Strategic Pricing to Stimulate Node Cooperation in Wireless Ad Hoc Networks

Mingmei LI

DOCTOR OF
PHILOSOPHY

Department of Informatics,
School of Multidisciplinary Sciences,
The Graduate University for Advanced Studies (SOKENDAI)

2007 (School Year)
March 2007

Strategic Pricing to Stimulate Node Cooperation in Wireless Ad Hoc Networks

Abstract

In wireless ad hoc networks, all nodes cooperate to provide network services. Due to the limited radio transmission range, data packets are usually forwarded through multiple relay nodes before they reach the destinations. If a node always serves as a relay to transmit the packets, it may quickly use up its own energy and other resources. Therefore, some nodes use a selfish approach: they try to avoid forwarding the packets. Such selfish behavior would probably cause the network to break down. Selfish nodes are common within ad hoc networks because they are managed by different authorities.

In this thesis, the node cooperation problems are analyzed in two steps: 1) a game theoretic analysis is provided to stimulate node to cooperate; 2) a price-demand function based incentive model is proposed to optimize the nodes' service demand and service provision, and encourage the relay nodes to be honest.

Firstly, a game theoretic analysis is proposed to study node cooperation. In the related chapter, a "payment and compensation" scheme is used as a less-aggressive way to avoid nodes' non-cooperative behavior. It is assumed that once a packet is sent from a source node, the packet is associated with a sending fee, i.e, when a node needs sending the packets as a source node, a sending fee is required (e.g. reasonably some money). The fee is adjustable according to the network status, whereas the node can also accept or reject the fee. In order to induce voluntary forwarding, the network will also compensate the nodes who consume their energy in forwarding the packets for others. If I think the sending fee as the penalties to the source nodes and the compensation fee as the encouragement to relay nodes, then local optimization of the node, (the desired performance plus the compensation then minus the cost to be paid) will yield an optimal point. Each node can only select its own packet generation strategy, however the final utility of each node is determined by the strategy set constituted by the other nodes. With the game theoretic analysis, I found that by introducing an incentive pricing policy "payment and compensation",

the relay nodes have less motivation to drop the packets. However, I also found that game theoretic literature may not be directly applicable in the scenario where cheating nodes exist and how to reasonably charge the source nodes and compensates the relay nodes.

Therefore, secondly, a price-demand function based incentive model (PDM) is proposed. In the PDM model, the network is modeled as a market, where the pricing is determined by the source node's demand and the relay node's service supply. The source nodes make use of a price-demand function, which allocates payments to the service provider (relay nodes). The relay nodes are encouraged to cooperate in the PDM model, which is based on the assumption that each relay node wishes to maximize its payoff. Then the source nodes can optimize their prices and the number of sending packets to satisfy the relay nodes' payoff requirement. Once the payoff requirements of the relay nodes are satisfied, the relay nodes have no reason to be selfish. In the PDM model, a source node that has packets to send initially broadcasts RREQ in the network. Once the relay node(s) are selected, each relay node replies to the source node for its forwarding cost. Then the source node calculates the price of the sending packets it will pay for each relay node and the number of packets it will send. According to the source nodes' demand, it chooses the route with the lowest payment or the route with the largest number of sending packets. The PDM pricing model seeks to address two main issues: 1) to determine how much to charge the source nodes and how much to compensate the relay nodes; 2)to avoid the relay nodes to dishonestly report their forwarding costs. Hence, the contributions are summarized as follows: 1) The relay nodes intend to dishonestly report their forwarding cost to gain a high payoff from the source nodes, which obviously contradicts with the motivation to stimulate cooperation. In the PDM model, however, the relay nodes will have no reason to report a false forwarding cost, since only telling the truth guarantees the relay nodes' final payoff. Such a property is shown by the proof. 2) The PDM pricing model reflects the relationship between the service demand of the source nodes and the service supply of the relay nodes. The PDM model can save money for the source nodes for sending the packets, which is indicated by the simulation results.

Acknowledgements

This thesis is the outcome of three and a half year of research, which started from October 2003 at the Graduate University for Advanced studies, and National Institute of Informatics in Japan.

First and foremost, I would like to express my profound gratitude to my research supervisor Prof. Shigeki Yamada, who supported my work throughout these years. This work could never be completed without his invaluable encouragement and constant support. He guided me to think and solve the problems in the academic way, which would be very helpful in my future work and study.

Many thanks to Assistant Prof. Eiji Kamioka. He provided a lot of pleasant and deep discussions on my topics in our research group. His instruction and advices were a great help for me.

I would also like to thank Asso. Prof. Yusheng Ji, Prof. Tomohiro Yoneda, Asso. Prof. Shunji Abe, Asso. Prof. Katsunori Yamaoka for their helpful technical discussions, careful reading and valuable comments on my thesis.

This thesis is dedicated to my parents, my sister and my husband, who supported and encouraged me in my difficult time. I thank my mother for her mind that I chose this way of my life. I thank my husband for sharing with me the happy marriage life and difficult times.

This Ph.D. has been financially supported by Japanese Government MEXT scholarship and Prof.Shigeki Yamada's research fund from Grant in Aid for Scientific Research. I would like to thank all people in the above cited organizations that support me to finish my Ph.D study.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

In the next generation of wireless communication systems, there will be a need for the rapid deployment of independent mobile users. Significant examples include establishing survivable, efficient, dynamic communication for emergency or rescue operations, disaster relief efforts, and military networks. Such network scenarios cannot rely on centralized and organized connectivity, and can be conceived as applications of wireless ad hoc networks. A wireless ad hoc network is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. The set of applications for wireless ad hoc networks is diverse, ranging from small, static networks that are constrained by power sources, to large-scale, mobile, highly dynamic networks (Fig.1.1). Moreover, in a military environment, preservation of security, latency, reliability, intentional jamming, and recovery from failure are significant concerns. Military networks are designed to maintain a low probability of intercept and/or a low probability of detection. Hence, nodes prefer to radiate as little power as necessary and transmit as infrequently as possible, thus decreasing the probability of detection or interception. A lapse in any of these requirements may degrade the performance and dependability of the network [67].

Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activity including discovering the topology and delivering messages must be executed by the nodes themselves, i.e., routing functionality will be incorporated into mobile nodes. The design of network protocols for these networks is a complex issue. Regardless

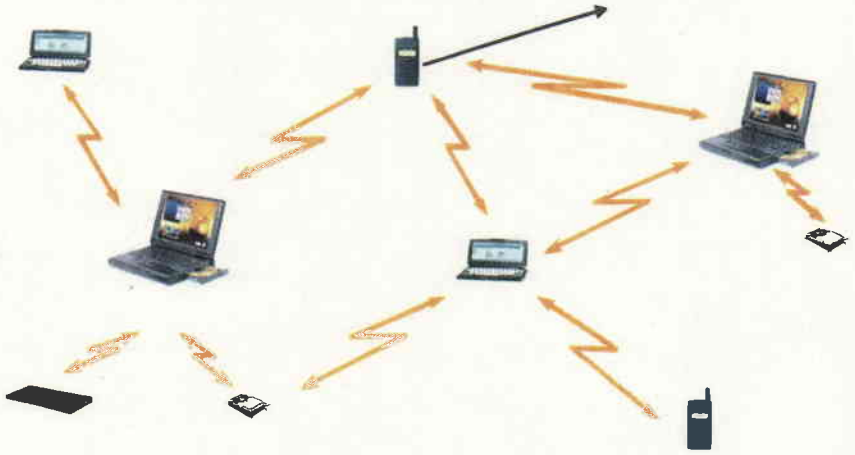


Figure 1.1: An example of wireless ad hoc networks in civilian environment

of the application, wireless ad hoc networks need efficient distributed algorithms to determine network organization, link scheduling, and routing. Cooperation among nodes is vital in wireless ad hoc networks. Without nodes forwarding other nodes packets, communication over multiple hops is impossible and the nodes remain disconnected. Thus, a constant contribution from all participants of a wireless ad hoc network is necessary to keep the nodes connected and thereby the network operational [68].

In the thesis, node cooperation problem in wireless ad hoc networks are analyzed by two methods: firstly, a game theoretic analysis is proposed; secondly, a price-demand function based incentive model is proposed.

- To improve the network throughput, a game theoretic analysis is proposed. In the analysis, I use a "payment and compensation" policy as a less-aggressive way to avoid nodes' selfish behaviors. Each node only selects its own packet generation strategy; however the final utility to each node is determined by the strategy set constituted by the other nodes. With the game theoretic analysis, I found that by introducing an incentive pricing policy "payment and compensation", the relay nodes have less incentive to drop the packets.

- To avoid relay node cheating and determine an optimal pricing model for the networks, an incentive model (PDM) based on a price-demand function is proposed. In the PDM model, the network is modeled as a market, where

the pricing is determined by the source node's demand and the relay node's service supply. The source nodes make use of a price-demand function, which allocates payments to the service provider (relay nodes). The relay nodes are encouraged to cooperate in the PDM model, which is based on the assumption that each relay node wishes to maximize its payoff. The PDM pricing model seeks to address two main issues: 1) The relay nodes intend to dishonestly report their forwarding cost to gain a high payoff from the source nodes, which obviously contradicts with the motivation to stimulate cooperation. 2) The PDM pricing model reflects the relationship between the service demand of the source nodes and the service supply of the relay nodes.

In the following and Chapter 2, I will describe why these two methods root in game theory and economic analogy.

1.1 Motivations and Objectives

Over the last few years, people have realized that selfish users in a society is caused at least as often by bad incentives as by bad design. Systems are particularly prone to failure when the person guarding them is not the person who suffers. Game theory and microeconomic theory are becoming important to the network engineer [37, 54, 61, 66, 68]. The growing use of strategic mechanisms for digital rights management, accessory control and other business models that exert power over system owners, rather than to protect them from outside enemies, introduces many strategic and policy issues. The service provider becomes the enemy; her interests conflict directly with the cooperation mechanisms on her machine. Here too, game theoretic and economic analysis can shine light in some murky darkness.

Considering the military origin of wireless ad hoc networks, cooperation among nodes is not an issue in the corresponding application scenarios. This is true for all scenarios, where nodes are under control of a single authority and the wireless ad hoc network is established for the purpose of the application [68]. Example scenarios include military operations and disaster recovery. In scenarios without any single authority, cooperation among nodes is not obvious. A single authority prescribes

the behavior for all nodes respecting this authority. Thus, the single authority can ensure cooperation. When each user of a node is her own authority, she can decide by herself what to do. This individual freedom of each user leads to selfishness. Helping other users by forwarding their packets results in the consumption of the own node self's limited resources, such as processing and transmission time as well as battery power. Regarding the resource consumption, it is better for a node owner to be selfish, because he can save the resources for his own transmissions. When applying this attitude to all nodes in a wireless ad hoc network, no forwarding takes place and communication over multiple hops becomes impossible. Although a common goal in connectivity among the nodes might exist, the necessity of cooperation to achieve that goal is difficult to comprehend by individual users. Therefore, the cooperation in non-single authority application scenarios must be managed by additional measures. Cooperation in wireless ad hoc networks can be studied from two sides, the network and the user or node perspective.

From the network perspective, the nodes have to cooperate because they act as the backbone infrastructure. If they do not cooperate, the communication over multiple nodes becomes impossible. Thus, any selfish node harms the network and poses a threat to the network's correct functioning. Often, a selfish node is considered as a security threat, because it reduces the number of available communication paths and thereby the overall connectivity in the network. The consequence is, that cooperation must be enforced by all possible means. In the cooperation enforcement schemes, selfish nodes get punished so severely, that they have no other choice but to cooperate. The underlying assumption is that all nodes are always able to cooperate. So, no cooperation is just a sign of bad behavior and must be corrected using appropriate measures. However, this assumption ignores situations, where a node may not be able to cooperate at all, even if it wants to. This includes nodes running on very low battery power, nodes located at border areas with few packets to forward or nodes with a full buffer. A node might be located at a congestive point in the network and it might not be able to process all packets in time, thus the queue fills up and packets get dropped. Another problem arises in the determination of a node. In enforcement approaches it is common to perform

some kind of neighborhood watch, that means each node is monitored and evaluated by its neighbors [6, 9, 12, 41]. Therefore, the enforcement approaches are also called detection-based schemes. The surveillance results are then used to optimize the operation of the network.

From the user perspective, cooperation is costly, because it consumes resources such as processing and transmission time as well as battery power. It is not obvious for a user, to allow her node to forward other users' packets. Reasons for selfish behavior include the avoidance of additional costs imposed on a user (node) or the inability caused by the state of the node or the network, e.g. congestion. To make up for this loss in resources caused by cooperation, researchers recently have become interested in using game theoretic approach [20, 24, 35, 52, 53, 58] or an incentive pricing model [15, 17, 19, 45, 47, 56] to stimulate nodes to cooperate. Game theory provides a framework to study the behavior of selfish but rational participants in any strategic interaction. Recently it is widely used in networking problems, where the users intend to modify the pre-programmed protocols of their devices [68]. However, the results from game theoretic approach relies on each user's strategy, it may bring cheating behaviors among the users in the system. Therefore, it requires extra security measures beyond simple trust relations, a pricing mechanisms can be used to deal with this problem [19]. A pricing model to stimulate node cooperation in wireless ad hoc networks is based on the assumption that nodes may be reluctant or unable to cooperate. To make up for the additional costs of cooperation, the user should be compensated. The compensation should be high enough to overcome the users' reluctance and make cooperation attractive. Due to the usage of incentives to encourage cooperation, an additional valuable good is introduced into the architecture. Therefore, the encouragement approaches are also called incentive-based schemes. Besides the connectivity, the chosen incentives must be protected from misuse.

1.2 Contributions

The contributions of this thesis are summarized as

1. I proposed a game theoretic analysis to study node cooperation behavior in wireless ad hoc networks. I found that by introducing an incentive policy – "payment and compensation", the selfish nodes have less motivation to drop the packets. Therefore, the system throughput is improved compared with random strategies. However, this game theoretic approach is not applied for the scenario where relay nodes may cheat.

2. I proposed a price-demand function based incentive model (PDM) to stimulate nodes to be cooperative and honest: 1) the relay nodes intend to dishonestly report their forwarding cost to gain a high payoff from the source nodes, which obviously contradicts with the motivation to stimulate cooperation. In the PDM model, however, the relay nodes will have no reason to report a false forwarding cost, since only telling the truth guarantees the relay nodes' final payoff. Such a property is shown by the proof. 2) The PDM pricing model reflects the relationship between the service demand of the source nodes and the service supply of the relay nodes. The PDM model can reduce the source node payment for the source nodes for sending the packets, which is indicated by the simulation results.

1.3 Organization of the Thesis

In this thesis, node cooperation problems are studied by two methods: 1) a game theoretic analysis is provided to reduce the packets dropping; 2) an incentive model based on a price-demand function is proposed to stimulate node to be honest and cooperation. The remainder of the thesis is organized as follows,

Chapter 2 firstly introduces wireless ad hoc networks, the challenges of node cooperation in wireless ad hoc networks, then illustrates the basic concepts of using game theory and economic model in the wireless networks.

Chapter 3 compares the main features of the related works for node cooperation in wireless ad hoc networks and points out their limitations.

In chapter 4, a game theoretic analysis is proposed to study node cooperation. In this chapter, I use an incentive policy –"payment and compensation" scheme as a

less-aggressive way to encourage the relay nodes not to drop the packets in wireless ad hoc networks.

In chapter 5, to determine an optimal pricing model to stimulate node cooperation in wireless ad hoc network, I propose a new pricing model based on a price-demand function(PDM). In the PDM model, the wireless ad hoc network is modeled as a market, where the pricing is determined by the source node's demand and the relay node's service supply.

Chapter 6 summarizes the thesis and discusses future works.

Chapter 2

Stimulating Nodes to Cooperate in Wireless Ad Hoc Networks

2.1 Introduction and Motivation

In this chapter I start with the concepts of wireless ad hoc networks. Then I explain the challenges of node cooperation in wireless ad hoc networks. I continue with a description of economic market. Finally, I illustrate the possible solutions to apply economic model in wireless ad hoc networks.

2.2 Overview of Wireless Ad Hoc Network

On wireless computer networks, a MANET (Mobile Ad Hoc Network) consists of a collection of mobile nodes communicating in a multi-hop way without any fixed infrastructure such as access points or base stations. Operating in an ad-hoc mode allows all wireless devices within range of each other to discover and communicate in peer-to-peer fashion without involving central access points.

2.2.1 Application Areas

In the next generation of wireless communication systems, there will be a need for the rapid deployment of independent mobile users. Significant examples include establishing survivable, efficient, dynamic communication for emergency/rescue op-

erations, disaster relief efforts, and military networks. Such network scenarios cannot rely on centralized and organized connectivity, and can be conceived as applications of Mobile Ad Hoc Networks. A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activity including discovering the topology and delivering messages must be executed by the nodes themselves, i.e., routing functionality will be incorporated into mobile nodes.

The first work on MANET dates from the early 70s. The US military was in need of a communication infrastructure, which would not depend on pre-placed components and be easily movable. Radio communication was chosen to mobilize the network infrastructure. However, it also introduces limitations. Radio frequencies higher than 100MHz do not propagate beyond the line of sight. Moreover, in a military environment, preservation of security, latency, reliability, intentional jamming, and recovery from failure are significant concerns. Military networks are designed to maintain a low probability of intercept and/or a low probability of detection. Hence, nodes prefer to radiate as little power as necessary and transmit as infrequently as possible, thus decreasing the probability of detection or interception. A lapse in any of these requirements may degrade the performance and dependability of the network.

2.2.2 Wireless Technologies

With the advancement in radio technologies like Bluetooth, IEEE 802.11 or Hiperlan, a new concept of networking has emerged. This is known as ad hoc networking where potential mobile users arrive within the common perimeter of radio link and participate in setting up the network topology for communication.

To set up an ad-hoc wireless network, each wireless adapter must be configured for ad-hoc mode versus the alternative infrastructure mode. In addition, all wireless adapters on the ad-hoc network must use the same SSID and the same channel number. An ad-hoc network tends to feature a small group of devices all in very close proximity to each other. Performance suffers as the number of devices grows,

and a large ad-hoc network quickly becomes difficult to manage. Ad-hoc networks cannot bridge to wired LANs or to the Internet without installing a special-purpose gateway. Ad hoc networks make sense when needing to build a small, all-wireless LAN quickly and spend the minimum amount of money on equipment. Ad hoc networks also work well as a temporary fall back mechanism if normally-available infrastructure mode gear stop functioning. Therefore, a wireless ad hoc network is characterized by a distributed, dynamic, self-organizing architecture. Each node in the network is capable of independently adapting its operation based on the current environment according to predetermined algorithms and protocols.

2.2.3 Routing Protocols

In this section, several existing routing protocols for ad hoc Wireless Networks were briefly described. The four ad-hoc routing protocols that are currently supported are Destination Sequence Distance Vector (DSDV), Dynamic Source Routing (DSR), Temporally ordered Routing Algorithm (TORA) and Adhoc On-demand Distance Vector (AODV). Usually, there are two categories of routing protocols: table-driven and on-demand routing protocols. In table-driven protocols, each node maintain up-to-date routing information to all the nodes in the network where in on-demand protocols a node finds the route to a destination when it desires to send packets to the destination. DSDV are table-driven protocols that use destination sequence numbers to keep routes loop-free and up-to-date. AODV is an on-demand version of DSDV routing protocol. DSR is a source routing mechanism where the route is in each packet.

- DSR

The Dynamic Source Routing Protocol is a source-routed on-demand routing protocol. A node maintains route caches containing the source routes that it is aware of. The node updates entries in the route cache as and when it learns about new routes. The two major phases of the protocol are: route discovery and route maintenance. More details of DSR routing protocol is written in [28].

- DSDV

The Destination-Sequenced Distance-Vector (DSDV) Routing Algorithm is based on the idea of the classical Bellman-Ford Routing Algorithm with certain improvements. Every mobile station maintains a routing table that lists all available destinations, the number of hops to reach the destination and the sequence number assigned by the destination node. The sequence number is used to distinguish stale routes from new ones and thus avoid the formation of loops. The stations periodically transmit their routing tables to their immediate neighbors. More details of DSDV Routing Protocol is in [38].

- AODV

Ad hoc On-demand Distance Vector Routing (AODV) is an improvement on the DSDV algorithm. AODV minimizes the number of broadcasts by creating routes on-demand as opposed to DSDV that maintains the list of all the routes. To find a path to the destination, the source broadcasts a route request packet. The neighbors in turn broadcast the packet to their neighbors till it reaches an intermediate node that has a recent route information about the destination or till it reaches the destination. More details of DSDV routing protocol is written in [40].

- TORA

The Temporally Ordered Routing Algorithm (TORA) is a highly adaptive, efficient and scalable distributed routing algorithm based on the concept of link reversal. TORA is proposed for highly dynamic mobile, multihop wireless networks. It is a source-initiated on-demand routing protocol. It finds multiple routes from a source node to a destination node. The main feature of TORA is that the control messages are localized to a very small set of nodes near the occurrence of a topological change. More details of TORA routing protocol is written in [39].

2.3 Challenges of Node Cooperation in Wireless Ad Hoc Networks

The wireless ad hoc networks not only brings benefits, but also introduces challenges. Assume that each node in a civilian wireless ad hoc network stands for an individual.

There are several reasons for a node to deny cooperation and refrain from forwarding other nodes' packets. Forwarding packets occupies transmission time, which the node can not use for transmitting its own packets. Transmitting packets consumes battery power, which is an exhaustible resource on mobile devices. However, with uncooperative nodes communication over multiple hops becomes impossible, since no packets are forwarded and the multi-hop ad hoc network ceases to exist. Therefore, cooperation is one of the key factors in civilian wireless ad hoc networks.

The solution is to stimulate the cooperation of nodes either by punishing non-cooperative behavior or by rewarding cooperative behavior. In Chapter 3 I discuss these cooperation works in more detail. In the following sections, I explain the challenges of node cooperation in MANET.

2.3.1 Mobility Management

In contrast to infrastructure based networks, in ad hoc networks all nodes are mobile and can be connected dynamically in an arbitrary manner. All nodes of these networks behave as routers and take part in discovery and maintenance of routes to other nodes in the network. The mobility of the nodes in wireless ad hoc networks raises two issues. One is how to locate a node in such a network. The other is how to keep the location information up to date. Therefore, a node requires a unique identification and some means to propagate and retrieve location information of nodes. A centralized solution is available with Mobile IP. The presence of a base station is a clear advantage over mobile ad hoc networks. However, the wireless multi-hop connections over mobile nodes limit the scalability of a centralized mobility management scheme. Anastasi et al. [1] describe some location service schemes in the context of position-based routing in mobile ad hoc networks.

