CHAPTER 1

INTRODUCTION

The advent of wireless technology has revolutionized the lifestyle of millions and millions of people around the globe through pervasive communication. Pervasive communication infrastructure aids them to incorporate seamless integration of technology in their day-to-day life. This pervasive technology covers a wide range of applications ranging from cellular data services to ultra wide band services. These technologies are readily available on the personal mobile devices such as laptops, mobile phones, PDAs, etc., that enable people to get connected with the wide variety of networks.

1.1 Preamble

Majority of the wireless networks depend on a centralized infrastructure either as a base station or as an access point for operation. For instance, GSM and CDMA of cellular networks necessitate a base station for establishing communication between the mobile nodes. But there exist a kind of wireless networks called ad hoc network that operates independently without the support of any pre-established fixed infrastructure. Since it is a self-organized, self-controlled and self-configurable network which can be deployed anywhere at any time with minimal administration. Further, the communication between the mobile nodes can either be point-to-point or multi-hop. Point-to-point communication between the mobile nodes is feasible only when they are within the radio communication range. However, multi-hop communication is possible through a multiple set of intermediate mobile nodes called relay nodes that must participate in routing activity only when they possess adequate energy for transmission. These intermediate relay nodes not only transmit their own generated packets but also forward packets for their neighbouring nodes. Furthermore, mobile ad hoc networks cover a wide variety of applications ranging from critical applications (military operation, disaster recovery) to personal applications (patient monitoring). In addition, the routing decisions in an ad hoc network are always performed in a distributed manner at each and every mobile node. Hence, co-operation is considered as the most significant issue that need to be addressed for reliable packet delivery in the network. Thus the essential factors that need to be resolved for enhancing
co-operation between the mobile nodes through effective energy conception in the event of routing has been explored in this research.

1.1.1 Mobile Ad hoc Network

MANET is an autonomous collection of mobile nodes that forms a temporary network with reliable communication as their common objective. The mobile nodes of the network may join or leave the network at any point of time and they are free to roam around the network in the absence of any centralized infrastructure [1, 2]. Hence, the topology of the network is unpredictable. Further, MANET needs to provide a variety of services to its users at any time and at any place through its potentially large infrastructure-less wireless network. Furthermore, user services are made feasible by enabling reliable routing process that effectively forwards packets between the mobile nodes [3]. Moreover, this act of routing packets mainly depends on the degree of active collaboration existing among the mobile nodes [4]. The challenges and issues that influence the routing of packets are:

i) **Unpredictable Topology**: The mobile nodes in the ad hoc network possess the freedom to move randomly in an arbitrary fashion. Thus the network topology is unpredictable for maintaining connectivity between the dynamically changing topology,

ii) **Wireless Links**: The wireless links of mobile ad hoc network are highly unreliable and vulnerable to different kind of attacks. These wireless links between the nodes are not consistent for communication due to the energy constraint and mobility nature of nodes,

iii) **Node Mobility**: The mobile nodes in an ad hoc network independently and dynamically change their position and topology i.e., the routing information shared between the mobile nodes change frequently with respect to their random motion. Hence, interacting with a mobile node in a specific point of time becomes extremely difficult,

iv) **Energy limitation**: The mobile nodes are powered by energy-constrained resources like small batteries. This utilization of energy-constrained resources induce attacks that target on the disconnection of nodes and drain them at a rapid rate by highly engaging the mobile nodes for no reason. In addition, it also stimulates a mobile node to exhibit selfish behaviour that refuses to forward packets for their neighbours,
v) **Self-Configuring:** The mobile nodes are interconnected with one another and function as routers in a decentralized environment. They perform network activities that include reliable delivery of messages and discovery of topology through co-operation.

vi) **Variable capacity links:** The wireless links of ad hoc networks possess considerably a lower capacity than the links of wired counterparts. The capacity of the wireless links get degraded or varied with the passage of time due to factors like interference, noise, fading and multiple access that reduces the throughput, and

vii) **Co-operation:** The reliable communication between the source and destination pairs necessitates the co-operation of intermediate mobile nodes to act as routers for forwarding packets due to the lack of a centralized infrastructure in ad hoc networks.

In this research, issue of co-operation among mobile nodes is considered as the primary factor for investigation.

