MCDM has been measured in terms of throughput, Packet Delivery Ratio (PDR), Normalized Routing Overhead (NRO) and End-to-End Delay, which are defined next.

- *Throughput*: Throughput is computed as the amount of data transferred (in bytes) divided by the simulated data transfer time (the time interval from sending the first CBR packet to receiving the last CBR packet).
- *Packet Delivery Ratio* (PDR): PDR is the ratio of the number of packets delivered and the number of packets generated by CBR sources.
- *Normalized Routing Overhead* (NRO): NRO is defined as the ratio of number of control packets propagated in the network to the number of data packets received by destination nodes.
- *End-to-End Delay* : End to End delay is defined as the average transit time of a packet, i.e., the time taken for a packet to reach destination from the source.

4.6.4 Results and analysis

This section analyzes the set of results that have been obtained from the simulation study to evaluate the efficiency of the TB-MCDM framework. The effectiveness of the TB-MCDM framework has been evaluated under three different networking scenarios with varying degree of misbehaving nodes, traffic load, and node speed. A comparative analysis with Adapt-PSS, and TM-OLSR is also provided to justify its suitability in a hostile HetMesh environment.

Impact of number of misbehaving nodes

In this set of simulations, the impact of the number of misbehaving nodes on the performance of Adapt-PSS, TM-OLSR, and Adaptive-TB-MCDM are investigated. The percentage of misbehaving nodes are varied proportionately from each of the two different groups, i.e., static mesh routers and mobile clients of HetMesh nodes.

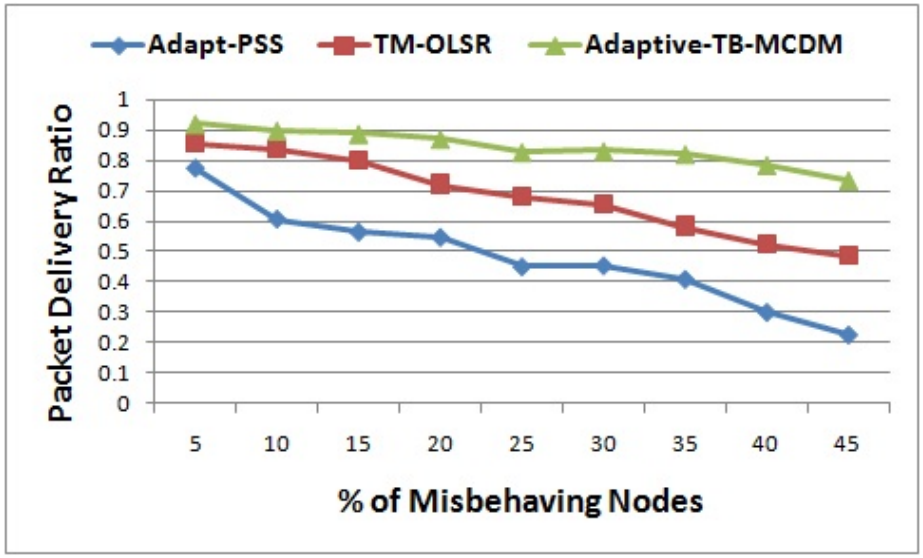


Figure 4.14: Packet Delivery Ratio Vs. Percentage of Misbehaving Nodes

Figure 4.14 depicts the packet delivery ratio (PDR) as a function of the percentage of misbehaving nodes for Adapt-PSS, TM-OLSR, and TB-MCDM based routing i.e., Adaptive-TB-MCDM in the underlying HetMesh environment. PDR is calculated as the ratio of the number of packets successfully delivered and the number of packets generated by CBR sources. In the simulation study, a decreasing trend in delivery ratio for all protocols have been observed. This is due to the fact that, with increased number of misbehaving nodes, the chances that a good node encounters a bad node for packet forwarding also increases,

which eventually drops the packet or may not forward it for onward transmission to the destination. It is noticeable that with less number of misbehaving nodes (i.e, with 25%), the message delivery probability of Adapt-PSS degrades significantly. This is due to non-consideration of any security framework in the forwarder selection scheme. This causes inclusion of misbehaving nodes in the routing path. But in comparison to TM-OLSR protocol, the performance of Adaptive-TB-MCDM routing have shown better results in terms of packet delivery ratio in a hostile HetMesh environment. This is due to the consideration of trusted mobile clients as well as routers in the routing path calculation. The performance degradation of TM-OLSR is due to the non availability of trusted forwarder in the routing path since it only relies on static routers for communication. Further, the routing capability of the mobile clients in Adaptive-TB-MCDM increases the chances of packet delivery through multiple paths that comprise of trusted mobile clients and backbone routers.

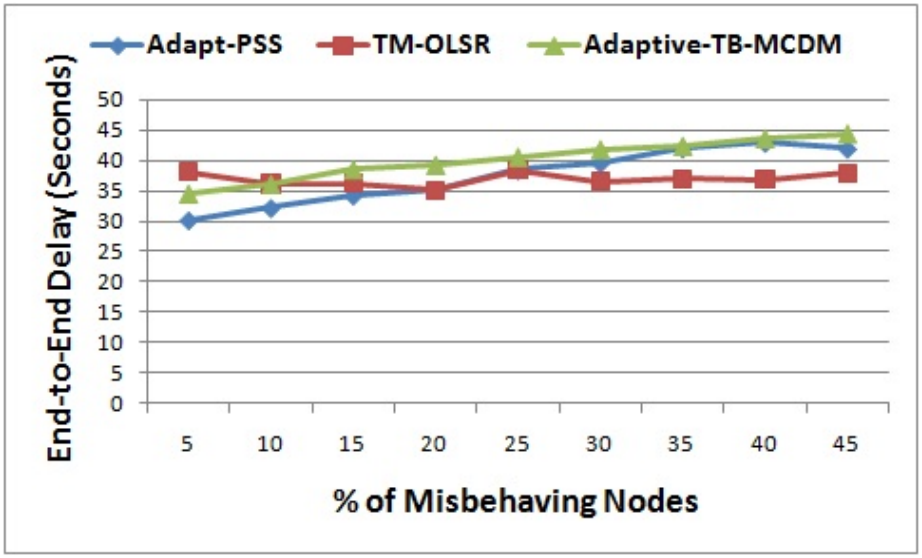


Figure 4.15: End-to-End Delay Vs. Percentage of Misbehaving Nodes

Figure 4.15 exhibits the end-to-end delay for delivering a packet with the variation of misbehaving nodes in HetMesh. The end-to-end delay is defined as the average transit time of a packet, i.e., the time taken for a packet to reach destination from the source. It has been observed that with increasing number of misbehaving nodes the end-to-end delay for Adapt-PSS, TM-OLSR, and Adaptive-TB-MCDM routing protocols increase sharply. This is due to the presence of either maliciousness or selfishness in node's behavior that cause more packets either to get dropped or may not be forwarded for onward transmission to the destination. It is noticeable that the end-to-end delay of Adaptive-TB-MCDM is slightly more than that of trust-based (i.e., TM-OLSR) and non trust-based (i.e., Adapt-PSS)

protocols under consideration. The reason for increase in delay with increasing number of malicious nodes in Adaptive-TB-MCDM is due to the integration of the proposed trust based framework framework with the path selection metric of Adapt-PSS. In Adaptive-TB-MCDM, a next hop forwarder is selected on the basis of feedback, estimated technical competency, and trust components in a hop-by-hop manner for path determination. But the rise in delay in Adaptive-TB-MCDM is insignificant as compared to Adapt-PSS and TM-OLSR.

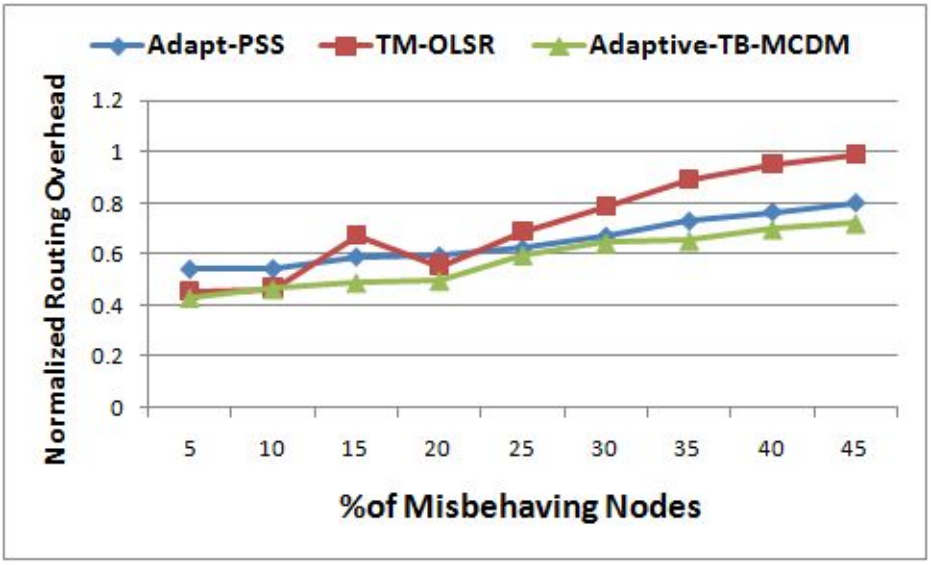


Figure 4.16: Normalized Routing Overhead Vs. Percentage of Misbehaving Nodes

Figure 4.16 depicts the Normalized Routing Overhead (NRO) for all the protocols under consideration. The NRO is defined as the ratio of number of control packets propagated in the network to the number of data packets received by destination nodes. It has been observed that Adaptive-TB-MCDM protocol outperforms TM-OLSR protocol in terms of routing overhead with increasing number of misbehaving nodes. It is justifiable due to Adaptive-TB-MCDM's adaptiveness in link quality and trust estimation and the availability of multi-hop capability of mesh clients. These quality of Adaptive-TB-MCDM reduces the chance of packet drops and repeated route estimation process.

Impact of volume of traffic load

In this scenario, simulations are carried out with different traffic load condition i.e. varying number of data packets sent per seconds while keeping the number of connections/flows constant. The performance of the protocols under consideration are evaluated in terms of Throughput, PDR , NRO and End-to-End Delay. This set of simulation experiments is performed in presence of 25 number of misbehaving nodes. The other simulation parameters

remain same as referred in the Table 4.2.

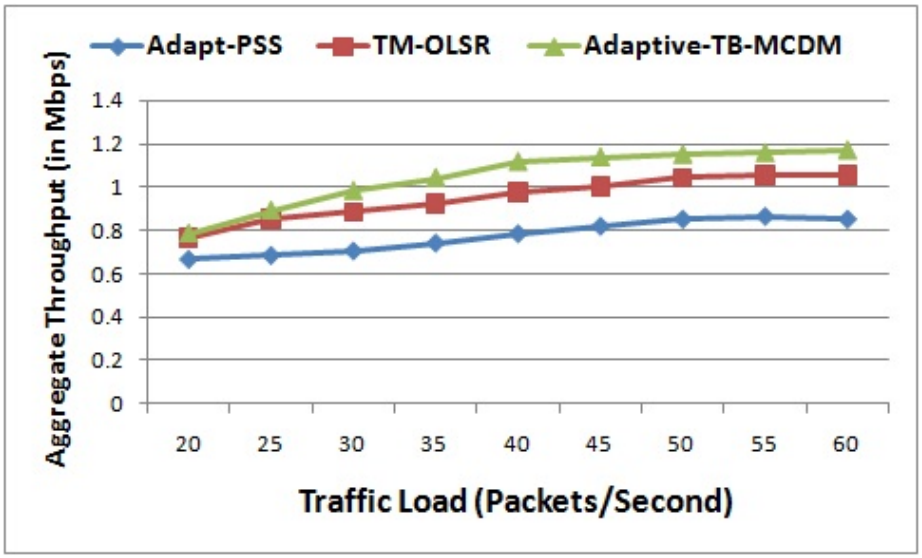


Figure 4.17: Aggregate Throughput vs. Traffic Load

From Figure 4.17, it has been observed that the aggregate throughput of TM-OLSR and Adaptive-TB-MCDM confirms resilience to increasing traffic load. In fact, Adaptive-TB-MCDM outperforms TM-OLSR. It is noticeable that, aggregate throughput of both the protocols increases with increasing traffic load and then tends to reach a saturation point according to the network conditions, e.g. 40 packets/flow for Adaptive-TB-MCDM and 50 packets/flow for TM-OLSR. But Adaptive-TB-MCDM performs better at TM-OLSR's saturation point too. The reason for improved performance in Adaptive-TB-MCDM is due to its' capability of incorporating path selection quality in trusted computation of next hop forwarder selection. The reason for performance degradation in Adapt-PSS is non-consideration of trust building mechanism in route calculation. The simulation results consistently proved that when compared with Adapt-PSS, and TM-OLSR, Adaptive-TB-MCDM exhibits a much better scalability on traffic loads.

Figure 4.18, shows that as offered traffic load intensifies, aggregate PDR decreases for all the protocols because of increased intra-flow and inter-flow interference and contention. However, performance of Adaptive-TB-MCDM degrades gracefully than TM-OLSR. The degradation in TM-OLSR is almost 25% higher than Adaptive-TB-MCDM. Although, both the protocols calculate best available routes using trusted nodes, but the chances of link breakage is minimum in Adaptive-TB-MCDM. This is possible because of the incorporation of of multiple attribute path selection criteria with trust evaluation process. This increases the chances of packet delivery and hence chances of packet drops due to misbehaving and

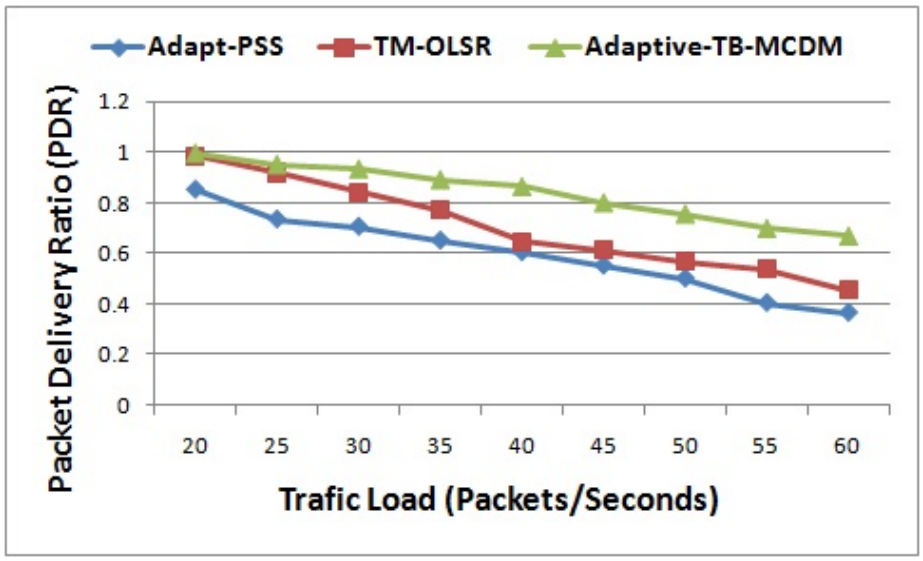


Figure 4.18: Packet Delivery Ratio vs. Traffic Load

malicious nodes are minimized.

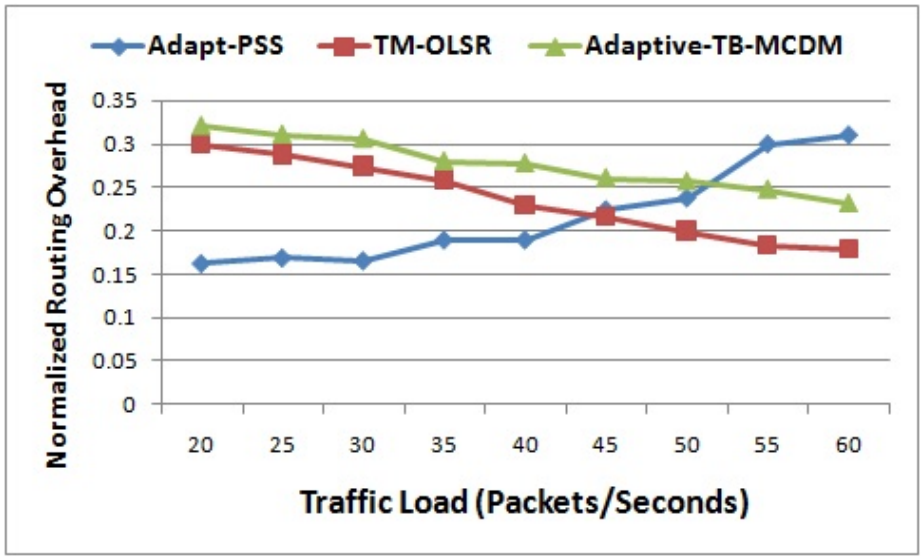


Figure 4.19: Normalized Routing Overhead vs. Traffic Load

Figure 4.19 depicts normalized routing overhead (NRO) as a function of offered traffic load for the three protocols under consideration. TM-OLSR performs slightly better than Adaptive-TB-MCDM. The reason is that, TM-OLSR uses a proactive component called M-OLSR for route calculation. Being having proactive component, TM-OLSR shows overhead immunity to traffic load. Once route is available to a source node, data packets follow the same route to reach a destination. As traffic load increases, aggregate throughput also increases, whereas overhead of control packets is almost constant because of proactive

routing. But, the reason for higher routing overhead (which is insignificant as compared to M-OLSR) in Adaptive-TB-MCDM is due to the added path selection quality metric with security features. The rise in NRO of Adaptive-TB-MCDM is by .05% as compared to TM-OLSR. However, NRO of Adapt-PSS increases significantly due to the incorporation of misbehaving nodes in the routing path which further increases the chances of packet drops and repeated estimation process.

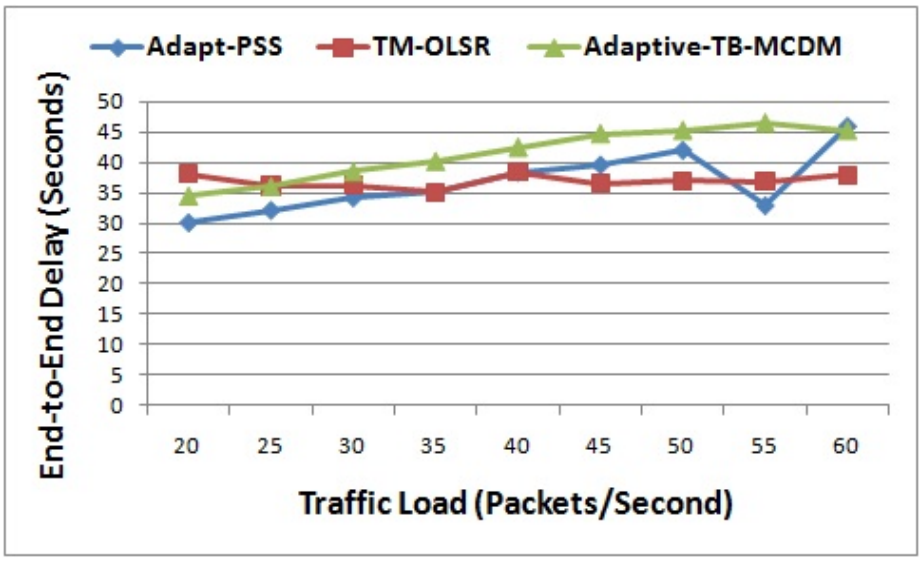


Figure 4.20: End-to-End Delay vs. Traffic Load

From Figure 4.20, we observed the end-to-end delay for all three protocols with varying degree of traffic load. The delay rises in a linear fashion for both TM-OLSR and Adaptive-TB-MCDM protocols. The amount of delay incurred in Adaptive-TB-MCDM is slightly more than TM-OLSR. The reason is that, in Adaptive-TB-MCDM the process of trusted forwarder selection coupled with path selection quality incurs additional amount of end-to-end delay by filtering undesirable encounter opportunities (i.e., misbehaving nodes) in the routing path.

Impact of node dynamics

To analyze Adaptive-TB-MCDM's scalability with network dynamics, we performed simulations by varying the speed of mobile clients from 1meter/sec to 5meter/sec., and comparison is carried out with TM-OLSR and Adapt-PSS. The number of misbehaving nodes are 25 and the other simulation parameters are kept same as referred in the Table 4.2.

Table 4.3 and Table 4.4 depict the aggregate CBR throughput, PDR, NRO and end-to-

Table 4.3: Comparative Performance of Adapt-PSS and Adaptive-TB-MCDM in a Dynamic Network

Data Sheet									
		Throughput		PDR		NRO		End-to-End Delay	
Traffic Load	Mobility	Adapt-PSS	TB-MCDM	Adapt-PSS	TB-MCDM	Adapt-PSS	TB-MCDM	Adapt-PSS	TB-MCDM
20 packets/sec	1meter/sec	0.714	0.785	0.910	0.984	0.38	0.299	12.74	40.103
	3meter/sec	0.705	0.764	0.897	0.967	0.444	0.398	15.933	41.150
	5meter/sec	0.684	0.743	0.865	0.956	0.492	0.456	11.452	35.977
25 packets/sec	1meter/sec	0.779	0.890	0.829	0.920	0.347	0.237	19.205	43.138
	3meter/sec	0.754	0.862	0.795	0.910	0.450	0.390	19.556	47.136
	5meter/sec	0.751	0.845	0.774	0.903	0.484	0.437	15.587	36.771
30 packets/sec	1meter/sec	0.863	0.982	0.799	0.870	0.354	0.224	29.239	38.203
	3meter/sec	0.845	0.968	0.762	0.853	0.429	0.359	19.421	48.116
	5meter/sec	0.826	0.952	0.741	0.840	0.427	0.414	18.248	42.362
35 packets/sec	1meter/sec	0.865	1.0426	0.769	0.819	0.365	0.189	17.767	37.103
	3meter/sec	0.858	0.970	0.720	0.785	0.435	0.309	26.138	49.973
	5meter/sec	0.840	0.955	0.712	0.775	0.426	0.415	18.823	1.362
40 packets/sec	1meter/sec	0.888	1.116	0.710	0.786	0.360	0.19	31.523	48.387
	3meter/sec	0.878	0.987	0.697	0.752	0.383	0.336	24.279	57.519
	5meter/sec	0.875	0.978	0.652	0.710	0.445	0.407	21.747	45.533
45 packets/sec	1meter/sec	0.940	1.118	0.655	0.733	0.335	0.166	32.862	35.567
	3meter/sec	0.896	1.101	0.616	0.701	0.425	0.303	21.813	59.086
	5meter/sec	0.88	0.982	0.605	0.682	0.444	0.381	17.340	44.971
50 packets/sec	1meter/sec	0.973	1.109	0.633	0.663	0.288	0.189	44.781	37.965
	3meter/sec	0.967	0.986	0.594	0.629	0.391	0.297	27.010	58.374
	5meter/sec	0.956	0.976	0.563	0.609	0.437	0.394	21.345	45.264
55 packets/sec	1meter/sec	0.952	1.127	0.6175	0.676	0.250	0.162	29.192	45.475
	3meter/sec	0.937	0.980	0.537	0.598	0.430	0.302	18.646	57.280
	5meter/sec	0.926	0.970	0.517	0.586	0.396	0.380	17.273	46.589
60 packets/sec	1meter/sec	0.985	1.109	0.596	0.645	0.262	0.169	18.483	43.899
	3meter/sec	0.945	0.974	0.518	0.562	0.344	0.283	21.519	60.110
	5meter/sec	0.929	0.969	0.485	0.521	0.366	0.362	20.252	43.080

end delay versus client mobility under different load condition for Adapt-PSS, TM-OLSR, and Adaptive-TB-MCDM protocols. As the speed increases, throughput and PDR drops for all protocols under observation, because mobile nodes lose connectivity with its next hop more often leading more route breaks and data loss. However, with increased mobility, as compared to TM-OLSR, degradation in throughput and PDR for Adaptive-TB-MCDM are insignificant because the client nodes in Adaptive-TB-MCDM collaborate among themselves for routing and use their trust table for forwarder selection. So chances of packets drop is minimized. The low performance of Adapt-PSS is obvious for existence of malicious nodes in the routing path. It has been observed that NRO of Adaptive-TB-MCDM rises insignificantly as compared to TM-OLSR in dynamic network. This is due to added path selection quality with trust mechanism which increases the flow of control packets in the networks. End-to-End delay of both TM-OLSR and Adaptive-TB-MCDM increase in a linear fashion with increase in load and speed, because the process of trusted forwarder selection may incur additional amount of end-to-end delay by filtering undesirable encounter opportunities (i.e., misbehaving nodes) in the routing path.

Finally, Table 4.5 summarizes the comparison of TB-MCDM, TM-OLSR, and Adapt-PSS protocols depicted in experimental results/graphs provided in this chapter of the thesis.