2.3.2 Power Control and Bandwidth Allocation

Wireless hosts are usually powered by batteries which provide a limited amount of energy. Therefore, techniques to reduce energy consumption are of interest. One way to conserve energy is to use power saving mechanisms. Power saving mechanisms

allow a node to enter a doze state by powering off its wireless network interface when deemed reasonable [57]. Another alternative is to use power control schemes which suitably vary transmit power to reduce energy consumption [21]. In addition to providing energy saving, power control can potentially be used to improve spatial reuse of the wireless channel. Different power levels among different nodes introduce asymmetric links. Therefore, RTS and CTS are transmitted using the highest power level and DATA and ACK are transmitted using the minimum power level necessary for the nodes to communicate.

In wireless ad hoc networks, the link level bandwidth plays an important role in QoS provisioning for end-to-end flows. If an end-to-end flow crosses several hops in the link layer, then the bandwidth that can be assigned to such flow is determined by the capacity of the bottleneck link. Traditionally, in order to provide QoS routing and be able to perform tasks such as admission control, an end-to-end flow's requested bandwidth is checked against the link layer bandwidth hop-by-hop to find a feasible and admissible path. Therefore, QoS routing relies on the ability of the system in quantifying link layer bandwidth. While this was not a major problem in traditional networks, it becomes challenging problem in wireless ad hoc networks due to the volatile nature of the network topology, and as a consequence to the variable capacity of link layer bandwidth.

QoS routing algorithms for wireless ad hoc networks proposed in the literature (e.g. [1,3]) sometimes directly use bandwidth as the metric to achieve QoS routing, and assume the link layer is capable of providing such bandwidth without considering the complexity of these assumptions. In addition, QoS support frameworks and differentiated services frameworks such as INSIGNIA [3] also utilize hop-by-hop link layer bandwidth to check feasibility of routes and to reserve resources along the paths. Today MAC schemes for wireless ad hoc networks are not capable of providing QoS. Therefore, it is very important to design techniques and tools to study the effects of bandwidth sharing principles on the QoS.

2.3.3 Privacy and Security

The build up of wireless ad hoc network can be envisaged where support of wireless access or wired backbone is not feasible. Wireless ad hoc wireless network does not have any predefined infrastructure and all network services are configured and created on the fly. Thus it is obvious that with lack of infrastructure support and susceptible wireless link attacks, security in ad hoc network becomes inherent weakness. Achieving security within ad hoc networking is challenging due to following reasons [1]:

The vulnerabilities in wireless ad hoc networks are numerous. The wireless medium allows for passive attacks, e.g. sniffing of information. This information can then be used by an adversary to perform an active attack. Due to the wireless communication, an intermediate node can drop packets instead of forwarding them. An adversary can also attack the management protocols (routing, cooperation) of the wireless ad hoc network, either provoking a disruption or a malfunction of the provided services.

Nodes within nomadic environment with access to common radio link can easily participate to set up ad hoc infrastructure. But the secure communication among nodes requires the secure communication link to communicate. Before establishing secure communication link the node should be capable enough to identify another node. As a result node needs to provide his/her identity as well as associated credentials to another node. However delivered identity and credentials need to be authenticated and protected so that authenticity and integrity of delivered identity and credentials cannot be questioned by receiver node. Every node wants to be sure that delivered identity and credentials to recipient nodes are not compromised. Therefore it is essential to provide security architecture to secure ad hoc networking.

The above mentioned identification problem simultaneously leads to privacy problem. In general mobile node uses various types of identities and that varies form link level to user/application level. Also in mobile environment very frequent mobile node is not ready to reveal his/her identity or credentials to another mobile node from privacy point of view. Any compromised identity leads attacker to create privacy threat to user device. Unfortunately the current mobile standards [1] do

not provide any location privacy and in many cases revealing identity is inevitable to generate communication link. Hence a seamless privacy protection is required to harness the usage of ad hoc networking.

A major source for the security problems lies in the lack of a reliable authentication of nodes. Although, base stations are available in wireless ad hoc networks, many nodes do not have a direct (single-hop) connection to them. In a communication session, it is thus necessary to authenticate all nodes on the path within the wireless ad hoc network. However, with increasing node mobility the establishment and maintenance of security sessions between nodes and the base station does not scale. Depending on the scenario the security issues in wireless ad hoc networks are closely related to the ones in mobile ad hoc networks. Sanzgiri et al. [49] propose a protocol called authenticated routing for ad hoc networks, which is based on public key cryptography and allows secure routing in managed and open environments, where not all participants need to be authenticated in order to participate.

2.4 From Economic Markets to Wireless Ad Hoc Networks

It is well known that economics plays an important role in the success of a technology. Recently, researchers in electrical sciences are applying the tools and techniques from the domain of economic theory to solve various problems in the networking. Utility models, game theory, auction theory, etc. have been successfully applied to various optimization problems. Use of pricing models to stimulate node cooperation in wireless ad hoc networks is just one example [2, 10, 11, 15, 17, 19, 20, 22, 24, 25, 35, 36, 47, 52, 56, 58]. However, it is known that an economic model simply attempts to abstract from complex human behavior in a way that reflects a particular aspect of the behavior. In the following, I briefly describe the concepts used in economic theory and then i explain how economic theory can be used to solve the problems in wireless ad hoc networks.

2.4.1 Demand and Supply

Economic theory centers on creating a series of supply and demand relationships, describing them as equations, and then adjusting the factors which produce "stickiness" between supply and demand. Analysis is then done to see what "trade offs" are made in the "market", which is the negotiation between sellers and buyers. Analysis is done to the point that the ability of sellers becomes less useful than other opportunities. This is related to "marginal" costs, or the price to produce the last unit that can be sold profitably, versus the chance of using the same effort to engage in some other activity [61].

The economic model asserts that in a free market, the amount of a product supplied by the producer and the amount demanded on the consumer are dependent on the market price of the product. The law of supply states that supply is directly proportional to price; the higher the price of the product, the more the producer will supply. The law of demand states that demand is inversely proportional to price; the higher the price of the product, the less the consumer will demand. Thus, supply and demand both vary with price [66].

- Supply schedule.

  The supply schedule is the relationship between the quantity of goods supplied by the producers of a good and the current market price. It is graphically represented by the supply curve. Since supply is generally directly proportional to price, supply curves are almost always upwards-sloping. Also, the slope of a supply curve is usually increasingly upwards-sloping (i.e., the curve is a convex function) due of the law of diminishing marginal returns.

- Demand schedule.

  Demand is economic requirement backed up by purchasing power. The demand schedule, depicted graphically as the demand curve, represents the amount of a good that buyers are willing and able to purchase at various prices, assuming all other non-price factors remain the same. The demand curve is almost always downwards-sloping, meaning that as price increases, consumers will buy less of a good.

The main determinants of individual demand are the price of the good, level of income, personal tastes, the price of substitute goods, and the price of complementary goods. Just as the supply curves are equal to marginal cost curves, demand curves are equal to marginal utility curves. As described above, the demand curve is generally downward sloping. There may be rare examples of goods that have upward sloping demand curves.

It should be noted that on supply and demand curves both are drawn as a function of price. Neither is represented as a function of the other. Rather the two functions interact in a manner that is representative of market outcomes. The curves also imply a somewhat neutral means of measuring price. In practice any currency or commodity used to measure price is also the subject of supply and demand.

2.4.2 Economic Models in the Networks

The success of a technology is directly related to its economic viability. A well established technology might lose its stake for new customers to a competitor stepping up in the market. An industry can meet the customer challenges by defining subscriber values, determining a target prospect's propensity to be acquired, or determining a current subscriber's inclination to purchase additional services [61]. When the customers are better understood and actions taken according to their buying preferences, not only is valuable data added, but also the profit margin of the service provider is improved. In the case of wireless data services, as technology evolves and customer demands rise, providers will continue to encounter the life-cycle management challenges of customer acquisition, customer retention/loyalty, and service cost reductions. Increasing market penetration levels and declining average revenue per customer amplify these challenges. Many service providers (or operators) have invested in the infrastructure development to support wireless data services as a means of differentiation and generating additional revenue.

The utility of the network services comes from the users' perspective. To retain its customer base, a service provider must make sure that customers are satisfied with the QoS they receive for the premium they pay. The level of customer satisfaction received from the system can be represented by utility-based functions due to the

fact that each customer spends his/her disposable income in the way that yields the greatest amount of satisfaction or utility. By understanding how new services diffuse, service providers can define the demand function, which is then used to derive the real network demand. Thus, a sound econometric model is required to determine the impact of demand on the resources in wireless data networks such as the wireless Ad hoc networks. Consistent economic models should guide the creation of demand on content, services, and applications. This approach would require new algorithms and protocols, the development of which must combine ideas from economics and networking research. It has been well accepted that the current wireless data network models are flawed, in the sense that they fail to capture.

The impact of user demands on revenue utility comes from the service providers' perspective. The deployment of new wireless ad hoc services is also impeded by the lack of market incentives to improve network services and applications along with their efficient use by the common people. Recent history has demonstrated that even with all the technological successes, perhaps the bottleneck for better services still lies in economics. Finally, wireless service providers are not too sharp on implementing the Internet Engineering Task Force (IETF) defined protocols due to lack of economic incentives. In the rush to provide quick solutions for immediate market returns, it is believed that the algorithms and protocols being developed should carefully consider users' demands [61, 66]. For technology, the users will be willing to adopt these technologies. Careful analysis reveals that most research on resource management in wireless networks mainly focuses on QoS provisioning and traffic management to optimize an objective function like overall system throughput or resource utilization. However, such an objective function in most cases is too generic and fails to capture the true utility from both the users' and provider's viewpoints.

In the future, new wireless data services with better utility may be introduced to substitute for some existing services. These new services, however, may not necessarily provide additional revenue to the providers. This is because users will almost always attempt to replace old services with newer ones without exceeding their budget. This gradual replacement of services will allow new services to diffuse

into the market as more and more users accept them.

2.4.3 Free Services and Selfish Nodes

There has been a lot of effort to understand the pricing for wireless network services from both the economics and engineering perspectives.

In mobile ad-hoc networks, nodes are both routers and terminals. For lack of routing infrastructure, they have to cooperate to communicate. Cooperation at the network layer means routing, i.e., finding a path for a packet, and forwarding, i.e., relaying packets for others. Selfish behavior means deviation from regular routing and forwarding. Intentional misbehavior can aim at an advantage for the misbehaving node or just constitute vandalism, such as enabling a malicious node to mount an attack or a selfish node to save power. If for every packet transmitted, every node in the route has to be compensated, the overhead of a charging system could become significant. It may be desirable if nodes that are idle are willing to help others without expecting any payment. But the obvious problem with this is that nodes can lie about how busy they are. They can always ask for payment, even when they are not busy, and still able to enjoy free-of-charge services from others. When the rest of the users realize this, they would not choose to offer free services anymore.

A monopolist who is unable to price discriminate will support a smaller network and charge higher prices than perfectly competitive firms. This is despite the fact that the monopolist has influence over the expectations of the consumers, and he recognizes this influence, while no perfectly competitive firm has such influence. Influence over expectations drives the monopolist to higher production, but the monopolist's profit-maximizing tendency towards restricted production is stronger and leads it to lower production levels than perfect competition. Thus, consumers and total surplus will be lower in monopoly than in perfect competition. Therefore the existence of network externalities does not reverse the standard welfare comparison between monopoly and competition; it follows that the existence of network externalities cannot be claimed as a reason in favor of a monopoly market structure.

The detrimental effects of misbehavior can endanger the entire network. Unless

misbehavior is addressed to provide reliable and trustworthy ad-hoc networks, users might be reluctant to use them. Therefore the following questions are meaningful: How to make an existing system keep working despite misbehavior? Can one weed out misbehaving nodes when fewer nodes deviate from the protocol? To address these questions, I am going to compare three aspects of main solutions in Chapter 3 as, detection and reputation systems, economic incentives, and game theoretic approach.

2.5 Summary

In this chapter, I first describe the features of wireless ad hoc networks, then I explained that it is a promising work to use economic tools to study node cooperation problems in wireless ad hoc networks.

Chapter 3

Limitation of Cooperation Works

3.1 Introduction and Motivation

Node cooperation is a challenge work in the packet forwarding process for MANET. As I explained in Chapter 2, depending on the application scenario, cooperation among nodes can not be taken for granted. The research community in the wireless network area has studied this problems for several years now. Marti et al. [34] as well as Buttyan and Hubaux [10] were the first to present cooperation work and concepts in this area. However, existing works relies on specific scenarios and system or security assumptions.

In this chapter I describe the limitation of existing cooperation works in MANET in detail. I illustrate three possible approaches to implement cooperation. The related works are presented in detail and a comparison based on the key characteristics of the presented works are given. I conclude with a summary on the current state of the cooperation works in MANET.

3.2 Works on Detection and Reputation Mechanisms

The goal of a detection and reputation system is to enable nodes to realize the changes caused by selfish nodes in the network. These systems aim at isolating

misbehavior nodes by not using them for routing and forwarding. Most systems also isolate them by denying their service. This isolation has three purposes. The first is to reduce the effect of misbehavior by depriving the misbehaving node to participate in the network. The second is to serve as an incentive to behave well to be denied service. Finally, the third is to obtain better service by not using misbehaving nodes on the path. The isolation is done by each node autonomously, without consensus or human intervention.

- Monitoring.

The goal of monitoring is to gather first-hand information about the behavior of nodes in the network. Monitoring systems detect misbehavior that can be distinguished from regular behavior by observation. Packet forwarding is just one of the possible types of misbehavior in wireless ad-hoc networks. The other routing misbehavior such as black hole routing, gray hole routing, worm hole routing are also suggested.

To detect misbehavior, nodes take into account the packets they receive (e.g. a received acknowledgment from the destination means that all the nodes on the route cooperated in forwarding)and they can also use enhanced passive acknowledgments (PACK) by overhearing the transmissions of the next hop on the route, since they are within wireless range when using omnidirectional antennas. For instance, if they do not overhear a retransmission to the following node within a timeout of e.g. 100 ms or if the overheard transmission shows that the packet header has been illegitimately modified, they conclude misbehavior.

To distinguish from physical failures of the next hop, the timeout allows for retransmission attempts if the transmission of the next hop fails. If there are link failures over a longer time, the node can expect a route error (RERR). To account for connectivity problems at the monitoring node itself, it disregards PACK timouts in the case of link-layer error messages received from its own interface. In addition to a list of known types of misbehaviors, nodes can automatically learn about new misbehavior in analogy to the human immune system [34].

- Reputation.

Reputation systems are used in some on-line auctioning systems. They provide a method for the participants of transmission to obtain a rating record, which is based on the feedback given by the nodes in the networks.

The two main ideas in reputation systems are that, 1) it is used to serve as an incentive for good behavior to avoid the negative consequences a bad reputation can entail; 2) second, it provides a basis for the choice of prospective transaction partners. The relevant description of a reputation system is discussed in the next sections.

The terms reputation and trust have been used for various concepts. Reputation here is defined as the performance of a node when it participates in the base protocol. For wireless ad hoc networking this means participation in routing and forwarding. Trust is denoted as the performance of a node in the policing protocol that protects the base protocol. The use of second-hand information, i. e. reputation information obtained from others, enables nodes to find out about misbehaving nodes before making a bad experience. Also, in wireless ad hoc networks, nodes might not meet every node that they need for multi hop forwarding, but with second-hand information they can make informed decisions about which nodes to use for their paths [7].

Some of the detection and reputation-based schemes are compared in Table 3.1. They were all designed for wireless ad hoc networks, use a decentralized architecture and require network interface cards to operate in promiscuous mode. All detection and reputation-based enforcement approaches also assume some pre-existing trust relations between nodes, which exchange reputation information and unchangeable identities of all nodes, e.g. tamper resistant hardware to ensure the effectiveness of the punishment. Usually, the cooperation of each node is observed by its neighbors and punished by (partial) exclusion from the network. The gain can be measured in increased throughput and decreased number of lost packets, i.e. needless transmissions [34]. Note that the energy cost is much higher than that of simple computations. Nodes have to listen to traffic at all time to find out whether it is for them. Detection and reputation-based approaches built on the user self's fear of being punished. The biggest challenges in these schemes are the secure trust man-

agement, reliable node identification and event detection. Today, these issues have not been solved satisfactorily. The reports on node reputation are also vulnerable to misuse and increase the signaling overhead.

Table 3.1: Comparison of Detection and Reputation Mechanisms

Schemes/Authors	Marti [34]	CONFIDENT [12]	CORE [33]
Cooperation	Neutral	Enforcement	Enforcement
Goals	Avoidance	Exclusion	Exclusion
Topology	Local	Global	Local
Reintegration	/	Impossible	Possible
Announcement	/	Misbehavior	Cooperation
Anno- receiver	/	Source	Whole network
Routing	DSR	DSR	DSR
Mobility Support	low	low	/

In the subsections 3.2.1, 3.2.2, and 3.2.3, I am going to explain three representative works on detection and reputation mechanisms.

3.2.1 Marti: Watch Dog and Pathrater

Marti et al. [34] are the first to introduce detection-based routing protocol enhancements for wireless ad hoc networks. They use a watchdog that identifies misbehaving nodes and a pathrater that helps routing protocols avoid these nodes.

Assumptions: The authors assume bidirectional communication and promiscuous mode operations between two nodes. The authors use the source routing protocol (DSR) [28] to implement their tools.

Main Scheme: There are two tools in each node to detect and mitigate routing misbehavior: a watchdog to identify misbehaving nodes and a path rater to support the routing protocol in avoiding these nodes. The watchdog is implemented by maintaining a buffer of recently sent packets and uses a tally to record the packets that are not delivered. If the tally exceeds a certain threshold bandwidth, it determines that the node is misbehaving and sends a message to the source nodes. Each node

rates every other node in the networks, and calculates a path metric by averaging the node rating. The pathrater maintains an original value of 0.5, increments each active node in the path with a value of $0.01/200ms$, decrements a node rating by 0.05 when it is detected to be a link break during packet forwarding.

Results: Through simulation the authors evaluate watch dog and pathrater using packet throughput, percentage of overhead (routing) transmissions, and the accuracy of misbehaving node detection. When used together in a network with moderate mobility, the two techniques increase throughput by 17% percentage in the percentage of 40% misbehaving nodes, and with extreme mobility, they can improve the throughput by 27%.

Limitation: The scheme has some critical issues. A malicious node is possible to circumvent the watchdog by dropping the packets at a lower rate than the threshold. Furthermore, the authors do not give the method to define an appropriate threshold. The authors do not consider the problem of node identification and trust among nodes. Thus, false accusations are easily possible. Also, there is neither a disadvantage for an uncooperative node nor an advantage for a cooperative one.

3.2.2 CONFIDANT Protocol

Buchegger and Le Boudec [12] propose a protocol, called CONFIDANT, to make misbehavior unattractive. They add observation, detection and reaction mechanisms to a routing protocol to exclude uncooperative nodes from the network. The security architecture is based on a distributed trust manager running on each node.

Assumptions: The authors assume that each node is authenticated and that no identities can be forged, i.e. some tamper resistant hardware is used. Trust management has to be distributed and adaptive.

Main Scheme: CONFIDANT consists of four components: the Monitor, the Reputation System, the Path Manager, and the Trust Manager. As a component in each node, the monitor records misbehavior and informs it to the reputation system. The trust manager of a node sends ALARM messages to warn others of the malicious nodes, however, the source of an ALARM message has to be checked before sending out. Reputation system provides a means of obtaining a quality

rating of participating nodes. At each node, there is a local rating list and/or a black list, which are potentially exchanged with friends.

Results: The authors present a performance analysis of DSR fortified by CONFIDANT and compare it to regular defenseless DSR. It shows that a network with CONFIDANT and up to 60% of misbehaving nodes behaves almost as well as a normal network, compared with a defenseless network.

Limitation: The idea to implement CONFIDANT protocol is limited to a few nodes, timeouts for reputations, and different thresholds for events that are used to infer the malicious character of nodes. However, current implementation does not consider observable attacks other than forwarding defection, e.g. route diversion.

3.2.3 CORE: a collaborative reputation mechanism

Michiardi and Molva [33] show a generic mechanism based on reputation to enforce cooperation among the nodes of a MANET to prevent selfish behavior. Each network entity keeps track of other entities' collaboration using a technique called reputation. Simple denial of service attacks are prevented by the collaboration technique.

Assumptions: The authors assume that each node self's network interface card operates in promiscuous mode, so that neighbors can overhear their communication. The authors also base their model on the source routing protocol DSR. Each node has a watchdog and a reputation table. The authors distinguish between different types of reputation (subjective, indirect and functional) to reflect the information source, which has been used to calculate the reputation. Nodes are seen as service requesters and providers.

Main Scheme: The network entity represents a mobile node. Each entity has two components: Reputation tables (RT) and a watchdog mechanism (WD). The reputation table is a data structure stored in each node, and the watchdog mechanism is used to detect misbehaving nodes. When the network entity wants to monitor its neighboring entity, it triggers a watchdog to compare the neighbor's information with the one stored in its buffer. The protocol is that if a provider refuses to cooperate, the CORE scheme will decrease the reputation of the provider, preventing the non-cooperative behavior.

Results: Negative ratings are only performed locally at the monitoring node and not propagated throughout the network. A misbehaving node has the possibility to repent by providing service to other nodes, by which it has not been rated negative yet.

Limitation: The exclusive distribution of positive information protects against misuse. A weakness of the model seems to be the high computation and communication overhead, as each successful request results in the adjustment of the reputation table and in propagating the success. Each unsuccessful request also results in an adjustment. How to identify nodes and to trust the propagated messages in such an environment is also not obvious.

3.3 Works on Incentive-based Mechanisms

Beginning of 2003, the majority of publications in the area of cooperation focussed on incentive-based mechanisms. In these literatures, the cooperation of each node is simulated by the help of virtual currency. Each relay node is remunerated according to its contribution.