### 1.1.2 Co-operation in MANET

First and foremost, co-operation between mobile nodes is considered to be essential for enhancing the performance of MANET in terms of packet delivery rate and throughput [5]. But the mobile nodes in MANET may exhibit selfish or malicious behaviour. Since the energy requirements and communication requirements of the mobile nodes are incongruous [6]. For instance, a laptop may have a high energy and communication requirement than the mobile phones. Further, an ad hoc network is a multi-hop network in which the mobile nodes could not share a common radio communication range. They require intermediaries for establishing and maintaining communication with nodes far apart from each mobile node’s radius of communication. Furthermore, the topology of an ad hoc network is highly dynamic in nature due to the nodes’ mobility [7, 8]

Some of the terminologies that are necessary for understanding the issue of co-operation in MANET are:

i) **Co-operative nodes:** A mobile node that forwards maximum number of packets for the sake of its neighbouring nodes is considered more co-operative than its counterpart that drops maximum number of packets received from its neighbours,
ii) **Misbehaving nodes:** Misbehaving nodes refer to the broad category of mobile nodes that act selfishly for conserving energy or causes damage to the network either by dropping packets or injecting unwanted packets. Hence, misbehaving nodes can be categorized into selfish and malicious nodes,

**Selfish nodes:** Misbehaving mobile nodes are said to be selfish when they utilize all the network services and resources for forwarding their own generated packets but deny forwarding their neighbour nodes’ packets in order to conserve their energy. It is active in the network but does not collaborate with the other mobile nodes in order to save energy for its own participation.

**Malicious nodes:** The malicious nodes belong to a specific category of misbehaving nodes that exploit the vulnerability of the network and causes maximum damage either by dropping packets or by injecting unwanted traffic intentionally.

iii) **Reputation:** Reputation quantifies the degree of co-operation rendered by the mobile nodes participating in the network. A mobile node is considered as co-operative when its reputation value in the network is maximum. On the other hand, a node is said to be misbehaving when its reputation value is minimum. Reputation of a mobile node is computed through three different ways viz., a) direct interaction, b) neighbour recommendations and c) hybrid method that combines both direct interaction and neighbour recommendations, and

iv) **Fairness Index:** A mobile node in the network is considered to be fair if the ratio of number of packets transmitted to the number of packets forwarded for the sake of its neighbours converges to unity. Therefore, a maximum fairness index value of each participating mobile node represents its highest possibility in ensuring reliable packet delivery to its neighbouring nodes.

In this research, the degree of co-operation between the mobile nodes are quantitatively measured using reputation factor that are uniquely calculated using statistical reliability coefficient.

### 1.1.3 Reputation of Mobile nodes

Reputation of a mobile node quantifies the degree of collaboration rendered by the mobile node and estimates their reliability in forwarding neighbouring node’s packets [9, 10]. Generally, reputation of mobile nodes can be calculated based on statistical reliability coefficient. According to classical theory of statistics,
reliability coefficient is universally accepted for nodes’ behavioural analysis [11, 12]. Hence, this advantage of statistical reliability coefficient is utilized in this research for behavioural investigation of mobile nodes. Further, each reliability coefficient highlights the fairness index of mobile nodes’ behavioural consistency measurement that ranges from 0 to 1. Furthermore, this behavioural measurement is highly significant because they interpret the proportion that relates the deviation in observed-score to the expected-score [13, 14].

1.1.4 Impact of Energy towards Co-operation

A number of energy efficiency schemes are successfully implemented in the infrastructure-based wireless networks [15]. Since a centralized authority called base stations store energy for the sake of mobile nodes by turning them to doze state under negligible traffic [16]. But this cannot be successfully utilized in MANET as they lack a centralized infrastructure analogous to base stations. Moreover, a mobile node with substantial least amount of energy may misbehave in order to remain active in the network [17]. Further, majority of the protocols proposed for ad hoc networks always choose an optimal path that balances the energy consumption of the mobile nodes for enhancing network lifetime. Furthermore, it is also essential to stabilize the trade-off between the mobile node’s energy consumption rate and its network performance in terms of packet delivery ratio, throughput, control overhead, total overhead and packet latency [18, 19]. Finally, this research exclusively targets on the computation of reputation factor that estimates the reliability of the participating mobile nodes with due consideration to energy and packet delivery rate. This research also focuses on the issues that need to be resolved for enhancing the possibilities of network connectivity and network lifetime. However, the co-operation and energy consumption of mobile nodes are highly influenced by various misbehaving actions of mobile nodes.

Various misbehaving actions performed by the mobile nodes in the ad hoc environment are detailed in the following section.

1.1.5 Misbehaviour Actions in MANET

The inherent openness nature of MANET makes them highly vulnerable to a wide range of misbehaving actions. These misbehaving actions may be either intentional or non-intentional attacks. These attacks are classified into physical layer attack, data link layer attack, network layer attack, transport layer attack and application layer attack. Figure 1.1 depicts the classification of attacks in various layers of an ad hoc network. This research specifically concentrates on a
mobile node misbehaviour called selfish node behaviour which belongs to the class of network layer attack.