Table 4.4: Comparative Performance of TM-OLSR and Adaptive-TB-MCDM in a Dynamic Network

Data Sheet									
		Throughput		PDR		NRO		End-to-End Delay	
Traffic Load	Mobility	TM-OLSR	TB-MCDM	TM-OLSR	TB-MCDM	TM-OLSR	TB-MCDM	TM-OLSR	TB-MCDM
20 packets/sec	1meter/sec	0.76734	0.785	0.9347	0.984	0.38134	0.299	34.5612	40.103
	3meter/sec	0.7191	0.764	0.8964	0.967	0.43724	0.398	30.8135	41.150
	5meter/sec	0.70631	0.743	0.83172	0.956	0.491372	0.456	28.562	35.977
25 packets/sec	1meter/sec	0.8561	0.890	0.9214	0.920	0.39145	0.237	36.135	43.138
	3meter/sec	0.77952	0.862	0.83123	0.910	0.48563	0.390	32.5619	47.136
	5meter/sec	0.74913	0.845	0.78123	0.903	0.49561	0.437	29.6572	36.771
30 packets/sec	1meter/sec	0.8862	0.982	0.90132	0.870	0.35612	0.224	38.5392	38.203
	3meter/sec	0.79652	0.968	0.75813	0.853	0.51932	0.359	36.25617	48.116
	5meter/sec	0.75312	0.952	0.741234	0.840	0.54927	0.414	31.5672	42.362
35 packets/sec	1meter/sec	0.865	1.0426	0.769	0.819	0.365	0.189	17.767	37.103
	3meter/sec	0.858	0.970	0.720	0.785	0.435	0.309	26.138	49.973
	5meter/sec	0.840	0.955	0.712	0.775	0.426	0.415	18.823	1.362
40 packets/sec	1meter/sec	0.888	1.116	0.710	0.786	0.360	0.19	31.523	48.387
	3meter/sec	0.878	0.987	0.697	0.752	0.383	0.336	24.279	57.519
	5meter/sec	0.875	0.978	0.652	0.710	0.445	0.407	21.747	45.533
45 packets/sec	1meter/sec	0.940	1.118	0.655	0.733	0.335	0.166	32.862	35.567
	3meter/sec	0.896	1.101	0.616	0.701	0.425	0.303	21.813	59.086
	5meter/sec	0.88	0.982	0.605	0.682	0.444	0.381	17.340	44.971
50 packets/sec	1meter/sec	0.973	1.109	0.633	0.663	0.288	0.189	44.781	37.965
	3meter/sec	0.967	0.986	0.594	0.629	0.391	0.297	27.010	58.374
	5meter/sec	0.956	0.976	0.563	0.609	0.437	0.394	21.345	45.264
55 packets/sec	1meter/sec	0.952	1.127	0.6175	0.676	0.250	0.162	29.192	45.475
	3meter/sec	0.937	0.980	0.537	0.598	0.430	0.302	18.646	57.280
	5meter/sec	0.926	0.970	0.517	0.586	0.396	0.380	17.273	46.589
60 packets/sec	1meter/sec	0.985	1.109	0.596	0.645	0.262	0.169	18.483	43.899
	3meter/sec	0.945	0.974	0.518	0.562	0.344	0.283	21.519	60.110
	5meter/sec	0.929	0.969	0.485	0.521	0.366	0.362	20.252	43.080

Table 4.5: Comparative Analysis of TB-MCDM with TM-OLSR and Adapt-PSS

Works, Year Ref. No.	**Methodology used**	**Performance evaluation**		**Validation**	
		Routing metrics	**Security metrics**	**Protocol considered**	**Experimental setup**
TM-OLSR, 2013 [126]	Trust and MCDM based	Throughput, PDR NRO, End-to-end delay	None	M-OLSR	Simulation based
Adapt-PSS, 2015 [119]	Link-aware, resource based	Throughput, PDR NRO, End-to-end delay	None	M-OLSR, E-AODV, M-HRP,HWMP	Simulation, Testbed based
TB-MCDM	Trust and MCDM Technique	Throughput, PDR NRO, End-to-end delay	Detection rate, False positive, False negative	TM-OLSR, Adapt-PSS	Simulation, Testbed based

4.7 Conclusion

In this chapter, we have presented a trust based next-hop carrier selection framework called TB-MCDM for HetMesh routing security. The most important feature of TB-MCDM is that it integrates multiple criteria decision making technique with multiple trust measuring criteria for assigning trust values of each node in HetMesh. The TB-MCDM has been evaluated and analyzed through an extensive set of simulation study. The performance of the existing data forwarding protocol viz., Adapt-PSS designed for HetMesh has been found to get enhanced with the incorporation of the TB-MCDM framework and has shown more resilience to the increasing percentage of misbehaving nodes in a hostile HetMesh environment. The performance of TB-MCDM is evaluated for its resiliency against different kind

of attacks and a comparative analysis has been carried out with TM-OLSR under various networking scenarios with varying proportion of misbehaving nodes, traffic load, and node speed. The applicability of the TB-MCDM as a security framework for HetMesh routing has advantages of less complex computational overheads, as learning of the entire network is based on trust. Excellency in these qualities of the TB-MCDM makes it a worthy security framework for HetMesh routing in presence of misbehaving nodes. In the next chapter of this thesis, we have addressed the challenges of forwarder selection in a hostile delay tolerant networks (i.e., in the presence of misbehaving nodes).

5

A unified next-hop carrier selection framework based on trust and MCDM for assuring reliability, security and QoS in DTN routing

5.1 Introduction

Delay/Disruption Tolerant Networks (DTNs) [127] have evolved as a new communication paradigm for ensuring reliability to a class of challenged networks which mostly operate under harsh networking conditions. Examples of such networks include terrestrial mobile networks, military ad hoc networks, exotic media networks, sensor networks, etc. [128]. DTNs are characterized by intermittent connectivity, frequent link disruption, existence of non-contemporaneous end-to-end path, node sparsity, long and variable communication latency etc., which make routing challenging and may not be well served by the current end-to-end TCP/IP model [128]. Unlike Mobile Ad hoc Networks (MANETs), where packets are forwarded along a "stable" end-to-end path hiding node mobility, DTNs exploit node mobility to create contact opportunities. Thus, to cope with the prevailing intermittent connectivity, routing in DTNs is mobility-assisted and is characterized by a message propagation scheme called "store-carry-and-forward" [102]. Specifically, according to this scheme, the inter-

mediate nodes (known as carriers) on a communicating path are expected to take custody of the in-transit messages (called bundles) being transferred while they move around the network area until they get in contact with a suitable next-hop carrier. The protocols designed to address the routing issues in DTNs are broadly classified into two categories viz., *flooding* and *forwarding* [33]. The protocols in the flooding family induce multiple "replicas" of each message in the network without considering the potentiality of the candidate node for being selected as a next-hop carrier [34, 35, 36]. Though, these protocols in the flooding family increase the chances of message delivery but suffer from excessively high network overhead, leading to significant network congestion. So, forwarding-based routing has been explored to restrict the generation of bundle replicas in the network. The protocols in the forwarding family calculate an utility metric based on "knowledge" to qualify the candidate node as the next-hop carrier on the routing path. A single copy of each message is forwarded to the qualified node. Most of these knowledge-based protocols select a suitable next-hop carrier based on contact history of potential carriers [37, 38], knowledge about traffic patterns in the network [39] or on probability of encountering the destination node [40]. Furthermore, some of them have used multi-copy spraying mechanisms to improve reliability amidst intermittent connectivity [41, 42]. Recently, social based routing has become popular in DTN specific applications like vehicular networks, mobile social networks, pocket switched networks etc., where social network properties of the underlaying networks have been exploited for forwarding.

Although these various routing schemes look promising and work well in a friendly (i.e., congenial) DTN environment, they may not be accurate in a hostile scenario, (i.e., in the presence of "malicious" and "selfish" nodes), where behavior of nodes is unpredictable from the network as well as social perspectives [118], [57]. Therefore, under such circumstances these knowledge, social and probabilistic approach-based protocols may lead a node to select a misbehaving node (viz., malicious or socially selfish) as the next-hop carrier. Thus, a misbehaving node can attract messages from a legitimate node, then move away and drop those messages which in turn detrimentally degrade the DTN's performance. The misbehaving nodes have either negative or limited contributions to the network. Consequently, a communicating node has to be cautious when selecting a next-hop carrier for in-transit messages. The presence of misbehaving nodes in the forwarding path may cause a serious threat to DTN-based communication and thus routing becomes vulnerable to different kinds of attacks. Malicious nodes might attempt to generate black hole, DoS, and spoofing attacks, whereas selfish nodes may try to maximize their own benefits and may decide to

forward a message if they have good social ties with source, current carrier or destination node [58].

The subject of this chapter is the introduction of a novel unified next-hop carrier selection framework in DTNs, that is based on trust and Multiple Criteria Decision Making (MCDM) Technique [121]. The proposed framework is called “Multiple Attribute Trust Evaluation and Management" (MATEM) and takes into account multiple trust measuring criteria to address the different issues in a hostile DTN scenario. The trust criteria “Risk” and “Co-operativeness” are proposed to combine the malicious and social behavior of nodes. The measures of “Uncertainty” and “Average Message Forwarding Delay” are proposed to quantify the inherent risk involved in DTNs’ message propagation scheme as well as to ensure QoS requirement of DTN routing in a hostile environment. The effectiveness and robustness of MATEM against attacks are evaluated through extensive simulations and testbed implementation.

The rest of the chapter is organized as follows. The background study, existing works, issues, motivation, and contributions are presented in Section 5.2. The proposed MATEM framework and its’ different components are detailed in Section 5.3. The framework resiliency against different attack conditions is verified in Section 5.4. Also this section presents the evaluation of MATEM against different security metrics viz., attack detection rate, false positive, false negative rate etc., in presence of bad-mouthing, good-mouthing, and selfish attacks. Section 5.5 presents the simulation results of MATEM against different routing metrics viz., message delivery ratio, delivery latency, and message delivery cost. This section also includes the comparative analysis of MATEM with other recently proposed trust-based framework available in the literature for DTN routing security. An evaluation of MATEM in the real testbed forming people-centric application domain is presented in Section 5.6. Section 5.7 concludes the work.

5.2 Background and Existing Works, Issues, Motivation, and Contributions

This section discusses the irrelevancy of the traditional approaches for ensuring DTN routing security and the motivation behind the application of trust-based framework for addressing the issue of next-hop carrier selection and thus ensuring the security and reliability of DTN routing in a hostile environment. Further, the techniques available in DTNs literature for detecting misbehaving nodes and to ensure routing security are detailed in Section 5.2.1 and Section 5.2.2, respectively.

The use of traditional cryptographic primitives are insufficient to handle the uncongenial situations (e.g., node compromise, continuously changing nodes' behaviors to bypass traditional security walls etc.) in hostile DTNs because of their assumption of continuous network availability. Even though strong cryptography can provide integrity, confidentiality, and authentication, it fails in the face of insider attackers. Moreover, in highly delayed or disrupted network conditions, key management and key distribution services are hard to implement. In addition, credit or reputation-based mechanisms are ineffective in DTNs as smooth propagation of credit or reputation values as well as end-to-end acknowledgements cannot be guaranteed due to node sparsity, infrequent and intermittent node contacts etc. These situations motivate the application of trust-based strategy for secure and reliable routing in DTNs. The concept of trust has originated from social sciences and is defined as the "subjective belief" about the behavior of an entity under consideration [62]. The application of trust in DTNs enables network entities to collaborate even in a delayed and disrupted environment using their Local Information Base (LIB). The LIB is the outcome of their own observations and collective recommendations about other nodes on opportunistic contacts. Thus, trust reflects the mutual relationships and maintains a reliable communication only with nodes which are trustworthy and avoids inclusion of misbehaving nodes (i.e., untrustworthy) in the routing path. Therefore, *a distributed trust based next-hop carrier selection framework is the main motivation behind selecting a trusted next-hop carrier in DTNs as well as improving security, reliability and QoS of the underlying routing schemes*.

In the existing literature, the available techniques to detect misbehaving nodes to ensure routing security in DTNs can be classified into two broad categories viz., (i) *Trust-Based Routing*, and (ii) *Social-Aware Routing*. An analysis of these techniques is detailed next.

5.2.1 Trust-Based Routing Protocols

The available trust-based approaches to deal with misbehaving nodes basically rely on recommendations or feedback mechanisms to build trust among participating nodes. This trust value is then used to identify misbehaving nodes and avoid selecting such nodes as message carriers in DTN routing.

In [79], a Secure Reputation-based Dynamic (SReD) window scheme has been proposed to estimate the trust in DTNs. It considers three different sources to compose trust: cryptographic operation, node's behavior, and reputation. In this work cryptographic operations like encryption and decryption mechanisms are used to provide authentication and confi-

dentiality to each node and to defend the network from outside attackers. To monitor the node's behavior, a watchdog mechanism is adopted. The output generated from watchdog is then combined with cryptographic operations using a weighted sum to estimate a local trust value for each node. A limitation of their work is that no consideration is taken to tackle inside attackers which are malicious and selfish in nature.

The authors in [80] have addressed the problem of misbehaving carriers and propose a solution based on reputation. According to their scheme, every node in the network maintains a reputation about other peer nodes. Then the reported delivery probability of each node is weighted by their reputation value for carrier selection. The shortcoming of the proposed method is that the reputation building mechanism is based on the assumption that the system is capable of keeping track of intermediate carriers as a whole for message delivery, which is infeasible in an opportunistic environment.

The authors in [75] proposed an Iterative Trust and Reputation Mechanism (ITRM) to detect and isolate malicious nodes from the network iteratively. In this scheme, each node acts as a judge node to create a rating table of the other nodes by collecting indirect recommendations or feedbacks. It also periodically collects rating tables of other nodes to have a recent estimate of their reputation values. They used discrepancies of indirect recommendations for adversary detection and used authentication as the underlying mechanism to evaluate a node. But this scheme is solely aimed at preventing Byzantine type of attack in DTNs.

The work in [78] has proposed a weighted average of social trust and quality of service trust to analyze the trust level of each node in DTNs. The trust evaluation protocol relies on the use of direct trust evidence and indirect recommendations to estimate the trust value of each node in DTNs. Recommendation collection or indirect trust measurement is possible in DTNs, however, it is unclear as how to obtain an accurate measurement for recommendation trust in an opportunistic scenario. Moreover, the work does not focus on the prevailing uncertainty in DTNs' message propagation scheme, and the functionality offered by mobile devices in a people-centric opportunistic communication scenario is not explored from social networking perspective.

To evaluate an encounter's competency of delivering data, the authors in [76] have proposed a reputation assisted framework that is based on collected evidences of nodes' packet-forwarding behavior. In fact, a special message, called "Positive Feedback Message" (PFM), is proposed to help the reputation mechanism process for monitoring the forwarding be-

havior of a node. The proposed scheme is solely aimed at preventing black hole attack in opportunistic networks.

In [77], a probabilistic misbehavior detection scheme (iTrust) has been presented that adopts the concept of "Inspection Game" to stimulate cooperation of misbehaving nodes and consider a periodically available central Trusted Authority (TA) to judge the nodes' packet forwarding behaviors. The TA is provided with collected forwarding history information of each node in the network in response to a broadcast query made by the TA agent. Again, a signature-based authentication is used to avoid malicious nodes from providing duplicate or modified forwarding history. However, if misbehaving nodes do not follow the game strategies, a low message delivery ratio would still result. Moreover, the authors in [76, 77] have not assessed the nodes' behavior from a social networking perspective to address the issues that arise from socially selfish nodes in a people-centric DTN scenario.

5.2.2 Social-Aware Routing Protocols

The available routing protocols in this category try to optimize social characteristics of mobile users for selecting a message carrier and thus ensure reliability and security of DTN routing. The available approaches are detailed next.

The work in [81] has provided an overview of routing and data dissemination issues in opportunistic DTNs with a special attention on characteristics of Mobile Social Networks (MSNs) and analysis metrics, human mobility models, dynamic community detection methods, routing and data dissemination protocols. However, none of these protocols have considered routing trade-offs between conflicting requirements and goals in the protocol design. Further sufficient attempts have not been made to study the impact of social selfishness on the performance of routing and data dissemination protocols.

In another social-based approach [82], the authors have proposed a distributed optimal Community Aware Opportunistic Routing (CAOR) algorithm for DTN-based MSNs. The work is based on the assumption that mobile users with a common interest autonomously form a community and their frequently visited common location is defined as home. However no attempt has been made to address the uncertainty issues that might arise in a hostile DTN scenario.

In [83], a Trust Based Intelligent Routing (TBIR) using Artificial Neural Network (ANN) is proposed for DTNs which exploits the "Call Data Record" from "Call Detail Record" in

socially active communities. However, information regarding community formation and detection have not been provided in TBIR. Moreover, the work has not addressed the reliability and QoS issues in DTN-based communication.

In a very recent work [84], the authors have proposed a trust and reputation management mechanism entitled Socially-Aware Reputation mechanism for Opportunistic diSsemination (SAROS), for opportunistic networks. The functionality of SAROS is based on local and global trust computation, gossiping, and uses a quorum-based algorithm to decide the correctness of the received messages. After selecting the correct message version, SAROS increases the trust values of all the nodes falling in the correct paths, and decreases trust in the nodes from the paths corresponding to wrong messages. This scheme is solely aimed at detecting malicious nodes that tamper with messages in the network. SAROS is implemented as a component of Interest Spaces [129, 130], which is an interest-based framework for publish/subscribe-like data dissemination in opportunistic networks. The experimental results exhibit the efficiency of SAROS in terms of the routing metric called "correct message hit rate", but reported with high delivery latency. Further, the protocol's resiliency against the security attacks is not reported in the current work. Moreover, SAROS may require modifications to be directly applied to pure opportunistic-DTNs. It may be noted that SAROS mainly works by keeping track of intermediate carriers responsible for forming correct and incorrect *paths as a whole* for message delivery. In DTN, however, contemporaneous end-to-end paths between source-destination pairs are hard to achieve due to the existence of frequent link disruptions, intermittent connectivity etc.

To summarize, the main issues of the existing trust-based and social-aware routing protocols for secure communication in DTNs are as follows.

- *Non-consideration of malicious and social behavior simultaneously*: They have not considered the nodes' malicious and social behaviors together to judge the competency of a node as a message carrier. In a people-centric social environment a non-malicious node may exhibit selfish behavior in message forwarding and this will lead messages to drop either due to buffer overflow or Time-to-Live (TTL) expiration. Again, a socially good node may behave maliciously by providing false recommendations about other peer nodes to increase their individual gain. Therefore, it is an important issue to address such conflicting node behaviors (i.e., the act of maliciousness and social selfishness) together to deal with misbehaving nodes in a hostile DTN environment.

- *Non-consideration of inherent risk and QoS requirement*: None of these techniques

could focus on the inherent risk involved in DTN's message propagation scheme as well as the QoS requirements (i.e., delay minimization) of secure routing amidst uncertainty. In a hostile scenario, an intermediate honest node, after taking the custody of in-transit messages, may misbehave either by dropping messages or by not forwarding them to the intended recipients. So, a measure of risk in communication is an important issue to address. Again, the trusted carrier selection process in DTN incurs an additional amount of end-to-end delay during the filtering process of misbehaving nodes in the routing path. Though DTN is delay tolerant, minimizing delay ensures the QoS requirement of secure routing in a people-centric application domain.

- *Use of non-compliant techniques for trust assessment*: The use of feedback mechanisms and acknowledgement (ACK) for building trust or reputation may not work well in DTN due to its' lack of stable common multi-hop path from source to destination. Further, the use of "Watchdog Mechanism" to observe nodes' packet forwarding behavior may result in low network performance in DTN. This is due to frequent link disruption and intermittent connectivity pattern that cause a node to lose connectivity with the intermediate node which it desires to monitor.

- *Non availability of real testbed implementation*: The effectiveness of the schemes discussed above is not evaluated in a real DTN scenario (i.e., in a people-centric mobile social environment) in presence of misbehaving nodes.

Therefore, compared to the works cited above, the proposed MATEM framework takes into account multiple conflicting trust-measuring criteria evolving from nodes' malicious and social behaviors together to address the issues of misbehaving nodes in a hostile DTN. It also addresses the inherent risk involved in DTN's message propagation scheme as well as the QoS requirement of secure routing. MATEM facilitates a trustor (i.e., the trust evaluating node) to initiate a trust-building process for a trustee (i.e., the node for whom trust will be evaluated) on direct contacts. It uses direct observations and collected indirect opinions (i.e., recommendations) from other neighboring nodes on different trust-measuring criteria viz., "Risk", "Cooperativeness", "Connectivity", and "Average Message Forwarding Delay" (AMFD). These criteria are conflicting in nature in view of the objective of optimization, and thereby on the overall utility of the MATEM framework. Therefore, instead of using normalized weighting method for computing the final trust value, the proposed method invokes a MCDM technique [121] known as *Technique for Ordered Priority with Similarity to Ideal Solution* (TOPSIS) [73] for assessing the absolute trust level of each node in DTNs.

The TOPSIS method attempts to choose the best alternative (i.e., solution) in presence of multiple conflicting criteria. The different application areas of TOPSIS include manufacturing system, supply chain issue, business and management, energy and safety, environmental science and so on [74], [131]. In MATEM, a trust-based TOPSIS is used for facilitating a trustor to choose the next-hop message carrier in the presence of multiple conflicting node behaviors that exist in a hostile DTN environment. As per the knowledge goes, the proposed work is the first of its kind that integrates TOPSIS, a multidisciplinary technique originally used in the field of *"Design, Engineering and Manufacturing Systems"* with the various network-specific trust measuring criteria and their computational aspects to address the routing security in DTNs. These make the proposed framework an *"interdisciplinary"* one to learn and compute absolute trust value of each node in a DTN.

5.3 Proposed Framework for Next-hop Carrier Selection in DTNs

This section details the proposed framework for ensuring routing security in a hostile DTNs environment. The system model and the network model under consideration are detailed in Section 5.3.1 and Section 5.3.2, respectively. Section 5.3.3 details the novel unified trust-based framework called Multiple Attribute Trust Evaluation and Management (MATEM) for next-hop carrier selection in DTNs.

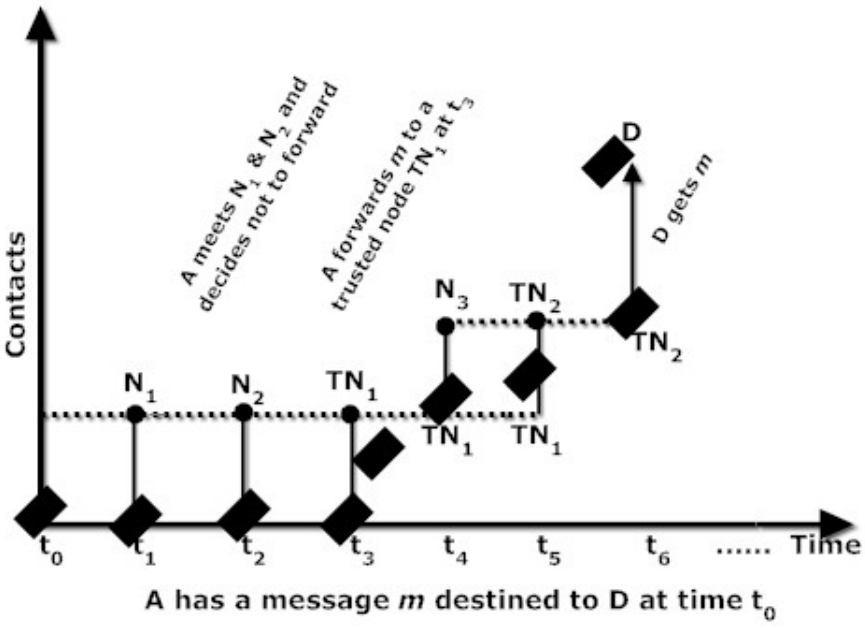


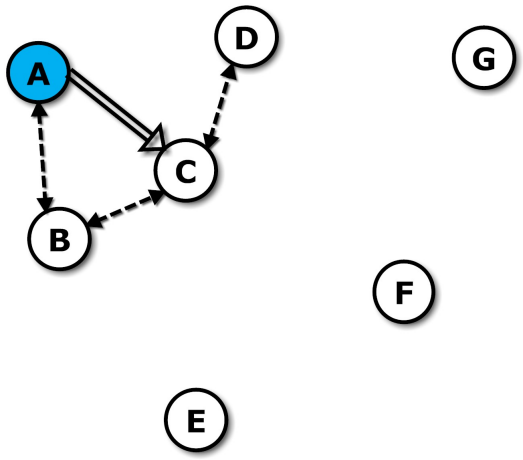
Figure 5.1: Trust Based Next-hop Carrier Selection in Hostile DTNs Environment

5.3.1 System Model

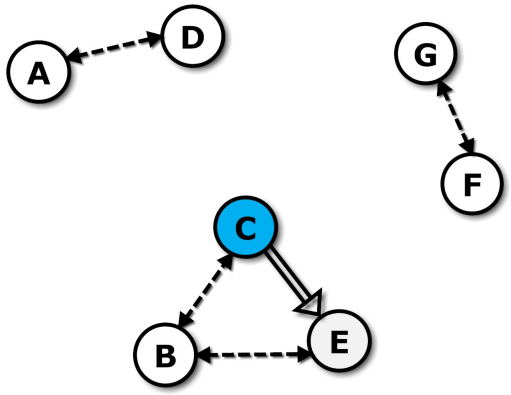
The proposed work focuses on trusted carrier selection for message forwarding in user-centric hostile DTN environment. Figure 5.1 depicts a communication scenario in DTNs where node $\mathcal{A}$ has a message $\mathfrak{M}$ destined for node $\mathcal{D}$. In the absence of trust, node $\mathcal{A}$ generally selects an encountered node having higher probability of reaching $\mathcal{D}$ as a next-hop message carrier or forwards multiple copies of $\mathfrak{M}$ to the neighboring nodes $\mathcal{N}_i$ in the network. Whereas, in the presence of trust, $\mathcal{A}$ selects a trusted node that ensures secure and reliable delivery of the message $\mathfrak{M}$ to the destination $\mathcal{D}$. However, this process of trusted carrier selection may incur additional amount of end-to-end delay by filtering undesirable encounter opportunities (i.e., untrusted nodes) in the routing path. In Figure 5.1, node $\mathcal{A}$ could have delivered message $\mathfrak{M}$ to node $\mathcal{D}$ through $\mathcal{N}_1$ or $\mathcal{N}_2$, but while selecting $\mathcal{TN}_1$ (a trusted node) as a next-hop message carrier, node $\mathcal{A}$ may loses an opportunity to deliver $\mathfrak{M}$ with shorter delay. DTN-based applications are expected to be delay-tolerant, but this does not mean that they would not benefit from decreased delay. Though the primary objective of message forwarding in a hostile DTN is for secure and reliable delivery to the destination, minimizing delay lowers the time the messages spend in the network and reduces contention for resources such as buffer space and indirectly conform to the pervasiveness and Quality of Service (QoS) requirements of underlying routing protocols. Thus, the work in this chapter considers "average message forwarding delay" of each node in the network as one of the trust measuring criteria among others (viz., "Risk" to address malicious activity, "Connectivity" to assure reliability, "Cooperativeness" to avoid social selfishness, etc.) for judging nodes' competency as a message forwarder in the next-hop carrier selection problem in a hostile DTN environment. However, decision on which node is to be selected as next-hop carrier is usually difficult to be reached, since multiple factors of different conflicting importance have been taken into consideration.