Some of the incentive-based schemes are listed in Tables 3.2 and 3.3. All of them introduce a virtual currency and most of them offer the possibility of spending real money to adjust the balance on the virtual account. I specify the accounting architecture and how a node can proof its cooperativeness. I indicate how nodes are authenticated, how a symmetric session is established and whether the system supported node mobility, which are derived from the usage of sessions and the employed routing protocol. Incentive-based approaches built on the user self's interest in financial or other type of gain. The challenges in incentive-based schemes lie in the reliable proof of node cooperation and in the protection from misuse of the scheme to increase the reward. Another issue is trade-off between scalability and computational complexity of the security mechanisms.

In the subsections 3.3.1, 3.3.2, and 3.3.3, I am going to explain three representative works on incentive-based mechanisms.

Table 3.2: Comparison of Incentive-based Mechanisms (I)

Schemes/Authors	Yang [19]	Paul [41]	Frank [46]
Cooperation	Enforcement	Enforcement	Enforcement
Goals	Reward	Throughput reduction	/
Topology	Local	Global	Global
Reintegration	Impossible	Impossible	Possible
Announcement	Misbehavior	Misbehavior	Misbehavior
Anno- receiver	Source	Whole network	Group member
Routing	AODV	AODV	DSR
Mobility Support	low	high	/

3.3.1 Nuglet and a Micro-Payment Scheme

Buttyan and Hubaux [10] present a scheme to ensure cooperation among nodes in wireless ad hoc networks. They introduce a virtual currency called Nuglet, which is used to charge for the transmission of packets and to reward the forwarding process.

Assumption: The authors assume that each node has a tamper resistant hardware module, so that their behavior cannot be modified by their users. They also assume that the user can modify the behavior of the node, but never that of the tamper resistant hardware module. The security infrastructure is based on public-key cryptography, with additional symmetric-key sessions between each communicating pair of neighbors.

Main Scheme: The protocol requires the node to pass each packet to its security nodule. The security module has a component called a nuglet counter. When the nodes wants to send a packet as source nodes, they first estimate the number n of for-warding nodes that required. The nuglet counter is decreased by n. When the node successfully forward one packet, its nuglet counter is increased by one. And the nuglet counter must keep positive, if it is negative, it cannot send the packets any more. By the tamper resistant hardware module, the nuglet counter is protected from illegally manipulation.

Results: The author give an analysis of the implementation. Always forwarding

Table 3.3: Comparison of Incentive-based Mechanisms (II)

Schemes/Authors	Nuglet [10]	Sprite [56]	Jakobsson [48]
Cooperation	Hybrid	Encouragement	Encouragement
Goals	Reward/Exclusion	Reward	Reward
Topology	MANET	MCN	MANET
Record	Decentralized	Centralized	Centralized
Cooperation proof	Neighbor session	Payment token	Packet receipt
Security	Certificate	Shared secret	Certificate
Routing	/	/	source routing
Mobility Support	medium-low	high	/

the packets perform the best in the simulation results.

Limitation: The introduction of a virtual currency shows good control over the cooperation among nodes. The drawbacks in this scheme lie in the charging mechanisms. In the packet purse model, the correct estimation of the amount of nuglets required for a packet to reach the destination and not being dropped along the way seems very difficult. Another one is that resources (battery power and bandwidth) of all involved nodes and the network will not reach the destination and has to be retransmitted. An overestimation lets nodes run out of nuglets quickly, as the overestimated amount of nuglets is lost. As the overall amount of nuglets in the network decreases, the number of packets being successfully transmitted also decreases, which leads to a useless network. In the packet trade model, the source node is not charged, but the destination node pays the total costs from all the resales. Because the nuglet account balance of the destination is not considered when the packet is generated, the network can become overloaded quickly.

Buttyan and Hubaux [11] proposed a revision of their previous scheme, with a new charging mechanism. They evaluate it using simulations. The simulation results show that the amount of virtual currency in the network is related to the cooperativeness of the nodes. Instead of sending nuglets along with each packet, each originating node is charged with the estimated number of intermediate nodes to the

packet destination. If a node can not afford the transmission, the packet is dropped. The rewarding is now done by the neighbors of a node. A node keeps a pending Nuglet counter for each neighbor node, with which it has established a symmetric-key session. When a node receives a forwarded packet, it increases its Nuglet counter by receiving the certification from the neighbor node. The distribution of the pending nuglets is done periodically, via a specific synchronization protocol based on a timer.

Results: Despite the usage of a virtual currency to stimulate cooperation, the mechanism really enforce cooperation as there is no alternative for the node. If nodes do not cooperate for whatever reason, they will be excluded from the network.

Limitation: The problems in this proposal lie in the additional network traffic caused by the synchronization protocol and the correct coordination of the synchronization phase itself. The initial and the revised scheme are that a node can be excluded from the network without any fault. When it might not get enough packets to forward from its neighbors, it will not earn enough nuglets to transmit its own packets. Also, the complete scheme must rely on the tamper resistant card.

3.3.2 Sprite: A simple, Cheat proof, Credit-based System

Zhong et al. [56] make one of the first proposals, which uses rewards to encourage cooperation among nodes in wireless ad hoc networks. The authors propose a virtual currency called Credits and a centralized account management via a Credit Clearance Service for all nodes.

Assumptions: To correctly balance the accounts, the Credit Clearance Service needs to keep track of each transmissions in the wireless ad hoc network. A node generates and keeps a receipt of each forwarded message. Each node periodically submits the collected receipts to the Credit Clearance Service, which determines the charges and rewards based on all reported receipts. To prevent nodes from cheating, the security architecture is based on public-key cryptography. Game theory is used to give a formal model and analysis.

Main Scheme: When a node transmits a packet, it loses credits to the network and when it forwards packets, it gains Credits. For each transmission, the Credit Clearance Service balances the accounts of all active nodes, according to their role

in the network, e.g. the originator is charged and the forwarders get rewarded. The nodes have the possibility to buy additional Credits from the Credit Clearance Service. The Credit Clearance Service uses different rewards for cooperative and selfish nodes. To prevent colluding attacks with false receipts, the amount charged from the originator and rewarded to the intermediate nodes depends on the successful delivery of a message.

Results: The authors implement a prototype of Sprite and their evaluation find that the introduced overhead is low.

Limitation: Sprite only supports sender-based payment, since it avoids DoS attacks on the receiver. And the other problems of Sprite lie in the centralized accounting, authentication as well as the local collection of receipts on each node. The central accounting allows a global view of the nodes involvement in each transaction. The possibility of filling up its own account using real money gives the freedom of choice to the node. The centralization of the accounting and the authentication is not very realistic in a wireless ad hoc network.

3.3.3 iPass: An Incentive Compatible Auction Scheme

Chen et al. [17] propose an auction-based incentive scheme (called iPass) to enable cooperative packet forwarding behavior in MANET. Each flow pays the market price of packet forwarding service to the intermediate routers. The resource allocation mechanism in ipass is based on the generalized Vickrey auction with reserve pricing. The authors prove that user's truthful bidding of utility remains a dominant strategy, users and routers have incentive to participate in the scheme, and packet forwarding always leads to higher social welfare for the whole network. The authors design a signaling protocol to implement the scheme, and show that it can serve as an explicit rate-based flow control mechanism for the network. Therefore, iPass is a joint solution of incentive engineering and flow control in a non-cooperative MANET. Simulation results show that iPass is able to determine the auction outcome quickly, and at the same time achieves the goals of flow control.

Limitation: the work mainly studies flow control problem in MANET.

3.4 Works on Game Theoretic Models

Besides the detection and incentive-based cooperation mechanisms, formal models based on game theory also provide solutions for cooperation in MANET. In these works, the node cooperation in MANET are treated as a cooperative or noncooperative game. Game theory is used to derive optimal strategies (Nash Equilibrium) [42] under certain conditions (typically energy constraints). One example of these model is that the nodes represent the players and their actions are to forward or not to forward other node self's packets.

3.4.1 Tit-for-tat Strategy

Urpi et al. [53] develop a general model which formally describes the characteristics of wireless ad hoc networks. They analyze different cooperation enforcement mechanism from the literature and propose a simple strategy resulting in an equilibrium. This indicates that in their model, cooperation is possible out of a node self's self-interest. Srinivasan et al. [47] obtain similar results. They use an algorithm based on the generous tit-for-tat (GTFT) strategy. GTFT has been the winning strategy to solve the iterated prisoner's dilemma in a tournament. In GTFT each player mimics the action of the other player in the previous game and in addition is also slightly generous. In the case of packet forwarding, a node would occasionally also forward packets from selfish nodes. Wrona and Mfahonen propose a dynamic game theoretic model of cooperation based on evolutionary game theory in [54]. In this model the network is comprised of selfish nodes and learning nodes, which can dynamically adjust their strategies to maximize their payoff. The authors show that if an ad hoc network implements a reputation mechanism, the majority of the nodes in the network will be cooperative.

3.4.2 VCG

L. Anderegg et.al in [2] introduce a game-theoretic setting for routing in a wireless ad hoc network that consists of greedy, selfish agents who accept payments for forwarding data for other agents if the payments cover their individual costs incurred

by forwarding data. In this setting, the authors propose Ad hoc-VCG, a reactive routing protocol that achieves the design objectives of truthfulness (i.e., it is in the agents' best interest to reveal their true costs for forwarding data) and cost-efficiency (i.e., it guarantees that routing is done along the most cost efficient path) in a game-theoretic sense by paying to the intermediate nodes a premium over their actual costs for forwarding data packets. The authors show that the total overpayment (i.e., the sum of all premiums paid) is relatively small by giving a theoretical upper bound and by providing experimental evidence. The routing protocol implements a variation of the well-known mechanism by Vickrey, Clarke, and Groves in a wireless network setting. The routing protocol that is an adaptation of the Packet Purse Model with auctions is shown in the setting. However, unfortunately, it does not achieve cost-efficiency or truthfulness.

3.4.3 Game Theoretic Models without Incentive Mechanisms

Felegyhazi et al. [22] investigate whether cooperation can exist in wireless ad hoc networks without incentive mechanisms. They propose a model based on game theory and graph theory to investigate equilibrium conditions for packet forwarding strategies. Their model is the first to considers the network topology. They find that in theory conditions for cooperation out of self-interest exist, but their simulation show that in practice these conditions are almost never satisfied and there will always be nodes which need an incentive to cooperate.

3.5 Joint Solutions

In detection and reputation based works, secure routing using cryptography, such as providing preventive means for specific malicious attacks, e.g. compromising routes. Secure routing applies to route discovery. Once a route is found, its use is not secured. Secure routing solves a part of the question, but not all. There remains a variety of observable types of misbehavior that they cannot cure easily, such as silent route changes, which may be addressed by detection and reputation systems. They monitor and rate the behavior of other nodes in routing and forwarding, such

that nodes can respond according to their opinion about other nodes. The opinion a node has of another is called reputation. The goal of a reputation system is to enable nodes to make informed decisions about which nodes to cooperate with or exclude from the network. Reputation systems can be used to cope with any kind of misbehavior as long as it is observable.

Economic incentives such as payment schemes aim at making selfish nodes forward for others despite the power usage and effort this entails. Nodes are paid for forwarding and pay for the forwarding of their own packets by other nodes. An example are nuglets, a virtual currency, or the credit counter [10] in secure hardware, where nodes keep track of remaining battery power and credit. These approaches make it undesirable for selfish nodes to deny forwarding. They do not, however, target other types of misbehavior. Economic models could also be used to prove that the system is free from cheating.

In game-theoretic terms, cooperation in mobile ad-hoc networks poses a dilemma. To save battery, bandwidth, and processing power, nodes should not forward packets for others. If this dominant strategy is adopted, however, the outcome is a non-functional network when multi-hop routes are needed, so all nodes are worse off. Without countermeasures, the effects of misbehavior have been shown to dramatically decrease network performance [34]. Depending on the proportion of misbehaving nodes and their strategies, network throughput decrease, packet loss, denial of service, and network partition can result.

3.6 Summary

Recently, node cooperation becomes a challenging issue in wireless ad hoc networks. Researchers have considered solutions for this issue for several years. This chapter compares the related works in three aspects: detection and reputation based mechanisms, incentive-based mechanisms and game theoretic approaches. It is found that detection and reputation based mechanisms brings high expense into the systems, therefore they is not widely used; incentive-based mechanisms reduce the selfish node behaviors, however these mechanisms also produce nodes' cheating behaviors;

and implementation of game theoretic approaches requires for the specific network topology.

In the next chapter, I am going to illustrate my own works. In this thesis, node cooperation problem in wireless ad hoc networks are solved by two steps: first, to encourage the relay nodes not to drop the packets, a game theoretic analysis is proposed in chapter 4. However, this game theoretic approach is not applied for the scenario where relay nodes may cheat. Therefore second, to avoid relay node cheating and determine an optimal pricing model for the networks, an incentive model (PDM) based on a price-demand function is proposed in chapter 5.

Chapter 4

A Game Theoretic Analysis for Non-Cooperative Nodes

4.1 Introduction and Motivation

Encouraged by the power of game theoretic approach [20, 24, 35, 52, 53, 58], firstly I tried to use game theory to help formulate and analyze solutions to induce autonomous nodes in a multi-hop wireless network to forward packets for each other. This problem involve interacting autonomous users, and have other features that exhibits the classical group versus individual rationality tension: nodes need to forward packets for the network to be connected, but an individual node decreases its energy and throughput by doing so.

As mentioned earlier, a node in an wireless ad hoc network is faced with two primary constraints. Firstly, in the transmission of data packets, energy (in terms of the battery levels of the nodes) is consumed. Thus, since PDAs or laptops are portable systems allowing users to process information on the way, they are heavily dependant on the limited battery power that they carry. Consequently, nodes would want to conserve as much energy as possible. Secondly, nodes would also like to have the maximum throughput (number of packets accepted by the relays over the number of packets sent out as a source) possible. However this would require relay nodes to cooperate all the time. While it may be intuitive that relay nodes should help to forward packets for other nodes all the time, it is not in their interest to do

so. If a relay node were to transmit data continuously for other nodes, there may be little or no energy left for its own use.

In the following analysis, I assume that once a packet is sent from a source node, the packet is associated with a payment, i.e, when node i needs sending packets as a source node, reasonably some compensation money is required. The cost is adjustable according to the network status, whereas the node can also accept or reject the cost. In order to induce voluntary forwarding, the network will also compensate the nodes who consume energy in forwarding packets for other nodes. If I think of the implied costs as the penalties to be paid by the source nodes and the compensation as the encouragement to relay nodes then local optimization of the node, for example, the desired performance plus the compensation then minus the payment, will yield an optimal point. Each node can optimize only its packet generate strategy (However the final utility is determined by the strategy set constituted by all other nodes).

4.2 Game Theory

In this section, I apply the basic concept of game theory in the strategic form. The following definitions will be used throughout this thesis.

4.2.1 Game in the strategic Form

Let us first understand the basic concepts of game theory as widely used in the economics domain to model interactions among parties with conflicting interests, where each party is called a player. In a game, each players' strategy has impact not only on his/her own payoff, but also on other players' payoffs. Depending on whether cooperation is allowed among players, games can be divided into cooperative and non-cooperative categories. The most basic form of non-cooperative games is a two player game in which each player has a set of strategies with associated payoff values; each player makes an independent decision on a strategy so as to get the most out of the game on the basis that the other player is not cooperating. Thus, the outcome of the game is to find a pair of strategies, one for each player, that

optimizes the payoffs of both players. Games can be played in two forms [31]:

- Normal form where each player makes a strategy decision without knowing the decision of the other player.
- Extensive form where at least one player has partial information about the other player's decision.

Mathematically, a two-player non-cooperative game consisting of players $P1$ and $P2$ is defined by payoff matrices A and B, respectively. Assume $P1$ has m strategies denoted $s_1, s_2, ...s_m$ and $P2$ has n strategies denoted as $t_1, t_2, ..., t_n$. Thus, the rows in the payoff matrices represent $P1$'s strategies, while the columns represent $P2$'s strategies. More precisely, the element a_{ij} of matrix A defines $P1$'s payoff when $P1$ chooses strategy s_i and $P2$ chooses strategy t_j. The element b_{ij} of matrix B is $P2$'s payoff when $P1$ chooses s_i and P_2 chooses t_j. Since this type of game is defined by two payoff matrices, it is also called a bi-matrix game, as shown in Tables 4.1 and 4.2.

Table 4.1: Payoff Matric A (player 1)

P2/P1	s_1	s_2	s_3	...	s_m
t_1	a_{11}	a_{12}	a_{13}	...	a_{1m}
t_2	a_{21}	a_{22}	a_{23}	...	a_{2m}
...	...	...	...	a_{ij}	...
t_n	a_{n1}	a_{n2}	a_{n3}	...	a_{nm}

Table 4.2: Payoff Matric B (player 2)

P2/P1	s_1	s_2	s_3	...	s_m
t_1	b_{11}	b_{12}	b_{13}	...	b_{1m}
t_2	b_{21}	b_{22}	b_{23}	...	b_{2m}
...	...	...	...	b_{ij}	...
t_n	b_{n1}	b_{n2}	b_{n3}	...	b_{nm}

Usually, games used to simulate real-life situations include five elements: 1) players, or decision makers; 2) strategies available to each player; 3) rules governing players' behavior; 4) outcomes, each of which is a result of particular choices made by players at a given point in the game; 5) and utility accrued by each player as a result of each possible outcome.

In the following I provide an informal introduction to strategic form game using an example. The two players are accused of conspiring in two crimes, one minor crime for which their guilt can be proved without any confession, and one major crime for which they can be convicted only if at least one confesses. The prosecutor promises that, if exactly one confesses, the confessor will go free now but the other will go to jail for 6 years. If both confess, then they both go to jail for 5 years. If neither confesses then they will both go to jail for only 1 year. So each player i has two possible strategies: to cooperate or defect. The payoffs, measured in the number of years of freedom that the player will enjoy over the next 6 years, as shown in Table 4.3.

Table 4.3: Prisoners' Dilemma game in strategic form

		Player I	
		cooperates	defects
Player II	cooperates	(5,5)	(0,6)
	defects	(6,0)	(1,1)

Players are the two friends. Each player has two strategies: cooperate and defect; "plea bargain" is the rule governing players's behavior; the numbers in the table are called payoffs, the player 1 payoff is listed first.

The Prisoner's Dilemma game illustrates both the benefits and the difficulties in achieving cooperation. To achieve the optimum solution, both players must trust the other. But trust involves the risk of being sucker.

From above example, it shows that the objective of this approach is to stimulate the players to cooperate, when the situation is competitive to everyone, and then find the optimal solutions for all. But when we try to find optimality, several

requirements of the problem need consideration:

1) Why different players should compromise with each other? 2) How a situation (selection of an agreed decision) is made meaningful, such that each player does not tend to deviate his strategy from the situation? 3) Which of the equilibria can be taken as an optimality principle convenient to all players?

To meet these requirements, however in this chapter, I choose Nash Equilibrium (will be presented in section 4.2.2) as the desired optimal point, due to its importance and properties in the context of non-cooperative optimization [55].

4.2.2 Nash Equilibrium

Intuitively, the Nash equilibrium is the point where no player in the game can improve his/her payoff by changing his/her own strategy, if all other players' strategies remain unchanged. In other words, the Nash equilibrium is the point where there is no incentive for players to change their strategies if there is no cooperation among them.

Definition 1. The situation $x^* = (x_1^*, \ldots, x_i^*, \ldots, x_n^*)$ [1] is called the Nash Equilibrium in the Game Γ, if for all nodes give strategies $x_i \in X_i$ and $i = 1, \ldots, n$ there is

$$U_i(x^*) \geqslant U_i(x^* \parallel x_i) \tag{4.1}$$

Remark. It follows from the definition of the Nash equilibrium situation that none of the nodes i is interested to deviate from the strategy x_i^*, (when such a node uses strategy x_i instead of x_i^* , its payoff may decrease provided the other nodes follow the strategies generating an equilibrium x^*). Thus, if the nodes agree on the strategies appearing in the equilibrium then any individual non-observance of this

[1] Note $(x_1, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_n)$ is an arbitrary nodes' strategy set in cooperative game, and x_i is a strategy of node i. I construct a nodes' strategy set that is different from x only in that the strategy x_i of node i has been replaced by a strategy $x_i^{'}$. As a result I have a nodes' situation $(x_1, \ldots, x_{i-1}, x_i^{'}, x_{i+1}, \ldots, x_n)$ denoted by $(x \| x_i^{'})$. Evidently, if node i's strategy x_i and $x_i^{'}$ coincide, then $(x \| x_i^{'}) = x$.

agreement is disadvantageous to such a node. In this chapter, I will simplify Nash Equilibrium as NE.

4.2.3 Nash Equilibrium Existence Theory

A strategic game G has at least one NE if $\forall i \in N$ the following conditions hold

- the set A_i of actions is non-empty, compact and convex subset of a Euclidean space
- the preference relation is continuous and quasi-concave on A_i.

4.3 Games from the Networks

Internet pricing is important because it has a competitive market, and regulating user traffic. The application of game theory in the Internet domain has been based primarily on the leader-follower framework in which the Internet service providers (ISPs) publish the price and customers react to that price. The task of the ISP is to strike a balance between the price and demand to maximize the provider's revenue. Cooperative game theory has been used to obtain a Nash bargaining framework to address issues like network efficiency, fairness, revenue maximization, and pricing [55]. Repeated non-cooperative games have also been used for market-based modeling for network resource management [35]. In most cases, the existence of a unique Nash equilibrium and its convergence using a decentralized approach has been studied. Game theory has also been used to study the pricing structure of a network service. To recover cost, network providers must understand user behavior and demands to offer different service plans. It has been shown how the network can behave as an active player in order to maximize its revenue. The network solely decides on the favorable operating point and forces the users accordingly. Similar approaches using game theory have been used to determine the Internet pricing model. For example, a pricing model proposed in [30] is for differentiated network services with one seller, one broker, and multiple users. The existence of a Nash equilibrium with two Internet service providers (ISPs) is studied in [5]. It has been

shown that cooperation between two ISPs benefits both of them as well as users. Indeed, a lot of progress has been made on Internet pricing since the relationship between congestion control and pricing was first introduced in [55].

Important parallels between peer-to-peer environments and ad hoc networks exist when considering the impact of selfish behavior on achieving socially-desirable equilibria. In peer-to-peer environment, the effectiveness of the system depends on the willingness of individuals to advertise and contribute files; in ad-hoc networks, the network may become partitioned unless nodes are willing to forward packets for others. In either case, in the absence of incentives, the equilibrium for the nodes is not to contribute to the network [24].