The network layer attacks greatly influence the network activities like routing and packet transmission [20, 21]. These network layer attacks include selfish node behaviour and malicious attacks like worm hole, black hole and gray hole attacks. Selfish nodes use the network but do not co-operate in order to save battery life for their own communication and they are not intended for damaging other mobile nodes. On the other hand, malicious nodes damage other nodes by causing network outage that partitions the network.

The characteristic behaviour of selfish nodes and its impact towards network performance is detailed in the following section.

1.1.6 Selfish Node Behaviour

The mobile nodes that exhibit selfish behaviour intentionally delay and drop packets when the packets are relayed between the source and destination nodes. Selfish nodes do not support any packet forwarding activity that could benefit their neighbouring nodes. The selfish node also utilizes limited energy for its own purpose with the objective of saving its resources to a maximum extent. In addition, this misbehaviour is specifically observed only when the residual energy possessed by the mobile nodes is inadequate [22]. Thus a selfish node refuses
to participate in the routing process and poses a negative impact on reliability, fairness and efficiency in packet forwarding. Further, the selfish nodes are classified into TYPE I, TYPE II and TYPE III selfish nodes. TYPE I selfish nodes actively co-operate in the route establishment process but intentionally deny to forward data packets for their neighbours regardless of its energy resources. While TYPE II selfish nodes neither co-operate in route establishment nor in data transmission. Whereas TYPE III selfish nodes co-operate in route establishment but do not forward data packets because of its limited availability of residual energy [23].

1.1.7 Impacts of Selfish Behaviour

The selfish behaviour of mobile nodes in an ad hoc network induce the following impacts [24, 25].

i) Network partitioning: The selfish behaviour of mobile nodes end up with network partitioning. This network partitioning is considered as a serious problem in a dynamic network like MANET. Since the intermediate mobile nodes that forward the desirable data may get isolated and results in reduced data accessibility among the active mobile nodes.

ii) Reduced data availability: The selfish node behaviour of mobile nodes results in the loss of certain number of mobile nodes and breakage of wireless links that originate a number of disjoint partitions in the network. The mobile node in one disjoint partition hinders the data accessibility of other mobile nodes present in other partitions of the network. This situation greatly impacts the data availability.

iii) Decrease in network lifetime: Network lifetime generally refers to the time-span during which the network operates actively prior to the cease of its actions. Since the selfish nodes do not participate in transmitting the packets and also it drains considerable amount of energy. This typical behaviour of selfish nodes drastically decreases the lifetime of the network.

iv) Decrease in throughput: Selfish behaviour of mobile nodes induce them to drop packets intentionally. Hence, the throughput that defines the number of packets forwarded by the mobile node for the sake of their neighbours gets degraded.

v) Increase in packet dropping rate: The selfish nodes drop the maximum number of packets that are received from their neighbouring nodes for conserving its limited energy. This increases the packet drop rate which results in communication overhead in the network.
vi) **Increase in end-to-end delay:** End-to-end delay represents the quantum amount of time consumed by the data packets to reach the destination from the source node. Selfish behaviour of mobile nodes increases the time in transmission of data packets relayed between the source and destination nodes.

### 1.2 Motivation of the Research

Reliable routing in an ad hoc network necessitates co-operation and sufficient energy from the mobile node’s perspective. Since the activity of packet forwarding is feasible only through co-operation among active mobile nodes and further this co-operation is ensured when the residual energy possessed by them is sufficient enough for packet forwarding [26]. Moreover, the lifetime of the mobile node depends on its limited battery resource. Furthermore, network performance is adversely affected when the residual energy possessed by the mobile node reaches below a threshold level. Since a mobile node may misbehave in a selfish manner for conserving its energy in order to remain active in the network [27]. This misbehaviour disturbs the degree of co-operation maintained between the mobile nodes and considerably reduces the network lifetime. Besides this, decrease in network lifetime leads to catastrophic impacts especially in critical applications like disaster monitoring and battlefield communication. Therefore, misbehaviour of mobile nodes that arise due to energy deficiency has to be detected and isolated for enhancing the network lifetime. Generally, reputation value of a mobile node aids in estimating the degree of misbehaviour. But this reputation value is comprehensive only when they are computed based on three possible monitoring approaches, viz., a) direct interaction, b) neighbour recommendations and c) hybrid approach that integrates both direct observation and neighbour recommendations into account. In addition, judging a node’s misbehaviour only based on past history poorly quantifies the intensity of misbehaving actions [28]. Hence, mitigation mechanisms that judge the nodes’ misbehaviour through its observed past historical behaviour, present-past conditional behaviour and futuristic forecasting behaviour need to be formulated.