5.3.2 Network model

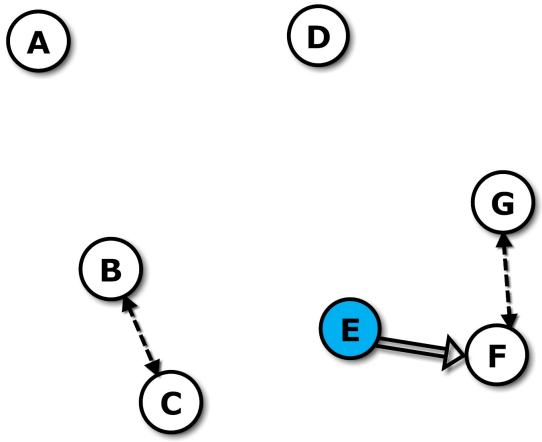
The work of this chapter considers a people-centric DTN environment, where wireless nodes of end-users move in a community and communicate opportunistically. All nodes are heterogeneous in nature and have comparable computing, communicating and storage capabilities. Their connectivity patterns over time are represented as a dynamic network graph with time varying links (called time-graphs) [132], similar to [133]. In a time-graph,



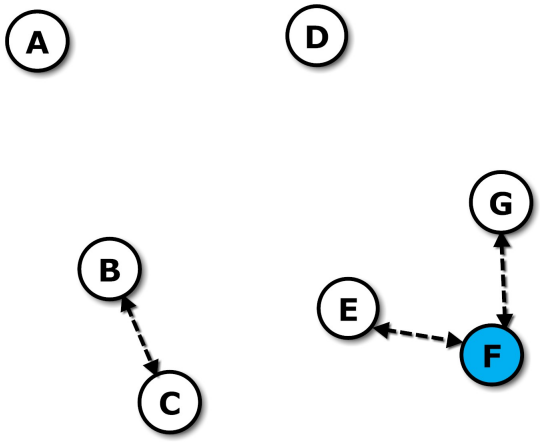
(a) Network Topology at t_0



(b) Network Topology at t_1



(c) Network Topology at t_2



(d) Network Topology at t_3

Figure 5.2: Illustrative example of a time evolving DTN "$\mathfrak{G}$", where the source node $\mathcal{A}$ and the destination node $\mathcal{F}$ are never connected. Still, end-to-end connectivity can be achieved between these nodes over time through intermediate carrier selection as marked with double-lined arrow

t_0	A	B	C	D	E	F	G
A	0	1	1	0	0	0	0
B	1	0	1	0	0	0	0
C	1	1	0	1	0	0	0
D	0	0	1	0	0	0	0
E	0	0	0	0	0	0	0
F	0	0	0	0	0	0	0
G	0	0	0	0	0	0	0

(a) Adjacency Matrix at t_0

t_1	A	B	C	D	E	F	G
A	0	0	0	1	0	0	0
B	0	0	1	0	0	1	0
C	0	1	0	0	0	1	0
D	1	0	0	0	0	0	0
E	0	0	0	0	0	0	0
F	0	1	1	0	0	0	1
G	0	0	0	0	0	1	0

(b) Adjacency Matrix at t_1

t_2	A	B	C	D	E	F	G
A	0	0	0	0	0	0	0
B	0	0	1	0	0	0	0
C	0	1	0	0	0	0	0
D	0	0	0	0	0	0	0
E	0	0	0	0	0	1	0
F	0	0	0	0	1	0	1
G	0	0	0	0	0	1	0

(c) Adjacency Matrix at t_2

t_3	A	B	C	D	E	F	G
A	0	0	0	0	0	0	0
B	0	0	1	0	0	0	0
C	0	1	0	0	0	0	0
D	0	0	0	0	0	0	0
E	0	0	0	0	0	1	0
F	0	0	0	0	1	0	1
G	0	0	0	0	0	1	0

(d) Adjacency Matrix at t_3

Figure 5.3: The adjacency matrix representation of a time evolving DTN "$\mathfrak{G}$" of Figure 5.2 representing the fact that an edge exists between the two nodes at different time instances of $\mathcal{T}$

denoted as $\mathfrak{G}$, vertices represent nodes and edges represent contacts between them at discrete time instances. $\mathfrak{G}$ is unweighted with bidirectional edges, where message delivery between nodes is modeled as flow of information among their vertices. Let n denote the cardinality of the set of vertices in $\mathfrak{G}$ and $\mathcal{T} = \{t_0, t_1, ..., t_m\}$ denote the set of discrete time instances. At time t_k, let $\mathcal{G}_k$ $(k = 1, ..., m)$ denote the snapshot of $\mathfrak{G}$, where any number of vertices may be connected (i.e., presence of edges between vertices) or disconnected (i.e., edges connecting vertices disappear). The time varying adjacency matrix of $\mathcal{G}_k$ is an n x n x m matrix, where an element a_{ijk} has value 1 if their is an edge between i-th and j-th vertices at t_k, or 0 otherwise. Figure 5.2 and Figure 5.3 represent the snapshots of time-graph $\mathfrak{G}$ and its corresponding adjacency matrix representation at different time instances of $\mathcal{T}$.

In Figure 5.2, there is no contemporaneous end-to-end path between node $\mathcal{A}$ and $\mathcal{F}$ at any time instant. Successful delivery of messages from $\mathcal{A}$ to $\mathcal{F}$ can be achieved only if intermediate nodes receive those messages from $\mathcal{A}$ and carry them to $\mathcal{F}$. However, node $\mathcal{F}$ is unreachable neither through direct contact nor through any predetermined end-to-end path. Instead, at time t_0, node $\mathcal{A}$ finds itself able to communicate with either node $\mathcal{B}$ or $\mathcal{C}$, both happening to be in it's communication range. Based on some information, $\mathcal{A}$ decides to forward the message to node $\mathcal{C}$ at time t_0. At this time, $\mathcal{C}$ has no potential neighbor that it can forward the message for delivery to $\mathcal{F}$. The node $\mathcal{C}$ in turn stores the message in it's buffer until time t_1 and sends it to $\mathcal{E}$ at this time. At t_2, node $\mathcal{E}$ forward the message to $\mathcal{F}$. The intermediate carrier selection in each individual time slot is indicated with a double lined right arrow.

However, in the hostile DTN environment under consideration, the selection of intermediate carriers is critical due to the presence of misbehaving nodes which can act maliciously or exhibit social selfishness in message forwarding. A node can behave maliciously by falsifying its encounter history information in an intention to boost its trust values related to different trust measuring criteria. These cause messages to be attracted towards the malicious nodes instead of intended destinations. A malicious node may drop these received messages to launch *black hole* attacks. Moreover, as node behaviors are typically unpredictable and dynamic, an honest node may turn malicious by providing false recommendations to launch attacks, viz., *bad-mouthing* and *good-mouthing* attacks. Again, the misbehaving nodes may launch *selfish* attacks by dropping the buffered messages to free their own buffer space. The detail analysis of these attack scenarios are presented in Section 5.4.

5.3.3 Proposed MATEM Scheme

The MATEM framework consists of four modules viz., information exchange module, trust composition module, trust computation module, and trust prediction module. In the MATEM, "*Trust*" is considered as a quantitative measure of a relationship established between two entities for some specific "*Action*". In particular, one entity trusts the other entity on performing some desired *Action*. In this relationship, the first entity is called the *Trustor*, the second entity is called the *Trustee*. The trustor executes the trust protocol independently and performs its direct and indirect trust assessment towards the trustee on performing some actions (i.e., on each individual trust criteria). The notation (*Trustor* : *Trustee*, *Action*) is used to describe a trust relationship in MATEM. The *Action* set is denoted by $\mathcal{X}$ and each component of $\mathcal{X}$ represents individual trust measuring criteria that are proposed in the framework. These criteria are derived directly or indirectly based on specific composition procedures as detailed in *Trust Composition Module* or through recommendations, respectively. The *Action* set $\mathcal{X}$ is represented as

$$\mathcal{X} = \{Risk, Connectivity, Cooperativeness, AMFD\}$$

In MATEM, a trustor obtains the trustee's direct and indirect trust related to each trust measuring criteria $\mathcal{X}$ on encountering another node (i.e., either the trustee or any other DTN nodes). These collected trust values are aggregated together to derive initial trust and thereby TOPSIS is applied to evaluate absolute trust value (represented as $\mathbb{T}^*$) of the trustee node. The absolute trust level of each node is defined as a continuous real number in the range of $[0,\ 1]$, with 1 indicating complete trust, 0.5 ignorance, and 0 complete distrust. The trust computation process of MATEM assumes a minimum trust threshold as $\mathbb{T}^*_{\text{min}}$ and the threshold-limit is set to $(\delta = 0.5)$. A positive trust evaluation for a node depends on whether the absolute trust computed for the node is above the threshold-limit (δ). For example, if $\mathbb{T}^*_{\mathcal{AB}}(t) > \mathbb{T}^*_{\text{min}}$, node $\mathcal{A}$ will consider node $\mathcal{B}$ as "trustworthy" (i.e., as an honest node) at time t. A next-hop carrier is chosen on the basis of absolute trust value of a trustee node. Figure 5.4 shows a comprehensive framework of MATEM. The functionality as well as applicability of each individual module of MATEM for choosing a trusted next-hop carrier in a DTN is detailed next.

Information Exchange module

In MATEM, each DTN node maintains a contact history information and trust information of other encountered nodes in the `Contact History` table and `Trust Table`, respectively. The entries in the `Contact History` table are accumulated from the time-graph $\mathfrak{G}$, as de-

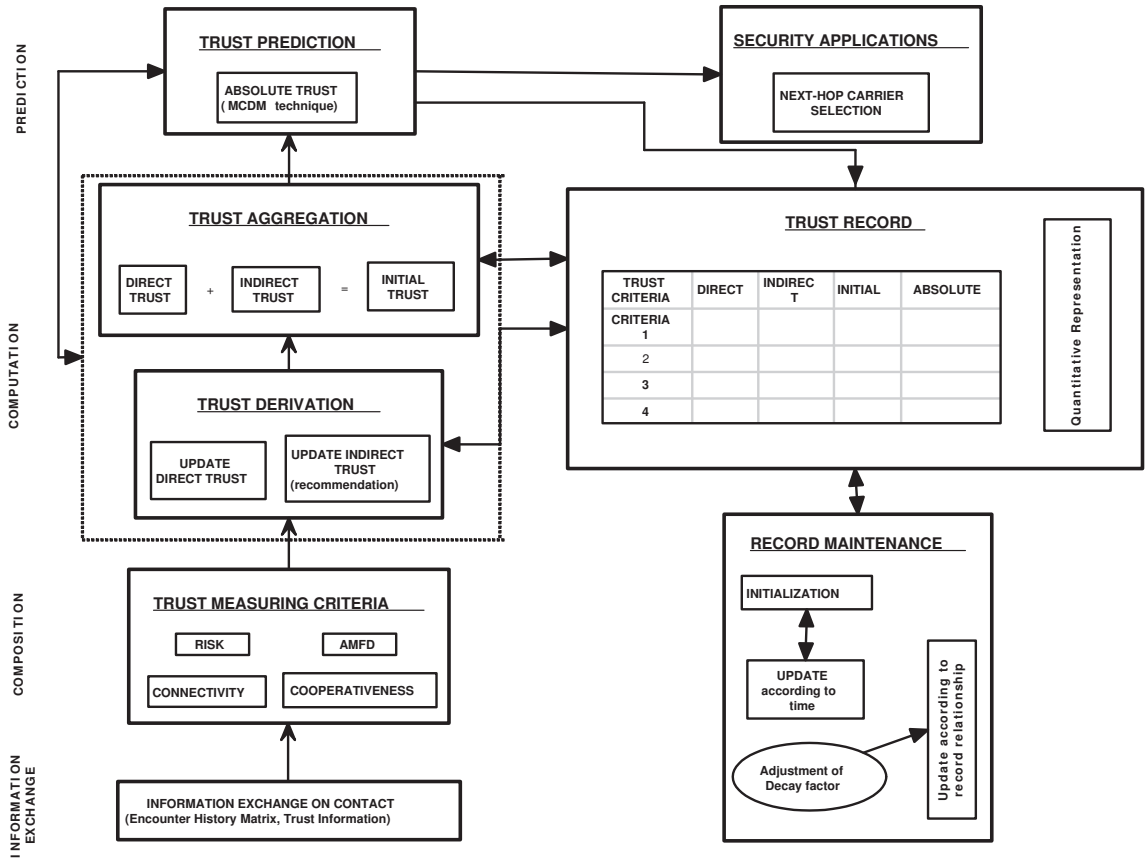


Figure 5.4: MATEM: Multi-Attribute Trust Evaluation and Management Framework for next-hop carrier selection in hostile DTNs

scribed in Section 5.3.2, over time $\mathcal{T}$. The entries in the `Trust Table` are the trust values of different trust measuring criteria. As depicted in the lower part of Figure 5.4, on encountering, each node in the network exchanges its own contact information as well as the associated trust information about those contacts. A $Trustor$ computes its direct and indirect trust for a $Trustee$ from the observations made on contact information and from collected evidences gathered as recommendations, respectively. However, it may be possible for a misbehaving node to misrepresent its own contact history information to draw packets towards itself and thereby gaining a significant advantage for being selected as a next-hop message carrier. Therefore, for preventing misbehaving nodes from providing false contact history information and to secure the exchange of contact evidences, the notion of *encounter tickets* [134] has been considered. Each node in DTN is required to submit the encounter tickets during exchange of contact history information. *Encounter tickets* are verifiable contact evidences that guarantee the truthfulness of DTNs contact history information. The outcome of information exchange is the composition of different trust measuring criteria

(or metrics) that form the $Action$ set of MATEM, which are detailed next.

Trust Composition module

In MATEM, four different trust measuring criteria are proposed viz., "Risk", "Connectivity", "Cooperativeness", and "Average Message Forwarding Delay (AMFD)" for assessing nodes' potentiality as a trustworthy message carrier. These criteria reflect the amount of *uncertainty* and *maliciousness* in nodes' behavior, encounter possibility of nodes, social interaction patterns of end-users, and estimated delay for message forwarding. The derivation of each criteria is a subjective judgment made by each node based on observed `Contact History` information accumulated over a time period including the new contact information received from another node on encounter. The different trust criteria and their derivation mechanisms that have been designed for trust compositions in MATEM are described next.

- ***Risk***: Instead of using the generic replication mechanism to handle uncertainty, the trust criteria "Risk" is introduced to predict and quantify the unpredictable nature of nodes' behavior in a hostile DTN environment. "Risk" represents the associated uncertainty in information exchange event and quantifies the risk of interaction between a $Trustor$ and a $Trustee$. This criteria has been taken into consideration for portraying unpredictable and uncertain behaviors of malicious nodes and has been derived from a quantitative measure of associated uncertainty in `Contact History` and `Trust Information` exchange event. During information exchange if the `Contact History` is not certified, or is certified but inconsistent with the trustor's own `Contact History` table, it is considered as a negative experience and counted as an unsuccessful interaction. Again, if evidences provided in the trust information appear to be inconsistent with the trustor's own observations, the counter for unsuccessful interaction is incremented. In the MATEM, the entropy function [135] is used for measuring Risk and it is represented as

$$\mathbb{T}^{\text{Risk}} = \mathcal{H}(p) = -p\log_2(p) - (1-p)\log_2(1-p) \tag{5.1}$$

where $\mathcal{H}$ is the entropy function and $p = \mathcal{IP}_{AB}$ is the predictable interaction pattern of the two nodes $\mathcal{A}$ and $\mathcal{B}$ under consideration and derived from Equation (5.2).

$$\mathcal{IP}_{AB} = (\frac{S^{ip}_{AB}}{S^{ip}_{AB} + U^{ip}_{AB}}) * (1 - \frac{1}{S^{ip}_{AB} + 1}) \tag{5.2}$$

Here, (S^{ip}_{AB}) and (U^{ip}_{AB}) are the total number of successful and unsuccessful interactions of node A with node B, respectively and $(1-\frac{1}{S^{ip}_{AB}+1})$ is the balancing factor whose value lies between $[0, 1]$. The value of the balancing factor approaches 1 with an increase in the number of successful interactions. The lesser value of "Risk" minimizes uncertainty and thus– ensures security in a next-hop carrier selection problem.

- ***Connectivity***: The trust criteria "connectivity" represents the change of rate in the connectivity pattern of a node, i.e., the number of connections and disconnections a node observed over time $\mathcal{T}$. In the absence of any predetermined connectivity pattern in a people-centric DTN, the connectivity of one node with another node in the network is inherently associated with its mobility pattern as well as social ties. The connectivity trust measures relative mobility, and consequently, an estimated meeting probability of an encountered node with the destination. It is calculated as the ratio of the number of connections between encountered node and the destination node and the total number of connections the encountered node observed with other nodes including the destination over time $\mathcal{T}$. A node estimates the change rate of connectivity of an encountered node from its observed `Contact History`, as explained in *Information Exchange Module*, which is accumulated over time $\mathcal{T}$ including its recent contact information. Say, node $\mathcal{A}$ has a message $\mathfrak{M}$ destined for $\mathcal{D}$ and encounters opportunistically node $\mathcal{B}$. Node $\mathcal{A}$ calculates $\mathcal{B}$'s connectivity trust as the ratio of number of connections between $\mathcal{B}$ and $\mathcal{D}$ and total number of connections and disconnections $\mathcal{B}$ experienced with other DTN nodes including $\mathcal{D}$. The representation is as follows:

$$\mathbb{T}^{\text{connectivity}}_{BD} = \frac{\mathcal{B}_{\mathcal{D}}}{\mathcal{B}_{all}} \tag{5.3}$$

where, $\mathcal{B}_{\mathcal{D}} =$ number of encounters between $\mathcal{B}$ and destination $\mathcal{D}$, and $\mathcal{B}_{all} =$ total number of encounters with other nodes including $\mathcal{D}$.

The bigger value of "connectivity" trust assures higher forwarding opportunities and thus, increases delivery probability which successively meets the QoS in DTNs.

- ***Cooperativeness***: The "Cooperativeness" trust criteria is proposed for enabling nodes

to take better forwarding decisions in the presence of social selfishness. It measures the quality of connectivity and predicts the social relationship among nodes by measuring their ties. Social Ties relate the quality of interaction pattern between users to the level of acquaintance between them. For measuring ties, it is necessary to assimilate the relationship between the trustor, trustee and the destination node, because there may not exist the same level of cooperation among all nodes. A $Trustee$ may have a good social tie with the $Trustor$, but it may not have the same tie with the destination. When a node becomes selfish, it will only forward messages if it is a friend of the source, current carrier, or the destination node. In this work tie is considered to be comprised of two indicators viz., "frequency", and "longevity" which are derived from the observations in $\mathfrak{G}$. The frequency indicator, represented as F, is based on the frequency with which a $Trustor$ encounters a $Trustee$ as well as the encounter frequency of trustee with the destination node. Again the "longevity" indicator, represented as L is based on the amount of time (i.e., duration) a node stays connected to a given node i.e., the amount of time a $Trustor$ spend with $Trustee$ as well as the time spent between the trustee and the destination node. These two tie strength indicators are aggregated to evaluate an overall single tie strength measure and provides an estimation of "cooperativeness" trust criteria between each pair of nodes. More formally, the cooperativeness trust of trustee $\mathcal{B}$ for a destination node $\mathcal{D}$, as evaluated by trustor $\mathcal{A}$ is represented using a simple yet expressive mathematical relation as :

$$\begin{aligned} \mathbb{T}_{BD}^{\text{Cooperativeness}} &= \mathfrak{F}(F, L) \\ &= \frac{f_{\mathcal{AB}} + f_{\mathcal{BD}} + l_{\mathcal{AB}} + l_{\mathcal{BD}}}{f_{\mathcal{A}}(all) + f_{\mathcal{B}}(all) + l_{\mathcal{A}}(all) + l_{\mathcal{B}}(all)} \end{aligned} \tag{5.4}$$

Here, $f_{\mathcal{AB}}$, $f_{\mathcal{BD}}$ are the number of times node $\mathcal{B}$ encountered node $\mathcal{A}$, node $\mathcal{D}$, respectively. $[f_{\mathcal{A}}(all)]$, $[f_{\mathcal{B}}(all)]$ indicate the total amount of encounters node $\mathcal{A}$ and node $\mathcal{B}$ have observed including the destination node $\mathcal{D}$. Again, $l_{\mathcal{AB}}$, $l_{\mathcal{BD}}$ are the total amount of time node $\mathcal{B}$ is connected to node $\mathcal{A}$ and $\mathcal{D}$, respectively. $[l_{\mathcal{A}}(all)]$, $[l_{\mathcal{B}}(all)]$ are the total amount of time node $\mathcal{A}$ and $\mathcal{B}$ are connected across all encountered nodes in the network. The bigger value of "Cooperativeness" assures higher delivery probability due to better node cooperation, and successively increases reliability amidst socially selfish environments in DTNs.

- ***AMFD***: The trust criteria "AMFD" represents the estimated average message forwarding delay of each potential carrier node in the network. In general, the time required for a message to move from one node to another can be divided into four components, viz., waiting time, queuing time, transmission time, and propagation time. However, it is difficult to calculate end-to-end delay in DTNs due to the existence of non-contemporaneous paths and intermittent connectivity. From a DTN's perspective, waiting time is most significant among these four delay components since the waiting time for a message might range from seconds to days under the store-carry-and-forward paradigm. The AMFD trust criteria computes the expected delay or waiting time for a message to go from one node to another using an opportunistic contact and assumes that message arrival times are equally likely in nature. When the contact is up (i.e., connected with destination), the waiting time wt_i is zero. When the contact is down (i.e., disconnected from the destination but connected with other nodes), the waiting time is the time until the contact comes back up again, as shown in Figure 5.5.

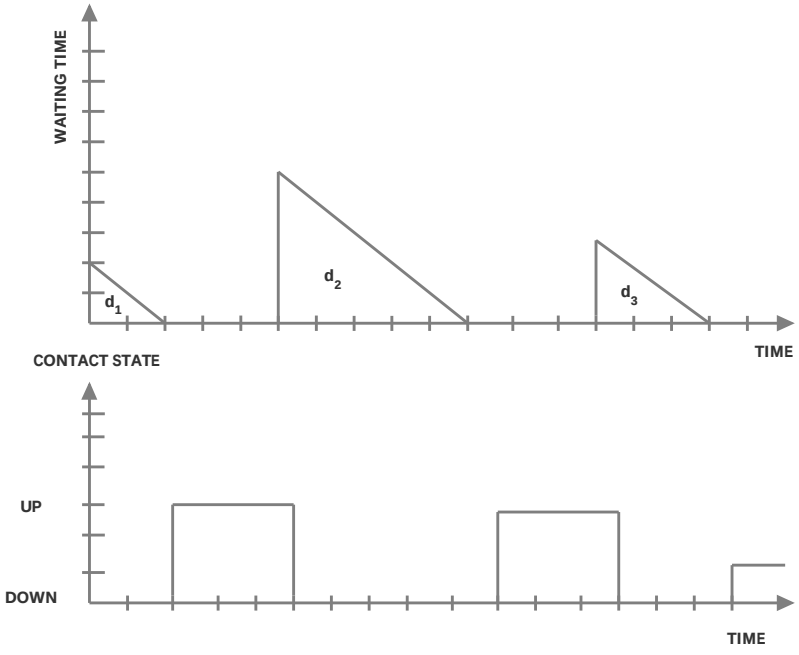


Figure 5.5: Contact waiting time and state

Since the probability distribution of message arrival time is uniform, to estimate waiting time, the area under the curve in Figure 5.5 is computed and then divided by the

length of the time interval. For a single disconnected interval, wt_i, the area under the curve is given by $\frac{1}{2}wt_i^2$. The area under a connected interval is 0. Thus, a $Trustor$ node uses the observed contact evidences derived from $\mathcal{G}_k$ over time $\mathcal{T}$ to compute the AMFD trust criteria of a $Trustee$ node and is given by:

$$\begin{aligned} \text{AMFD} &= \frac{\sum_{i=1}^{n} \frac{1}{2} wt_i^2}{\mathcal{T}} \\ &= \frac{\sum_{i=1}^{n} wt_i^2}{2\mathcal{T}} \end{aligned} \tag{5.5}$$

where, n is the total number of disconnected periods, wt_i is the duration of a given disconnected period, and $\mathcal{T}$ is the total time interval over which this connectivity is observed. A lesser value in "AMFD" trust criteria assures lower contention of resources along with lesser delay and in turn helps in achieving QoS requirements in DTNs.

Trust Computation Module

This module as depicted in the middle portion of Figure 5.4 focuses on how to derive and aggregate the collected observations to generate the initial trust value related with each individual trust criteria of each node in DTNs. Such observations basically include direct estimations and indirect opinions on an encounter's current and recommended behavior related to different trust measuring criteria, as adopted in MATEM. Upon encounter, a trustor node, say $\mathcal{A}$, obtains its direct trust for a trustee node, say $\mathcal{B}$ (if $\mathcal{A}$ encounters $\mathcal{B}$) and indirect trust of trustee $\mathcal{B}$ (if $\mathcal{A}$ encounters $\mathcal{C}$, where $\mathcal{C} \neq \mathcal{B}$). The direct trust between the trustor $\mathcal{A}$ and the trustee $\mathcal{B}$ on $\mathcal{X}$ (i.e., different trust measuring criteria) are evaluated based on computational procedures as detailed in *Trust Composition Module*. Once the direct trust is composed and updated, the trustor collects opinions against the trustee in the form of recommendations from its 1-hop neighbors. These collected opinions are processed further to built "indirect trust" about the trustee and are maintained in a record format called `Trust Record`. These estimated direct trust and collected indirect recommendations are aggregated together to build the "initial trust" value related with each individual trust measuring criteria of each node in MATEM.

The initial trust evaluation towards $Trustee$ $\mathcal{B}$ by $Trustor$ $\mathcal{A}$ at time t is represented as

follows:

$$T^{\mathcal{X}}_{\mathcal{AB}}(t) = DT^{\mathcal{X}}_{\mathcal{AB}}(t) + IT^{\mathcal{X}}_{\mathcal{AB}}(t) \tag{5.6}$$

Where, $DT^{\mathcal{X}}_{\mathcal{AB}}(t)$ and $IT^{\mathcal{X}}_{\mathcal{AB}}(t)$ are the "direct trust" and "indirect trust" of $\mathcal{A}$ toward node $\mathcal{B}$ on trust criteria $\mathcal{X}$ at time t, respectively. Now, each individual sub-components of trust computation module of MATEM, as depicted in Figure 5.4, are detailed in the following subsections.