4.4 Basic Framework

Given a N-node wireless ad hoc network, the transmission radius is assumed to be identical for all nodes. A node can only directly communicate with the nodes which are inside its transmission range. Each node cannot receive more than one packets or cannot transmit and receive a packet simultaneously and I do not consider channel errors.

The basic setting of our non-cooperative node game (NCG) is set as : players are denoted by N mobile nodes in wireless ad hoc networks. x_i is defined as packet generation rate, which satisfies the bounds $0 < x_i \leqslant C_{max}$. C_{max} indicates maximum packet generation rate constraint. $S\{i\}$ is the set of routes in which node i is a source node. $R\{i\}$ is the set of routes in which node i is a relay node. t^m represents time slot m.

Let U_i denotes utility function for node i, u_i denotes the payoff function for node i. The latter is obtained by joining the game NCG as the usage of the network, formally expressed as the traffic successfully sent from individual node i. Here logarithmic function is used. In [29], it has been shown by Kelly that if the user payoff functions are logarithmic, then the maximization of the sum of the function leads to an allocation which has been termed as proportionally fair. And the allocation will be a Pareto optimum. This optimum is referred to as a social optimum [55].

$$u_i = \sum_{t=t^0, i \in S(i)}^{t=t^m} \ln(x_i) \tag{4.2}$$

Nodes access wireless Ad Hoc network through the air interface which is a common resource, so cost function ${C_i}^1$ is assigned to node i, which models the node's cost for sharing this common resource. Compensation function ${C_i}^2$ is also assigned to node i, which means, in order to induce voluntary forwarding, the rewards associated with forwarding should be compensated by the network. The cost function ${C_i}^1$ and compensation function ${C_i}^2$ are expressed separately as,

$${C_i}^1 = \alpha \sum_{t=t^0, i \in S(i)}^{t=t^m} x_i \tag{4.3}$$

$${C_i}^2 = \lambda \sum_{t=t^0, i \in R(i)}^{t=t^m} X_{-i} \cdot {p_i}^{sd} \tag{4.4}$$

Cost factor α represents the cost incurred per unit of packet size by node i as a source node. Compensation factor λ represents the compensation associated with per unit of packet size node i forwards for other nodes. p_i^{sd} is the probability the assigned packets are forwarded by node i from node s to node d, P_i^{sd} is the set of p_i^{sd} for node i.

Note that both "cost" and "compensation" do not refer to energy consumption, but a kind of an economic model. As the basic policy in our work,

1) when a node serve as a source node, from the viewpoint of the whole system, it is selfish, so it is asked to pay for some money to generate packets.

2) when a node serve as a relay node, from the viewpoint of the whole system, this transmit behavior should be encouraged, so it will gain some money once the relayed packets reach the correct destination successfully.

3) when a node serve as a destination node, we consider it will neither lose nor gain money.

Let us denote

$$U_i = u_i - C_i^1 + C_i^2 \tag{4.5}$$

$u_i, C_i{}^1, C_i{}^2$ are all functions of variable x_i. The objective of each node is to maximize its utility in a distributed fashion, considered as ,

$$(\mathbf{NCG}) max_{x_i \in X_i} U_i(x_i, X_{-i}) \tag{4.6}$$

Note that equation (4.6) demonstrates each mobile node wants to maximize total utility it accumulate over time by expending least expense. The final utility of each node depends on its own PGR strategy and also on the choice of other nodes' strategies. Since nodes are selfish and rational in nature, there is no guarantee that they will follow a particular strategy unless they are convinced that they that cannot do better by following some other strategy. It is necessary to characterize a set of strategies where the mobile nodes are satisfied with the utility they receive. Searching such a set of operating points called Nash Equilibrium is the main goal of this chapter.

4.4.1 Node Problem

The objective of each node is to maximize its net utility, which is the difference between the network utility and the cost of accessing the network, considered as,

$$max_{\{x_i\}}(x_i \prod_{j \in S\{i\}} {P_j}^{sd} - \alpha \sum_{i \in S\{i\}} ln x_i + \lambda \prod_{j \in R\{i\}} x_s {P_j}^{sd})$$
$$0 \leqslant x_i \leqslant MR. \tag{4.7}$$

4.4.2 Network Problem

The objective of network is that to determine the optimal packets generating rates to nodes that maximizes its total revenue, based upon the difference between charging and compensation for nodes,

$$max_{\{\underline{x}\}}(\alpha \sum_{i \in S\{i\}} ln \underline{x} - \lambda \prod_{j \in R\{i\}} x_s {P_j}^{sd})$$
$$0 \leqslant A\underline{x} \leqslant MR. \tag{4.8}$$

In this chapter, I assume all the nodes are "rational", which means nodes' behavior are totally determined by themselves. In the game, the nodes control their packet generating rates $\underline{x}$ and forwarding preferences $\underline{p}^{sd}$to optimize their utilities; the network controls cost coefficient α and compensation coefficient λ to maximize its revenue.

4.5 The Distributed Algorithm

In this section, I give an algorithm to compute NE of non-cooperative node game, and illustrate the implementation issue on ad hoc networks.

As mentioned above, the algorithm could easily be implemented as a local procedure (optimization of $U_i(\cdot)$). For the case of more general networks, I need to calculate the derivative of the utility function of equation 4.7. Then the problem is reduced to a single variable optimization problem: a node does an iterative step to compute its optimal packet generating rate. Thus, I compute the derivative with respect to equation 4.1,

$$\frac{dx_i}{dt} = \dot{x_i} = \frac{\alpha}{x_i} - \prod_{j \in S\{i\}} {P_j}^{sd} \tag{4.9}$$

Note that in the above expression I first assume that the packet forwarding probabilities ($\underline{p}$), "payment and compensation" factor of all the source nodes in the network are same initially and then compute the derivative with respect to this ($\underline{x}$). This is because during the computation the node must take both payment and compensation into account to get the optimal strategies.

Thus, solving the problem is reduced to a single variable optimization issue. A node does an iterative ascent to compute its optimal packet generating rate. Thus, in its k^{th} computation, a node i uses the iteration

$$x_i(k+1) = x_i(k) + \xi(k)(\frac{\alpha}{x_i(k)} - K \prod_{j \in S\{i\}} {P_j}^{sd}) \tag{4.10}$$

where $\xi(k)$ is a sequence of positive numbers satisfying the usual conditions imposed on the learning parameters in stochastic approximation algorithms, i.e.,

$\Sigma_k \xi(k) = \infty$ and $\Sigma_k \xi(k)^2 < \infty$. Note that it is possible that different nodes settle to different local maxima. I define here that the imposed "payment and compensation" policy ensures that all the node settle Nash Equilibrium (Nash Equilibria) in the highest packet generate rate.

However, in case of any change in the network, there will typically be some delay till a node completely recognizes the change. Note that it is possible that different nodes settle to different local maxima. I define here that the imposed "payment and compensation"" policy ensures that all the node settle Nash Equilibrium (Nash Equilibria)in the highest payoff. I am going to discuss the implementation issue of this algorithm in the following description.

Above algorithm requires a node to know neighborhood status around itself. In order to get effective knowledge about the network status in topology-blind ad hoc networks, feedback signals are included in the packet header to measure or estimate the network status. Simply to say, the feedback signals reflects the node willingness to pay α and network compensation factor λ. The iterations can be run at each network node using local information. In the following, I describe the local procedures associated with the scheme only with parameter α, because that compensation factor λ could be integrated in the packet header in a similar way.

Source Node Procedure:
1: The source node S sends a forward packet and inserts P_S^{SD} in the corresponding fields.
2: It sends the packets to the destination D.
3: At the reception of a backward packet with α, S adjusts its P_S^{SD}, according to α contained in the backward packet.
4: It is considered that S has a variable called P_S^{SD} which is updated as follows: $P_S^{dk} \longrightarrow P_S^{d(k+1)}$.

Relay Node Procedure:
1: Let $\underline{x}(0)$ be the initial N-vector of nodes' generating rates.
2: The source node S is associated with a cost factor α according to its packets generating rate. This is a global parameter of the system.
3: At the k iteration step of the game, S chooses a new packets generating rate according to equation 4.5.
4: S broadcasts the new packet generating rate to its neighbor.
5: All other nodes in the same session will likewise update their choice of forward probability strategies according to step 3.
6: Those nodes advertise their new forward probability according to their neighbors $\underline{x}(1)$.
7: S checks the currently active nodes, n_j;
8: S broadcasts the value of optimal strategy $\underline{x}*$ to all the active nodes;
9: If the session has changed (e,g, topology changed) go to back to 2; otherwise go back to step 3.

4.6 Case Study

As a simplified example, let us firstly consider an ad hoc network with 3 nodes, denoted by N_1, N_2, N_3. Transmission could be finished through one intermediate node or to the destination directly. N_1 has one unit packet to send to N_3, it sends its packet to other nodes and keeps its desired cost. N_2 also has packet to send to N_3. N_3 has no knowledge of whether N_1 or N_2 will send the packet directly to it or using a relay node. (Suppose the network cannot verify any claims the nodes might make about their strategies.)

Let $\underline{x}\{1,2\}$ represent the set of possible strategies that $N1$, $N2$ originally generate. The disagreement outcome is $U*(0,0)$, where the network gets neither contribution nor utility from the node, and the node gets no utility from the network. That is, each other could guarantee itself a payoff of 0 by refusing the cooperation. Then I have optimal strategies for $N1$, $N2$, the network separately as,

Depending on the value of x_3, $\frac{\partial U}{\partial \underline{x}}$ takes on different values:

$$\frac{\partial U_2}{\partial x_2} = \frac{\alpha}{x_2} - P_1^{23} \tag{4.11}$$

$$\frac{\partial U_1}{\partial x_1} = 1 - \frac{\alpha}{x_1} \tag{4.12}$$

Then I draw the conclusion that the strategy combination achieves a Nash Equilibrium $(x_1, x_2) = (\frac{\alpha}{1+\alpha}, \frac{\alpha}{1+\alpha})$ in the 3-node game, which means neither N_2 or N_3 can benefit by unilaterally deviating from this strategy combination.

Figure 4.1 illustrates how Nash Equilibrium is determined by using the payment and compensation function. In this example, the packet forward probability for $N1$ and $N2$ are both [0,1] and both x_1 versus U_2 and x_2 versus U_1 are plotted in the same figure. The intersection point of the two plots is a Nash Equilibrium, which means both N_1 and N_2 can benefit each other only when they use the forward probability strategy approaching 0.5.

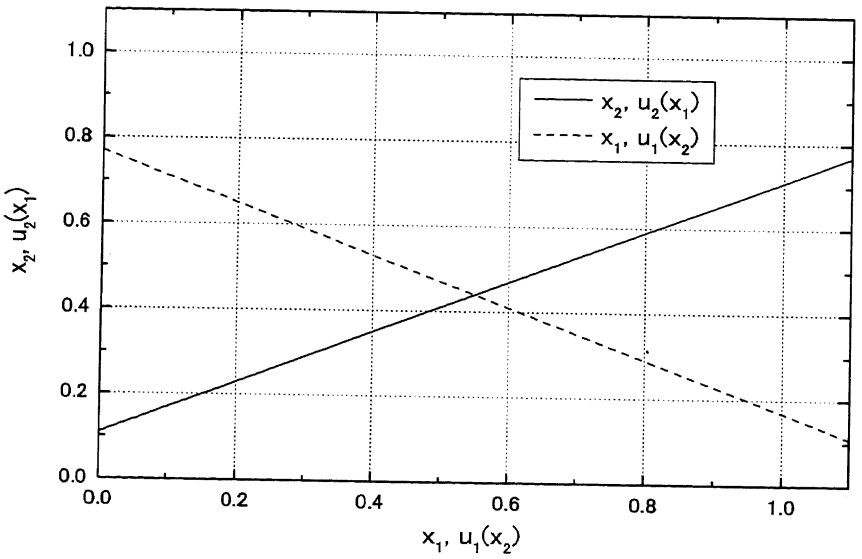


Figure 4.1: Nash Equilibrium in 3-Node game

4.7 Evaluation Results

In this section, I evaluate the performance of "payment and compensation" policy in a general setting, which is closer to the realistic topology scenario of wireless ad hoc networks.

4.7.1 Scenario

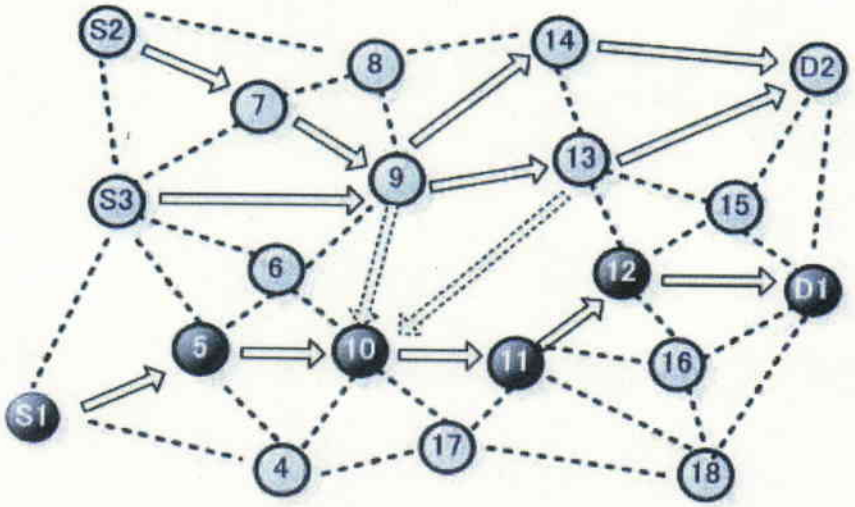


Figure 4.2: The packet forwarding graph of the random scenario

Table 4.4: Main Simulation Parameters

Parameters	Value
Space	$1000m \times 1000m$
Number of Nodes	20
MAC	802.11b
Cost Factor	0.1, 0.2, 0.3, 0.4, 0.5, 0.6
Compensation Factor	0.3, 0.5
Packet Generating Rate	Initial Value= 0.6packet/s
Packet Forward Probability	Initial Value=0.5
Strategy Updating Interval	1s
Simulation Time	300s

A network with 20 nodes is studied (Fig.4.2). It is located randomly according to a uniform distribution within a geographical area of 1000m by 1000m. The simulation parameters are listed in Table I. For each parameter, the default value and their varying range are provided. In the simulation, the network topology is high density and the moving speed of the nodes is rather low, so the packets drop rate could be ignored. Since the size of the packets is assumed to be the same, only the number of packets that are generated and forwarded will be considered.

The following process is repeated: nodes randomly choose a destination, and generate packets according to a Poisson process with the initial value 0.6packet/s. At each updating step, relay nodes decide whether to forward the packets as before, or to cease forwarding for a while. The decision is taken on the base of their current payoff function (equation 4.5): relay nodes observe the updating cost associated with the former packet generating rate for the new destination node. The new packet forward probability is chosen randomly. Considering the cost and compensation the nodes decide whether to generating own packet or to forward packet for other nodes in the next step. For each node, NE is defined as the point that results in the highest packet generate rate.

4.7.2 Metrics

The main metrics of the simulation is:

- Packet Forward Probability: computes the probability that the packets are successfully forwarded to the destination nodes.
- Individual Average Throughput: computes the accumulative packets that are originating from the node in 5s intervals.

4.7.3 Analysis of Results

In evaluation, node 1 is selected, as it is the most extreme source node in the network; and node 9 is also selected as it could represent the mobile nodes near the center of the network, which are frequently used as relay nodes. In Fig.4.3-4.5, both Nash

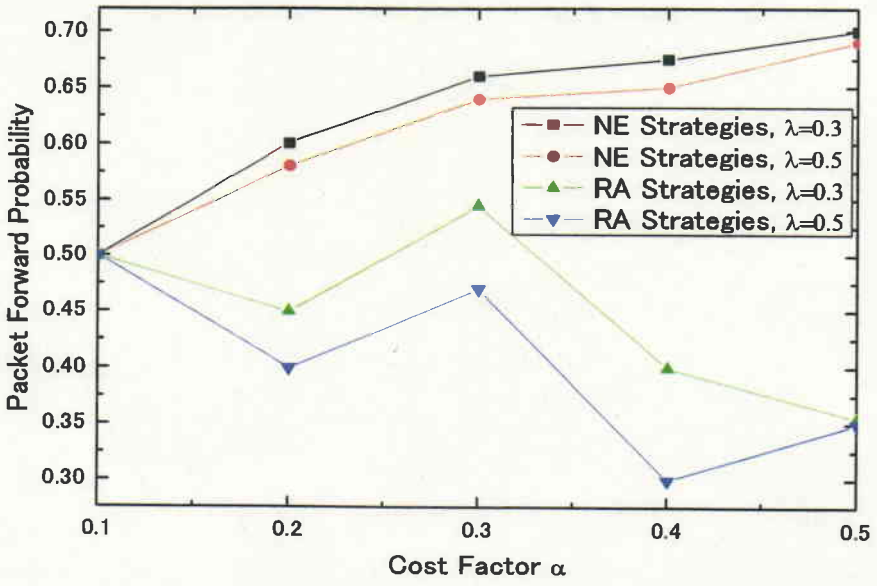


Figure 4.3: Individual Average Throughput, (Nash Equilibrium Strategies vs. Random Strategies)

Equilibrium (NE) strategy and Random (RA) strategy are used by node 1 and 9, cost factor α varies from 0 to 0.6 in step of 0.1, compensation factor is set to 0.3 and 0.5. It is obvious that the results for node 1 and 9 can be applied for the other nodes that locate in the similar area.

Fig.4.3 presents packet forward probability as a function of the cost factor α and compensation factor λ. It is seen that when using NE strategies, packet forward probability is much better than that when RA strategies are used, thus choosing NE strategies is beneficial than random strategies. In both cases, as the compensation factor λ increases, packet forward probability increases. This is due to the fact that when the cost factor α increases, the nodes are not interested in sending many packets, but when the compensation factor λ is high, the relay nodes become interested in forwarding the packets. At the same time, if the number of active sessions is low, nodes may operate far from the central region. However, as the value of α increases, which means the number of active session also increases. In order to reduce the number of sending packets in the network, the cost factor α should

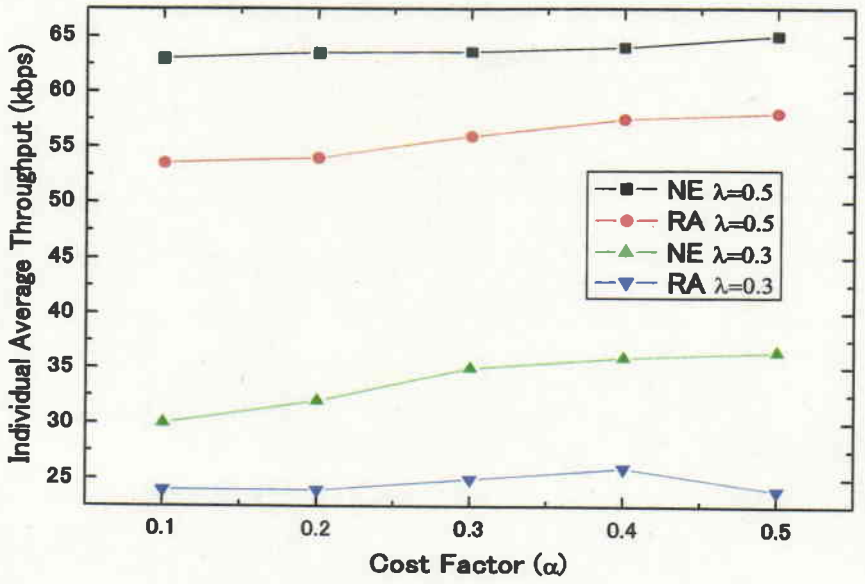


Figure 4.4: Packet Forwarding Probability, (Nash Equilibrium Strategies vs. Random Strategies)

increase. More nodes may have less incentive to send the packets. As the compensation factor λ increases, accordingly, it is a good incentive for the relay nodes to forward the packets.

It is observed from Fig. 4.4 that small values of λ lead to low individual average throughput. This is due to the fact that if the traffic is low, nodes will operate far from the central region and their strategies will not be strongly coupled. However, as the value of λ increases, the individual average throughput also increases. This is due to the fact that as λ increases, the compensation is more. Accordingly, there is less incentive for the nodes behave selfishly. This figure also shows individual average throughput as a function of the cost factor α with different λ value. It is found that using the NE strategies, individual average throughput is higher than that using cost strategies, thus choosing cooperation is more beneficial to the nodes than non-cooperative behavior.

4.8 Related Works

There has been recent research in modeling file sharing networks (such as enabled by KaZaA [63] and Gnutella [62]) using game theory. If the nodes in the file sharing network are assumed to be rational and homogeneous, the analysis leads to a Nash equilibrium in which nodes do not share their files, and their best strategy is to only download files and allow zero uploads. The result is not surprising, as most of the file sharing problems are modeled based on some variant of the prisoners' dilemma, which leads to socially non-optimal solutions. Note, however, that if this were the observed behavior of all the nodes participating in a peer-to-peer network, the network would cease to exist. Golle et. al [26] consider the presence of altruistic nodes (thereby some level of heterogeneity) in the network. In this heterogeneous network, not surprisingly, the Nash equilibrium is for the altruistic nodes to share their files, thereby leading to a better socially optimal state. To achieve a socially optimal equilibrium for a network with homogeneous nodes, different incentive mechanisms have been proposed in the literature. Marti et. al [34] include these incentives by establishing and maintaining a reputation index for every node in the network. Srinivasan et. al incorporate a tit-for-tat behavior based on past history of the other peers' behavior. It is interesting to note the significant overlap in the type of game theory that have been suggested to achieve social optimality in peer-to-peer and wireless ad hoc networks. Also, game theoretic based mechanisms [53] have been shown to be effective in solving the problem of misbehaving nodes in routing and forwarding. I also note that, since these incentive mechanisms require repeated interaction, it might be difficult to implement them effectively if the network exhibits high node mobility. Node mobility is a crucial consideration in repeated games, since it affects the chances of the nodes to play again with one another. It can improve the efficiency of the incentive mechanisms or lead to better decision making by the nodes, as I will show in the chapter 5.