### 1.3 Need for the Research

The specific issue that is highly focused in this research is the reliability of mobile nodes that perform network layer functionalities like packet forwarding and routing. This act of packet forwarding is mainly achieved by routing packets through co-operative nodes rather than misbehaving nodes. Further, misbehaving mobile nodes may be co-operative for a time period but may suddenly change its
behaviour into selfish node depending on the unfavourable situation like energy scarcity prevailing in them. Therefore, a mobile node may initially agrees to forward packets but later fails to carry out its activities due to its selfishness. Hence, it is evident that the selfish nodes utilize maximum network resources but refuse to forward packets for their neighbouring nodes [29]. Thus selfish nodes invalidate the premise of co-operation in maximum of the routing algorithms proposed for MANET. Moreover, maintaining co-operation between mobile nodes in the presence of selfishness is a challenging issue because, i) ad hoc network fails to possess a well-defined line of defense more than its wired and infrastructure counterpart [30] and ii) the topology of MANET is unpredictable and energy-constrained in nature.

Furthermore, considerable number of reputation-based mitigation approaches available in the literature for detecting and isolating selfish nodes lack in the following issues such as, i) they do not consider past or present behaviour of mobile nodes for detecting selfish nodes, ii) they are not capable in forecasting the futuristic misbehaviour of mobile nodes based on a non birth-death Markov process and iii) they fail to integrate of multiple trust coefficient parameters for categorizing selfish nodes. Besides, comprehensive set of solutions that could handle the aforementioned issues through statistical reliability coefficient by projecting three contexts of monitoring need to be investigated. Hence, this research needs to focus on the design of an integrated selfish node mitigation framework for enhancing co-operation and network lifetime.

1.4 Scope of the Research

MANET is an important network option for many critical applications like military communication and disaster recovery operation in which infrastructure-less communication is the only possible choice. Its application within the military field is feasible due to its high mobility, survivability and self-organized nature [31]. In a hostile environment, such as the battle field, ad hoc networks distributive architecture eliminates the problem of a vulnerable network host or the loss of the network host [32]. But when the mobiles nodes in this kind of self-organized ad hoc network refuse to co-operate, i.e., behave in a selfish manner, the core objective of an ad hoc network is even more crucial and the degree of survivability of network becomes a critical issue to be investigated [33]. Further, cryptographic schemes proposed in the literature fail to detect these selfish nodes [34]. Thus reputation-based mitigation mechanisms are highly reliable in identifying functional misbehaviour of mobile nodes in the network.
1.5 Problem Statement and Objectives

The aim of this research work is to develop three categories of reliability coefficient-based mitigation mechanisms for selfish nodes in order to enhance the degree of cooperation among the mobile nodes by evaluating their past, present and future behaviour. This aim also include the design of context-aware multi-reliability coefficient-based mitigation framework that integrates three types of reliability coefficient for achieving rapid detection of selfish nodes.

The main objectives of this research are:

i) to devise hybrid history-aware mitigation algorithms for selfish nodes by utilizing reliability coefficient that highlights the past behaviour of mobile nodes,

ii) to formulate conditional probabilistic mitigation algorithms that detects and isolates selfish nodes by considering the present and past behaviour of the mobile nodes into account,

iii) to develop a futuristic trust-based mitigation mechanism that forecasts mobile nodes selfishness depending purely on the present behaviour of nodes, and

iv) to design an integrated multi-reliable factor-based reputation framework that categorizes selfish nodes through grey whitenization function.

1.6 Methodology and Approach

Multi-hop communication in an ad hoc network highly depends on the reliability of each and every intermediate node that acts as router in forwarding packets between the source and destination pairs. Moreover, the approach that enhances cooperation should be distributed to each and every node for making routing decision, in which every node is monitored through a) direct observation, b) neighbour recommendations and c) hybrid technique that incorporates both direct and neighbour recommendations. Hence, the proposed detection approaches follow a reputation-based scheme that detects and isolates selfish nodes using reputation value estimated through statistical reliability coefficient. In these approaches, each mobile node monitors their neighbouring nodes’ behaviour by direct interaction, through neighbour recommendations or a hybrid mechanism that integrates direct interaction and neighbour recommendations. The monitoring activity is mainly based on packet delivery and residual energy of mobile nodes. The classification of mobile nodes’ behaviour into selfish or co-operative is achieved through thorough investigation of the mobile nodes’ activity based on past history, conditional
probability and Semi-Markov prediction process. The past history, the conditional probability and Semi-Markov prediction process aid in quantifying the reputation value that determines the reliability of the intermediate mobile nodes participating in the routing activity. Based on the quantification, the selfish node is detected and isolated from the routing path.