- **Update direct trust**:

  On encounter, the trustor $\mathcal{A}$ calculates direct trust of trustee $\mathcal{B}$ (if $\mathcal{A}$ is in contact with $\mathcal{B}$) on each individual trust criteria, viz. Risk, Connectivity, Cooperativeness and AMFD, following Equations (5.7), (5.8), (5.9), (5.10), as detailed next, and updates its trust table (as depicted in Figure 5.4) accordingly. The trust values are computed upon analytical observations and calculations carried on nodes' `Contact History` as explained in *Trust Composition Module*.

  $$DT^{Risk}_{\mathcal{AB}}(t) \;=\; \mathbb{T}^{\text{Risk}}_{AB} \tag{5.7}$$

  here, $DT^{Risk}_{\mathcal{AB}}(t)$ is the direct trust of trustor $\mathcal{A}$ on trustee $\mathcal{B}$ on risk trust criteria and updated at time t based on the risk of interaction between the trustor $\mathcal{A}$ and the trustee $\mathcal{B}$, as derived from Equation (5.1).

  $$DT^{Connectivity}_{\mathcal{AB}}(t) \;=\; \mathbb{T}^{\text{connectivity}}_{BD} \tag{5.8}$$

  here, $DT^{Connectivity}_{\mathcal{AB}}(t)$ is the direct trust of trustor $\mathcal{A}$ on trustee $\mathcal{B}$ on connectivity trust criteria and updated at time t based on the meeting probability of trustee $\mathcal{B}$ for destination $\mathcal{D}$, as derived from Equation (5.3).

  $$DT^{Cooperativeness}_{\mathcal{AB}}(t) \;=\; \mathbb{T}^{\text{cooperativeness}}_{BD} \tag{5.9}$$

  here, $DT^{Cooperativeness}_{\mathcal{AB}}(t)$ is the direct trust of trustor $\mathcal{A}$ on trustee $\mathcal{B}$ on cooperativeness trust criteria and updated at time t based on the quantified social tie between the

trustee $\mathcal{B}$ and destination $\mathcal{D}$, as derived from Equation (5.4).

$$DT_{\mathcal{AB}}^{AMFD}(t) \;=\; \mathbb{T}_{BD}^{\text{AMFD}} \tag{5.10}$$

here, $DT_{\mathcal{AB}}^{AMFD}(t)$ is the direct trust of trustor $\mathcal{A}$ on trustee $\mathcal{B}$ on AMFD trust criteria and updated at time t based on the expected waiting time for a message to go from trustee $\mathcal{B}$ to destination $\mathcal{D}$ and derived from Equation (5.5).

Once the direct trust of an encountered node is updated on contact at time t, the stored direct trust values of other nodes maintained in the trustor's own trust records are decremented with a decay element and updated accordingly. Again, if the trustor node is unable to estimate all trust measuring criteria required for trust calculation of the trustee node due to some unpredictable reasons (e.g., insufficient contact period etc.), then the past value of direct trust between the trustor and the trustee is updated with a decay time factor. Therefore, $DT_{\mathcal{AB}}^{\mathcal{X}}(t)$ in Equation (5.6) is updated depending upon the given conditions as in Equation (5.11), represented below.

$$DT_{\mathcal{AB}}^{\mathcal{X}}(t) = e^{-\rho t} \times DT_{\mathcal{AB}}^{\mathcal{X}}(t-1) \tag{5.11}$$

where, $e^{-\rho t}$ is considered as an exponential decay time factor.

- **Update indirect trust**:

  The trustor $\mathcal{A}$ updates the indirect trust of trustee $\mathcal{B}$ on encountering another node $\mathcal{C}$ (where $\mathcal{C} \neq \mathcal{B}$) and uses its 1-hop neighbors set $\mathcal{K}_r$, where r= $(0.....n)$, as recommenders including node $\mathcal{C}$. To avoid malicious nodes during recommendation collection, the MATEM considers the condition for allowing node $\mathcal{K}_r$ to provide its recommendations to $\mathcal{A}$ for evaluating $\mathcal{B}$'s indirect trust is as follows:

$$\mathbb{T}_{\mathcal{AK}_r}^{*}(t) > \mathbb{T}_{\text{min}}^{*} \tag{5.12}$$

where, $\mathbb{T}_{\text{min}}^{*}$ is set to ignorance (i.e., 0.5). It states that– recommendations from trustworthy nodes are only considered for indirect trust calculation because untrustworthy node's recommendations could be totally unrelated with the trust. Thus, the best strategy is not to take recommendations from untrustworthy parties. Again, in a hostile environment, nodes' behavior are uncertain, i.e., to say a good node may behave maliciously by providing false information about other peer nodes making trust com-

putation vulnerable to attackers. Thus, to ensure robustness of MATEM against such vulnerabilities, a set of specific rules have been designed in MATEM, for building indirect trust of a trustee in a hostile DTN environment. These rules are necessary for ensuring robustness of our trust based security framework against bad-mouthing and ballot stuffing attacks and are detailed next. In MATEM, the trustor $\mathcal{A}$ uses its 1-hop neighbors set as recommenders to update the "indirect trust" value of trustee $\mathcal{B}$ in its trust table (as depicted in Figure 5.4) with $IT^{\mathcal{X}}_{\mathcal{AB}}(t)$ in Equation (5.6). Let $\mathcal{K}_r$, where $r = (0.....n)$ be the set of 1-hop neighbors of $\mathcal{A}$. On receiving recommendations, the trustor computes the offset value (λ) between the received recommended trust and the direct trust of the trustee stored in trustor's own trust table. If the value of the offset is ≥ 0.2 (i.e., $\lambda \geq 0.2$), the trustor considers it as a malicious activity and update the "indirect trust" value of the trustee by decrementing the stored direct trust value using Equation (5.11). Now, the different DTN scenarios considered in MATEM for establishing indirect trust through collective recommendations are detailed below:

Case I**:** The $Trustor$ receives no recommendation for the $Trustee$ (i.e., $|\mathcal{K}_r| = 0$).

This situation is very common in an opportunistic network with sparse connectivity where 1-hop neighbors may not be available. In this case, since trustor $\mathcal{A}$ is unable to obtain current indirect trust value for trustee $\mathcal{B}$, the $IT^{\mathcal{X}}_{\mathcal{AB}}(t)$ in Equation (5.6) is updated with its past experience decayed over time (t), as represented below:

$$IT^{\mathcal{X}}_{\mathcal{AB}}(t) = e^{-\rho t} \times IT^{\mathcal{X}}_{\mathcal{AB}}(t-1) \tag{5.13}$$

Here, trustor $\mathcal{A}$ simply updates the indirect trust of trustee $\mathcal{B}$ with its past experience (i.e., old indirect trust value) $IT^{\mathcal{X}}_{\mathcal{AB}}(t-1)$ decayed over time t, and $e^{-\rho t}$ is considered as an exponential decay time factor.

Case II**:** The $Trustor$ receives single recommendation for the $Trustee$ (i.e., $|\mathcal{K}_r| = 1$).

While dealing with single recommendation value, trustor $\mathcal{A}$ updates $IT^{\mathcal{X}}_{\mathcal{AB}}(t)$ in Equa-

tion (5.6) as follows:

$$IT^{\mathcal{X}}_{\mathcal{AB}}(t) = \mathbf{min}\big(|T^{\mathcal{X}}_{\mathcal{AK}}(t)|, |RT^{\mathcal{X}}_{\mathcal{KB}}(t)|\big) \tag{5.14}$$

Here, trustor $\mathcal{A}$ receives recommendation for $\mathcal{B}$ from $\mathcal{K}$ ($\mathcal{K}$ may be any encountered node and $\mathcal{K} \neq \mathcal{B}$). $\mathcal{K}$'s recommendation for $\mathcal{B}$ to $\mathcal{A}$ is represented as $RT^{\mathcal{X}}_{\mathcal{KB}}$. The recommendation is obtained in a situation where $\mathcal{A}$ has already established trust relationship with $\mathcal{K}$ and its value is greater than the minimum trust thresh hold (i.e., $\mathbb{T}^{*}_{\mathcal{AK}_r}(t) > \mathbb{T}^{*}_{\text{min}}$), and the computed λ is less than 0.2. Equation (5.14) states that when a trustor establishes an indirect trust relationship with a trustee on each trust criteria through recommendation, the "indirect trust" value between trustor and trustee is minimum of the two values derived as initial and recommended trust about the trustee.

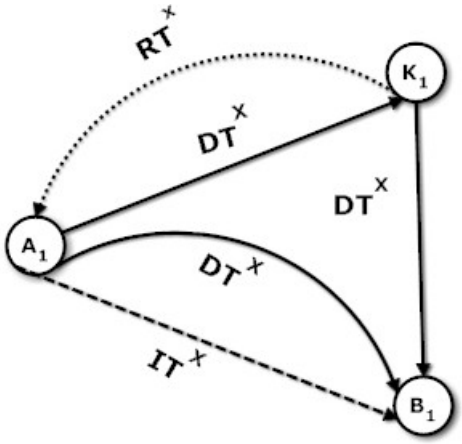


Figure 5.6: Trustor receives recommendation from single source

In Figure 5.6, trustor $\mathcal{A}_1$ establishes indirect trust with trustee $\mathcal{B}_1$ through single recommendation, whereas in Figure 5.7, $\mathcal{A}_2$ establishes indirect trust with $\mathcal{B}_2$ through recommendations from multiple 1-hop neighbors $\mathcal{K}_r$ as recommenders.

CASE III**:** The *Trustor* receives recommendations for the *Trustee* from multiple sources (i.e., $RT^{\mathcal{X}}_{\mathcal{K}_1\mathcal{B}} \neq RT^{\mathcal{X}}_{\mathcal{K}_2\mathcal{B}}$).

If trustor $\mathcal{A}$ receives multiple recommendations for trustee $\mathcal{B}$ from multiple 1-hop recommenders $\mathcal{K}_r$, then indirect trust of $\mathcal{B}$ towards node $\mathcal{A}$ is the weighted average of the recommendations derived from Equation (5.14), as follows:

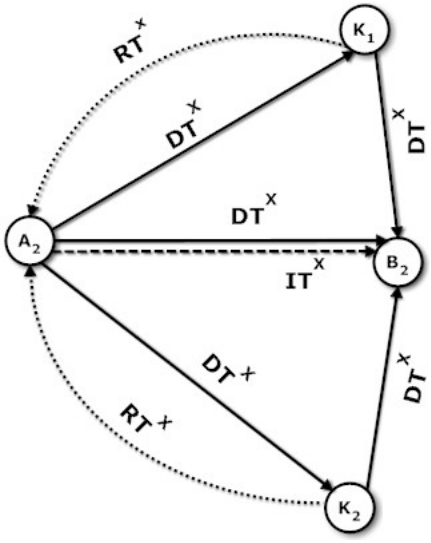


Figure 5.7: Trustor receives recommendations from multiple sources

$$IT^{\mathcal{X}}_{\mathcal{AB}}(t) = \frac{\sum_{r=1}^{\mathcal{R}} \Big(\omega_{\mathcal{A},\mathcal{K}_r} \times \mathbf{min}\big(|T^{\mathcal{X}}_{\mathcal{AK}_r}(t)|, |RT^{\mathcal{X}}_{\mathcal{K}_r\mathcal{B}}(t)|\big) \Big)}{\sum_{r=1}^{\mathcal{R}} \omega_{\mathcal{A},\mathcal{K}_r}} \tag{5.15}$$

where, $\omega_{\mathcal{A},\mathcal{K}_r}$ is the trustor's weight to the recommender $\mathcal{K}_r$, and is calculated as:

$$\omega_{\mathcal{A},\mathcal{K}_r} = \frac{RT^{\mathcal{X}}_{\mathcal{K}_r\mathcal{B}}(t)}{RT_{\text{avg}}(t)} \tag{5.16}$$

$$\text{and } RT_{\text{avg}}(t) = \frac{\sum_{r=1}^{\mathcal{R}} RT^{\mathcal{X}}_{\mathcal{K}_r\mathcal{B}}(t)}{\mathcal{R}} \tag{5.17}$$

here, $\mathcal{R}$ being the total number of 1-hop neighbors of trustor $\mathcal{A}$.

- **Update initial trust**:

  As depicted in the trust computation module of Figure 5.4, each trustor node derives its direct trust and/or indirect trust towards the trustee node and calculates its initial trust value $T^{\mathcal{X}}_{\mathcal{AB}(t)}$, as presented in Equation (5.6). We aggregate direct and indirect

trust to get initial trust level of a node. The trust table is updated with the new value against each individual trust criteria. Once the initial trust is formed, the node executes trust prediction module of Figure 5.4 for computing "absolute trust" of each node it encountered.

Trust Prediction Module

This module details how a trustor node computes "absolute trust" i.e., $[\mathbb{T}^*]$ value of a trustee locally, given observations related to the various trust criteria that are computed and stored as initial trust level of each node in the network. Based on this absolute trust value of a trustee node, a trustor selects its next-hop message carrier in DTN routing. In MATEM, each node in the network maintains a local trust table that contains direct trust, indirect trust, and initial trust values which have been evaluated from Equation (5.6) on the basis of direct observation and recommendation against each encountered node. The trust prediction module makes use of a MCDM [121] technique called TOPSIS [73] for calculating absolute trust value from initial trust values of each node. MCDM-based techniques have been designed to designate a preferred alternative with respect to the different attributes or criteria. These techniques have been explored and extended to many application areas [131, 136, 137, 138] for making decisions in the presence of multiple, potentially conflicting criteria. Among numerous MCDM methods developed to solve real-world decision problems, TOPSIS continues to work satisfactorily across different application areas. In recent years, TOPSIS has been successfully applied to the areas of human resources management [139], transportation [140], product design [141], manufacturing [142], water management [143], quality control [144], and location analysis [145]. In addition, the concept of TOPSIS has also been connected to multi-criteria decision making [73]. While solving a multiple criteria decision making problem, the TOPSIS method attempts to choose alternatives that simultaneously have the shortest geometric distance from the Positive Ideal Solution (PIS) and the farthest geometric distance from the Negative Ideal Solution (NIS). Briefly, the PIS is made up of all best values attainable for each criteria under consideration, whereas the NIS is composed of all worst values attainable for those criteria. Thus, PIS maximizes the benefit criteria and minimizes the cost criteria, whereas the NIS maximizes the cost criteria and minimizes the benefit criteria. Thus, the TOPSIS method, originally used in the field of *"Design, Engineering and Manufacturing Systems"* for decision making purposes has been integrated with different computational aspects of DTN routing security to deal with the conflicting node behaviors, making MATEM an interdisciplinary technique

for ensuring routing security in DTNs.

In the proposed MATEM framework, a trust-based TOPSIS paradigm is used for facilitating a trustor to find the best option from all of the feasible alternatives i.e., encountered nodes for whom trust is being calculated. This is achieved while measuring the impact of each trust measuring criteria which are conflicting in nature in view of the nodes' behavioral perspectives as well as from the objective of optimization, and thereby on the overall utility of the trustee. To elaborate, a non-misbehaving node may be socially selfish, or a non-selfish node may misbehave by providing false information. Further, from the optimization point of view, the trustor would always try to maximize "Connectivity" and "Cooperativeness" trust criteria, while minimizing "Risk" and "AMFD" trust for the trustee. Thus, to address such issues, all the trust measuring criteria are given equal importance, since trade offs between these conflicting criteria are not permissible in MATEM. An unfavorable value in one criteria cannot be offset by a favorable value in other criteria. Hence, comparisons are carried out on a criteria-by-criteria basis. To facilitate the comparisons, all trust criteria are classified into two categories. The criteria having positive impact for routing are grouped into `Benefit Criteria` and those having negative impact are grouped into `Cost Criteria`. The `Benefit Criteria` includes "Connectivity" and "Cooperativeness" trust, whereas `Cost Criteria` includes "Risk" and "AMFD" trust. Now the different steps that are followed to compute absolute trust value of encountered nodes in MATEM are detailed next.

1. *Construction of a trust evaluation matrix*: The trust evaluation matrix viz., $\mathbb{D} = \left[d_{ij}\right]_{m\text{x}n}$ is comprised of m nodes and n trust measuring criteria. Node ID's are maintained in rows and initial trust values associated with different trust measuring criteria are represented in columns. Each component d_{ij} represents the initial trust value of node $\mathcal{N}_i$ with respect to trust criterion $\mathcal{C}_j$ and represented in Table 5.1.

Table 5.1: Trust Evaluation Matrix

	$\mathcal{C}_1$	$\mathcal{C}_2$	...	$\mathcal{C}_n$
$\mathcal{N}_1$	d_{11}	d_{12}	...	d_{1n}
$\mathcal{N}_2$	d_{21}	d_{22}	...	d_{2n}
...	...	...	...	...
$\mathcal{N}_m$	d_{m1}	d_{m2}	...	d_{mn}

2. *Construction of normalized trust evaluation matrix*: Multiple different trust measur-

ing criteria as detailed earlier often generate trust scores of incongruous dimensions. Hence normalization is done to make these scores conform to a non-dimensional unit. To compare the trustee nodes on each trust criteria, the normalization process that is made column-wise to deal with incongruous criteria dimensions is called vector normalization. Therefore, each element of $\mathbb{D}$ is normalized to form the new matrix as $\mathbb{R} = \left[r_{ij}\right]_{m\text{x}n}$ as follows:

$$r_{ij} = \frac{d_{ij}}{\sqrt{\sum_{i=1}^{m} d_{ij}^2}}, \quad i = 1, \ldots, m, \text{ and } j = 1, \ldots, n \tag{5.18}$$

The outcome normalized value r_{ij} is a positive value between 0 and 1.

3. *Construction of weighted normalized trust evaluation matrix*: A weight vector $\mathcal{W}_j$ is assigned to each trust measuring criteria. Equal weights are assigned for each of the trust criteria, since MATEM framework considers similar priority for each of it's trust measuring criteria. Therefore each column of the normalized matrix $\mathbb{R}$ is multiplied by its associated weight and a new weighted normalized trust evaluation matrix $\mathbb{T} = \left[\hat{t}_{ij}\right]_{m\text{x}n}$ is obtained. The weighted normalized value $\hat{t}_{ij}$ is calculated as

$$\hat{t}_{ij} = \omega_j \times r_{ij} \tag{5.19}$$
$$\text{where, } i = 1, \ldots .m, \text{ and } j = 1, \ldots, n$$
$$\text{and } \sum_{j=1}^{n} \omega_j = 1$$

4. *Computation of ideal and non-ideal solutions*: In this step an ideal solution set and a non-ideal solution set comprising of numeric values associated with each trust measuring criteria are selected. The values are taken from the weighted normalized trust evaluation matrix. An ideal solution set is made up of all best values (i.e., maximum for `Benefit Criteria` and minimum for `Cost Criteria`) attainable for each trust criteria. Whereas a non-ideal solution is composed of all worst values (i.e., minimum for `Benefit Criteria` and maximum for `Cost Criteria`) attainable for the criteria under consideration. The ideal ($\mathbb{I}^+$) and the non-ideal ($\mathbb{I}^-$) solution sets are computed as follows:

$$\mathbb{I}^{+} = \{\hat{t}_1^{+},\ \hat{t}_2^{+}, \ldots,\ \hat{t}_n^{+}\}$$
$$= \left\{\left(\max_i \hat{t}_{ij} \mid j \in \mathbf{Z}\right), \left(\min_i \hat{t}_{ij} \mid j \in \mathcal{Z}\right) \mid i = 1 \ldots m\right\} \tag{5.20}$$
$$\mathbb{I}^{-} = \{\hat{t}_1^{-},\ \hat{t}_2^{-}, \ldots,\ \hat{t}_n^{-}\}$$
$$= \left\{\left(\min_i \hat{t}_{ij} \mid j \in \mathbf{Z}\right), \left(\max_i \hat{t}_{ij} \mid j \in \mathcal{Z}\right) \mid i = 1 \ldots m\right\} \tag{5.21}$$

where $\mathbf{Z}$ is associated with benefit criteria, and $\mathcal{Z}$ is associated with cost criteria.

5. *Calculation of separation measures of each node from the ideal and non-ideal solutions individually*: Separation measures are calculated using the n-dimensional Euclidean distance. This step is executed to calculate the distance of each trustee nodes from the ideal and non-ideal solution sets. The basic idea of choosing a trustee node as a next hop message carrier is that the chosen node should have the shortest distance from the ideal solution and the longest distance from the non-ideal solution. The separation measures, $\mathbb{S}_i^{+}$ and $\mathbb{S}_i^{-}$, of each node from the ideal solution and non-ideal solution sets, respectively, are derived from:

$$\mathbb{S}_i^{+} = \sqrt{\sum_{j=1}^{n} \left(\hat{t}_{ij} - \hat{t}_j^{+}\right)^2}, \quad i = 1, \ldots, m \tag{5.22}$$

$$\mathbb{S}_i^{-} = \sqrt{\sum_{j=1}^{n} \left(\hat{t}_{ij} - \hat{t}_j^{-}\right)^2}, \quad i = 1, \ldots, m \tag{5.23}$$

6. *Calculation of absolute trust value of each trustee nodes*: The absolute trust value of each trustee node is derived from the relative closeness measure of each node to the ideal solution set. The trustor updates its own table with the derived absolute trust value $\mathbb{T}_i^{*}$ associated with each trustee node. The relative closeness of each node $\mathcal{N}_i$ with respect to the ideal solution $(\mathbb{I}^{+})$ is obtained as follows:

$$\mathbb{T}_i^{*} = \frac{\mathbb{S}_i^{-}}{\left(\mathbb{S}_i^{+} + \mathbb{S}_i^{-}\right)}, \quad i = 1, \ldots, m \tag{5.24}$$

Since $\mathbb{S}_i^{+} \geq 0$ and $\mathbb{S}_i^{-} \geq 0$, then clearly, $\mathbb{T}_i^{*} \in [0, 1]$.

7. *Rank the nodes according to the absolute trust value*: The node with higher $\mathbb{T}_i^{*}$, where $\mathbb{T}_i^{*} > 0.5$ is considered to be trusted and given priority according to preference for selection as a next-hop forwarder. The i^{th} node will be the best if $\mathbb{T}_i^{*}$ is maximum.

A forwarding based routing strategy (i.e., single copy forwarding) for DTN shall consider the node having $^{\mathbf{max}}\mathbb{T}_i^*$ value as a next-hop message carrier, whereas a flooding based routing (i.e., multi-copy forwarding) shall consider the set of nodes having trust value $\mathbb{T}_i^* > 0.5$ from its local trust table and thus, aims for an optimized flooding.

5.4 MATEM's Resiliency against Attacks

In MATEM, the evaluation of trustworthiness of each participating node ensures an effective method to simulate nodes misbehavior and thus to improve routing security in hostile DTNs. But, generally any trust evaluation and management system itself is an attractive target for attackers. Section 5.4.1 details the probable attacks that may hinder MATEM's efficiency and the preventive measures that have been considered while designing the proposed secure framework. Detailed simulation-based results and their analysis are also provided in Section 5.4.2 to claim the resiliency of the MATEM framework against attacks.

5.4.1 Attacks on MATEM

The trust building process of MATEM is based on direct observations and collected evidence. The direct trust is evaluated on contact and indirect trust is accumulated through collective recommendations from neighboring nodes. In a hostile scenario, an honest node may turn dishonest and behave maliciously by providing false recommendations about other nodes in the network. Thus, a malicious node can undermine the trust management system by boosting trust values for malicious parties or framing up good nodes to launch *bad-mouthing* and *good-mouthing* attacks. These types of activities by misbehaving nodes lead a trustor to make unreliable decisions and thus undermine the effectiveness and performance of MATEM in a hostile DTN scenario. Moreover, the consideration of nodes' selfish behavior is also another important issue to address MATEM's resiliency against *Selfish* attacks. Here, we detail the prominent attacks that may be launched by misbehaving nodes in MATEM.

- *Bad-mouthing attacks*: A malicious node can launch this attack on the indirect trust computation module of MATEM. In this attack, the malicious nodes provide unfairly low recommendations related to different trust measuring criteria for good nodes. This attack is launched with an ill intent to tarnish the trust value of good nodes and so as to reduce their chances of being selected as the message carrier in the routing

path. This situation may reduce the presence of good nodes in the network and may confuse a trustor to select a next-hop carrier for message forwarding.

- *Good-mouthing attacks*: In this attack, the malicious nodes provide unfairly positive recommendations for some colluding nodes and boost their trust values in the network. The intention of such an attacker is to increase the chance of message routing through malicious nodes and thus dropping those messages from the network leading to performance degradation of the MATEM framework.

- *Selfish attacks*: The selfish nodes are those who are unwilling to spend their resources on forwarding messages of other nodes with whom they do not have good social relationships. Thus, they may launch selfish attacks by dropping unwanted buffered messages to free their own buffer space.

5.4.2 Performance Evaluation of MATEM against Attacks

This section presents the experimental study that has been carried out to confirm the MATEM's resiliency against *Bad-mouthing*, *Good-mouthing*, and *Selfish* attacks. The experimental environment is created with the Opportunistic Networking Environment (ONE) simulator [146], which is designed to evaluate DTN routing and application protocols. Extensive simulations are carried out to evaluate MATEM's resiliency in terms of standard security metrics viz., *Attack Detection Rate* (ADR), *False Negative Rate* (FNR), and *False Positive Rate* (FPR) in the presence of bad-mouthing, good-mouthing and selfish attacks. The metric ADR represents the number of misbehaving nodes providing dishonest recommendations identified by MATEM, while FNR indicates the number of dishonest recommendations identified as honest, and FPR represents the number of honest recommendations identified as dishonest by the MATEM framework. The percentage of misbehaving nodes are varied to evaluate the MATEM's resiliency under different attack conditions. Further, the same set of experiments are also carried out with different trust threshold settings to get the best achievable performance of the MATEM under dynamically changing network conditions in a hostile DTN scenario.