4.9 Summary

In this chapter, a game theoretic approach is used to analyze non-cooperative nodes in wireless ad hoc networks. The proposed incentive scheme is based on a simple "payment and compensation" policy that can be implemented in a distributed system. From the simulation results, it is observed that selfish node behavior could be moved by the "payment and compensation" policy. The advantage of this proposed scheme is to lead to a less aggressive scenario where a node either generates all the own traffic, not forwarding any of the request, or forwards all the other nodes packets.

However, node-cheating behavior is not discussed in this chapter: Relay nodes are always interested in reporting a cheating cost to get a high compensation. Multiple players are interested in constituting a small group to be dishonest. It is well known that in a game theoretic approach, one player's payoff depends on the other player's strategies. Therefore, game theory is not appropriate to solve node-cheating problem. In the next chapter, I am going to use an incentive-based model to deal with this issue.

Chapter 5

A Price-demand Function based Incentive Model

5.1 Introduction and Motivation

By introducing an incentive policy "payment and compensation1", I found that the relay nodes are simulated to forward the packets, however game theory literature may not be directly applicable in an optimal pricing model. Incentive based pricing model may solve this problem and stimulate the relay nodes to forward the packets in the networks.

In this chapter, I propose a price-demand function based pricing model for non-cooperative nodes, called PDM, which focus on how to determine an optimal pricing model for incentive packet forwarding and encourage the relay nodes to honestly report their forwarding cost. Before formally introduce PDM, I explain the concepts that will be used in the chapter.

Mobile nodes access a wireless network through the air interface, which is a common resource, and each node's transmission is a source of interference for others.

Consider a given route (Fig.5.1) between the source node S and the destination node D of the form $(S, r_1, r_2, \ldots, r_j, D)$, where r_j is the j_{th} relay node in the route. This given route is called an S-D session. In Fig.5.1, suppose that S wants to send packets to D. S pays the relay nodes r_j when r_j forwards packets for S and r_j receives the money after successfully forwarding the packets. One way of implementing this

h

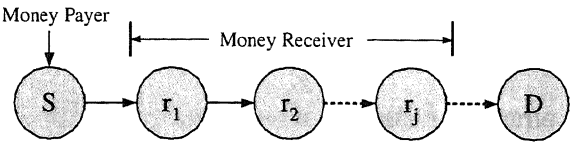


Figure 5.1: A Source-destination Session (S, r1, r2,..., rj, D)

charge and reward model is by introducing "virtual currency" as in [10]. In this method each node is rewarded with 'tokens' for providing service, which are then used by the node for seeking services from others. References such as [2, 9–11, 15, 17, 18, 25, 27, 36, 45, 47, 56] have also propose the use of incentive mechanisms. From the available incentive models I choose "Sprite" as a comparison reference [56] because that: 1) it is a general approach that models players' charge and credit as a welfare function; 2) it motivates each node to report its actions (submit the forwarding receipts to CCS) honestly. As it has a similar viewpoint as our work, it is reasonable to compare it with our approach. Note that the description of the "Sprite" below is limited to only the aspects that are relevant to this comparison. The details of the "Sprite" is in [56].

Zhong et al. developed the "Sprite" system, which uses the idea of credit to solve the problem of routing in ad hoc networks composed of self-interested nodes. The credit system presented therein subsumes all packet routing– the underlying ad hoc protocol only exists for packet delivery, not for routing decision making. To handle payment, the system relies upon a centralized credit clearance service (CCS), which handles receipt processing after nodes receive payment from others. Zhong et al. [56] model the receipt collection process as a game in which pricing ensures that truth-telling is an optimal strategy for all involved nodes.

In the "Sprite", a source node is charged in two ways. If the packet reaches the destination, the source node is charged by equation (5.1)

$$P_s = [(d-1)\alpha + \beta] \tag{5.1}$$

where P_s is the charge of the source node S, d is the number of hops from the

first relay node to the last relay node on the S-D session, $d \geqslant 1$, β is the payment to the last relay node that successfully forwarded the packet, α is the payment to the relay node before the last one, and $\alpha > \beta$.

Otherwise if the packet does not reach the destination node, the charge for the source node is calculated by equation (5.2),

$$P_s = [((d-1)\alpha + \beta - (d-e)\gamma\beta)] \tag{5.2}$$

where e is the number of the relay node who last successfully forwards the packet, γ is a multiplier parameter and $\gamma < 1$.

In particular, "Sprite" studies three cheating behaviors of a selfish node: 1) After receiving a message, the node saves a receipt but does not forward the message; 2) The node has received a message but does not report the receipt; 3) The node does not receive a message but falsely claims that it has received the message.

I summarize the major disadvantages in "Sprite" is that:

1) The major metric to evaluate the performance of "Sprite" is the packet success rate, i.e., the percentage of packet successfully relayed from the sender to the destination. How to fine-tune the payment parameters to optimize the system performance is not well illustrated. This is an important problem, since efficiently utilize the limited budget is necessary for the source nodes.

2) "Sprite" studies three cheating behaviors of the relay nodes. However, to get more payoff from the source nodes, the relay node may also dishonestly report its forwarding cost. "Sprite" does not analyze this aspect.

5.2 Preliminaries

5.2.1 Who pays whom

Before determining the amount of credit or charge to each node, the two basic questions are discussed in [56]. The first question is who pays whom. Considering forwarding a packet from a sender to a destination as a transaction, I need to decide who should be charged for the packets and who should receive credit for relaying the packets. Although I can charge the destination, I decide that charging the sender

will be a more robust and general approach. There are two reasons for charging only the sender. First, charging the destination may allow other nodes to launch a denial-of-service attack on the destination by sending it a large amount of traffic. Even sharing the cost between the sender and the destination could have a similar problem, because the sender could collude with the intermediate nodes, who could secretly return the sender's payment back, so that only the destination pays for the traffic. On the other hand, if only the sender is charged, a node will not have incentive to send useless packets. Second, if the destination benefits from the content of a packet and thus should pay for it, the sender can get compensation from the destination, for example, through an application-layer payment protocol. Given these reasons, only the sender will be charged in PDM.

A closely related question is who will receive credit for forwarding a packet. Ideally, any node who has ever tried to forward a packet should be compensated because forwarding a packet will incur a cost to the node, no matter successful or not. However, a forwarded packet may be corrupted on the link, and there is no way to verify that the forwarding action does occur. Although some local wireless networks such as IEEE 802.11 do provide link layer acknowledgments, such acknowledgment schemes are not universal and I refrain from changing basic network functions. Given this decision, the credit that a node receives will depend on whether or not its forwarding action is successful - the forwarding is successful if and only if the next node on the path receives the packet.

5.2.2 Price-Demand Functions

The demand of a product in a market is related to its price. Usually, when the price is low, the demand is high. A price-demand function embodies the above relationship between quantity demanded by consumers and market prices. Let p denote a market price and Q a quantity demanded in a ceratin market; their relationship is given by a price-demand function $p(Q)$. One example of price-demand function $p(Q)$ (Fig. 5.2) is said to be linear if it takes the form of the equation (5.3) [43],

$$p(Q) = a - bQ \tag{5.3}$$

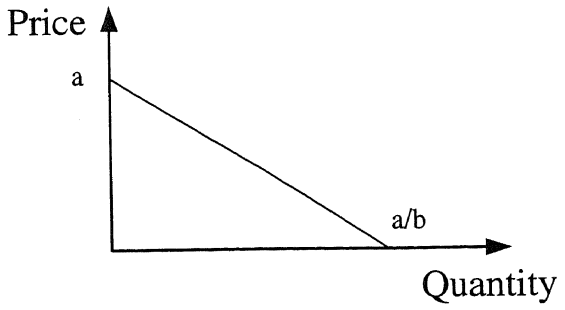


Figure 5.2: Linear price-demand function

where a and b are constant values, $a > 0, b > 0$, and they are determined by consumers according to their service request. In this chapter, I choose this liner price-demand function to describe the service demanded by the source nodes.

In this chapter, the consumer is the source node and the forwarding service provided by the relay node is the goods. The parameters a, b in the price-demand function are determined by the source nodes. Here, I suppose that the parameters are private to source nodes, which means that the source node is free to choose its favorite a and b value (The exact explanation for the choice of a, b will be presented in Section 4.3, 4.4). The demand (Q) is defined as the amount of traffic a source node requests relay nodes to send to a destination node (i.e. number of packets). The price (p) is the reward to a relay node for forwarding one unit of traffic (i.e. \$/packet). The price (p) is determined by the demand of the source nodes and the forwarding service of the relay nodes.

5.2.3 Forwarding Cost

Packet forwarding imposes resource costs on the relay nodes. Resource costs include energy consumption, CPU usage, etc. In this chapter, the forwarding cost C_{r_j} is a monetary resource cost, as measured by the following equation for a relay node r_j:

$$C_{r_j} = \alpha \cdot c_{r_j} \tag{5.4}$$

Where α is defined as monetary compensation for the unit resource cost. c_{r_j} is the unit resource cost of forwarding one unit of packets through node r_j. Clearly,

each relay node has its own resources. However, since recharging the battery can be gradual, I expect that the resource cost is relatively stable. I also allow each relay node to determine its own forwarding costs. In this chapter, I assume that each node does not know the others' forwarding costs.

5.2.4 Payoff of a Relay Node

In PDM, the payoff of a relay node corresponds to the received payment minus the incurred forwarding cost, computed as:

$$U_{r_j}(p_j) = (p_j - C_{r_j})Q_s \tag{5.5}$$

where p_j is the price requested by the relay node r_j, C_{r_j} is the forwarding cost of relay node r_1, Q_s is the traffic sent from the source node S. The relay node r_j will try to improve the price to maximize its final payoff. In section 4, I will illustrate how the price p_j is determined.

In PDM, to utilize the source nodes' money budget efficiently and compensate the relay node for its forwarding cost, I model the network as a market, where prices are determined by the source node's demand and the relay node's service supply. The routes between the source nodes and the destination nodes are pre-determined by some routing protocol (e.g. AODV).

In an incentive model, the final payoff for any relay node should be greater than its forwarding cost [56]. This condition is necessary, because if the compensation is smaller than or equal to the cost, it is not attractive for the relay node to be cooperative. Since the nodes might be selfish, without a proper payment model, they may try to cheat the system to get a larger payoff. An important advantage of PDM is that honestly reporting the forwarding costs is an optimal strategy for the relay nodes. In sections 5.1 and 5.2, I first explain PDM for the single relay node session, and then extend it for the multiple relay node session. In section 5.3, I explain the pricing protocol for the PDM.

5.3 Description of PDM

5.3.1 Price Resolution for a Single Relay Node Session

First, consider an S-D session (Fig.5.3) that there is only one relay node.

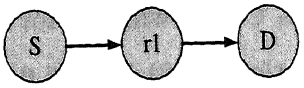


Figure 5.3: A Single Relay Node Session

By equation 5.5, the payoff for the relay node r_1 is computed as

$$U_{r_1}(p_1) = (p_1 - C_{r_1})Q_s \tag{5.6}$$

where p_1 is the price requested by r_1, C_{r_1} is the forwarding cost of r_1, Q_s is the traffic sent from S.

Since there is only one relay node in the session, r_1 will try to increase the price to maximize its payoff. According to the source node's price-demand function equation 5.3, the single relay node's motivation is expressed by

$$max\{U_{r_1}(p_1)\} = max\{(p_1 - C_{r_1})\frac{(a_s - p_1)}{b_s}\} \tag{5.7}$$

where a_s and b_s separately represents the parameters a and b of the source node S's price-demand function. From equation 5.7, S can calculate the optimal price p_1^o by

$$p_1^o = \frac{a_s + C_{r_1}}{2}. \tag{5.8}$$

According to equation (5.3) and (5.8), the optimal number of packets Q_s^o is calculated by

$$Q_s^o = \frac{a_s - C_{r_1}}{2b_s} \tag{5.9}$$

and p_1^o, Q_s^o should satisfy the source node's budget constraint in the form

$$p_1^o Q_s^o \leqslant M_s \tag{5.10}$$

where M_s represents the source node S's money budget. Therefore, the pricing model for a single relay node session is constituted by equations (5.8), (5.9), and (5.10).

Proposition 1. In a single relay node session, if $a_s \leqslant C_{r_1}$, then the relay node r_1 will not forward the packets for the source node; if the relay node r_1 receives packets more than Q_s^o, it will drop the packets.

Proof. I first prove that in a single relay node session, if the relay node receives information that $a_s \leqslant C_{r_1}$, it will not forward the packets for the source node.

Substituting equations (5.8) into (5.6), the payoff for r_1 is given as follows:

$$U_{r_1} = (p_1^o - C_{r_1})Q = [\frac{(a_s + C_{r_1})}{2} - C_{r_1}]Q. \tag{5.11}$$

For equation (5.11), if $a_s \leqslant C_{r_1}$, then $U_{r_1} \leqslant 0$, i.e., is that r_1 gets a negative payoff, which is not a good result for r_1. Therefore, the relay node can not accept this packet forward request if $a_s \leqslant C_{r_1}$.

Similarly, substituting equations (5.9) into (5.6), I could prove that if the relay node forwards packets more than Q_s^o, its payoff will be smaller than the maximum value. Since it is the single relay node in the session and its motivation is to maximize the payoff, when its payoff is smaller than the maximum value, it will not continue forwarding the packets.

Proposition 1 states that in order to guarantee that r_1 has a positive payoff, it is necessary that a_s be greater than C_{r_1}. If r_1 receives $a_s \leqslant C_{r_1}$, it does not reply to the packet forward request, because the price determined by equation (5.8) does not cover its forwarding cost.

Definition 1. For a relay node, an optimal strategy is one that guarantees a highest and positive payoff to the relay node.

Proposition 2. If only one relay node exists in an S-D session, where the source node keeps the same price-demand function, reporting the true forwarding cost is an optimal strategy for the relay node.

Proof. Let us suppose that r_1 tries to report a cheating forwarding cost $\hat{C_{r_1}}$ and gets a corresponding cheating payoff $\hat{U_{r_1}}$. Denote r_1's true payoff and true forwarding cost as U_{r_1} and C_{r_1}.

Since the source node S keeps the same price-demand function in the session, once the relay node's cheating forwarding cost $\hat{C_{r_1}}$ is reported to the source node, by equations (5.8) and (5.9), both the price $\hat{p_1}$ and the optimal number of packets

$\hat{Q}$ change, whereas r_1's true forwarding cost C_{r_1} is not changed. Then r_1's cheating payoff $\hat{U_{r_1}}$ is obtained by

$$\hat{U_{r_1}} = (\hat{p_1} - C_{r_1})\hat{Q} = [\frac{(a_s + \hat{C_{r_1}})}{2} - C_{r_1}]\frac{(a_s - \hat{C_{r_1}})}{2b_s}. \tag{5.12}$$

r_1's true payoff is expressed as

$$U_{r_1} = (p_1 - C_{r_1})Q = [\frac{(a_s + C_{r_1})}{2} - C_{r_1}]\frac{(a_s - C_{r_1})}{2b_s}. \tag{5.13}$$

Now I compare r_1's true payoff U_{r_1} with its cheating payoff $\hat{U_{r_1}}$ as

$$\hat{U_{r_1}} - U_{r_1} = \frac{-(C_{r_1} - \hat{C_{r_1}})^2}{4b_s} < 0. \tag{5.14}$$

From equation (4.14), I see that r_1's cheating payoff $\hat{U_{r_1}}$ is always lower than its true payoff U_{r_1} if it reports a cheating forwarding cost $\hat{C_{r_1}}$, no matter with $\hat{C_{r_1}} > C_{r_1}$ or $\hat{C_{r_1}} < C_{r_1}$. As a result, it is obvious that the r_1 can not get a better payoff if it tries to cheat with a different forwarding cost.

Proposition 2 states that in a single relay node session, reporting the true forwarding cost is the optimal strategy for the relay node.

5.3.2 Price Resolution for a Multiple Relay Node Session

I extend the above discussion to an S-D session with more than one relay node. In a multiple relay node session, when the source node's price-demand function satisfies equation (5.3), it may be impossible to maximize the payoff for every relay node if they have different forwarding costs. However, to ensure a steady traffic from the source nodes and give a non-negative payoff to each relay node, the pricing model should also reflect both the source node's demand and the relay nodes' forwarding costs. Here I assume that the nodes are selfish but rational, which means since each relay node realize it is impossible to maximize all of their payoffs in a multiple relay node session, and then a non-negative payoff is also acceptable for them, because a non-negative payoff is better than no payoff for forwarding the packets.

In a multiple relay node session, PDM is expressed by equations (5.15),(5.16)and(5.17), which is similar to the one described in single relay node session. The price p_j^o for relay node r_j is determined by equation (5.15). The optimal number of packets sent

by the source node Q_s^o is calculated by equations (5.16), where Q_s^o is calculated by the source node using the highest forwarding cost of all the relay nodes. In equation (5.16), $max(C_{r_j})$ represents the highest forwarding cost of all the relay nodes; a_s and b_s are the parameters of the source node's price-demand function. In equation (5.17), M_s is the money budget of the source node S.

$$p_j^o = \frac{a_s + C_{r_j}}{2} \tag{5.15}$$

$$Q_s^o = \frac{a_s - max(C_{r_j})}{2b_s} \tag{5.16}$$

$$(\sum_j p_j^o) Q_s^o \leqslant M_s \tag{5.17}$$

Note that in a multiple relay node session, each relay node has a different forwarding cost, therefore the maximum payoffs are not guaranteed for all the relay nodes. However, if each relay node wants to decide Q_s^o so that the payoff is maximized for itself, the other relay node may get a negative payoff. To solve the problem, I let Q_s^o be calculated by the source node. The source node calculates Q_s^o according to its own price-demand function and the highest forwarding cost reported by all the relay nodes. However, one problem with this calculation is that the relay nodes may dishonestly report their forwarding cost to maximize their own payoffs. In Proposition 4, I will show this problem could be solved by the PDM, since it is able to encourage the relay nodes to honestly report their forwarding cost.

Proposition 3. In a multiple relay node session, if $a_s > max(C_{r_j})$, the pricing model (15), (16), and (17) guarantees that all the relay nodes' payoffs are greater than 0 and at least one relay node has a maximum payoff; if $a_s \leqslant max(C_{r_j})$, the source node' packets can not reach the destination node.

Proof. I first prove that the pricing model guarantees that each relay node's payoffs are greater than 0. The payoff for any relay node r_j is calculated by

$$\begin{aligned} U_{r_j} &= (p_j^o - C_{r_j}) Q_s^o \\ &= [\frac{(a_s + C_{r_j})}{2} - C_{r_j}][\frac{a_s - max(C_{r_j})}{2b_s}] \\ &= [\frac{(a_s + C_{r_j})}{2} - C_{r_j}][\frac{a_s - C_{r_k}}{2b_s}] \end{aligned} \tag{5.18}$$

where C_{r_k} is the highest forwarding cost in the session reported by r_k. If $a_s > max(C_{r_j})$, then $U_{r_j} > 0$, which proves that the r_j's payoff is greater than 0.

Next, I prove that the pricing model guarantees at least one relay node has a maximum payoff. I compute r_k's payoff. Since Q_s^o is determined by C_{r_k} (equation (5.16)), it is easy to prove

$$(p_k^o - C_{r_k})Q_s^o = max(U_{r_k}) \tag{5.19}$$

where $max(U_{r_k})$ is r_k's maximum payoff.

Finally, I prove that if $a_s \leqslant max(C_{r_j})$, the source node' packets can not reach the destination node. If $a_s \leqslant max(C_{r_j})$, then for r_k, its payoff $U_{r_k} \leqslant 0$. Therefore r_k will not forward the packets for the source node, then the source node's packets can not reach the destination node.

Proposition 3 states that the source node could decide its a_s on the basis of the relay nodes' forwarding cost. Once a_s is determined, Q_s^o is computed by equation (5.17).

Proposition 4. In one multiple relay node session, where the source node keeps the same price-demand function, if the rational relay nodes do not know the other's forwarding cost, honestly reporting the forwarding cost is an optimal strategy for each relay node.

Proof. To discuss the outcomes of cheating reports for each relay node, let us consider an S-D session of the form $(S, r_1, \ldots, r_j, \ldots, r_k, D)$, where r_k is the relay node with the highest forwarding cost in the session, and r_j is any of the relay nodes except r_k, such that $C_{r_j} < C_{r_k}$. By proposition 3, assume that a_s is higher than C_{r_k}.

From equation (5.18), I see that a relay node's payoff depends on the behaviors of three nodes in the session: the source node, the relay node with the highest forwarding cost (denoted as HRN) and itself. Since the source node keeps the same price-demand function in the session, then a relay node's payoff only changes with the various behaviors of itself and HRN, no matter with what the other relay nodes do. As a result, I could simply discuss the outcome of the cheating reports for two representative relay nodes r_k and r_j.

Firstly, I focus on the relay node r_k. Denote that r_k reports a higher forwarding cost $\hat{C_{r_k}^1}$, such that $C_{r_k} < \hat{C_{r_k}^1}$; the corresponding cheating payoff is $\hat{U_{r_k}^1}$. Denote

that r_k reports a lower forwarding cost $\hat{C}^2_{r_k}$ or $\hat{C}^3_{r_k}$, such that $C_{r_{k-1}} < \hat{C}^2_{r_k} < C_{r_k}$ or $\hat{C}^3_{r_k} < C_{r_{k-1}} < C_{r_k}$, where $C_{r_{k-1}}$ is the second highest forwarding cost in the session. The corresponding payoffs are $\hat{U}^2_{r_k}$ and $\hat{U}^3_{r_k}$.

Case 1 of r_k: r_k reports a cheating forwarding cost $\hat{C}^1_{r_k}$. Since it reports the highest forwarding cost from all the relay nodes to the source node, now I compare $\hat{U}^1_{r_k}$ with U_{r_k},

$$\hat{U}^1_{r_k} = [\frac{(a_s + \hat{C}_{r_k})}{2} - C_{r_k}]\frac{(a_s - \hat{C}^1_{r_k})}{2b_s} \tag{5.20}$$

$$U_{r_k} = [\frac{(a_s + C_{r_k})}{2} - C_{r_k}]\frac{(a_s - C_{r_k})}{2b_s} \tag{5.21}$$

then

$$\hat{U}^1_{r_k} - U_{r_k} = \frac{-(C_{r_k} - \hat{C}^1_{r_k})^2}{4b_s} < 0 \tag{5.22}$$

Equation (5.22) shows that if r_k reports a cheating forwarding cost $\hat{C}^1_{r_k}$, it gets a lower payoff than if it claimed the true forwarding cost C_{r_k}. A similar proof can be derived for $\hat{C}^2_{r_k}$. Therefore, r_k has no reason to report $\hat{C}^1_{r_k}$ or $\hat{C}^2_{r_k}$.