The characteristic features of the proposed reputation-based mitigation approaches contributed in this research for enforcing co-operation are:

i) utilizing reputation value that exactly quantifies the ability of a mobile node in packet forwarding,

ii) estimating the influence of mobile nodes’ misbehaviour based on past, present and futuristic forecasting,

iii) incorporating a fully distributed decision mechanisms that estimate reputation of mobile node against any comprehensive misbehaviour,

iv) computing reputation factor in a highly customizable way that reduces computation and communication overhead,

v) assuming all nodes that participate in the routing process need not be co-operative.

vi) considering reputation value of mobile nodes as dynamic and subjective, and

vii) assuming the reputation of a mobile node recommended by their neighbours is asymmetric and non-transitive in nature.

Further, the proposed reputation-based selfish node detection approaches are thoroughly studied and investigated using ns-2 simulation with appropriate simulation setup. The performance of the proposed approaches are analyzed based on the network performance evaluation parameters, viz., Packet Delivery Ratio (PDR), throughput, control overhead, total overhead, end-to-end delay, energy consumptions and packet drop rate. In addition, these investigations are basically carried out by varying i) the number of mobile nodes, ii) the number of selfish nodes and iii) the traffic flow rate. Besides this, Ad hoc On-demand Distance Vector (AODV) protocol is the base protocol used for incorporating the complete set of reputation-based selfish node mitigation mechanisms proposed in this thesis as it is a reactive protocol that establishes paths only on demand. It also provides flexibility in modifying their control packets depending upon its application in ad hoc environment.
1.7 Organization of the Thesis

The core objective of this thesis is to design an integrated multi-reliability coefficient based mitigation framework for categorizing and mitigating selfish nodes in MANET. This thesis comprises seven chapters and it is organized as follows:

Chapter 1 introduces the challenges in mobile ad hoc network and importance of co-operation between mobile nodes in ad hoc network. It describes the node misbehaving anomalies that influences the reliable data communication in MANET. In addition, this chapter describes the research problem and the objectives of the research. The motivation behind choosing reliability coefficient for effective identification of selfish nodes is also explained in this chapter.

The general reputation-based selfish node detection algorithms present in the literature are thoroughly analyzed and presented in Chapter 2. It also presents brief analysis on various reliability factors specified for mitigating misbehaving anomalies along with their strength and weakness.

Chapter 3 deals with the development of history aware reputation mechanisms for mitigating selfish nodes based on exponential distribution and split half reliability coefficient. In this chapter three history-aware mitigation mechanisms such as, Exponential Normalized Reliability Factor-Based Detection Mechanism (ENRFBDM), Split Half Reliability Factor-Based Detection Mechanism (SHRFBDM), Exponential Hybrid Reliability Factor-Based Detection Mechanism (EHRFBDM) and its significance towards isolating the selfish nodes are presented.

Chapter 4 presents the design and implementation of conditional probabilistic approaches for deriving reputation coefficient of a mobile node based on its present and past behaviour. Two conditional probabilistic approaches, viz., Erlang Coefficient-Based Conditional Probabilistic Model (ECBCPM) and Laplace Stieltjes Transform-Based Conditional Probabilistic Mechanism (LSTBCPM) are presented and described in this chapter.

Chapter 5 presents the forecasting model called Futuristic Trust Coefficient-Based Semi-Markov Prediction (FTCBSMP) process to forecast the change in mobile node’s behaviour during routing activity. The development of non birth-death-based Semi-Markov model for estimating likelihood probability of the proposed futuristic trust model is also portrayed.
Chapter 6 presents a Context-Aware Integrated Multi-reliability Coefficient-Based Mitigation (CAIMCBM) framework for categorizing and mitigating selfish nodes based on Grey Whitenization function.

Chapter 7 presents the concluding remarks of this thesis and the foreseeable future enhancements of the proposed framework.

1.8 Summary

This chapter has presented the basic definitions and concepts that are essential for reliable communication in MANETs. It also elaborates on various misbehaving actions with an emphasis on selfish nodes and their impact. Further, the motivation, the need and the scope of the research problem are presented in this chapter. Finally, problem statement with its objectives and methodologies is also portrayed.