Simulation Environment

The resiliency of MATEM against different attack scenarios is evaluated on top of the Epidemic [34] (multi-copy flooding) routing protocol. In the experimental setup, we have

Table 5.2: Parameters For Attacks Scenario Simulation Model

Parameter	Value
Network Area	[2000 x 2000] m^2
Number of Nodes	100
Percentage of Misbehaving Nodes	[5% - 45%]
Mobility Pattern	RandomWayPoint
Node Speed	[0 - 5] m/s
Interface Type	SimpleBroadcastInterface
Transmission Speed	4 MBps
Transmission Range	25 m
Message Generator	MessageEventGenerator
Message Generator Interval	One message per 100 sec
Node's Buffer Size	30 M
Message size	[500 k]
Message TTL	240 min
Trust Threshold	[0.3, 0.5, 0.7]
Seeds	[1,2,3]
Scenario Update Interval	0.1
Total Simulation Run Time	43200 sec

considered both honest and misbehaving nodes moving in the network area. The node mobility is created with RandomWayPoint mobility model. The source-destination pairs are selected at random from the honest nodes for each message with a fixed message generation rate. The parameter settings for all our experiments are listed in Table 5.2.

Results and Analysis

Here we analyze the set of results that have been obtained from the simulation study to confirm the resiliency of MATEM under different attack scenarios. The effects of such attacks are also analyzed with different trust threshold settings.

Figures 5.8, 5.9, and 5.10 exhibit the effects of *Bad-mouthing* attack on MATEM's ADR, FNR, and FPR metrics. The simulations have been carried out by varying the proportion of attackers from 5% to 45% in the network. It has been observed that MATEM can effectively mitigate the dishonest recommendations propagated by the bad-mouthing attackers. The ADR and FNR metrics show optimal results in the presence of bad-mouthing attackers, while keeping the FPR at a very low level (3%). The results of the simulation study are ob-

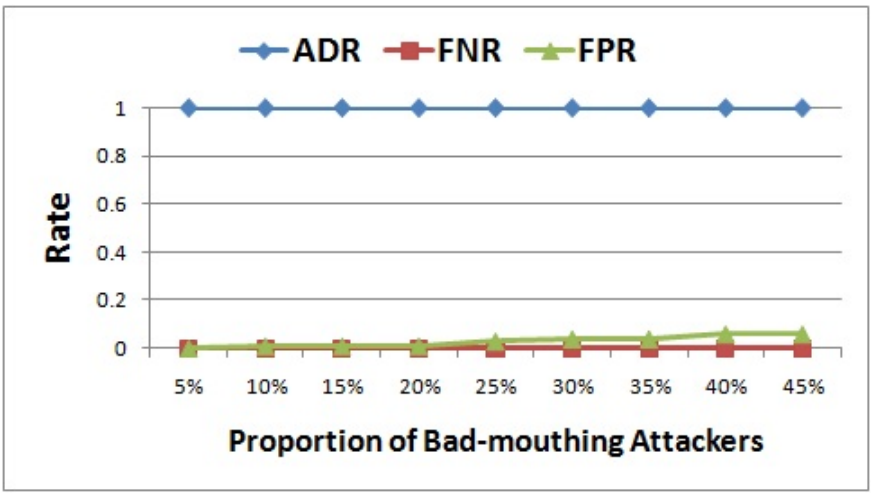


Figure 5.8: ADR, FPR, FNR against Trust Threshold 0.3

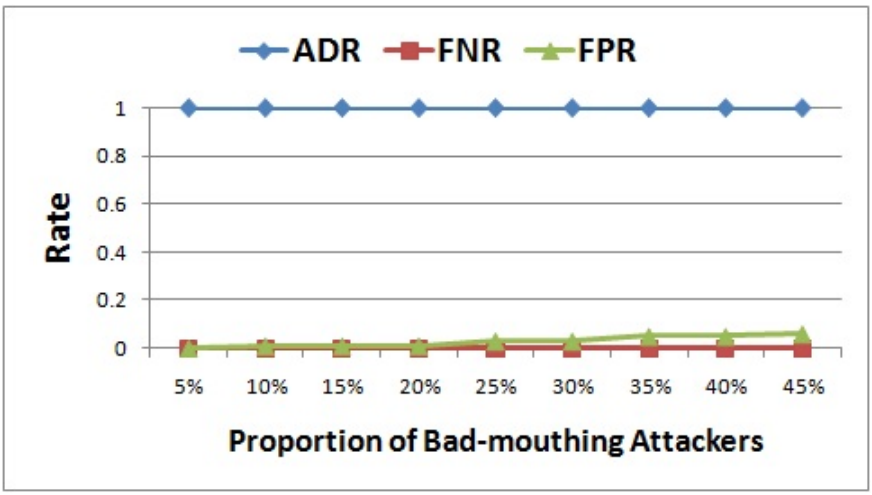


Figure 5.9: ADR, FPR, FNR against Trust Threshold 0.5

vious due to the consideration of different set of rules for recommendation collection and aggregation in MATEM. The MATEM framework allows a "trustor" to receive recommendations from trustworthy nodes only. Moreover, it has the capability of avoiding dishonest recommendations through the offset evaluation procedure that can segregate an honest recommendation from a dishonest one. Thus, the recommendations from the misbehaving nodes could be avoided in indirect trust calculation of MATEM. The reason for existence of low FPR is the consideration of the "offset" threshold value due to which some honest recommenders are treated as dishonest. Further, with different trust threshold settings, the

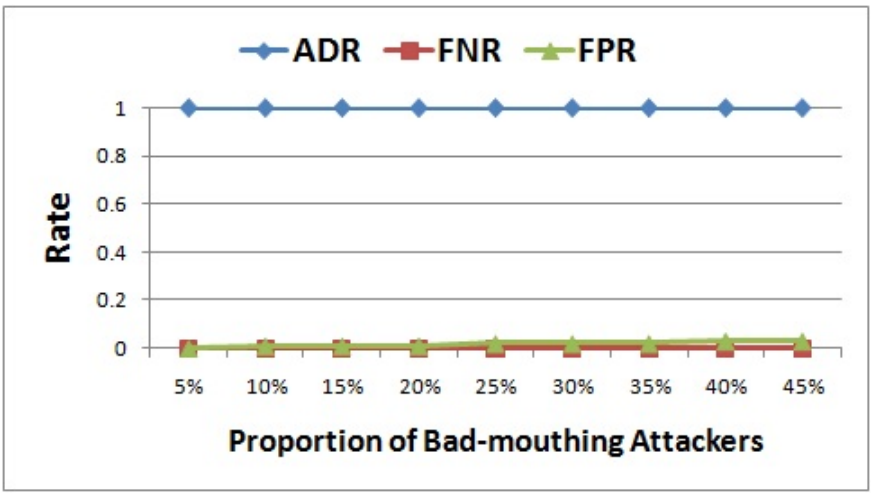


Figure 5.10: ADR, FPR, FNR against Trust Threshold 0.7

simulation results of MATEM represent a similar trend in terms of ADR, and FNR metrics. Whereas, the existence of FPR (with trust threshold 0.3 and 0.5) has been nullified with trust threshold 0.7, because this setting has allowed only high trust valued nodes to participate in trust building process and thereby minimizing the effects of recommendation offset.

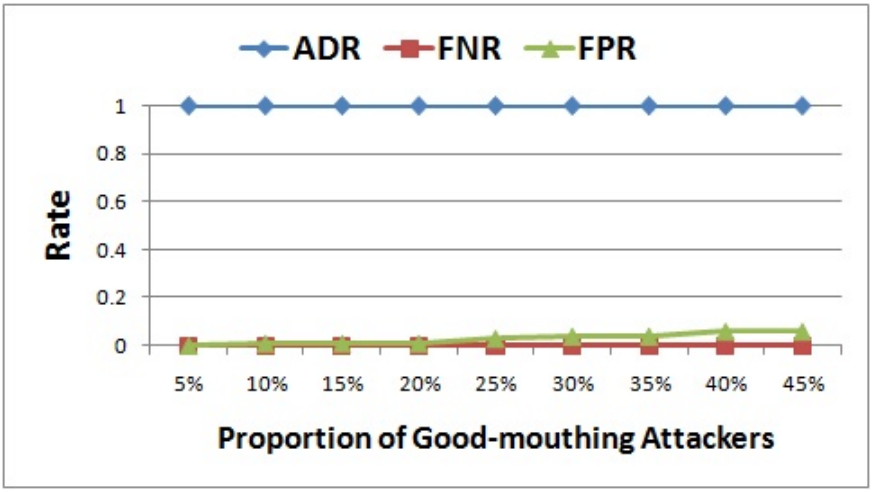


Figure 5.11: ADR, FPR, FNR against Trust Threshold 0.3

Figures 5.11, 5.12, and 5.13 depict the effect of *Good-mouthing* attack on MATEM's ADR, FNR, and FPR metrics. Similar, to bad-mouthing attack, in this set of simulations, the percentage of good mouthing attackers are varied from 5% to 45% to evaluate the resiliency

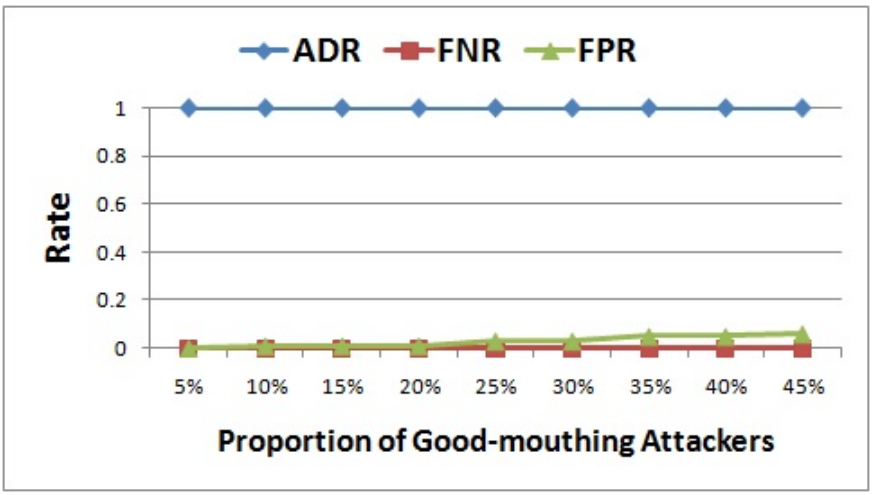


Figure 5.12: ADR, FPR, FNR against Trust Threshold 0.5

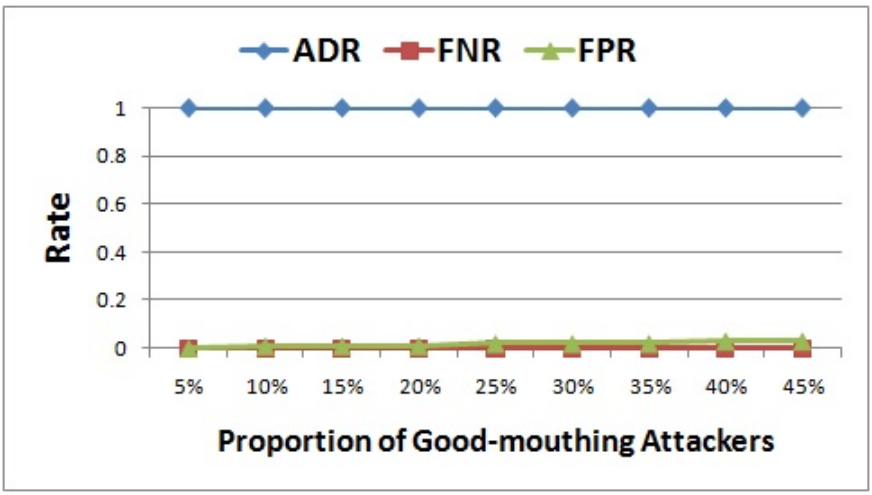


Figure 5.13: ADR, FPR, FNR against Trust Threshold 0.7

of the MATEM framework in terms of ADR, FNR, FPR. The proposed framework is seen to be identifying the dishonest recommendations and eliminating false negatives effectively. The proportion of false positives is maintained at a reasonable low level. The justification for such results is similar to what was explained in the case of *Bad-mouthing* attack.

Figures 5.14, 5.15, and 5.16 show the performance of MATEM in the presence of *Selfish* attacks. In a social environment, selfish nodes launch such attacks by dropping messages to save their resources if those messages are meant for the recipients with whom the attacker does not have good social ties. In our experimental study, we simulate this attack with

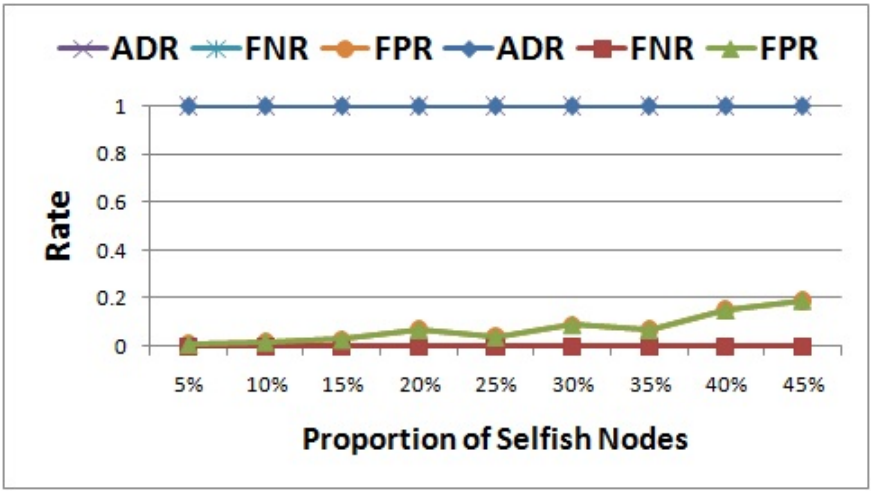


Figure 5.14: ADR, FPR, FNR against Trust Threshold 0.3

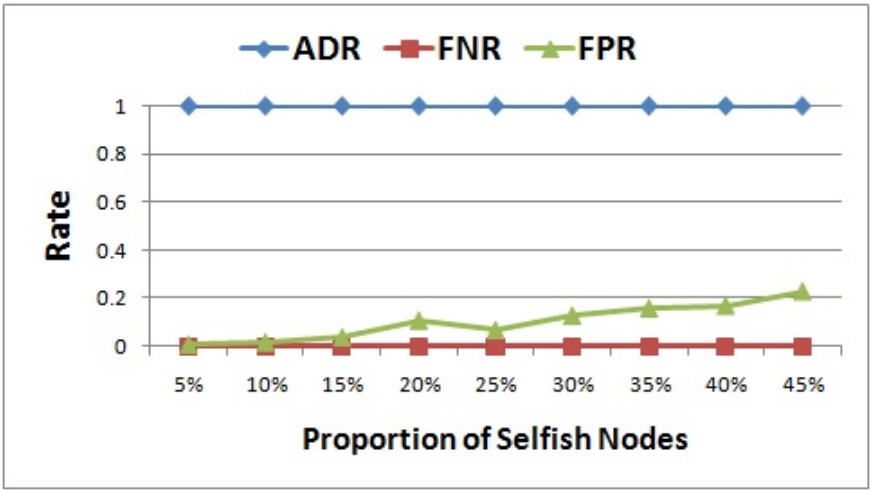


Figure 5.15: ADR, FPR, FNR against Trust Threshold 0.5

node's message dropping behavior. The results generated from the simulation study exhibit the efficiency of MATEM in terms of ADR and FNR. This could be achievable due to the consideration of "Cooperativeness" trust criteria to simulate the social behavioral pattern of DTN nodes (in terms of social ties) and thus can avoid *Social attacks* in the routing path. The increasing trend in the FPR with an increase in selfish attackers is an effect of nodes' message dropping due to buffer overflow and message's TTL expiration. Further, with high trust threshold settings, the chances of availability of competent forwarders get reduced and

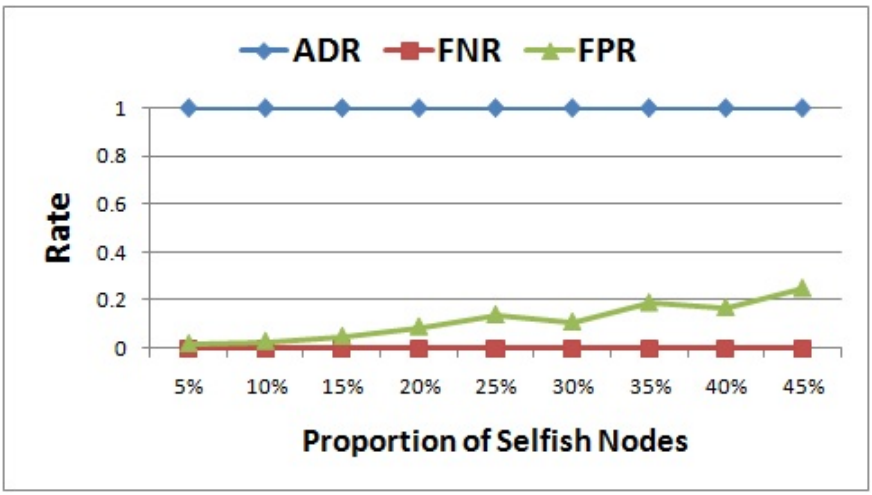


Figure 5.16: ADR, FPR, FNR against Trust Threshold 0.7

thus the scope of message forwarding in DTNs. These factors cause message TTL expiration and buffer overflow at the participating nodes leading to rise in FPR.

It has been observed from the simulation study that consideration of different recommendation collection methods as well as the "Cooperativeness" trust metric have a varied level of positive impacts on the performance of MATEM against different security attacks. The effects of "Bad-mouthing" and "Good-mouthing" attacks could be reduced to a great extent due to the incorporation of different recommendation collection and aggregation techniques in the MATEM framework. Again, the chances of "Selfish" attacks are minimized while considering "Cooperativeness" trust criteria for assessing node's cooperation in terms of social ties. These factors result in terms of optimal ADR and FNR. Further, MATEM's resiliency against different security attacks are also simulated with different trust threshold settings under dynamically changing network conditions in a hostile DTN scenario. The simulation results demonstrate that with different trust threshold settings (i.e., 0.3, 0.5, 0.7), the ADR and FNR remain stable in the presence of "Bad-mouthing", "Good-mouthing", and "Selfish" attacks. But the amount of FPR decreases by 2% with changes in threshold (i.e., from 0.5 to 0.7) for "Bad-mouthing" and "Good-mouthing" attacks, whereas it increases by 4% for "Selfish" attacks. The reason for low FPR with increasing trust threshold (i.e., 0.7) setting in case of "Bad-mouthing" and "Good-mouthing" attacks is that this threshold has allowed only high trust valued nodes to provide recommendations and thereby the effects of recommendation offset get minimized. Whereas an increase in FPR with trust threshold 0.7 in case of "Selfish" attacks is due to the non-availability of competent forwarders in the

routing paths. This causes honest nodes to drop messages due to message TTL expiration and buffer overflow leading to rise in false positive proportions. Therefore, it can be concluded that consideration of threshold setting as 0.5 enhances the performance of MATEM by eliminating nodes' misbehaving activities (i.e., dishonest recommendations and nodes' selfish behaviors) even though it could result in a small proportion of FPR (2% only) in all the attack scenarios under consideration.

5.5 Simulation of MATEM and Performance Evaluation

This section introduces the different sets of simulation study that have been carried out to test the adaptability and suitability of the MATEM framework for ensuring routing security in hostile DTN environment. The framework has not only been integrated with non-trust based forwarding algorithms [34, 36] available in DTNs, but also been compared with three different trust based routing protocols, as available in [76, 78], and [83], to evaluate an encounter's ability for secure and reliable delivery of data to the destination. The protocols under study are Epidemic [34], First Contact [36], T-PROPHET [76], Trust-Threshold based routing [78], and Trust Based Intelligent Routing (TBIR) [83].

MATEM has been implemented with Opportunistic Network Environment (ONE) simulator [146]. Extensive simulations are carried out to evaluate MATEM's performance in terms of message delivery ratio, delivery latency and delivery cost (i.e., overhead ratio) in a metropolitan city like network scenario with varying percentage of misbehaving nodes and nodes' buffer capacity. Moreover, the framework has also been simulated for its optimal trust threshold value to gain the best achievable performance of MATEM based routing since it is the key parameter to judge the competency of a node for being selected as a next-hop message carrier.

A comparative analysis of MATEM with Epidemic [34], First Contact [36], T-PROPHET [76], Trust-Threshold [78], and TBIR [83] has been studied to evaluate its adaptability and suitability in hostile DTN environment. The Epidemic [34], and First Contact [36] have been considered as the base line routing protocols for their performance in terms of message delivery ratio and message delivery cost, respectively. The epidemic routing is a flooding based protocol that replicates bundles at contact opportunities improving delivery probability and minimizing delivery latency at the cost of higher overhead. Whereas, First Contact is a forwarding based protocol and maintains a single copy of a bundle in the network requiring low resource utilization but resulting in low delivery ratios and long delays. T-PROPHET

is a reputation assisted framework for assisting data forwarding in DTNs. It is based on the collected evidences of nodes' packet-forwarding behavior. The Trust-Threshold based routing on the other hand relies on social trust and QoS trust to assess the nodes' behavior and a weighted average method is used to evaluate the trust level of a node in DTNs. The TBIR framework uses the function of ANN to calculate and learn trust value that can be shared among network devices. The routing performance of these protocols have been simulated and evaluated with and without integrating the MATEM framework in a hostile DTN environment. The Epidemic protocol with MATEM is called MATEM-ED and that of First Contact is renamed as MATEM-FC.

Table 5.3: Node Configuration in the Simulations

Group type	Buffer(M)	Speed (km/h)	Wait Time (s)	No. of Nodes	Movement Model
Pedestrian 1	10	0.5 - 1.5	0 - 120	40	**ShortestPathMapBased**
Pedestrian 2	10	0.5 - 1.5	0 - 120	40	**ShortestPathMapBased**
Cars	10	10 - 25	0 - 120	40	**ShortestPathMapBased**
Trams 1	50	7 - 10	10 - 30	2	**MapRouteBased**
Trams 2	50	7 - 10	10 - 30	2	**MapRouteBased**
Trams 3	50	7 - 10	10 - 30	2	**MapRouteBased**

5.5.1 Simulation Environment

The simulation study is conducted using the synthetic contact trace generated by the ONE simulator. In the synthetic contact trace, 126 number of mobile nodes having heterogeneous characteristics are scattered over 4500 m x 3400 m area of Helsinki City map (the default map in ONE simulator). These mobile nodes are then divided into six different groups (two pedestrians, one cars, three trams groups) based on node's configurations in terms of buffer size, moving speed, available interface, and movement model to generate a metropolitan city like node mobility pattern. The detailed node configurations are given in Table 5.3. The two pedestrian groups and three tram groups use different map route files for movement though they are configured with similar node characteristics. All nodes are configured with simple broadcast interface having different transmitting speeds and ranges. For tram1, it uses a high speed, long range interface with the transmission speed as 10 Mbps along with a transmission range set to 1000 m. Whereas, for all other groups the transmit speed is set

to 4 Mbps and the transmission range is set to 100 m. The default event generator of ONE simulator is used to generate messages with intervals between 145 s and 155 s, and the message size varies from 500 k bytes to 1 M bytes. The time-to-live (TTL) for each message is set to 240 mins. Table 5.4 depicts the value set for all simulations.

Table 5.4: Parameters For Simulation Model

Parameter	Value
Interface Type	SimpleBroadcastInterface
Transmission Speed	[4 , 10] MBps
Transmission Range	[100 , 1000] m
Node's Buffer Size	[10M - 100M]
Message Generator	MessageEventGenerator
Message Generator Interval	[145 - 155] sec
Message size	[500 k, 1 M]
Message TTL	240 min
Seeds	[1,2,3]
Scenario Update Interval	0.1
Total Simulation Run Time	43200 sec

During simulation study, the initial trust level of each node is set to ignorance (i.e., 0.5) for all trust components considered in MATEM. This is justifiable since at the beginning nodes do not know each other. Again, the trust threshold for seeking recommendation is also set to greater than 0.5, so that only trusted nodes can act as recommenders. To update trust, different random set of nodes are chosen from different groups to misbehave and such nodes are proportional to the total number of nodes in that group. A misbehaving node behaves maliciously either by dropping messages or by providing false recommendations about other nodes in the network. Moreover, to exhibit selfishness, a node's forwarding capability is restricted with 50 percent of the chance. The trust value of misbehaving nodes decrease over time and become untrustworthy. Following that, they are never able to gain trustworthy status again. In order to gain good confidence in the measured results, all simulations are run 5 times with different seed values to obtain mean values of the above mentioned parameters.

5.5.2 Results and analysis

This section analyzes the set of results that have been obtained from the simulation study to evaluate the efficiency of the MATEM framework. A comparative analysis with Epidemic, First Contact, T-PROPHET, Trust-Threshold based routing, and TBIR is also provided to justify its suitability in a hostile DTN environment.

Impact of trust threshold

The value of the trust threshold plays an important role for selecting a trustworthy message forwarder which in turn has an impact on the MATEM based routing in DTNs. A low value for it shall allow more number of nodes to participate in message forwarding making MATEM vulnerable to attacks. Again, a high value will restrict many trustworthy nodes to refrain from message forwarding resulting delivery ratio to drop. Therefore, selecting an optimal trust threshold for MATEM is crucial for ensuring secure routing and reliable delivery of data to the destinations. In this set of simulations, 50 percent of nodes from each of the six different groups are considered as misbehaving nodes and each simulation instances is run for 12 hours with different seed values. The message TTL is considered as 300s along with average node buffer size as 30 M and the regular data in the simulations are generated through Epidemic protocol.