Case 2 of r_k: if r_k reports a cheating forwarding cost $\hat{C}^3_{r_k}$, such that $\hat{C}^3_{r_k} < C_{r_{k-1}} < C_{r_k}$, then Q^o_s is calculated by the $C_{r_{k-1}}$:

$$\hat{U}^3_{r_k} = [\frac{(a_s + \hat{C}_{r_k})}{2} - C_{r_k}]\frac{(a_s - C_{r_{k-1}})}{2b_s} \tag{5.23}$$

$$\begin{aligned}
\hat{U}^3_{r_k} - U_{r_k} &= \frac{(a_s + \hat{C}^3_{r_k} - 2C_{r_k})(a_s - C_{r_{k-1}})}{4b_s} \\
&\quad - \frac{(a_s - C_{r_k})^2}{4b_s} \\
&< \frac{(a_s - C_{r_k})(a_s - C_{r_{k-1}}) - (a_s - C_{r_k})^2}{4b_s} \\
&= \frac{(a_s - C_{r_k})(C_{r_k} - C_{r_{k-1}})}{4b_s}
\end{aligned} \tag{5.24}$$

From equation (5.24), it is clear to see when $C_{r_{k-1}} < a_s < C_{r_k}$, $\hat{U}^3_{r_k} < U_{r_k}$. However, since $\hat{C}^3_{r_k} < C_{r_{k-1}} < C_{r_k}$, then $\hat{C}^3_{r_k} < C_{r_{k-1}} < a_s$. By Proposition

3, r_k still has to forward the packets for the source node. It is not a desired outcome for r_k. Obviously, r_k will not report a forwarding cost $\hat{C}^3_{r_k}$.

In summary, an optimal strategy for r_k is to honestly report its forwarding cost C_{r_k}.

Now I consider the relay node r_j, where $C_{r_j} < C_{r_k}$. r_j may report a high forwarding cost with two possibilities $C_{r_j} < C_{r_k} < \hat{C}^1_{r_j}$ or $C_{r_j} < \hat{C}^2_{r_j} < C_{r_k}$, and a low forwarding cost $\hat{C}^3_{r_j} < C_{r_j} < C_{r_k}$. I separately denote their corresponding payoffs as $\hat{U}^1_{r_j}, \hat{U}^2_{r_j}, \hat{U}^3_{r_j}$.

Case 1 of r_j: r_j reports a cheating forwarding cost $\hat{C}^1_{r_j}$, such that $C_{r_j} < C_{r_k} < \hat{C}^1_{r_j}$. Since $\hat{C}^1_{r_j}$ is the highest forwarding cost in the session, thus Q^o_s is changed. Then I get,

$$U_{r_j} = [\frac{(a_s + C_{r_j})}{2} - C_{r_j}]\frac{(a_s - C_{r_k})}{2b_s} \tag{5.25}$$

$$\hat{U}^1_{r_j} = [\frac{(a_s + \hat{C}^1_{r_j})}{2} - C_{r_j}]\frac{(a_s - \hat{C}^1_{r_j})}{2b_s} \tag{5.26}$$

From equation (5.26), it is clear to see when r_j reports $\hat{C}^1_{r_j}$, such that $C_{r_k} < a_s < \hat{C}^1_{r_j}$, r_j gets the cheating payoff $\hat{U}^1_{r_j} < 0$ (the source node will not send the packets in this session). However, by equation (5.25), C_{r_j} guarantees a positive payoff to r_j. Therefore, as a rational node, r_j has no incentive to report $\hat{C}^1_{r_j}$.

Case 2 of r_j: r_j reports a cheating forwarding cost $hat C^2_{r_j}$, such that $C_{r_j} < \hat{C}^2_{r_j} < C_{r_k}$. From equation (5.16), since C_{r_k} is still the highest forwarding cost in the session, Q^o_s will not change, then

$$\hat{U}^2_{r_j} = [\frac{(a_s + \hat{C}^2_{r_j})}{2} - C_{r_j}]\frac{(a_s - C_{r_k})}{2b_s} \tag{5.27}$$

$$\hat{U}^2_{r_j} - U_{r_j} = \frac{(\hat{C}^2_{r_j} - C_{r_j})(a_s - C_{r_k})}{4b_s} \tag{5.28}$$

Equation (5.28) shows that if r_j knows the exact value of C_{r_k}, then reporting $\hat{C}^2_{r_j}$ may bring it a higher payoff (if $C_{r_j} < \hat{C}^2_{r_j} < C_{r_k} < a_s$, then $\hat{U}^2_{r_j} > U_{r_j}$). But if r_j does not know C_{r_k}, once $\hat{C}^2_{r_j}$ is reported higher than C_{r_k}, r_j may obtain a negative payoff, as I show in case 1 of r_j. Therefore, $\hat{C}^2_{r_j}$ is not an optimal strategy for r_j.

Case 3 of r_j: r_j reports a cheating forwarding cost $\hat{C}^3_{r_j} < C_{r_j} < C_{r_k}$. Since the lower forwarding cost does not change Q^o_s, but instead cuts the price p^o_j. From equation (5.30), it is easy to see that r_j's cheating payoff is lower than its true payoff. Therefore, r_j has no incentive to report $\hat{C}^3_{r_j}$.

$$\hat{U^3_{r_j}} = [\frac{(a_s + \hat{C^3_{r_j}})}{2} - C_{r_j}]\frac{(a_s - C_{r_k})}{2b_s} \tag{5.29}$$

$$\hat{U^3_{r_j}} - U_{r_j} = \frac{(\hat{C^3_{r_j}} - C_{r_j})}{2}Q^o_s < 0 \tag{5.30}$$

In summary, if r_j does not know C_{r_k}, then reporting the true forwarding cost is an optimal strategy for it.

As a conclusion, reporting an honest forwarding cost will certainly bring a positive payoff to the relay node, but reporting a cheating forwarding cost can not guarantee a positive payoff to the node, as shown by the analysis for r_k and r_j. Since each relay node's payoff only depends on the behaviors of itself and HRN, the cheating behaviors of any other relay node has no effect on it. Consequently, the analysis for one cheating node could be straightforwardly extended to the multiple cheating nodes' case. Therefore, being a rational node, an optimal strategy is to honestly report its forwarding cost, no matter with what the other relay nodes do.

Proposition 4 states that if a rational relay node does not know the other's forwarding cost, an optimal strategy is to report its true forwarding cost to the source node.

5.4 A Pricing Protocol for PDM

5.4.1 Protocol for the Pricing Procedure

I assume that PDM working on top of AODV routing protocol. In the PDM, a source node that has the packets to send initially broadcasts RREQ in the network. Each node receiving the RREQ checks whether it is the destination node. If it is not the destination node, it forwards the request and broadcasts it again. The destination node sends back a route reply message RREP after it receives the RREQ. The RREP

is forwarded on a reverser route to the source node and each relay node along the route inserts its forwarding cost in the RREP message. Here I assume that each relay node does not know the other's forwarding cost. An existing security system can deal with this issue [9].

The source node decides its parameters a_s, b_s of price-demand function (equation 5.3) according to the relay nodes' forwarding costs (or chooses any parameters it likes) and inserts a_s, b_s in a data packet header. After the route is established, the source node can send its packets on it. The payment of each forwarding node is only delivered after a packet is received at the intended destination. Note that the work here focuses on the pricing model, whereas the previous works [2, 9] deal with the payment issue.

To illustrate this pricing procedure, let us consider an S-D session with three relay nodes. Assume that each relay node reports a different forwarding cost, e.g., $C_{r_3} < C_{r_2} < C_{r_1}$, to the source node, and the source node keeps the same price-demand function in the session. The pricing procedure in the session is shown in Fig.5.4.

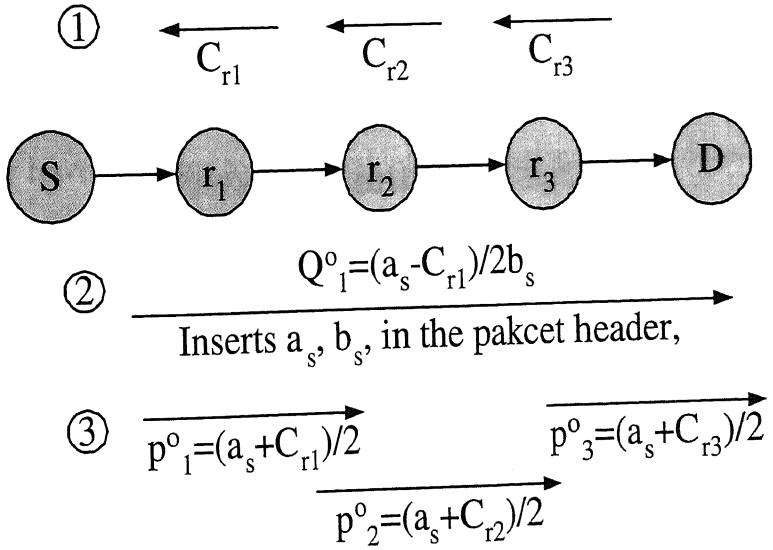


Figure 5.4: A Three-Relay-Node Session

5.4.2 Protocol for the Payment

In PDM, for each session, the source node payment is equal to the sum of all relay nodes' payoff. After one session is finished, the source node could establish a new session. In the new session, it may determine same or different price-demand functions. Then, the pricing model is calculated by the source node's new price-demand function and the new relay nodes' forwarding costs. For the complete sessions, after the nodes successfully send the packets to the destination nodes, their total money budgets reduce. However, the nodes' money budgets are added if they successfully forwarded the packets. For each node, once its money budget is used up, it can not send the packets until it accumulates enough budgets.

5.4.3 Protocol for the Route Selection

If there are multiple routes between a source node and a destination node, the source node could collect all the relay nodes' forwarding costs among the multiple routes. And then it calculates the payments and the optimal number of sending packets for each route. Finally, according to the source nodes' demand (either the lowest payment or the largest number of sending packets), it chooses one route to send the packets.

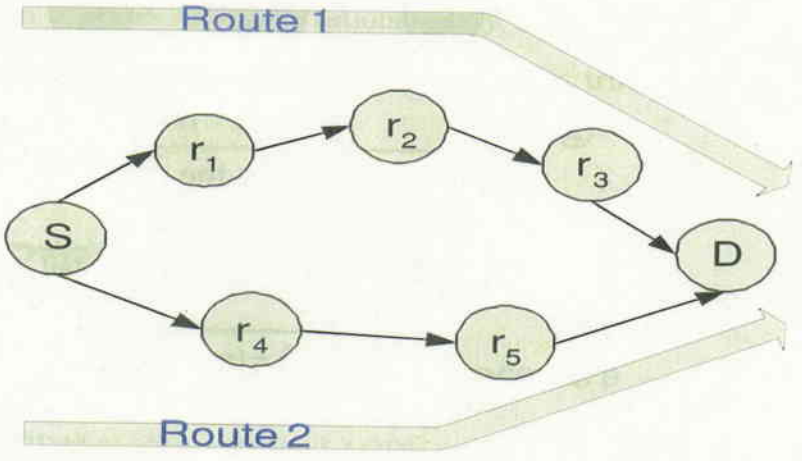


Figure 5.5: Protocol for the route selection

Then what will happen if charge is paid for every single forwarding? A way to

discourage lying is to incorporate a sense of loyalty when discovering routes. Price or route rediscovery is quite a time consuming process. A source node should not rediscover routes every time the routes in its cache become a little bit more expensive. So small price increase is tolerable. When discovering routes, nodes would tend to pick the cheapest routes unless an aspect of the more expensive one is desired. This creates an incentive for nodes to publish zero-price (when they are not busy). When the nodes are getting busier later, they can increase their price, and if they are still within a limit, the clients would stay with it. They can also pick cheaper routes in its cache, but that route would still be kept in the caches. Basically, there is an incentive to be in many nodes' route cache. Nodes that lie about how busy they are would not get picked in the initial price discovery process, and would not have the chance to get picked until the next price rediscovery. This idea has a problem in that nodes can offer low price initially, but after a short while increase their price within a limit that won't force route discovery, even when they are still idle. This can be prevented by giving newly discovered paths for a trial period, so that paths that change its price after just recently being incorporated into the route cache would be invalidated. The source node can then choose other routes in its route cache. While price rediscovery shouldn't be done too often so that overhead is minimized, and unpaid work is encouraged; it should be often enough so that nodes that are honestly busy have a chance to be picked later. Additionally, the decision of whether to pick another route in the cache when the current route increases its price should consider two factors. The first is the increased amount, and second is the fact that staying with previously used routes that have been proven to be reliable is desirable. This idea of incorporating loyalty in route discovery hasn't been proved to be free from cheating.

5.5 Simulation Setup

5.5.1 Simulation Parameters

I ran simulations on ns-2 [64]. The setup consisted of 10 nodes that were uniformly distributed in an area of 500×500 meters and 30 nodes in a an area of 1000×1000

meters. All simulations used a fixed topology. In 10 nodes scenario, traffic was sent from 5 source nodes to 5 destination nodes (5 S-D sessions): nodes 1,2,4,5,7, and 9 were randomly selected as source nodes. In 30 nodes scenario, traffic was sent from 10 source nodes to 10 destination nodes: nodes 0,2,5,7,9,12,15,18,21,26, and 28 were randomly selected as the source nodes. Destination nodes and relay nodes were chosen randomly from all the nodes. At the start of each S-D session, the source nodes sent CBR traffic. The relay node's forwarding strategy was considered that once their forwarding costs were covered by the source nodes, they did not drop the packets. In the simulation, I assume that the forwarding cost of each node is fixed and different, as listed in Tables 5.1 and 5.2. I used AODV as the routing protocol. Total simulation time was 600s. Table 5.3 lists the simulation parameters.

Table 5.1: Forwarding Cost (FC) of Each Node (N) in 10 Nodes Simulation

N	0	1	2	3	4	5	6	7	8	9
FC	0.05	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9

5.5.2 Metric

I measured the simulation results by the source node payment when they sends the packets in each session, which is defined as follows,

In the Sprite model, for each session, the source node payment is defined by equations (5.1) and (5.2). Since the source node payment should cover all the relay

Table 5.2: Forwarding Cost (FC) of Each Node (N) in 30 Nodes Simulation

N	0	1	2	3	4	5	6	7	8	9
FC	0.05	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9
N	10	11	12	13	14	15	16	17	18	19
FC	1.0	1.1	1.2	1.3	1.4	1.5	1.6	1.7	1.8	1.9
N	20	21	22	23	24	25	26	27	28	29
FC	2.0	2.1	2.2	2.3	2.4	2.5	2.6	2.7	2.8	2.9

Table 5.3: Simulation Parameters

Parameters	Value
Space	$500m \times 500m$, $1000m \times 1000m$
Number of Nodes	10, 30
MAC	802.11
Traffic	CBR
Packet Generation Rate	10 packets/s
Packet Size	512byte
Simulation Time	600s

nodes' forwarding cost, but it has no reason to pay too much for the relay nodes, thus I set $\alpha = max(C_{r_i}) + q\% \times max(C_{r_i})$, $\beta = max(C_{r_i}) + 0.5q\% \times max(C_{r_i})$, $\gamma = q\% \times max(C_{r_i})$; where $max(C_{r_i})$ is the maximum forwarding cost of all the nodes reported to CCS, $q = 20, 40, 60, 80, 100$.

In the PDM, for each session, the source node payment is defined as the sum of the payment for each relay node. The payment for each relay node is calculated by equations (5.8) and (5.15). The price-demand function of the source node is determined by two methods: 1) satisfying Proposition 1 and 3, thus I set $a_s = max(C_{r_j}) + p\% \times max(C_{r_j})$, where $p = 20, 40, 60, 80, 100$; Q_s is calculated by equations (5.9) and (4.16); 2) satisfying the source nodes' own like, thus I simply set each source node with the same a_s and b_s. In 10 nodes simulation, $a_s = 0.2, 0.4, 0.8, 1.0, 1.4, 1.8$ and in 30 nodes simulation, a_s varies from 1.0 to 5.5 in step of 0.5.

To make a fair comparison, I compared the simulation results for $p = q$. Finally, I found that the results' tendencies were similar, therefore the comparison results are meaningful. In this chapter, I gave the results for $p = q = 20$.

In each simulation, the number of packets were increased from 1000 to 5000 in step of 1000 and each figure is the average of 5 runs. Here, in the simulation, I measured the results for the average source node payment per 1000 packets and ARN is defined as the average number of relay nodes in one session.

5.5.3 Simulation Scenarios

I simulated 10 and 30 nodes with two simulation scenarios respectively: 1) the PDM was compared with the Sprite model, where in the PDM, the price-demand function of the source node is determined by the first method (as described in section 5.5.2); 2) the PDM was compared with the Sprite, where in the PDM, the price-demand function of the source node is determined by the second method (as described in section 5.5.2).

5.6 Evaluation in a Static Scenario

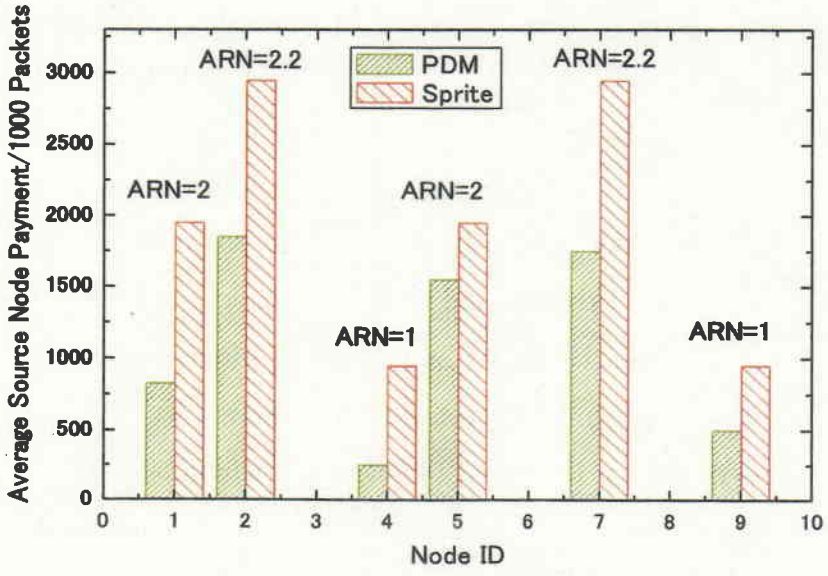


Figure 5.6: Average source node payment per 1000 packets, PDM vs Sprite, the first simulation scenario, 10 nodes simulation

5.6.1 Average Source Node Payment

Figures 5.5 and 5.6 separately show the comparison results for the selected source nodes from 10 and 30 nodes in the first simulation scenario. Fig.5.5 and Fig.5.6

indicate that the source nodes saved more money with the PDM than with the Sprite model. The advantage is verified by the average number of relay nodes (ARN) increases. The reason is that the pricing model in the PDM is more flexible than that in the Sprite. In the PDM, the source node payment is decided by its own service demand and the relay node forwarding costs, which means different relay nodes may get different payment from different source nodes. However, in the Sprite, the source node payment is only related with the number of the relay nodes in a session: almost all the relay nodes (expect the last relay node in each session) receive the same and fixed payment from different source nodes, thus the source nodes have to pay more to the relay nodes that have a low forwarding cost.

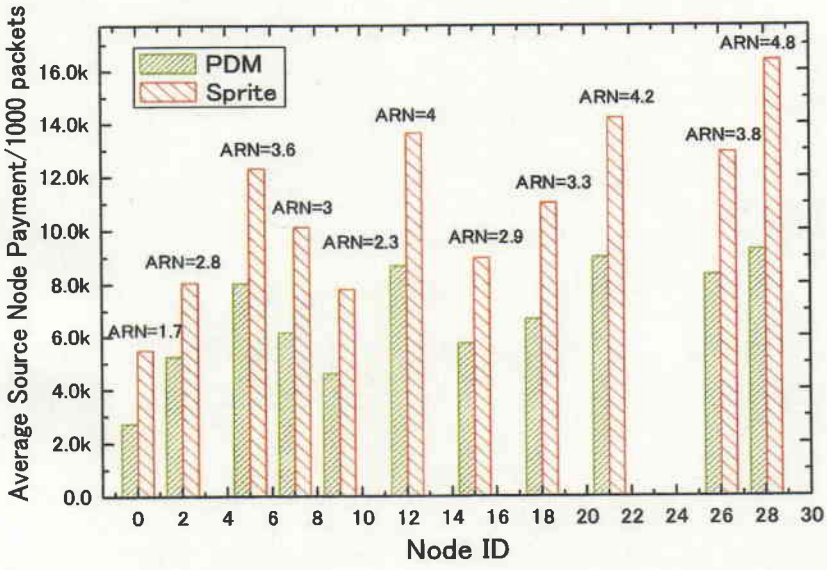
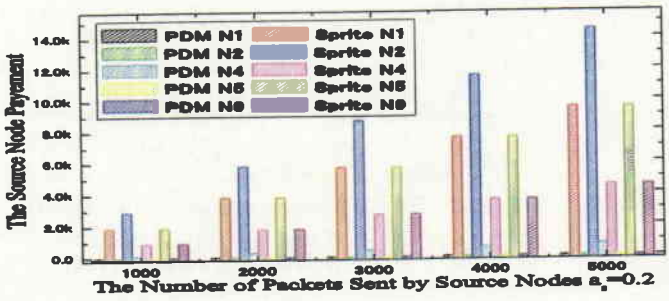
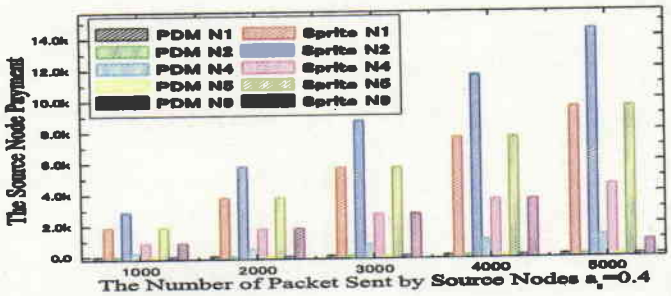


Figure 5.7: Average source node payment per 1000 packets, PDM vs Sprite, the first simulation scenario, 30 nodes simulation

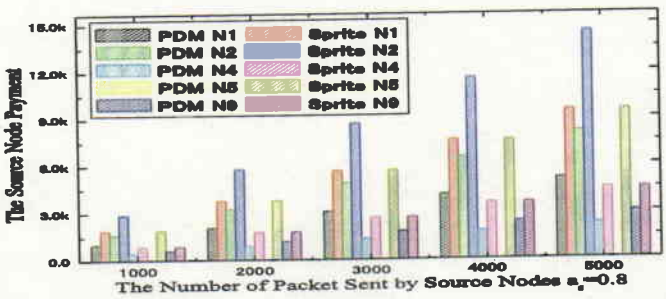
Figures 5.7 show the comparison results for the selected source nodes from 10 nodes in the second simulation scenario. Fig.5.8 shows the comparison results for 30 nodes simulation.



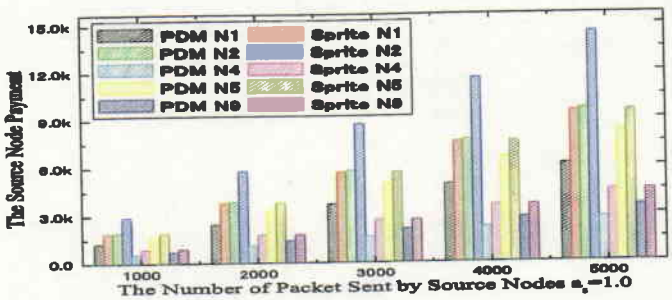
(a)



(b)



(c)



(d)

Figure 5.8: The source node payment, PDM vs Sprite, the second simulation scenario, 10 nodes simulation

From Fig.5.8 (a)(b)(c) and Fig 5.9 (a)(b), I observe that some source node payment is 0 in PDM (e.g. N1 in Fig.5.8(a) and N7 in Fig.5.9(a) at $a_s = 1.5$). 0 payment

means that the source nodes' packets do not reach the destination nodes. Therefore, it is risky for a source node to choose a low value of a_s, which verified Propositions 1 and 3. From Fig.5.9(a)(b), I observe that when a_s is a little bit larger than α, the source node payment in PDM is still lower than that in the Sprite model. This advantage verifies PDM saves the source node payment, when compared with the Sprite model.

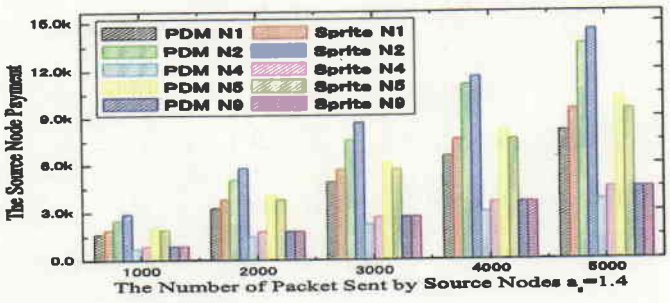
From all figures in Fig.5.8 and Fig.5.9, I observe that for each source node, as a_s increases, its payment increases. However, in Fig.5.8 (e)(f) and Fig.5.9 (a)(b), I notice that for some source nodes (e.g. N1 in Fig.5.8 (f) and N12 in Fig 5.9(b) at a_s=5.0), when the source nodes choose a high value of a_s in the PDM, their sending packets can be forwarded to the destination nodes. But meanwhile, the source nodes have to pay more than that in the Sprite model. Therefore, it is not good for a source node to choose a high value of a_s as well.

With the analysis for figures 5.6, 5.7, 5.8, and 5.9, it is easy to see that PDM is much more flexible than the Sprite model. It not only stimulates the relay nodes to forward packets, but also saves the payment for the source nodes. However, the choice of a_s, b_s is very important for the source nodes in PDM. To save the payments for sending the packets, and guarantee the packets to be forwarded, the source nodes may decide their price-demand function on the basis of Propositions 1 and 3.

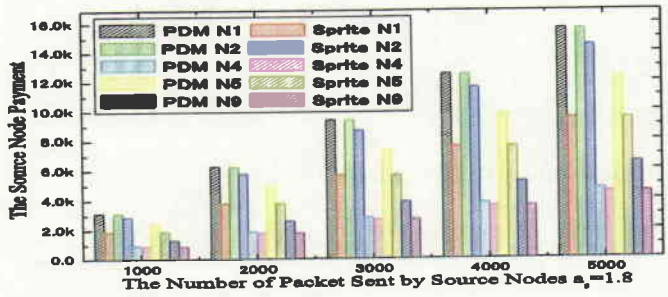
5.6.2 Extra Payoff of Relay Nodes who lies

Fig.5.9 studies the extra payoff for a relay node who dishonestly reports its forwarding cost. Extra payoff is defined as the difference between the relay node's cheating payoff (the payoff when it dishonestly report its forwarding cost) and its true payoff.

The dishonest relay node was defined as a relay node who cheated on the forwarding cost. I selected N4 as the dishonest relay node, since it acted as a relay node in most of the simulations. In each session where node 4 is a relay node, its dishonestly reported forwarding cost was varied from 0.2 to 1.4 in step of 0.2. Node 4's true forwarding cost was 0.4, as in Table 5.1. The definitions of payment and the price-demand function were the same as in the first simulation. I also chose representative results when p = q = 20. From the figure, I can see that PDM is

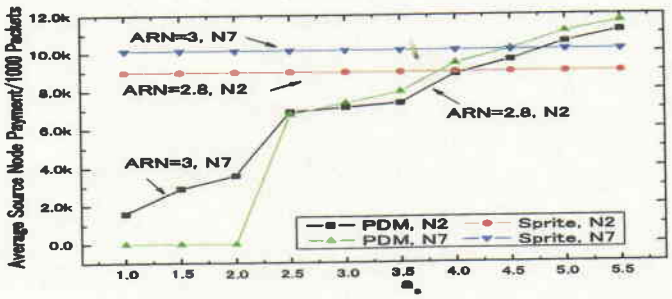


(e)

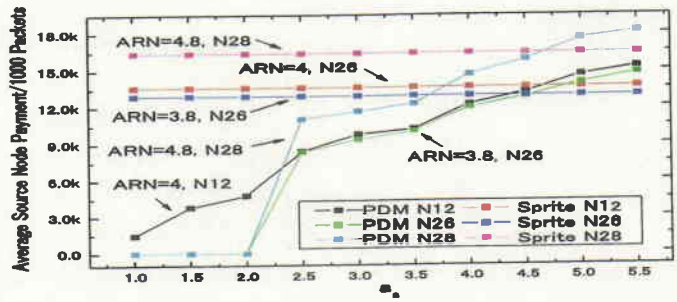


(f)

Fig.5.8 The source node payment, PDM vs Sprite, the second simulation scenario, 10 nodes simulation



(a)



(b)

Fig.5.9 Average source node payment per 1000 packets, PDM vs Sprite, the second simulation scenario, 30 nodes simulation

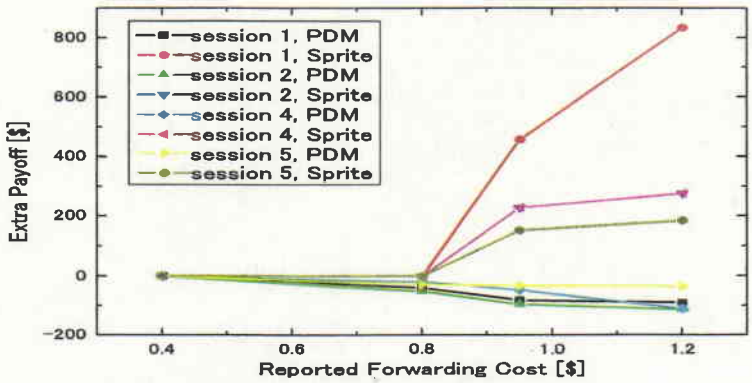


Figure 5.9: Extra Payoff of a relay node (N4), PDM vs Sprite, 10 nodes simulation

superior to "Sprite" in regard to the average source node payment when a dishonest relay node exists in the network. In each figure, for PDM, I observe that if node 4 reported its forwarding cost as higher or lower than 0.4, the source nodes' payment is always lower than the true payoff. For the "Sprite", the average source nodes' payment is the same as the true one when node 4 reports its forwarding cost as lower than 1; the source nodes' payment becomes higher when relay node 4 reports its forwarding cost as higher than 1. In "Sprite", the payment of the source node is determined by the maximum reported forwarding cost in the whole network and it is same for all the nodes. Therefore, in "Sprite", a relay node indeed has the intension to report a higher reporting cost, because it may get a higher payoff by cheating. The result indicated that when a relay node reports a higher forwarding cost in PDM, the source node does not need to pay more than it should; in "Sprite", the source node has to pay more than it should. Therefore, PDM performs better than "Sprite" when dishonest node exist in the network.

5.6.3 Money Balance of the Nodes

I try to determine whether PDM brings a money-benefit for a node. One metric that directly reflects a money-benefit is the difference between how much a node receives by forwarding the packets and how much it spends on its own traffic. Assuming that each node is provided a original money budget. Money balance of a node is

defined as original budget minus the total money paid by sending one's own packets plus the total money received by forwarding the packets.

I observe that the money balances of N4 increase monotonically while N1 decrease monotonically. N4 accumulates more money in the Sprite model than in PDM, however, N1 spends less payment in PDM. I can observe that the position and connectivity of a node are the major factors which determines the number of packets a node forwards as well as the payment it receives for forwarding each packet. In general the nodes in the center of the network forward more packets, thus earning more money.

5.7 Evaluation in Mobile Scenarios

PDM provides a cooperation and pricing model for wireless ad hoc networks. I want to analyze the impact of PDM on a mobile multiple hop ad hoc networks and evaluate its performance. To do so, I analyze the average source node payment and money balance for randomly selected individual nodes. The results from the evaluation of static scenario gave us some hints on the impact of the parameters on the network performance. On the basis of these results, I evaluated PDM under a variety of mobile scenarios.

In order to create a realistic simulation scenario, I expect the node moving in a a larger area. I generated the node movements based on the random way point mobility model as described in [65]. Mobility Simulation Parameters are listed in Table 5.4. In the simulation, I use the fixed forwarding cost for each node. The simulation results is the average of 10 movement files.

5.7.1 Average Source Node Payment

In mobile scenario, I used the first method as described in section 5.5.2 to determine the source node price-demand function in PDM. When compared with sprite model, the average source node payment is still low in PDM.

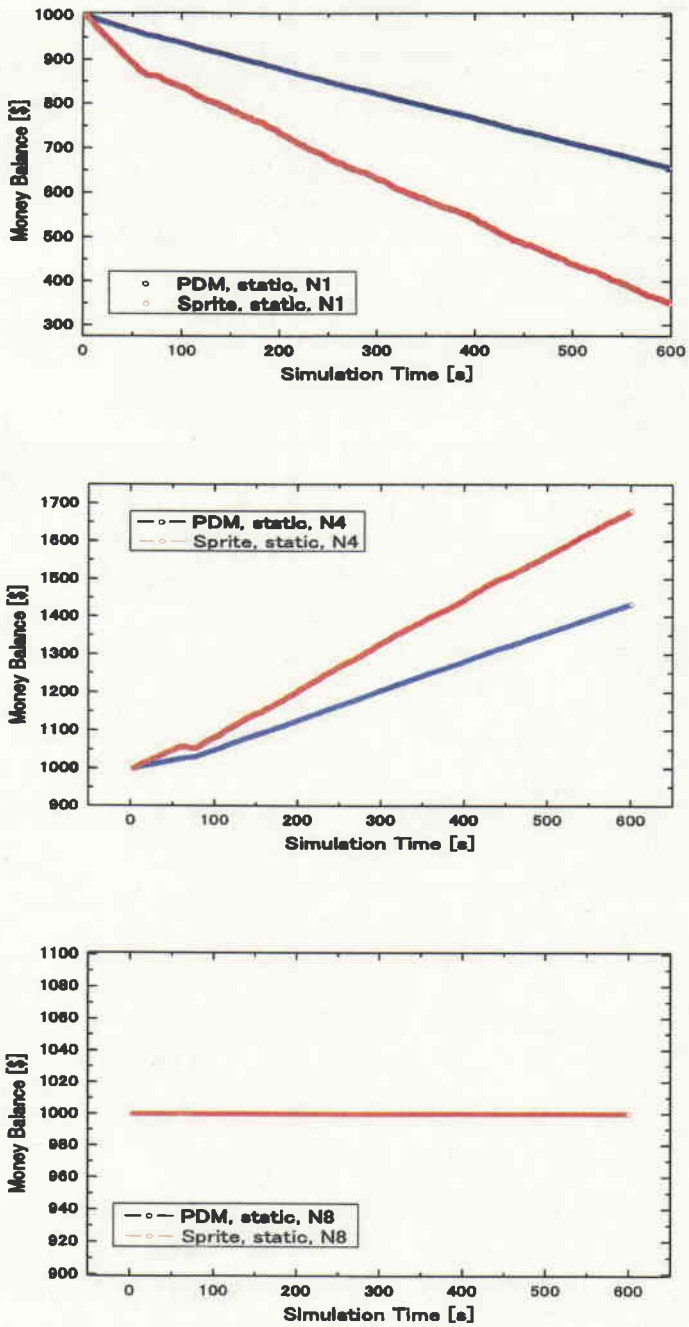


Figure 5.10: Money Balance of the nodes, static scenario, 10 nodes simulation

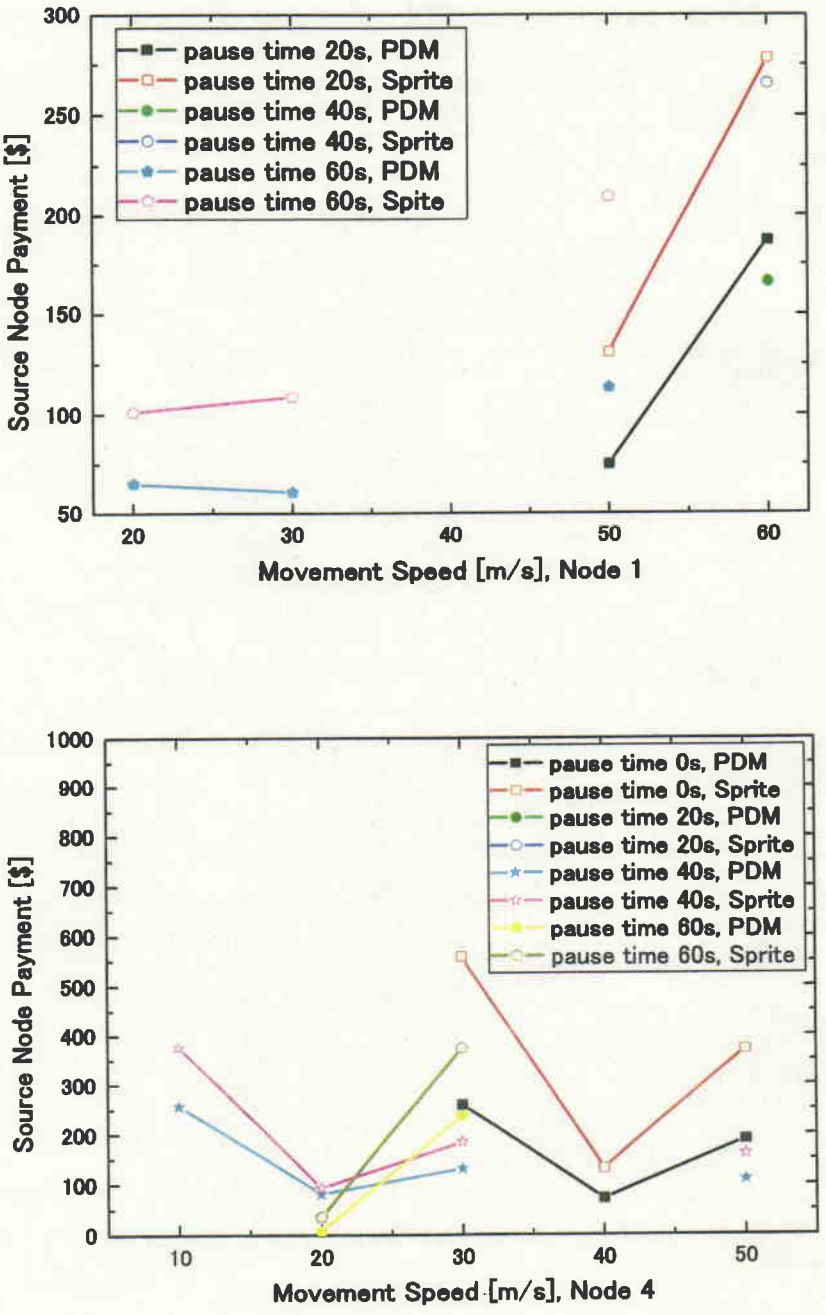


Figure 5.11: Average source node payment per 1000 packets, PDM vs Sprite, 10 nodes simulation

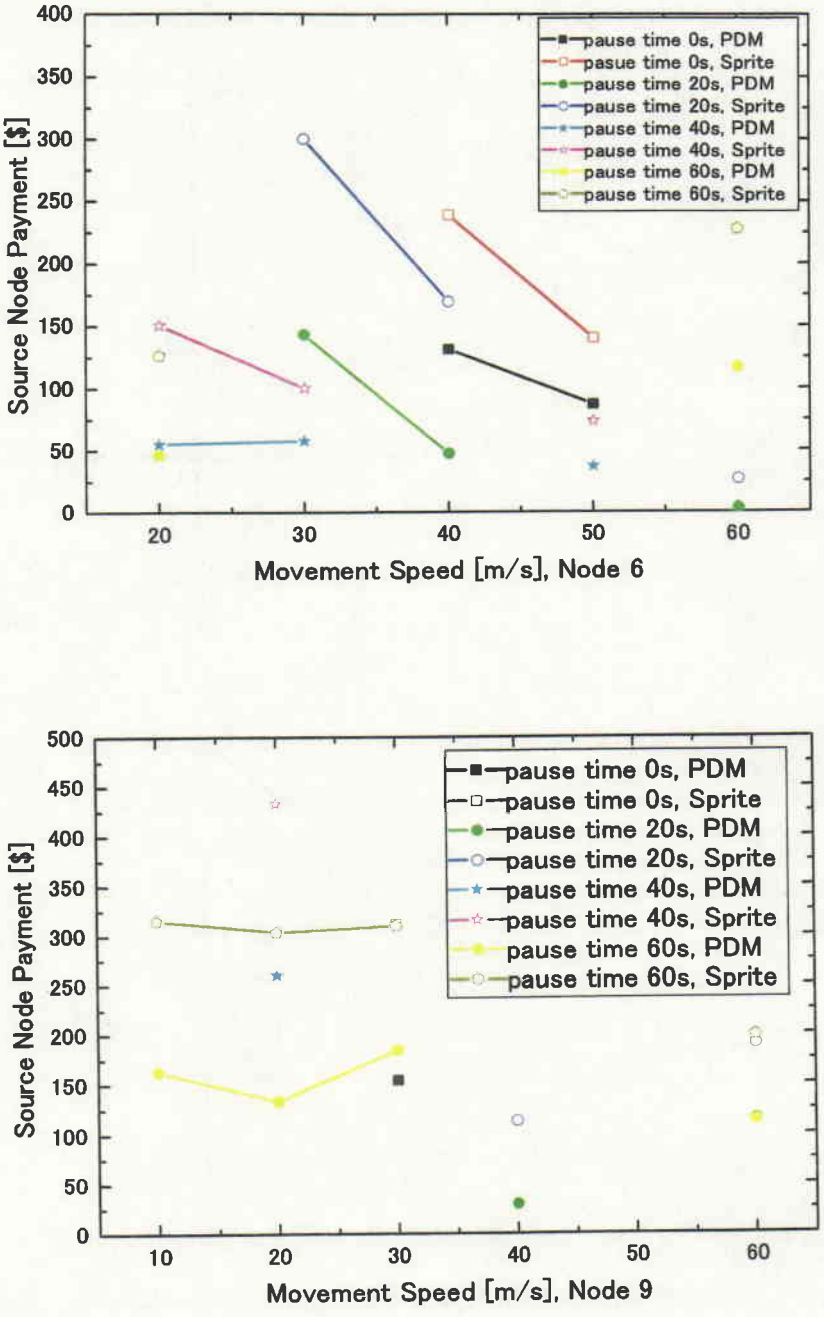


Figure 5.12: Average source node payment per 1000 packets, PDM vs Sprite, 10 nodes simulation

5.7.2 Money Balance of the Nodes

I try to determine whether node mobility brings a money-benefit for a node. In mobile scenario, I observe that the nodes accumulates more money when they forwards the packets for other nodes in Sprite model.

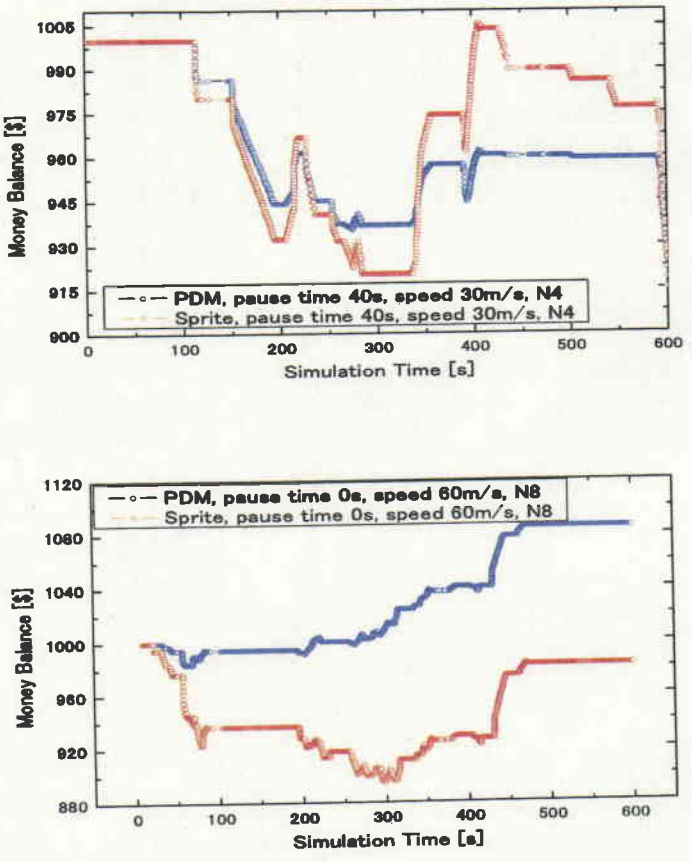


Figure 5.13: Money Balance, PDM vs Sprite, N8, 10 nodes simulation

Fig.5.13 to 5.16 show the money balance of the selected nodes in 10 nodes simulation. The initial budget of each node is 1000. The simulation assumes that each node will always forward packets if doing so can maximize its payoff or get payoff, and always generate packets if there is a request for communication. One interesting result is that a node will no longer generate any new packets after its money balance is too low. This is reasonable since if a node can have a negative money balance, then other nodes may not have incentives to forward its packets. The node has to

forward packets for others to accumulate enough money. However, I notice that Sprite model is more efficient in helping the relay nodes to accumulate the money, though PDM reduces the source node payment.