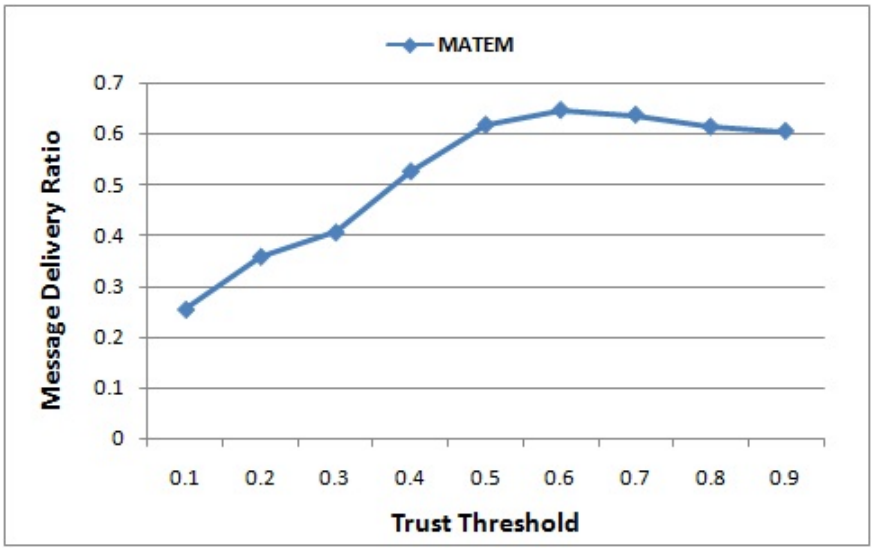


Figure 5.17: Impact of Trust Threshold on MATEM's Message Delivery Ratio

Figure 5.17 exhibits a three phase effect on MATEM's message delivery ratio with increasing trust threshold. Initially, a low delivery rate is observed against low trust threshold (here it is 0.1 to 0.4) values. This is because majority of nodes are treated as trustworthy and they

participate in message forwarding. A low trust threshold value allows misbehaving nodes to gain their access in message forwarding causing disruption in the normal routing behavior. However, the delivery rate increases with increased trust threshold and remains roughly stable up to a certain limit (here it is 0.7). This is due to the avoidance of misbehaving nodes in the forwarding path. But, after some extent (here it is 0.8) the delivery ratio starts showing a decreasing trend. This is due to the non-availability of competent forwarders due to the high threshold value that causes message's TTL expiration and buffer overflow at the participating nodes.

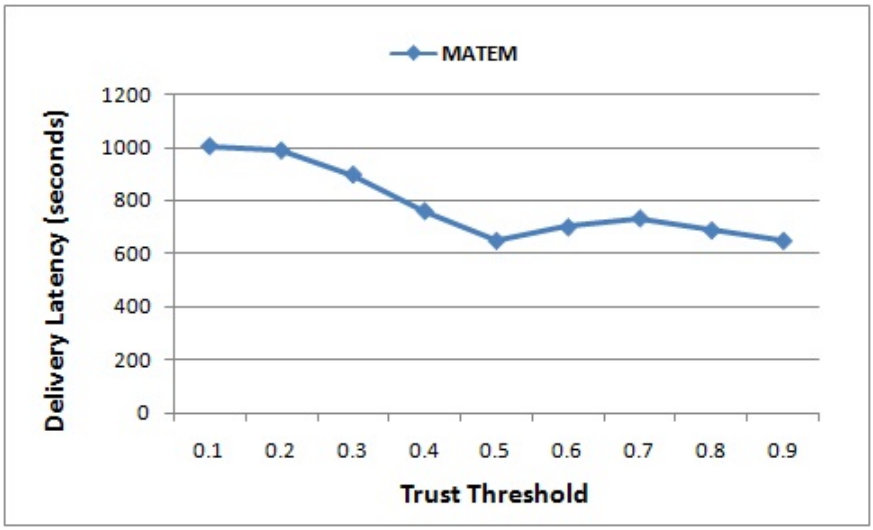


Figure 5.18: Impact of Trust Threshold on MATEM's Message Delivery Latency

Figure 5.18 exhibits the delivery latency of MATEM against varying trust threshold. It has been observed that delivery latency is high with low trust threshold. A low trust threshold setting in MATEM allows more number of nodes to get the message copies, however further reduces the chance of message delivery by 50 percent causing higher delivery latency. This is because of incorporation of less trustworthy nodes in routing. But with increased trust threshold (i.e., from 0.4 to 0.7), the delivery latency decreases. This is due to the avoidance of less trustworthy nodes as well as consideration of average message forwarding delay criteria in trusted carrier selection process. Further, an increase in average latency after a certain limit (here it is 0.7) is due to the increase in average queuing time, since a high trust threshold value reduces the scope of message forwarding in DTNs.

The impact of trust threshold on delivery cost of MATEM is depicted in Figure 5.19. Message delivery cost evaluates the efficiency of MATEM framework in terms of network resource consumption. The simulation result shows that low trust threshold increases the de-

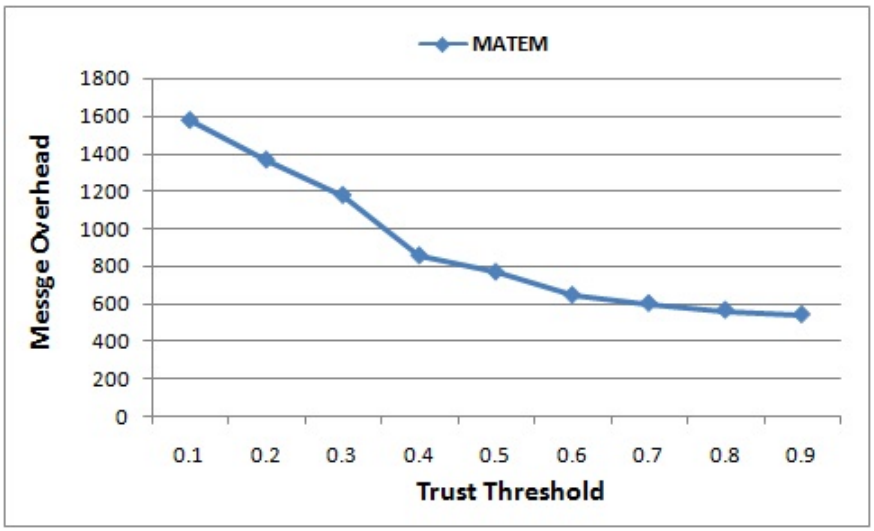


Figure 5.19: Impact of Trust Threshold on MATEM's Message Delivery Cost

livery cost. The reason is that, low trust threshold allows more message copies to propagate in the network and the messages may traverse several hops to reach the destination causing high amount of network resource consumption. Whereas, an increase in trust threshold gradually reduces the delivery cost to a certain extent and it remains stable with increasing threshold. This is due to the selection of more competent nodes for message forwarding that reduces the hop count as well as the amount of redundant messages in the network.

It has been noticed that MATEM's delivery ratio not only gets affected by the presence of misbehaving nodes but also due to the degree of connectivity and mobility issues of the nodes in a DTN scenario. The observations made on MATEM's performance for different trust threshold settings with 50% of misbehaving nodes reveal the facts that with low trust threshold (i.e., from 0.1 to 0.4), the delivery ratio decreases with an increase in delivery latency and cost. But with an increase in the threshold value (i.e., for 0.5 and 0.6), the delivery ratio of MATEM exhibits an increasing trend with a decline in delivery latency and cost. Further, an increase in the threshold beyond 0.7 results in a low message delivery ratio and high delivery latency. However, the delivery cost remains almost as steady as with the case of threshold value of 0.5. Therefore, it can be concluded that the MATEM framework gets its best achievable performance with 0.5 trust threshold setting and this enables the framework to effectively work together for preventing the influence of dishonest recommendations as well as avoidance of misbehaving nodes in a dynamically changing hostile DTN scenario.

Impact of number of misbehaving nodes

In this set of simulations, the impact of the number of misbehaving nodes on the performance of Epidemic, First Contact, T-PROPHET, Trust-Threshold based routing, TBIR, MATEM-ED, and MATEM-FC are investigated. The percentage of misbehaving nodes are varied proportionately from each of the six different groups of DTN nodes.

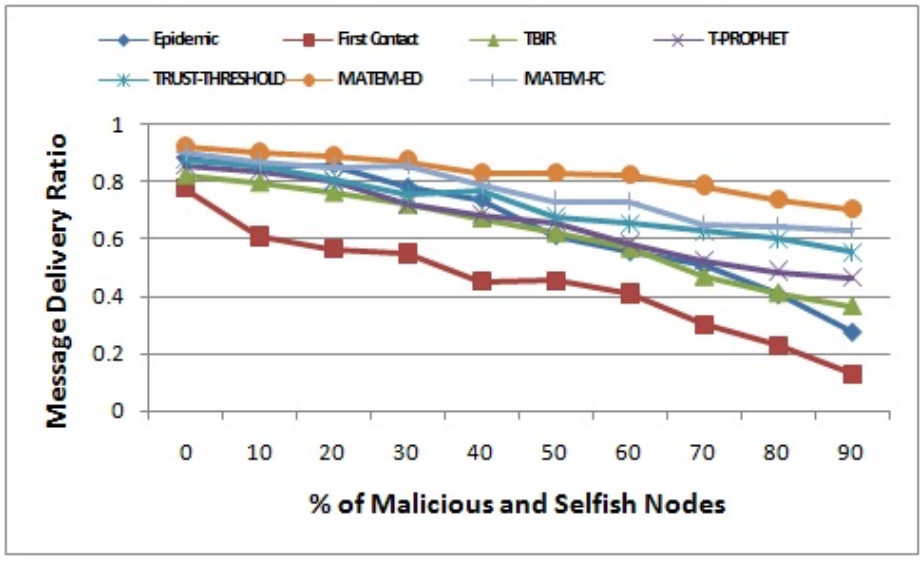


Figure 5.20: Message Delivery Ratio Vs. Percentage of Misbehaving Nodes

Figure 5.20 depicts the message delivery ratio as a function of the percentage of misbehaving nodes for Epidemic, First Contact, T-PROPHET, Trust-Threshold, TBIR and MATEM based routings (i.e., MATEM-ED, MATEM-FC) in the underlying DTN environment. It is calculated as the ratio between the number of messages successfully delivered to the number of messages created. In the simulation study, a decreasing trend in delivery ratio for all protocols has been observed. This is due to the fact that, with increased number of misbehaving nodes, the chances that a good node encounters a bad node for message forwarding also increases, which eventually drops the message or may not forward it for onward transmission to the destination. It is noticeable that with less number of misbehaving nodes (i.e, with 20%), the message delivery probability of Epidemic routing does not degrade significantly and shows some form of resiliency. This is due to the high density (126 nodes) that creates a closer association and availability of nodes in the network. However, with further increase in misbehaving nodes, their is a significant degradation in message delivery rate of Epidemic protocol. The delivery ratio of First Contact routing shows a steep decline since a single copy is forwarded in the network. The reasons behind the low delivery ratio of T-PROPHET with increasing number of misbehaving nodes are the lack of collective

evidences about nodes' malicious behaviors as well as non-consideration of nodes' selfish nature in trust computation process. These cause inclusion of misbehaving nodes in the routing path. The low performance of Trust-Threshold based routing is the aggregation of social trust with QoS trust that leads the protocol to select a node having high social trust value but low in QoS trust and vice-versa. These points increase the chances of message droppings and result in a low message delivery ratio. Further, the TBIR protocol shows a low message delivery ratio with increasing number of misbehaving nodes. This is due to the non-consideration of nodes' malicious and selfish nature in forwarder selection. But in comparison to these trust based routing protocols, the MATEM based routing protocols have shown better results in terms of message delivery ratio in a hostile DTN environment. This is due to the consideration of both malicious and selfish node behaviors in trust computation and thus enabling nodes to select a secure forwarder in the routing path. The MATEM based protocols outperform all these non-trust and trust based protocols under hostile DTN scenario and their performance come closer to the maximum achievable performance obtainable for Epidemic protocol under normal conditions. This becomes possible since the MATEM-based protocols are able to avoid misbehaving nodes and can select trustworthy nodes for message forwarding. The drop in delivery ratio for MATEM based routing is an effect of buffer overflow and message TTL expiration time. The cause behind this is that, with increasing number of misbehaving nodes in DTNs, the chances of encountering a good node gradually decreases, which forces a good node to retain bundles in it's buffer for an extra amount of time, causing bundle drops.

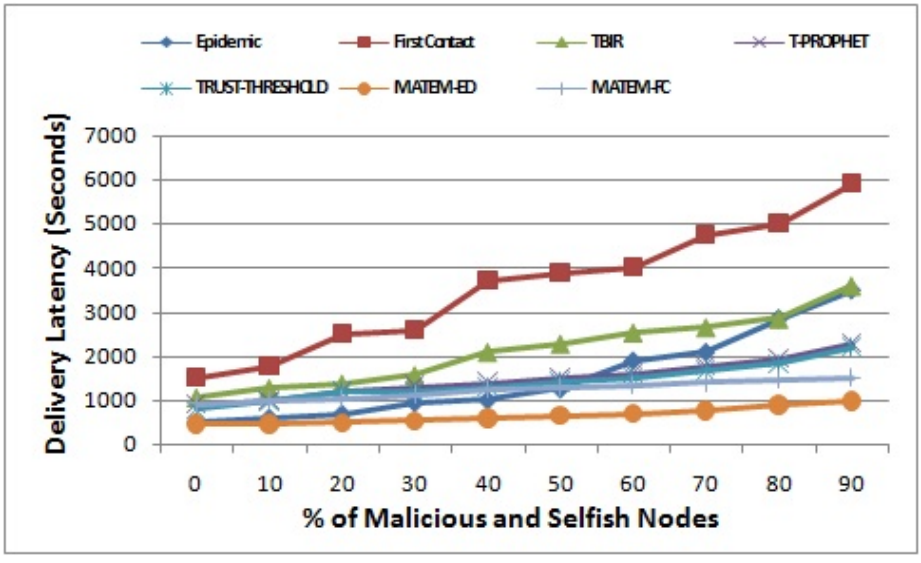


Figure 5.21: Message Delivery Latency Vs. Percentage of Misbehaving Nodes

Figure 5.21 exhibits the average latency for delivering a message with the variation of misbehaving nodes in the network. The average latency is defined as the average message transmission delay from creation to delivery. It has been observed that with increasing number of misbehaving nodes the message delivery latency for Epidemic, First Contact, T-PROPHET, Trust-Threshold based, and TBIR routing protocols increase sharply. This is due to the presence of either maliciousness or selfishness in node's behavior that cause more message copies either to get dropped or may not be forwarded for onward transmission to the destination. Further, messages in each destination have to wait for a longer period of time until one message copy is able to successfully come through and get delivered. It is noticeable that the average latency of MATEM-ED and MATEM-FC are significantly less than that of trust-based and non trust-based protocols under consideration. This is due to the consideration of "Connectivity" and "AMFD" trust components of the encountered node for meeting the destination as the criteria for selecting a next-hop message carrier. Moreover, the incorporation of "Risk" and "Cooperativeness" trust components in MATEM make it possible to avoid the selfish nodes and select a node having good social ties with the destination as a next hop message carrier. In fact, performance of MATEM-ED and MATEM-FC show resiliency in delivery latency with increasing number of misbehaving nodes. The performance of MATEM-ED shows better results as compared to MATEM-FC for maintaining multiple number of message copies in the network.

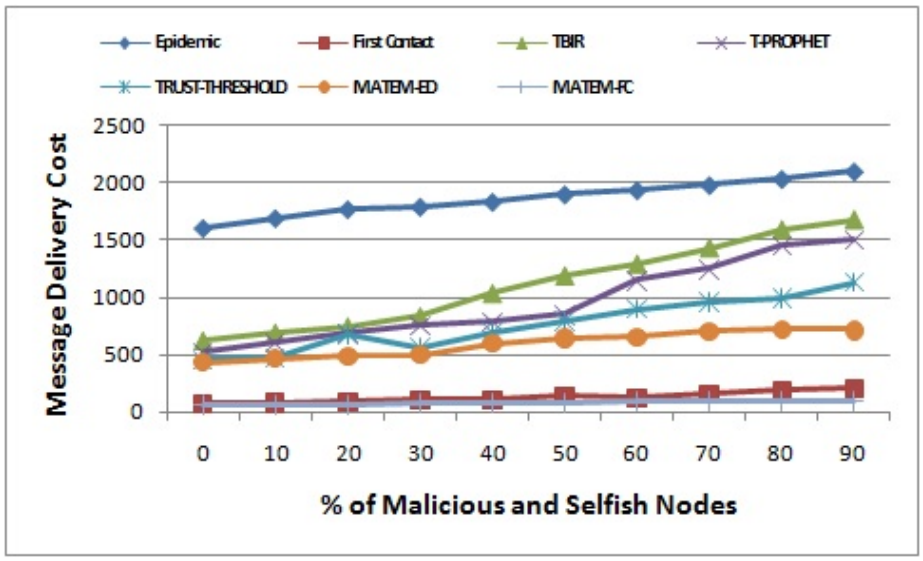


Figure 5.22: Message Delivery Cost Vs. Percentage of Misbehaving Nodes

Figure 5.22 depicts the delivery cost for all the protocols under consideration. In DTN based applications, delivery cost is measured by the number of replicas created for each

message's successful transmission to reach the destination. It has been observed that MATEM based protocols outperform trust-based and non trust-based protocols in terms of message delivery cost with increasing number of misbehaving nodes. It is justifiable by the fact that the carrier selection in these protocols is guided by multiple trust criteria that include "Connectivity", "Cooperativeness", and "AMFD" among others. Hence, the messages in MATEM-ED and MATEM-FC will avoid blind flooding and forwarding, and traverse less hops resulting in fewer relays to successfully reach the destination. The requirement of reduced delivery cost is essential to conserve nodes' scarce resources– battery and buffer. The delivery cost of MATEM-ED is more than MATEM-FC because of its multiple replication of bundles between the trusted forwarders.

Impact of nodes' buffer size

Generally, DTN nodes are considered to have much larger buffers than any conventional wireless network nodes. Even then, a node in practice cannot have infinite buffer size and thus, the consideration of varying buffer sizes become significant in measuring the effectiveness and practicability of the algorithms. In this set of simulation study, the impact of the node's buffer size on MATEM's performance is investigated. Here the node's buffer size is varied in between the range [10M - 100M] and the other parameters remain same as detailed in Table 5.3 and Table 5.4. The percentage of misbehaving nodes present in the network is kept at 50% comprising of nodes from each of the six different groups. Figures 5.23, 5.24, and 5.25 report the effect of varying buffer size for different protocols under consideration on delivery ratio, delivery latency and message's overhead ratio, respectively.

The Epidemic protocol and replication-based protocols are popular for their better performance in the presence of sufficient buffer size. From the simulation study, it has been observed that the Epidemic protocol, T-PROPHET, Trust-Threshold based, and TBIR are able to perform better with larger buffer sizes. The message dropping rate due to insufficient buffer is low in this case. But in a hostile DTN scenario, where forwarding depends on a node's own behavioral status, the performance of these flooding-based protocols (i.e., Epidemic, T-PROPHET, Trust-Threshold based, and TBIR) degrade with increasing number of misbehaving nodes. This is either due to the intentional buffering of messages allowing nodes' selfish behavior or attraction of messages by malicious nodes for launching more sophisticated attacks. Moreover, with small buffers, Epidemic and other trust-based protocols show their evident limitations due to the consideration of replication mechanisms.

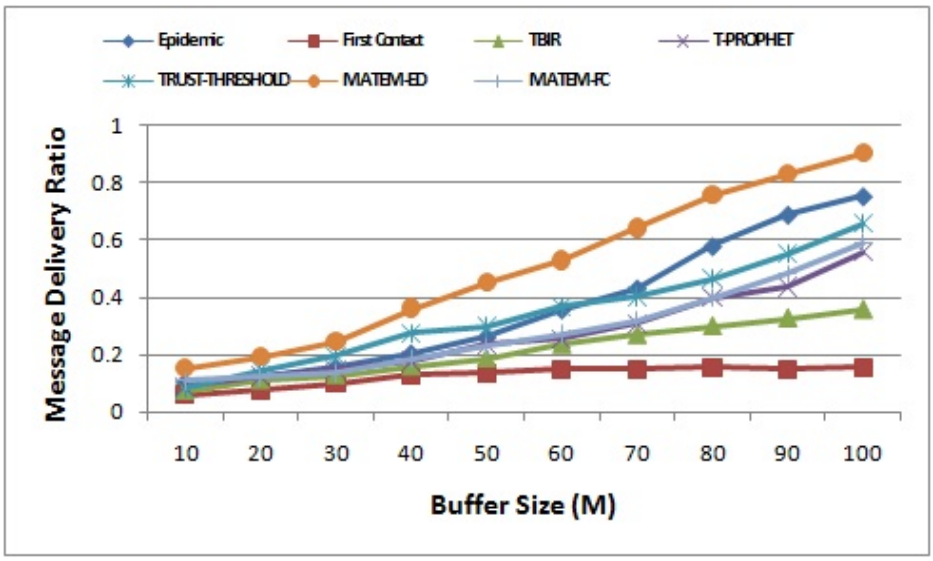


Figure 5.23: Message Delivery Ratio Vs. Buffer Size

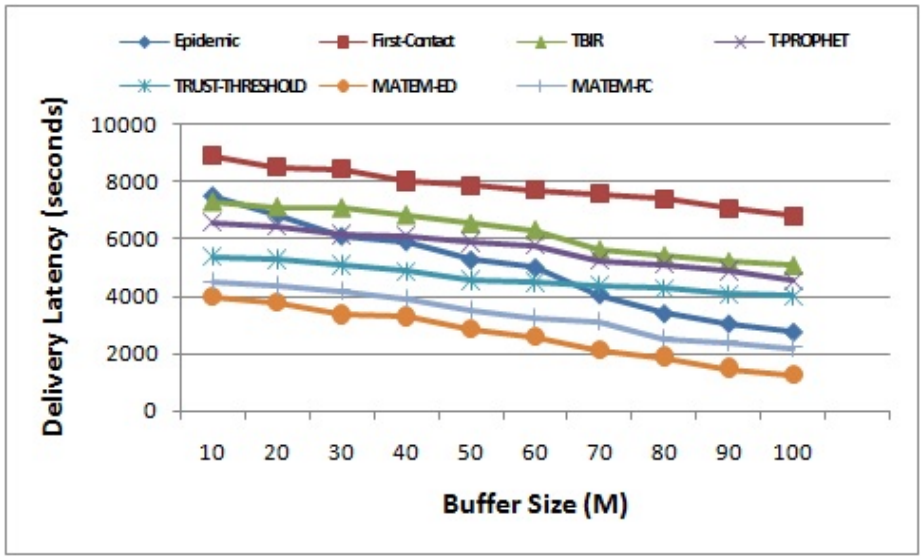


Figure 5.24: Message Delivery Latency Vs. Buffer Size

Interestingly, MATEM-ED shows a higher delivery ratio than Epidemic and other trust-based protocols for a buffer size equal to or smaller than 50 in a hostile DTN environment. It is justiciable since MATEM-ED restricts its replication mechanism based on trust and consideration of "AMFD" trust criteria reduces the average buffer occupancy time for each message in MATEM based protocols. Again, being a single copy routing, First contact does not show any negative impact on its delivery ratio with small buffer sizes. But, with misbehaving nodes, its performance degrades. Increasing buffer size has no significant impact on message delivery ratio since the chances of meeting a honest node is almost 50 percent always.

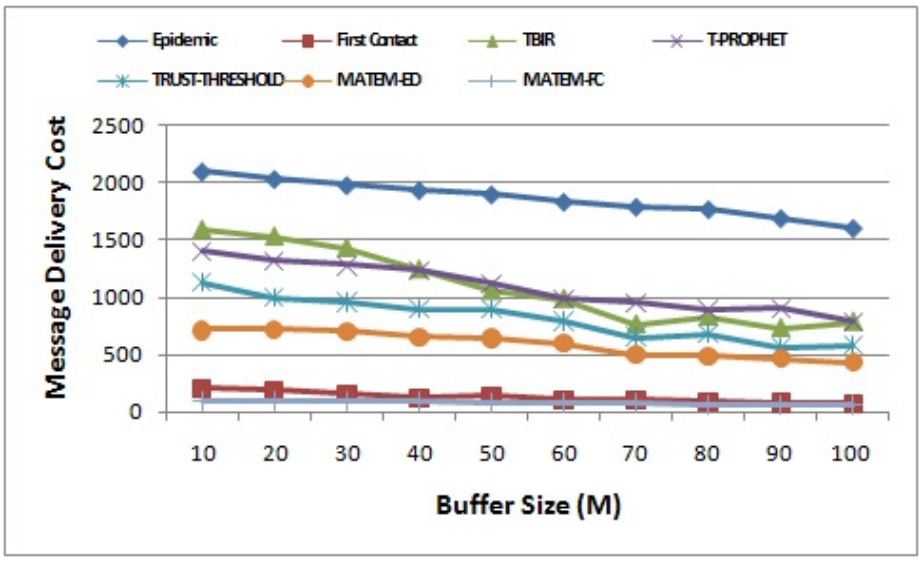


Figure 5.25: Message Delivery Cost Vs. Buffer Size

The performance of MATEM-ED and MATEM-FC have shown satisfactory results in delivery ratio with small buffer size. This is achievable because of MATEM's ability to differentiate between honest and misbehaving nodes for message forwarding in a hostile environment. It is noticeable that, as the buffer size increases the delivery ratio of MATEM-ED and MATEM-FC also increase along with increase in number of replications, henceforth cost increases too. However, from Figure 5.23 and Figure 5.25, it has been observed that MATEM-based protocols perform satisfactory in all conditions, giving better delivery ratio, and delivery latency than Epidemic, First contact, T-PROPHET, Trust-Threshold based, and TBIR. Further, MATEM also produces much fewer replications, which in turn reduces message delivery cost.

5.6 Evaluation of MATEM in a Real Testbed Scenario

This section validates MATEM's adaptability in a real people-centric social networking scenario. To validate MATEM with a real application scenario, we have developed an opportunistic Mobile Social Network (MSN) for mobile peer-to-peer file transfer. The mobile peer-to-peer file transfer runs as an Android application. In the application, every user has a set of contents (songs, videos) and an index of the available contents. Whenever two users come in contact of each other the index file gets synchronized. Based on the index file, an user may request for a song or video which is not in his or her mobile. The request is in the form (User_ID, Content_ID) where User_ID is the identity who has the content identified by

Content_ID. First, the search query is broadcast in the network, and if the user is available, the content gets downloaded via the underlying DTN environment. In the testbed application scenario the search query is PKI encrypted so as to avoid Byzantine attackers in the network. Thus, to facilitate the secure transfer of information within the MSN group, the MATEM framework leverages the conventional Public-Key Infrastructure (PKI) techniques to create a one-time PKI requirement that occurs during initial download and user signup for the application.

For downloading the content, we implement different forwarding protocols, like two different variants of MATEM protocol (MATEM-ED and MATEM-FC), the Epidemic routing protocol, the First Contact protocol, the TBIR protocol and the Community Aware Opportunistic Routing (CAOR) protocol. We evaluate the proposed mechanism in a campus scenario where 28 students have deployed the application in their smart-phones. To emulate malicious users, we installed a malicious code to a certain percentage (as shown in the individual graphs and discussed for individual cases) of the devices. The malicious users report false information about their device's properties, like they exaggerate the available buffer size (within 150% to 200% of the available buffer size), drops the packets from the buffer with a probability of 0.6 and falsify the encounter history (changes encounter history within 50% to 200% of the actual information). Under such hostile environment, each user of the application runs the MATEM framework to choose a trustworthy user for downloading or forwarding the set of available contents. It can be noted although the actual value of these maliciousness indicators impact the performance, here we are more interested in a comparative study among multiple protocols, rather than understanding the absolute performance that MATEM provides.

We evaluate the performance of the protocols in a free environment where the volunteers download contents whenever they wish. To give benefit to the volunteers so that they become interested to download the contents, we have distributed few popular and recent contents among different volunteers and announced the same among all the participants – so, the incentive here is to watch popular contents which otherwise require access to the outside Internet connectivity and data charges may apply. We distributed approximately 2000 such contents among the volunteers over the time, and the experiments are conducted for 2 months. However, we have given a maximum cap of downloading 2 contents per day, to have a regular control over the application usage. The application logs different performance data which are collected at the end of every week.

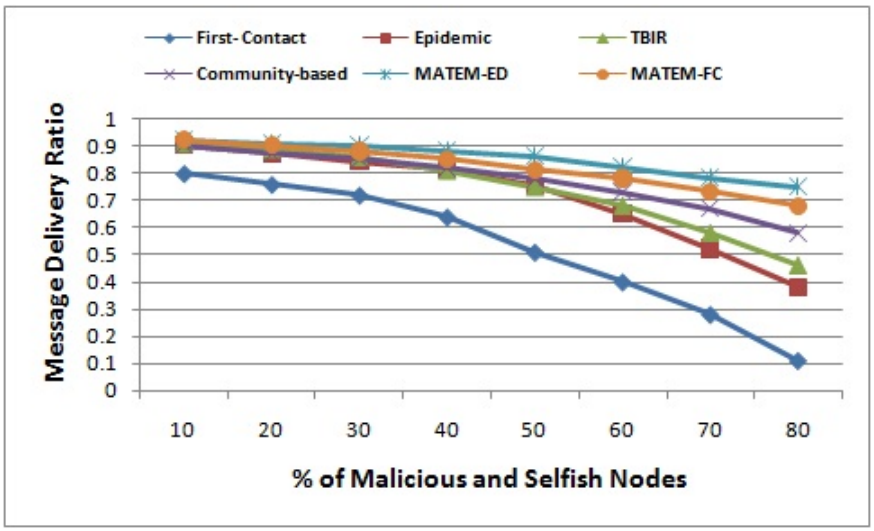


Figure 5.26: Message Delivery Ratio in Testbed Scenario

Figure 5.26 plots the message delivery ratio as obtained from different schemes. The figure indicates a similar trend as observed from the simulation – as we increase percentage of malicious and selfish users, the proposed scheme provides better message delivery ratio compared to others. Figure 5.27 indicates that the average delivery latency is less, as the proposed scheme reduces intermediate message drops.

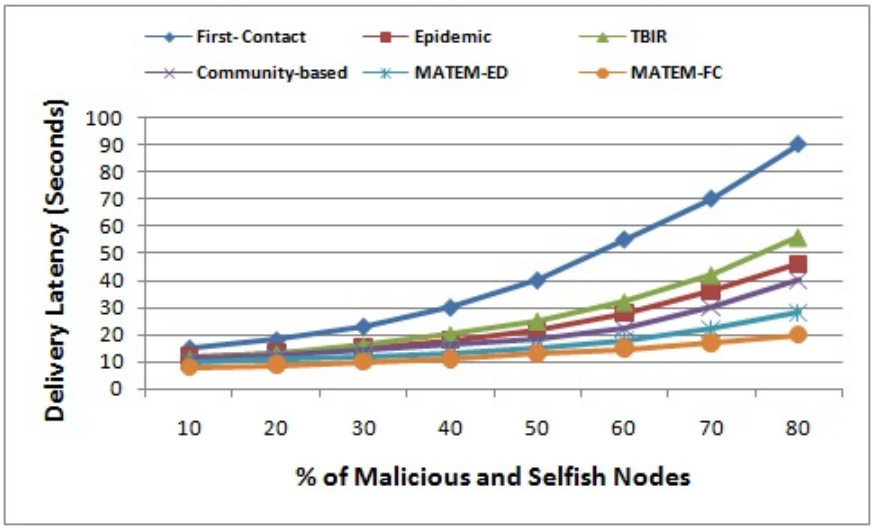


Figure 5.27: Average Message Delivery Latency in Testbed Scenario

On the other hand, Figure 5.28 shows the trade-off in proposed scheme – the average message overhead is slightly higher compared to others, except Epidemic where message overhead is very high. The reason for giving better performance in cost of higher message overhead is already explained during the analysis of the simulation results. In a nutshell,

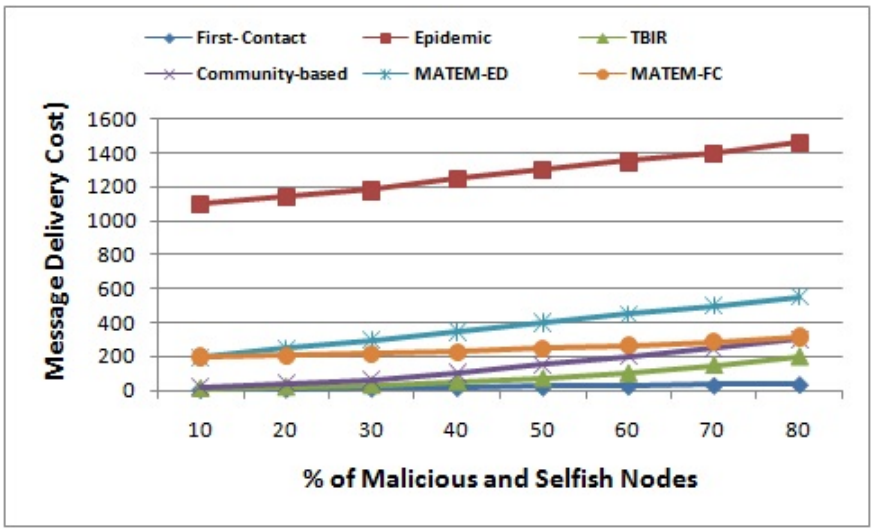


Figure 5.28: Message Delivery Cost in Testbed Scenario

the proposed mechanism significantly improves message delivery performance in a DTN based opportunistic MSN scenario, at a cost of slightly increased message overhead.

Table 5.5 summarizes the comparison of MATEM with other routing schemes viz., Epidemic, First Contact, TBIR, T-PROPHET, and Trust-Threshold (with 50% malicious nodes) depicted in the experimental results/graphs provided in this chapter of the thesis.

Finally, Table 5.6 summarizes the comparative analysis of MATEM with existing trust-based and social-aware routing schemes. It has been observed that MATEM performs better in terms of message delivery ratio, delivery latency, and delivery cost as compared to other similar protocols under consideration. However, a higher achievable delivery ratio is reported in CAOR [82] but with an increased delivery latency of 14 weeks which is impractical in a people-centric DTN scenario. Unlike other protocols that are validated only with simulation-based experiments, MATEM is evaluated with a real testbed implementation along with framework resiliency against different security attacks.

5.7 Conclusion

In this chapter, a novel unified trust based next-hop carrier selection framework called MATEM is proposed for DTN routing security. The salient feature of MATEM is that it not only integrates multi-criteria decision making technique with multiple trust measuring criteria having conflicting requirements and goals, but is also able to cope with uncertainty, long delay, social selfishness for choosing a next-hop carrier in a hostile DTN dynamically.

Table 5.5: Comparative Analysis of MATEM with Epidemic, First Contact, TBIR, T-PROPHET, and Trust-Threshold Routing Schemes

Works, Year Ref. No.	Methodology used	Performance evaluation		Validation	
		Routing metrics	Security metrics	Protocol considered	Experimental setup
Epidemic, 2000 [34]	Flooding based	Delivery ratio (62%) Delivery latency (168 minutes)	None	None	Simulation based
First Contact, 2004 [36]	Forwarding based	Delivery ratio (42%) Delivery latency (668 minutes)	None	Epidemic	Simulation based
T-PROPHET, 2013 [76]	Watchdog based, reputation assisted	Delivery ratio (68%) Delivery latency (160 minutes)	None	PROPHET	Simulation based
TBIR, 2016 [83]	Trust based, community-aware	Delivery ratio (60%) Delivery latency (382 minutes)	None	Epidemic, First Contact	Simulation based
Trust-Threshold 2014 [78]	Dynamic trust management	Delivery Ratio (63%) Delivery latency (168 minutes) Delivery Cost	None	PROPHET, Epidemic, Bayesian Trust	Simulation based
MATEM-ED	Trust based MCDM Technique	Delivery Ratio (83%) Delivery latency (80 minutes) Delivery Cost	Detection rate, False positive, False negative	Epidemic, First Contact TBIR T-PROPHET, Trust-Threshold, COAR	Simulation, Testbed based
MATEM-FC	Trust based MCDM Technique	Delivery Ratio (71%) Delivery latency (160 minutes) Delivery Cost	Detection rate, False positive, False negative	Epidemic, First Contact TBIR T-PROPHET, Trust-Threshold, COAR	Simulation, Testbed based

Table 5.6: Comparative Analysis of MATEM with existing Trust-based and Social-aware Routing Schemes

Works, Year Ref. No.	Methodology used	Performance evaluation		Validation	
		Routing metrics	Security metrics	Protocol considered	Experimental setup
T-PROPHET, 2013 [76]	Watchdog based, reputation assisted	Delivery ratio (65%) Delivery latency (158 minutes)	None	PROPHET	Simulation based
TBIR, 2016 [83]	Trust based, community-aware	Delivery ratio (20%)	None	Epidemic, First Contact	Simulation based
Trust-Threshold 2014 [78]	Dynamic trust management	Delivery Ratio (70%) Delivery latency (20 minutes) Delivery Cost (11 copies/message)	None	PROPHET, Epidemic, Bayesian Trust	Simulation based
CAOR, 2014 [82]	MSN based routing	Delivery Ratio (80%) Delivery latency (14 weeks)	None	Bubble rap SimBet	Simulation based
SAROS, 2017 [84]	Trust and reputation based (Interest Spaces assisted framework)	Correct Message Hit Rate (58%) Delivery latency Impact (17%)	None	Epidemic Social Trust	Simulation based
MATEM	Trust based MCDM Technique	Delivery Ratio (77%) Delivery latency (10 minutes) Delivery Cost (6 copies/message)	Detection rate, False positive, False negative	Epidemic, First Contact TBIR T-PROPHET, Trust-Threshold, COAR	Simulation, Testbed based

The MATEM has been evaluated and analyzed through an extensive set of simulations and a real testbed implementation. Results generated from simulations and the real testbed verified the usability and user acceptance of MATEM in DTN-based applications viz., Pocket Switched Networks (PSNs) or Mobile Social Networks (MSNs), for ensuring security, reliability and pervasiveness. The performance of the existing data forwarding protocols (viz., Epidemic, First Contact) designed for DTNs has been found to get enhanced with the incorporation of the MATEM framework and has shown more resilience to the increasing percentage of misbehaving nodes in a hostile DTN environment. Moreover, the performance results also inferred the QoS requirements of DTN routing amidst uncertainty. The applica-

bility of the MATEM for DTN routing security has advantages of less complex computational overheads, as learning of the entire network is based on trust. Excellency in these qualities of the MATEM makes it a worthy secure framework for DTN routing in presence of misbehaving nodes. The next chapter provides a summary of the thesis and scope for future work directions.

6

Conclusion and Future Directions

This thesis proposes a set of enhancements for forwarder/next-hop carrier selection protocols for a class of multi-hop networks. For this purpose, we have considered two application oriented multi-hop networking scenarios viz., Heterogeneous WMNs (HetMesh) and Delay Tolerant Networks (DTNs). The enhancements have been proposed with the primary objective of performance improvements of HetMesh and DTN routings, while considering the prevailing complexities and challenges of the underlying communication layouts in a congenial environment. Further, the reliability and security aspects of these newly enhanced protocols are examined for HetMesh and DTN in hostile environment. In this direction, the major contributions of this thesis is summarized as follows.

6.1 Summary of Contributions of the Thesis

The individual contribution of each chapter from Chapter 2 to Chapter 5 are as follows:

Contribution of Chapter 2: Heterogeneous Wireless Mesh Network (HetMesh) is a promising high throughput technology for multi-hop data forwarding by mobile clients and backbone routers in a dynamic environment. HetMesh supports Wifi-Direct facility and other separate access technologies in its mobile clients, which make the selection of a suitable next hop forwarder for data transmission challenging. In this chapter, we have proposed a new adaptive path determination technique called *Adaptive Path Selection Scheme* (Adapt-PSS) for high throughput HetMesh. In the proposed scheme, a novel resilient path metric

called “Multi-Attribute Adaptive Path Metric” (MAAPM) is defined by combining multiple path selection criteria to leverage the resource availability of clients for acting as potential forwarders. The proposed scheme can be augmented with any existing hybrid routing protocol in WMNs for its portability in HetMesh. The performances of Adapt-PSS have been evaluated through a testbed and extensive set of simulations. The analysis illustrates that the proposed path selection mechanism improves Constant Bit Rate (CBR) throughput of HetMesh. Further, other performance metrics are also improved. Moreover, the performance results also inferred the scalable nature of Adapt-PSS. Excellency in these qualities of Adapt-PSS makes it a worthy path selection scheme for public wireless access scenarios of high throughput HetMesh, supporting hundreds of mobile users.

Contribution of Chapter 3: DTNs have evolved as a new communication paradigm for ensuring reliability to a class of challenged networks which mostly operate under harsh networking conditions. Examples of such networks include terrestrial mobile networks, military ad hoc networks, exotic media networks, sensor networks, etc. In most of the terrestrial DTN applications, the mobile nodes/devices are carried and used by people and thereby making forwarding decision based on peoples' social behavioral perspectives. We have explored the social behavioral pattern in people's contacts in real mobility traces and have proposed *Seasonality Aware Social-based*" (SAS) forwarding, a novel seasonality aware adaptive forwarding technique in social DTNs, as the second contribution of this thesis. The work is based on the observation of existence of seasonal behavioral pattern in node contacts in real mobility traces. SAS invoked a weighted Katz based similarity measure and ego-betweenness centrality to evaluate an utility value of an encountered node. Based on this utility, it decides the competency of a candidate node for being selected as a next-hop message carrier in DTN routing. The proposed method has been evaluated against different routing metrics viz., *delivery ratio*, *delivery cost*, and *delivery latency* through extensive set of simulation study with real mobility trace data sets. The performances of SAS has been found to get enhanced compared to the existing baseline social based forwarding schemes, SimBet and BubbleRap available for DTNs.

Contribution of Chapter 4: HetMesh does not rely on any centralized administration and they are built by the connection of various fixed infrastructure mesh routers and mobile clients which are of ad hoc and dynamic nature. The mobile clients in HetMesh have the capacity to directly communicate to another client without intervening the mesh backbone

and can act as an intermediate forwarder. Such distributed nature of HetMesh increases the vulnerability of routing protocols to different kinds of attacks such as black hole, DoS, and spoofing attacks. Consequently, a communicating node has to be cautious when selecting a next-hop forwarder for routing packets in the network. In this work, we have proposed a trust based forwarder selection framework called *Trust Based Multiple Criteria Decision Making* (TB-MCDM) technique for routing security in HetMesh. The salient feature of TB-MCDM is that it integrates multiple criteria decision making technique with multiple trust measuring criteria for assigning trust values of each node in HetMesh. The TB-MCDM has been evaluated and analyzed through extensive set of simulation study. The performance of the existing data forwarding protocol viz., Adapt-PSS designed for HetMesh has been found to get enhanced with the incorporation of the TB-MCDM framework and has shown more resilience to the increasing percentage of misbehaving nodes in a hostile HetMesh scenario. The performance of TB-MCDM is evaluated through extensive simulations for its resiliency against different kind of attacks and a comparative analysis is carried out with TM-OLSR under various networking scenarios with varying proportions of misbehaving nodes, traffic load, and node speed. The performance analysis has proved TB-MCDM's efficiency in classifying each node in the network as trustworthy and untrustworthy, and thus avoiding malicious and misbehaving nodes in the routing path.

Contribution of Chapter 5: In this work, a novel unified trust based next-hop carrier selection framework called MATEM is proposed for DTN routing security. In MATEM, a node's malicious and social selfish nature are considered together to avoid misbehaving nodes from being selected as a next-hop message carrier in DTN routing. For this, the trust criteria "Risk", and "Cooperativeness" have been proposed. To deal with inherent risk in DTN's message propagation scheme, a measure of "Uncertainty" is proposed. Further, to ensure QoS requirement of MATEM, an estimation of delay in terms of "Average Message Forwarding Delay" (AMFD) of each potential carrier in the network is considered. The effectiveness and robustness of MATEM are evaluated through extensive simulations and a real testbed implementation. Simulation results demonstrate MATEM's robustness against several security attacks that attempt to disrupt the functionality of the proposed framework. The performance of the existing data forwarding protocols (viz., Epidemic, First Contact) designed for DTNs has been found to get enhanced with the incorporation of the MATEM framework and has shown more resilience to the increasing percentage of misbehaving nodes in a hostile DTN environment. Moreover, the performance results also inferred the

QoS requirements of DTN routing amidst uncertainty. Results generated from simulations and the real testbed verified the usability and user acceptance of MATEM in DTN-based applications viz., Pocket Switched Networks (PSNs) or Mobile Social Networks (MSNs), for ensuring security, reliability and pervasiveness.

6.2 Scope of Future Work

The performance of the forwarder/next-hop carrier selection protocols in congenial as well as in hostile environments of HetMesh and DTNs can be further enhanced with the amendments of more advanced features, which can be kept as the future directions in this research area. The following are possible future research directions.

The performance of the multi-hop heterogeneous WMNs can be further improved by efficient Transmission Control Protocol (TCP) design. For this purpose lower layer information (such as link characteristics, channel dynamics etc.) available at the end devices may be considered for assigning suitable values to the TCP parameters. Conversely, the end-to-end information available at TCP can also be used by the lower layers for mesh path selection purposes. This way, a cross layer design may be incorporated to improve TCP end-to-end utilization.

The performance of the proposed *Seasonality Aware Social-based* forwarding in DTNs can further be improved by incorporating incentive mechanisms to stimulate individual node cooperation in the network. In addition, a more accurate prediction in the forwarder selection process in DTNs can be achieved by combining multiple metrics such as, social-based metrics with traditional opportunity-based metrics or with other factors such as channel capacity, energy, buffer etc., which may provide better opportunities to improve the overall routing performance. In our future research, we shall put insight on these issues.

In our proposed trust-based frameworks for HetMesh and DTNs, trust thresholds are set with static values and different trust measuring criteria are assigned equal weights. In our future work, we like to explore the possibility of dynamic trust threshold determination and identification of optimal settings for weights assigned to multiple trust measuring criteria under various network and environmental conditions. Further, network dynamics can hinder the trust propagation and recommendation collection process and thus have an impact on the performance of the security frameworks. In future we aim to address the impact of network dynamics on trust evaluation system. These optimal settings can maximize the

overall trust of the system under consideration for successful mission executions. Additionally, in future, we aim to investigate the tradeoff between resource consumption (e.g., time or energy) and decision making accuracy based on trust in our proposed frameworks. This is required, since gathering information from sparsely connected nodes in HetMesh and DTNs consume more resources but facilitates in improved decision making.

In future, we also aim to extend and implement the trust based framework for ensuring routing security in the domain of Internet of Things (IoT) and Vehicular Ad hoc Network (VANET) based applications. IoT uses wireless communication as a major means of transmitting information making them vulnerable to the attackers. Further, the distributed and wireless nature of VANETs coupled with their unique characteristics such as highly dynamic topologies, heterogeneous vehicular traffic, frequently disconnected networks, narrow bandwidths, short transmission range, omni-directional broadcast etc., make them vulnerable to various type of security threats. The attacker can exploit the broadcast nature of IoT and VANETs to carry out various types of attacks like eavesdropping, jamming, DoS etc. The intermittent network connectivity, narrow bandwidth wireless radio spectrum and absence of centralized coordinating entities for monitoring node behaviors in these networks make the task of formulating an effective security measure difficult and challenging. A trust based framework can be used to ensure protection from malicious users under such environment.

Bibliography

[1] E. Charles, C. Perkins, M. Elizabeth, and Royer. Ad hoc On-Demand Distance Vector Routing. In *Proc. of Workshop on Mobile Computing Systems and Applications, 90-100*, 1999.

[2] C. Adjih, T. Clausen, P. Jacquet, A. Laouiti, P. Minet, P. Muhlethaler, A. Qayyum, and L. Viennot. Optimized Link State Routing Protocol (OLSR). *IETF Experimental RFC 3626*, October 2003.

[3] D. Johnson, Y. Hu, and D. Maltz. The Dynamic Source Routing Protocol (DSR) for Mobile Ad hoc Networks for IPv4. Technical report, 2007.

[4] M. Lewis, F. Templin, B. Bellur, and R. Ogier. Topology Broadcast based on Reverse-path Forwarding. *IEEE MANET Inernet Draft*, 2002.

[5] M. Conti and S. Giordano. Mobile Ad hoc Networking: milestones, challenges, and new research directions. *IEEE Communications Magazine*, 52(1):85–96, 2014.

[6] I. F. Akyildiz, X. Wang, and W. Wang. Wireless Mesh Networks: A Survey. *Computer Networks*, 47(4):445–487, 2005.

[7] K. Fall, K. L. Scott, S. C. Burleigh, L. Torgerson, A. J Hooke, S. W. Howard, R. C. Durst, and V. Cerf. Delay-Tolerant Networking Architecture. *RFC 4838, 1-35*, 2007.

[8] H. Hartenstein, K. P. Laberteaux, et al. A Tutorial Survey on Vehicular Ad hoc Networks. *IEEE Communications magazine*, 46(6):164, 2008.

[9] E. Alotaibi and B. Mukherjee. A Survey on Routing Algorithms for Wireless Ad hoc and Mesh Networks. *Computer Networks*, 56(2):940–965, 2012.

[10] A. B. Paul and S. Nandi. Modified Optimized Link State Routing (M-OLSR) for Wireless Mesh Networks. In *Proc. of Conference on Information Technology, 147-152*, 2008.

[11] A. B. Paul, S. Konwar, U. Gogoi, S. Nandi, and S. Biswas. E-AODV for Wireless Mesh Networks and its Performance Evaluation. In *Proc. of Conference on Broadband and Wireless Computing, Communication and Applications, 26-33*, 2011.

[12] J. Jun and M. L. Sichitiu. MRP: Wireless Mesh Networks Routing Protocol. *Computer Communications*, 31:1413–1435, 2008.

[13] S. Roy and J.J.Garcia-Luna-Aceves. Node-centric Hybrid Routing for Ad-hoc Wireless Extensions of the Internet. In *Proc. of GLOBECOM, 183-187*, 2002.

[14] S. Roy and J.J.Garcia-Luna-Aceves. Using Minimal Source Trees for On-demand Routing in Ad hoc Networks. In *Proc. of INFOCOM, 1172-1181*, 2001.

[15] MeshNetworks website. http://www.meshnetworks.com/.

[16] R. Ogier, F. Templin, and M. Lewis. Topology dissemination Based on Reverse Path Forwarding (TBRPF). *RFC 3484*, 2004.

[17] Firetide website. http://www.firetide.com/.

[18] Mesh Dynamics website. http://www.meshdynamics.com/.

[19] M. Bahr. Proposed Routing for IEEE 802.11s WLAN Mesh Networks. In *Proc. of Workshop on Wireless Internet, 5*, 2006.

[20] A.B. Paul, S. Konwar, S. Biswas, and S. Nandi. M-HRP for Wireless Mesh Networks and its Performance Evaluation. In *Proc. of Conference on Communication Systems and Networks, 1-4*, 2014.

[21] A. Damle, D. Rajan, and S. M. Faccin. Hybrid Routing with Periodic Updates (HRPU) in Wireless Mesh Networks. In *Proc. of Conference on Wireless Communications and Networking, 318-324*, 2006.

[22] R. Hou, K. S. Lui, F. Baker, and J. Li. Hop-by-hop Routing in Wireless Mesh Networks with Bandwidth Guarantees. *IEEE Transactions on Mobile Computing*, 11(2):264–277, 2012.

[23] D. Passos and C. VN. Albuquerque. A Joint Approach to Routing Metrics and Rate Adaptation in Wireless Mesh Networks. *IEEE/ACM Transactions on Networking*, 20(4):999–1009, 2012.

[24] A. Boukerche and A. Darehshoorzadeh. Opportunistic Routing in Wireless Networks: Models, Algorithms, and Classifications. *ACM Computing Surveys*, 47(2):22, 2014.

[25] S. Chakraborty and S. Nandi. Selective Greedy Routing: exploring the path diversity in backbone mesh networks. *Wireless Networks*, 20(7):1995–2017, 2014.

[26] T. Javidi and E. V. Buhler. Opportunistic Routing in Wireless Networks. *Foundations and Trends® in Networking*, 11(1-2):1–137, 2016.

[27] D. Das and A. Kumar. Algorithm for Multicast Opportunistic Routing in Wireless Mesh Networks. In *Proc. of Conference on Software and Computer Applications, 250-255*, 2017.

[28] M. J. Khabbaz, C. M. Assi, and W. F. Fawaz. Disruption-Tolerant Networking: A Comprehensive Survey on Recent Developments and Persisting Challenges. *IEEE Communications Surveys & Tutorials*, 14(2):607–640, 2012.

[29] T. Spyropoulos, R. N. Rais, T. Turletti, K. Obraczka, and A. Vasilakos. Routing for Disruption Tolerant Networks: Taxonomy and Design. *Wireless Networks*, 16(8):2349–2370, 2010.

[30] J. Broch, D. A. Maltz, D. B. Johnson, Y. C. Hu, and J. Jetcheva. A Performance Comparison of Multi-hop Wireless Ad hoc Network Routing Protocols. In *Proc. of ACM/IEEE Conference on Mobile Computing and Networking, 85-97*, 1998.

[31] W. Zhao, M. Ammar, and E. Zegura. A Message Ferrying Approach for Data Delivery in Sparse Mobile Ad hoc Networks. In *Proc. of ACM Symposium on Mobile Ad hoc Networking and Computing, 187-198*, 2004.

[32] R. C. Shah, S. Roy, S. Jain, and W. Brunette. Data Mules: Modeling and Analysis of a Three-tier Architecture for Sparse Sensor Networks. *Ad Hoc Networks*, 1(2):215–233, 2003.

[33] E. Jones and P. Ward. Routing Strategies for Delay Tolerant Networks. *ACM Computer Communication Review, 1-10*, 2006.

[34] Amin Vahdat, David Becker, et al. Epidemic routing for partially connected ad hoc networks. Technical report, Technical Report CS-200006, Duke University, 2000.

[35] A. Lindgren, A. Doria, and O. Schelén. Probabilistic Routing in Intermittently Connected Networks. *ACM SIGMOBILE Mobile Computing and Communications Review*, 7(3):19–20, 2003.

[36] S. Jain, K. Fall, and R. Patra. Routing in a Delay Tolerant Network. *SIGCOMM Comput. Commun. Rev.*, 34(4):145–158, 2004.

[37] R-I. Ciobanu, DG. Reina, C. Dobre, and P. Johnson SL. Toral. JDER: A History-based Forwarding Scheme for Delay Tolerant Networks using Jaccard Distance and Encountered Ration. *Journal of Network and Computer Applications*, 40:279–291, 2014.

[38] Q. Ayub, S. Rashid, M. Soperi, M. Zahid, and A.H. Abdullah. Contact Quality based Forwarding Strategy for Delay Tolerant Network. *Journal of Network and Computer Applications*, 39:302–309, 2014.

[39] K. Shin, K. Kim, and S. Kim. Traffic Management Strategy for Delay Tolerant Networks. *Journal of Network and Computer Applications*, 35(6):1762–1770, 2012.

[40] Q. Yuan, I. Cardei, and J. Wu. An Efficient Prediction-based Routing in Disruption-tolerant Networks. *IEEE Transactions on Parallel and Distributed Systems*, 23(1):19–31, 2012.

[41] E. Bulut, Z. Wang, and B. K. Szymanski. Cost-effective Multiperiod Spraying for Routing in Delay-tolerant Networks. *IEEE/ACM Transactions on Networking*, 18(5):1530–1543, 2010.

[42] J. Niu, D. Wang, and M. Atiquzzaman. Copy Limited Flooding over Opportunistic Networks. *Journal of Network and Computer Applications*, 58:94–107, 2015.

[43] Y. Zhu, B. Xu, X. Shi, and Y. Wang. A Survey of Social-based Routing in Delay Tolerant Networks: Positive and Negative Social Effects. *IEEE Communications Surveys & Tutorials*, 15(1):387–401, 2013.

[44] D. Liben-Nowell and J. Kleinberg. The Link-Prediction Problem for Social Networks. In *Proc. of Conference on Information and Knowledge Management, 556-559*, 2003.

[45] L. C. Freeman. Centrality in Social Networks Conceptual Clarification. *Social Networks*, 1(3):215–239, 1978.

[46] S. Fortunato. Community Detection in Graphs. *Physics Reports*, 486(3):75–174, 2010.

[47] P. Hui and J. Crowcroft. How Small Labels Create Big Improvements. In *Proc. of Conference on Pervasive Computing and Communications, 65-70*, 2007.

[48] J. Wu and Y. Wang. Social Feature-based Multi-path Routing in Delay Tolerant Networks. In *Proc. of IEEE INFOCOM,1368-1376*, 2012.

[49] A. Mei, G. Morabito, P. Santi, and J. Stefa. Social-aware Stateless Forwarding in Pocket Switched Networks. In *Proc. of IEEE INFOCOM, 251-255*, 2011.

[50] E. M. Daly and M. Haahr. Social Network Analysis for Routing in Disconnected Delay-tolerant Manets. In *Proc. of ACM Symposium on Mobile Ad Hoc Networking and Computing, 32-40*, 2007.

[51] P. Hui, J. Crowcroft, and E. Yoneki. Bubble Rap: Social-based Forwarding in Delay-tolerant Networks. *IEEE Transactions on Mobile Computing*, 10(11):1576–1589, 2011.

[52] M.S. Granovetter. The Strength of Weak Ties. *American Journal of Sociology*, 78(6):1360–1380, 1973.

[53] F. Li and J. Wu. LocalCom: A Community-based Epidemic Forwarding Scheme in Disruption-tolerant Networks. In *Proc. of Conference on Sensor, Mesh and Ad hoc Communications and Networks, 1-9*, 2009.

[54] T. Zhou, R. Roy Choudhury, and K. Chakrabarty. Diverse Routing: Exploiting Social Behavior for Routing in Delay-tolerant Networks. In *Proc. of Conference on Computational Science and Engineering, 1115-1122*, 2009.

[55] K. Wei, S. Guo, D. Zeng, K. Xu, and K. Li. Exploiting Small World Properties for Message Forwarding in Delay Tolerant Networks. *IEEE Transactions on Computers*, 64(10):2809–2818, 2015.

[56] E. Bulut and B. K. Szymanski. Exploiting Friendship Relations for Efficient Routing in Mobile Social Networks. *IEEE Transactions on Parallel and Distributed Systems*, 23(12):2254–2265, 2012.

[57] Q. Li and G. Cao. Mitigating Routing Misbehavior in Disruption Tolerant Networks. *IEEE Transactions on Information Forensics and Security*, 7(2):664–675, 2012.

[58] N. Magaia, P. R. Pereira, and M. P. Correia. Selfish and Malicious Behavior in Delay-Tolerant Networks. In *Proc. of Future Network and Mobile Summit, 1-10*, 2013.

[59] L. Santhanam, B. Xie, and D. P. Agrawal. Selfishness in mesh networks: wired multihop MANETs. *IEEE Wireless Communications*, 15(4):16–21, 2008.

[60] L. Buttyán and J. P. Hubaux. Enforcing service availability in mobile ad-hoc WANs. In *Proc. of the MobiHOC*, pages 87–96, 2000.

[61] K. Govindan and P. Mohapatra. Trust Computations and Trust Dynamics in Mobile Ad Hoc Networks: A Survey. *IEEE Communications Surveys & Tutorials*, 14(2):279–298, 2012.

[62] K. Cook. *Trust in society*. Russell Sage Foundation, 2001.

[63] C. Castelfranchi and R. Falcone. Trust is much more than Subjective Probability: Mental Components and Sources of Trust. In *Proc. of Conference on System Sciences, 1-10*, 2000.

[64] Y. Hu, A. Perrig, and D.B. Johnson. Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks. In *Proc. of MOBICOM*, 2002.

[65] M. G. Zapata and N. Asokan. SAODV : Securing Ad-hoc Routing Protocols. In *Proc. of ACM Workshop on Wireless Security, 1-10*, 2002.

[66] M. Jarrett and P. Ward. Trusted Computing for Protecting Ad-hoc Routing. In *Proc. of Conference on Communication Networks and Services Research, 1-8*, 2006.

[67] T. George and J. S. Baras. On Trust Models and Trust Evaluation Metrics for Ad Hoc Networks. *IEEE Journal on Selected Areas in Communications*, 24(2):318–328, 2006.

[68] X. Wang, L. Liu, and J. Su. RLM: A General Model for Trust Representation and Aggregation. *IEEE Transactions on Services Computing*, 5(1):131–143, 2012.

[69] Y. L. Sun, W. Yu, Z. Han, and K.J. R. Liu. Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks. *IEEE Journal on Selected Areas in Communications*, 24(2):305–317, 2006.

[70] P. Michiardi and R. Molva. Core: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks. In *Proc. of Advanced Communications and Multimedia Security, 107-121*. 2002.

[71] S. Marti, T. J. Giuli, K. Lai, and M. Baker. Mitigating Routing Misbehavior in Mobile Ad Hoc Networks. In *Pro. of Conference on Mobile Computing and Networking, 255-265*, 2000.

[72] S. Konwar, A.B. Paul, S. Nandi, and S. Biswas. MCDM based Trust Model for Secure Routing in Wireless Mesh Networks. In *Proc. of World Congress on Information and Communication Technologies, 910-915*, 2011.

[73] Y-J Lai, T-Y Liu, and C-L Hwang. Topsis for MODM. *European Journal of Operational Research*, 76(3):486–500, 1994.

[74] M. Behzadian, S. K. Otaghsara, M. Yazdani, and J. Ignatius. A State-of the-art Survey of TOPSIS Applications. *Expert Systems with Applications*, 39(17):13051–13069, 2012.

[75] E. Ayday and F. Fekri. An Iterative Algorithm for Trust Management and Adversary Detection for Delay-tolerant Networks. *IEEE Transactions on Mobile Computing,*, 11(9):1514–1531, 2012.

[76] N. Li and S. K. Das. A Trust-based Framework for Data Forwarding in Opportunistic Networks. *Ad Hoc Networks*, 11(4):1497– 1509, 2013.

[77] H. Zhu, S. Du, Z. Gao, M. Dong, and Z. Cao. A Probabilistic Misbehavior Detection Scheme Toward Efficient Trust Establishment in Delay-tolerant Networks. *IEEE Transactions on Parallel and Distributed Systems*, 25(1):22–32, 2014.

[78] R. Chen, F. Bao, MJ. 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*, 25(5):1200–1210, 2014.

[79] Z. Xu, Y. Jin, W. Shu, X. Liu, and J. Luo. SReD: A Secure Reputation-based Dynamic Window Scheme for Disruption-tolerant Networks. In *Proc. of Conference on Military Communications, 1-7*, 2009.

[80] G. Dini and A. L. Duca. A Reputation-based Approach to Tolerate Misbehaving Carriers in Delay Tolerant Networks. In *Proc. of Symposium on Computers and Communications, 772-777*, 2010.

[81] B. Jedari and F. Xia. A Survey on Routing and Data Dissemination in Opportunistic Mobile Social Networks. *arXiv preprint arXiv:1311.0347*, 2013.

[82] M. Xiao, J. Wu, and L. Huang. Community-aware Opportunistic Routing in Mobile Scial Networks. *IEEE Transactions on Computers*, 63(7):1682–1695, 2014.

[83] A. V. Singh, V. Juyal, and R. Saggar. Trust based Intelligent Routing Algorithm for Delay Tolerant Network using Artificial Neural Network. *Wireless Networks, 1-10*, 2016.

[84] R-I. Ciobanu, R-C Marin, C. Dobre, and V. Cristea. Trust and Reputation Management for Opportunistic Dissemination. *Pervasive and Mobile Computing*, 36:44–56, 2017.

[85] C. Boldrini, M. Conti, F. Delmastro, and A. Passarella. Context and Social-aware Middleware for Opportunistic Networks. *Journal of Network and Computer Applications*, 33(5):525–541, 2010.

[86] L. Gao, M. Li, A. Bonti, W. Zhou, and S. Yu. M-Dimension: Multi-characteristics based routing protocol in human associated delay-tolerant networks with improved performance over one dimensional classic models. *Journal of network and computer applications*, 35(4):1285–1296, 2012.

[87] R-I. Ciobanu, C. Dobre, M. Dascălu, S. T. Matu, and V. Cristea. Sense: A Collaborative Selfish Node Detection and Incentive Mechanism for Opportunistic Networks. *Journal of Network and Computer Applications*, 41:240–249, 2014.

[88] P. Yuan, P. Liu, and S. Tang. RIM: Relative-importance based Data Forwarding in People-centric Networks. *Journal of Network and Computer Applications*, 62:100–111, 2016.

[89] M. L. Sichitiu. Wireless Mesh Networks: Oppurtunities and Challenges. In *Proc. of Wireless World Congress, 1-21*, 2005.

[90] R. Bruno, M. Conti, and W. Wang. Mesh Networks: Commodity Multihop Ad Hoc Networks. *IEEE Communications Magazine*, 43:123–131.

[91] A. Qayyum, L. Viennot, and A. Laouiti. Multipoint Relaying: An Efficient Technique for Flooding in Mobile Wireless Networks. Technical report, 2000.

[92] A. B. Paul, S. Konwar, U. Gogoi, A. Chakraborty, N. Yeshmin, and S. Nandi. Implementation and Performance Evaluation of AODV in Wireless Mesh Networks using NS-3. In *Proc. of Conference on Education Technology and Computer, 298-303*, 2010.

[93] A. Joshi and M. Bahr. HWMP specification. *IEEE P802*, 11:802–11, 2006.

[94] A. Pyattaev, O. Galinina, K. Johnsson, A. Surak, R. Florea, S. Andreev, and Y. Koucheryavy. Network-assisted D2D over WiFi Direct. In *Proc. of Conference on Smart Device to Smart Device Communication, 165-218*. 2014.

[95] R. C. J. Neto, R. Andrade, R. B. Braga, F. Theoleyre, and C. T. Oliveira. Performance issues with Routing in Multi-channel Multi-interface IEEE 802.11s Networks. In *Proc. of IFIP Wireless Days, 1-6*, 2014.

[96] T. Issariyakul and E. Hossain. *Introduction to Network Simulator NS2*. Springer, 2010.

[97] asuswrt-merlin. https://github.com/RMerl/asuswrt-merlin.

[98] open80211s. http://open80211s.org/open80211s/.

[99] P. R. Pereira, J. JPC. Rodrigues A. Casaca, V. NGJ. Soares, J. Triay, and C. C. Pastor. From Delay-tolerant Networks to Vehicular Delay-tolerant Networks. *IEEE Communications Surveys & Tutorials*, 14(4):1166–1182, 2012.

[100] P. Hui, A. Chaintreau, J. Scott, R. Gass, J. Crowcroft, and C. Diot. Pocket Switched Networks and Human Mobility in Conference Environments. In *Proc. of ACM SIGCOMM Workshop on Delay Tolerant Networking, 244-251*, 2005.

[101] N. Vastardis and K. Yang. Mobile Social Networks: Architectures, Social properties, and key Research Challenges. *IEEE Communications Surveys & Tutorials*, 15(3):1355–1371, 2013.

[102] M. Conti and S. Giordano. Mobile Ad hoc Networking: milestones, challenges, and new research directions. *IEEE Communications Magazine*, 52(1):85–96, 2014.

[103] L. C. Freeman. Centered Graphs and the Structure of Ego Networks. *Mathematical Social Sciences*, 3(3):291–304, 1982.

[104] P. Hui, E. Yoneki, S. Y. Chan, and J. Crowcroft. Distributed Community Detection in Delay Tolerant Networks. In *Proc. of ACM/IEEE Workshop on Mobility in the Evolving Internet Architecture, 1-8*, 2007.

[105] J. Scott and R. Gass and J. Crowcroft and P. Hui and C. Diot and A. Chaintreau. CRAWDAD dataset cambridge/haggle (v. 2006-09-15). http://crawdad.org/cambridge/haggle/20060915, sep 2006.

[106] N. Eagle and A. S. Pentland. Reality mining: sensing complex social systems. *Personal and ubiquitous computing*, 10(4):255–268, 2006.

[107] L. Katz. A New Status Index Derived from Sociometric Analysis. *Psychometrika*, 18(1):39–43, 1953.

[108] A. Vahdat, D. Becker, et al. Epidemic Routing for Partially Connected Ad Hoc Networks. Technical report, CS-200006, Duke University, 2000.

[109] T. Spyropoulos, K. Psounis, and C. S. Raghavendra. Spray and Wait: An Efficient Routing Scheme for Intermittently Connected Mobile Networks. In *Proc. of ACM SIGCOMM Workshop on Delay Tolerant Networking, 252-259*, 2005.

[110] M. Grossglauser and D. Tse. Mobility Increases The Capacity of Ad-hoc Wireless Networks. In *Proc. of IEEE INFOCOM, 1360–1369*, 2001.

[111] A. Balasubramanian, B. Levine, and A. Venkataramani. DTN Routing as a Resource Allocation Problem. *ACM SIGCOMM Computer Communication Review*, 37(4):373–384, 2007.

[112] K. Wei, X. Liang, and K. Xu. A Survey of Social-aware Routing Protocols in Delay Tolerant Networks: Applications, Taxonomy and Design-related Issues. *IEEE Communications Surveys & Tutorials*, 16(1):556–578, 2014.

[113] P. V. Marsden. Egocentric and Sociocentric Measures of Network Centrality. *Social networks*, 24(4):407–422, 2002.

[114] N. Eagle, A. S. Pentland, and D. Lazer. Inferring Friendship Network Structure by using Mobile Phone Data. *Proc. of the National Academy of Sciences*, 106(36):15274–15278, 2009.

[115] J. Scott, R. Gass, J. Crowcroft, P. Hui, C. Diot, and A. Chaintreau. Crawdad dataset cambridge/haggle. *CRAWDAD wireless network data archive*, 2006.

[116] G. Bigwood and T. Henderson and D. Rehunathan and M. Bateman and S. Bhatti. CRAWDAD dataset st_andrews/sassy (v. 2011-06-03). http://crawdad.org/st_andrews/sassy/20110603/mobile, jun 2011.

[117] A. Keränen, J. Ott, and T. Kärkkäinen. The ONE Simulator for DTN Protocol Evaluation. In *Proc. of Conference on Simulation Tools and Techniques, 1-10*, 2009.

[118] K. Fall and S. Farrell. DTN: An Architectural Retrospective. *IEEE Journal on Selected Areas in Communications*, 26(5):828–836, 2008.

[119] A. B. Paul, S. Chakraborty, S. De, S. Nandi, and S. Biswas. Adaptive path selection for high throughput heterogeneous wireless mesh networks. In *Proc. of Conference on Advanced Networks and Telecommunications Systems, 1-6*, 2015.

[120] A. Naveed, S. S. Kanhere, and S. K. Jha. Attacks and security mechanisms. Technical report, 2008.

[121] C. L. Hwang and K. Yoon. *Multiple Attribute Decision Making Methods and Applications*. Springer-Verlag, New York, 1981.

[122] H. Wang, X. Zhai, and P. Chen. Trust Routing Protocol Framework Based on Bahavior Assessment for Wireless Sensor Networks. In *Proc. of Conference on e-Business Engineering, 487-492*, 2008.

[123] L. Zhang, Q. Wu, B. Qin, J. Domingo-Ferrer, and B. Liu. Practical Secure and Privacy-preserving Scheme for Value-added Applications in VANETs. *Computer Communications*, 71:50–60, 2015.

[124] M. Goyal, K. K. Ramakrishnan, and W. Feng. Achieving Faster Failure Detection in OSPF Networks. In *Proc. of Conference on Communications, 296-300*, 2003.

[125] NS-2. http://www.isi.edu/nsnam/ns/.

[126] A. B. Paul, S. Konwar, S. Nandi, and S. Biswas. Trusted M-OLSR for Secure Routing in Wireless Mesh Networks. *Journal of Information Assurance & Security*, 8(1):17–32, 2013.

[127] K. Fall. A Delay-tolerant Network Architecture for Challenged Internets. In *Proc. of SIGCOMM, 27-34*, 2003.

[128] K. Fall. A delay-tolerant network architecture for challenged internets. In *Proc. of Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, 27-34*, 2003.

[129] R-I. Ciobanu, R-C. Marin, C. Dobre, V. Cristea, C. X. Mavromoustakis, and G. Mastorakis. Opportunistic Dissemination using Context-based Data Aggregation over Interest Spaces. In *Proc. of Conference on Communications, 1219–1225*, 2015.

[130] R-I. Ciobanu, R-C. Marin, C. Dobre, and F. Pop. Interest Spaces: A Unified Interest-based Dissemination Framework for Opportunistic Networks. *Journal of Systems Architecture*, 72:108–119, 2017.

[131] A. Mardani, A. Jusoh, K. MD. Nor, Z. Khalifah, N. Zakwan, and A. Valipour. Multiple Criteria Decision-Making Techniques and their Applications. *Economic Research-Ekonomska Istraživanja*, 28(1):516–571, 2015.

[132] U. G. Acer, P. Drineas, and A. A. Abouzeid. Connectivity in Time-Graphs. *Pervasive and Mobile Computing*, 7(2):160–171, 2011.

[133] S. Ferretti. Shaping Opportunistic Networks. *Computer Communications*, 36(5):481–503, 2013.

[134] F. Li, J. Wu, and A. Srinivasan. Thwarting Blackhole Attacks in Disruption-tolerant Networks using Encounter Tickets. In *Proc. of IEEE INFOCOM, 2428-2436*, 2009.

[135] T. M. Cover and J. A. Thomas. *Elements of Information Theory*. John Wiley & Sons, 2012.

[136] Y. Deng, F. TS. Chan, Y. Wu, and D. Wang. A new Linguistic MCDM Method based on Multiple-Criterion Data Fusion. *Expert Systems with Applications*, 38(6):6985–6993, 2011.

[137] S. Galam and J-D. Zucker. From Individual Choice to Group Decision-Making. *Physica A: Statistical Mechanics and its Applications*, 287(3):644–659, 2000.

[138] Y. Deng and F. TS. Chan. A New Fuzzy Dempster MCDM Method and its Application in Supplier Selection. *Expert Systems with Applications*, 38(8):9854–9861, 2011.

[139] M-F. Chen and G-H. Tzeng. Combining Grey Relation and TOPSIS Concepts for Selecting an Expatriate Host Country. *Mathematical and Computer Modelling*, 40(13):1473–1490, 2004.

[140] M. Janic. Multicriteria Evaluation of High-speed Rail, Transrapid Maglev and Air Passenger Transport in Europe. *Transportation Planning and Technology*, 26(6):491–512, 2003.

[141] CK. Kwong and SM. Tam. Case-based Reasoning Approach to Concurrent Design of Low Power Transformers. *Journal of Materials Processing Technology*, 128(1):136–141, 2002.

[142] AS. Milani, A. Shanian, R. Madoliat, and JA. Nemes. The Effect of Normalization Norms in Multiple Attribute Decision Making Models: A Case Study in Gear Material Selection. *Structural and multidisciplinary optimization*, 29(4):312–318, 2005.

[143] B. Srdjevic, YDP. Medeiros, and AS. Faria. An Objective Multi-Criteria Evaluation of Water Management Scenarios. *Water resources management*, 18(1):35–54, 2004.

[144] T. Yang and P. Chou. Solving a Multiresponse Simulation-Optimization Problem with Discrete Variables using a Multiple-Attribute Decision-Making Method. *Mathematics and Computers in simulation*, 68(1):9–21, 2005.

[145] K. Yoon and C-L. Hwang. Manufacturing Plant Location Analysis by Multiple Attribute Decision Making: Part IŮsingle-plant Strategy. *International Journal of Production Research*, 23(2):345–359, 1985.

[146] A. Keränen, J. Ott, and T. Kärkkäinen. The ONE simulator for DTN protocol evaluation. In *Proc. of Conference on Simulation Tools and Techniques, 1-10*, 2009.

Publications Related to Thesis

Journals

1. **Amrita Bose Paul**, Santosh Biswas, Sukumar Nandi and Sandip Chakraborty. "MATEM: A unified framework based on trust and MCDM for assuring security, reliability and QoS in DTN routing", *Journal of Network and Computer Applications*, Elsevier, Volume 104, Pages 1-20, February 2018. (Available online: https://doi.org/10.1016/j.jnca.2017.12.005)

2. **Amrita Bose Paul**, Shantanu Konwar, Sukumar Nandi and Santosh Biswas. "Trusted M-OLSR for Secure Routing in Wireless Mesh Networks."*Journal of Information Assurance and Security*", MIR Labs, Vol. 8, Issue 1, Pages 17-32. 2013. (ISSN 1554-1010, http://www.mirlabs.net/jias/index.html)

Conferences

1. **Amrita Bose Paul**, Sandip Chakraborty, Suddhasil De, Sukumar Nandi and Santosh Biswas. "*Adaptive Path Selection for High Throughput Heterogeneous Wireless Mesh Networks*", In Proc. of International Conference on Advanced Networks and Telecommunications Systems (IEEE ANTS 2015), India, 2015.

2. **Amrita Bose Paul**, Shantanu Konwar, Santosh Biswas and Sukumar Nandi. "*M-HRP for Wireless Mesh Networks and its Performance Evaluation*", In Proc. of International Conference on Communication Systems and Networks (IEEE/ACM COMSNETS 2014), India, January 07-09, 2014.

3. Shantanu Konwar, **Amrita Bose Paul**, Sukumar Nandi and Santosh Biswas. "*MCDM based Trust Model for Secure Routing in Wireless Mesh Networks*", In Proc. of World Congress on Information and Communication Technologies (WICT 2011), India, December 12-14, 2011, (IEEE Press).

4. **Amrita Bose Paul**, Upola Gogoi, Shantanu Konwar, Sukumar Nandi and Santosh Biswas. "*E-AODV for Wireless Mesh Networks and its Performance Evaluation*", In Proc. of International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA 2011), Spain, October 2011, (IEEE Press).

Other Publications of the Author

- **Amrita Bose Paul**, Shantanu Konwar, Upola Gogoi, Angshuman Chakraborty, Nilufer Yeshmin and Sukumar Nandi. "*Implementation and Performance Evaluation of AODV in Wireless Mesh Networks using NS-3*", In Proc. of International Conference on Education Technology and Computer (ICETC 2010), China, June 2010 (IEEE Press).
- **Amrita Bose Paul**, and Sukumar Nandi. "*Impacts of Refresh Interval Parameters on M-OLSR Performance for Wireless Mesh Networks*", In Proc. of IEEE TENCON, Singapore, November 2009, (IEEE Press).
- **Amrita Bose Paul**, and Sukumar Nandi. "*Modified Optimized Link State Routing (M-OLSR) for Wireless Mesh Networks*", In Proc. of International Conference on Information Technology (ICIT 2008), December 2008, (IEEE Press).

Brief Biography of the Author

Amrita Bose Paul graduated in Bachelor of Science (BSc) with Economics (Hons), Mathematics and Statistics from Cotton College, Gauhati University, India, and then obtained her Master of Computer Applications (MCA) degree from Jorhat Engineering College, Dibrugarh University, Assam, India. She completed her Masters in Computer Science and Engineering from Indian Institute of Technology (IIT) Guwahati, India. She is currently working as Associate Professor in the department of Computer Applications at Assam Engineering College, Guwahati, India. Her research interests include routing and security issues in Wireless Mesh Networks (WMNs), Delay/Disruption Tolerant Networks (DTNs), Trusted computing in multi-hop wireless networks etc.