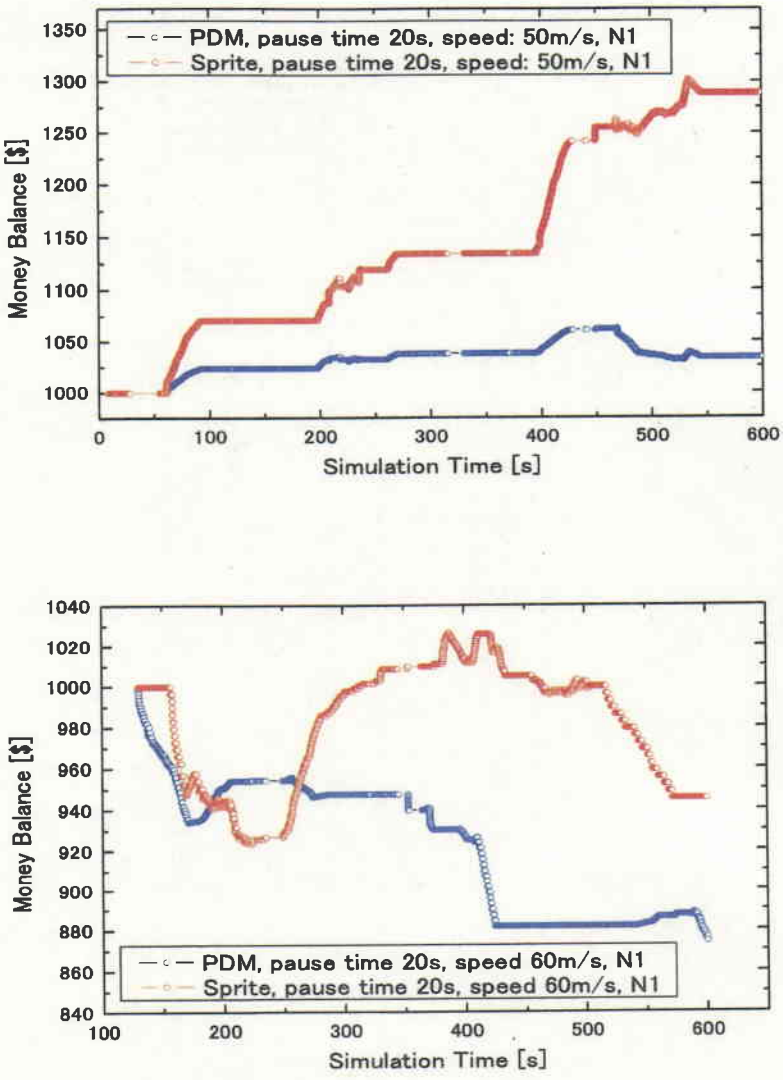


Figure 5.14: Money Balance, PDM vs Sprite, N1, 10 nodes simulation

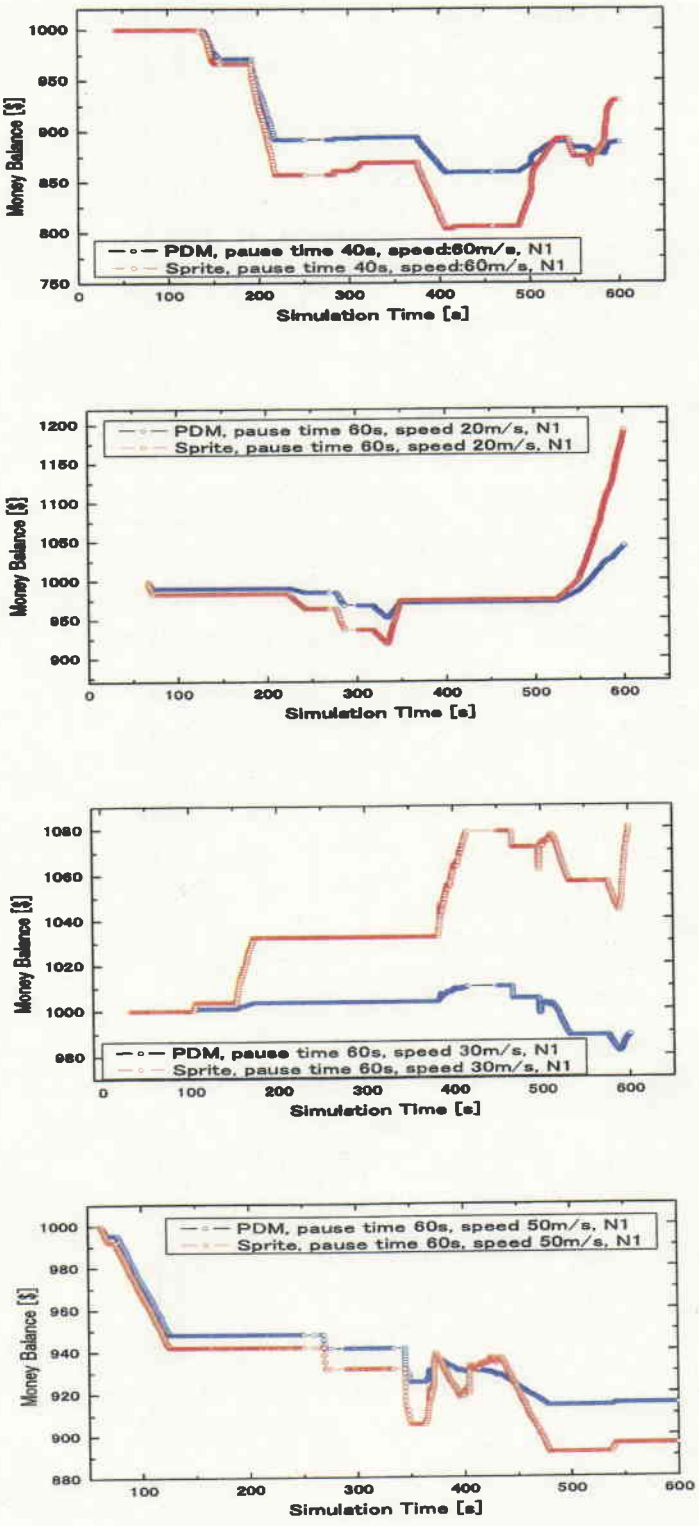


Figure 5.15: Money Balance, PDM vs Sprite, N1, 30 nodes simulation

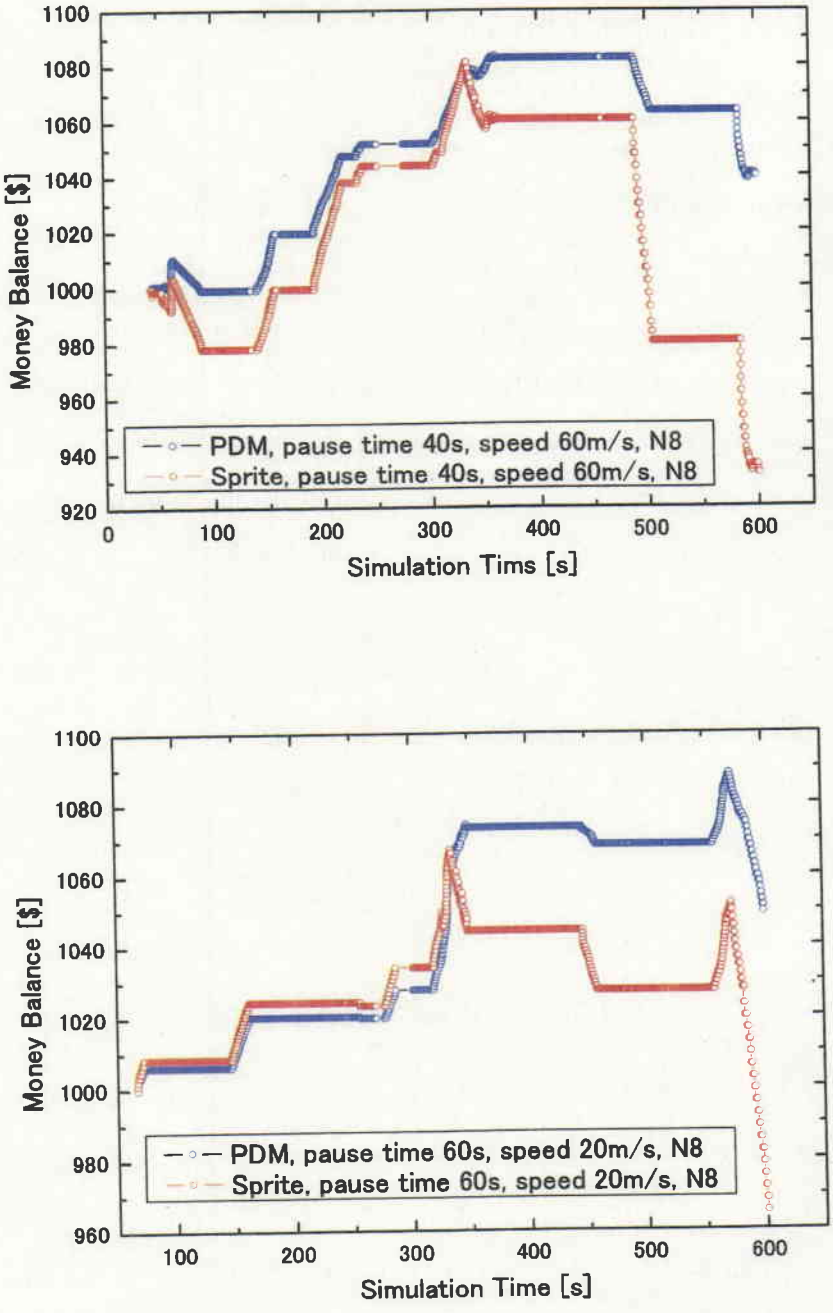


Figure 5.16: Money Balance, PDM vs Sprite, N8, 30 nodes simulation

5.8 Overhead of PDM

In this section, I will provide an estimation of the communication and computation overheads of the PDM.

I must admit that PDM adds some computational overhead to the system, which is mainly related to two aspects: cryptographic operations need energy and time to be performed. Regarding energy consumption, I note that the energy required to perform computation is negligible when compared to the energy required to perform transmission [11]. Therefore, I estimate that the execution of the payment calculations have a negligible energy cost when compared to the transmission cost. Regarding time, I note that the only time critical calculation are the generation and the verification of the payment header for every packet and for every hop. However, these require only simple function computations, which can be done very efficiently. Moreover, to some extent, the payment header can be accomplished by the main processor of the node.

Another issue is the communication overhead, which is due to delivering the forwarding cost and payment, i.e. the forwarding cost header and payment header. Assuming that the identifiers of the payment are 8 bytes long, the forwarding cost occupies 2 bytes long, and the output of the acknowledgement receipt is 16 bytes long, then the extra header is 26 bytes long. This seems to be an acceptable overhead.

5.8.1 Computation Overhead

In this subsection, the computation overhead for the nodes is considered. The computation overhead is expressed in terms of computation and energy consumption. However, the battery consumption due to computation can be considered as negligible compared to the energy needed for data transmission. In session setup phase, it requires the source node to perform payment computations. In packet sending phase, the main overhead is represented by the usage of some encryption (e.g. stream cipher) performed by the source and all the forwarder nodes which ensures the authentication of the nodes involved in the communication and prevents the free attack. But stream ciphers are very fast, and some operate at a speed comparable to

that of 32 bit CRC computation and have lower hardware complexity [13,44]. In acknowledgment computation, the destination node needs to perform the confirmation computation.

5.8.2 Communication Overhead

In this subsection, I consider the communication overhead.

In session setup phase, the forwarding cost field is used to inform the source nodes about the characteristics of the traffic; using (2*number of relay node) bytes to encode it seems to be reasonable.

In packets acknowledgment phase, sending the acknowledgment is done by the destination node once per session. It represents an overhead of (2*number of relay nodes) bytes per session. Assuming the number of relay node = 4, sending the acknowledgment represents an overhead of 8 bytes per session.

5.9 Summary

In this chapter, I modeled the system as a market where the pricing to stimulate nodes cooperation is determined by demand and supply. I studied a single relay node case and extend it to a multiple relay node session in PDM. In PDM, I showed that reporting the true forwarding cost is an optimal strategy for the relay nodes, if they do not know the others' forwarding costs. The proposed model is proved to refrain nodes from cheating reports, if they do not know the others' forwarding costs. The simulation results show that the proposed pricing model reduces the source node's payment to send a packet, when the source nodes determine their price-demand functions according to Propositions 1 and 3. Finally, I verify the results in static and mobile scenario. As a future work, I will extend the discussion to integration of pricing competition between nodes.

Chapter 6

Conclusions and Future Works

6.1 Roads Travelled

Before my work, there is a substantial amount of work on incentive compatible model of ad hoc networks [10,11,15,17,19,25,36,47,56,58]. If previous solutions that have provable properties in incentive compatibility are considered, there are two broad classes: those with strong incentive compatibility, and those with weak incentive compatibility. In game theory, a solution with strong incentive compatibility corresponds to a dominant-action solution in a strategic game, while one with weak incentive compatibility corresponds to a Nash solution. A dominant-action solution is that, no matter how other nodes behave, it always pushes a player to follow the protocol. For weak incentive compatibility (Nash equilibrium solution concept), an agent may change its strategies in response to other agents. The question is how fast the system can converge to a Nash equilibrium. Pure strategy Nash equilibrium may not exist. These issues have just begun to be explored [2, 20, 22, 24, 35, 52] in ad hoc networks.

In the thesis, I focused on the strategic pricing to stimulate the nodes cooperation in a wireless ad hoc network. One contribution of the thesis is that: In the game theoretic analysis, by using a pricing policy "payment and compensation", the relay nodes have less motivation to drop the packets. However, I also found that game theoretic literature may not be directly applicable in the scenario where cheating nodes exist. Therefore, a price-demand function based incentive model (PDM) is

proposed. In the PDM, I modeled the system as a market where the pricing to stimulate nodes cooperation is determined by the source nodes' demand and relay nodes' service supply. I studied a single relay node session and extend it to a multiple relay nodes session. In the PDM, I showed that reporting the true forwarding cost is the optimal strategy for the relay nodes, if they do not know the others' forwarding costs. Our simulation results show that the proposed pricing model also reduces the source nodes' budget and guarantees their packets to be delivered, when the source nodes determine their price-demand functions according to Proposition 1,3 in Chapter 5. Finally, I verify the results in static and mobile scenario.

6.2 Perspectives and Future Work

As the future work, I wish to extend the discussion into the following aspects.

Since PDM is a payment model in the network, it needs an entity such as a payment certification to resolve payment issues. A related assumption is the relay nodes do not know the others' forwarding cost information, therefore a public-key infrastructure is required to identify and authenticate users, otherwise, the payment between users can never be enforced. It can be challenging to setup a payment certification and infrastructure to satisfy trustworthy payment computation. More simulation results of the system would be helpful to find the threshold when and how the price rediscovery should be performed.

In PDM, I made the choice that it is the source node who computes the payment. However, it is possible that no entity is completely trustworthy in a civilian ad hoc network, unless a tamper-proof hardware is used to build nodes. An alternative may be that a node not involved in the game performs the computation of the mechanism. However, it is not clear whether such a node is really trustworthy. For example, a participant of the game may bribe this node to change the output.

Another important issue is "blind communication" between the relay nodes. In PDM, the assumptions are the connectivity of the network and some existing cryptographic techniques are used to protect the communication between the relay nodes. However, if the connectivity assumption is invalid or proper cryptographic

technique cannot be adopted (e.g., due to efficiency considerations), the relay nodes in the path can tamper with the messages. Furthermore, the relay nodes may drop routing messages to cheat the source nodes.

PDM assumes that there are no communications among the relay nodes. This assumption can be valid in many scenarios. However, there may be some scenario that nodes communicate with each other. Such communication is called as "secret communication" and it is not in the scenario that I considered. The existence of secret communications makes it impossible to find any dominant-strategy solution: suppose that a node broadcasts all its private and semi-private information to all other nodes. There is no reason for another relay node not to accept these private information and cheat the source node. Obviously, a relay node could use the information it received to get benefit. It is very possible to cheat the system by other methods.

Bibliography

[1] G. Anastasi, M. Conti, and E. Gregori, "IEEE 802.11 Ad Hoc Networks: Protocols, Performance and Open Issues," In S. Basagni, M. Conti, S. Giordano, and I. Stojmenovic, eds., Mobile Ad Hoc Networking, chap. 3, pp.69-116. Wiley-IEEE Press, 2004.

[2] L. Anderegg and S. Eidenbenz, "Ad hoc-VCG: a Truthful and Cost-Efficient Routing Protocol for Mobile Ad hoc Networks with Selfish Agents," Proc. of Mobicom, September 2003.

[3] M. K. A. Aziz, P. N. Fletcher, and A. R. Nix, "Performance analysis of IEEE 802.11n solutions combining MIMO architectures with iterative decoding and sub-optimal ML detection via MMSE and Zero forcing GIS solutions," Proc. of IEEE Wireless Communications and Networking Conference, pp.1451-1456, March 2004.

[4] R. Anderson and M. Kuhn, "Tamper Resistance - a Cautionary Note," Proc. of 2nd USENIX Workshop on Electronic Commerce, pp.1-11, November 1996.

[5] C. Buragohain, D. Agrawal, and S. Suri,"A Game Theoretic Framework for Incentives in P2P Systems" Proc. of the Third International Conference on P2P Computing, September 2003.

[6] S. Buchegger and J.-Y. Le Boudec,"Performance Analysis of the CONFIDANT Protocol: Cooperation Of Nodes - Fairness In Distributed Ad-hoc NeTworks," Proc. of MobiHoc, June 2002.

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

[8] L.Blazevic, L.Buttyan, S.Capkun, S.Giordano, J.P.Hubaux, and J.Y. Le Boudec, "Self-organization in mobile ad-hoc networks: The approach of terminodes," ACM/Kluwer MONET, vol.8, no.5, pp.579-592, October 2003.

[9] L. Blazevic, L. Buttyan, S. Capkun, S. Giordano, J.P. Hubaux, and J.Y. Le Boudec, "Self-organization in mobile ad-hoc networks: The approach of terminodes," ACM/Kluwer MONET, vol.8, no.5, pp.579-592, October 2003.

[10] L. Buttyan and J.P. Hubaux, "Nuglets: a Virtual Currency to Stimulate Cooperation in Self-Organized Mobile Ad Hoc Networks," Technical Report No. DSC/2001/001, Swiss Federal Institute of Technology (EPFL), January 2001.

[11] L. Buttyan and J.P. Hubaux, "Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks," ACM/Kluwer Mobile Networks and Applications, 8(5), October 2003.

[12] S. Buchegger, J.-Y. Le Boudec, "Performance Analysis of the CONFIDANT Protocol: Cooperation Of Nodes - Fairness In Distributed Ad-hoc NeTworks," Proc. of MobiHoc, June 2002.

[13] T. Beth and F. Piper, "The Stop-and-Go Generator," EUROCRYPT, pp88-92, 1084.

[14] K. Chen, "Cooperative and Non-cooperative Flow Control in Mobile Ad Hoc Networks," Ph.D. thesis, Computer Science, University of Illinois at Urbana-Champaign, October 2004.

[15] J. Crowcroft, R. Gibbens, F. Kelly and S. Ostring, "Modelling Incentives for Collaboration in Mobile Ad Hoc Networks," Proc. of Modeling and Optimization in Mobile Ad Hoc and Wireless Networks, March 2003.

[16] J. Cushnie, D. Hutchinson, and H. Oliver, "Evolution of Charging and Billing Models for GSM and Future Mobile Internet Services," Proc. of the First

COST 263 International Workshop on Quality of Future Internet Services, pp.312-323, September 2000.

[17] K. Chen and K. Nahrstedt, "iPass: an Incentive Compatible Auction Scheme to Enable Packet Forwarding Service in MANET," Proc. of the 24th International Conference on Distributed Computing Systems, March 2004.

[18] J. Cai and U. Pooch, "Allocate Fair Payoff for Cooperation in Wireless Ad Hoc Networks Using Shapley Vale," Proc. of the 18th International Parallel and Distributed Processing Symposium, April 2004.

[19] K. Chen, Z. Yang, C. Wagener, and K. Nahrstedt, "Market Models and Pricing Mechanisms in a Multihop Wireless Hotspot Network," Proc. of 2nd Annual International Conference on Mobile and Ubiquitous Systems, July 2005.

[20] L. A. DaSilva and V. Srivastava, "Node Participation in in Ad Hoc and Peer-to-Peer Networks: A Game-Theoretic Formulation," the First Workshop on Games and Emergent Behaviors in Distributed Computing Environments, September 2004.

[21] J.P. Ebert, A. Wolisz, "Combined Tuning RF Power and Medium Access Control for WLANs," In Jounal of Mobile Networks and Applications (Monet), vol 6, no.5, pp.417-426, September 2000.

[22] M. Felegyhazi, L. Buttyan, and J.P.Hubaux, "Equilibrium Analysis of Packet Forwarding Strategies in Wireless Ad Hoc Networks- the static Case," Proc. of Personal Wireless Communication, October 2003.

[23] Z. Fang and B. Bensaou,"Fair Bandwidth Sharing Algorithms based on Game Theory Frameworks for Wireless Ad-hoc Networks," Proc. of IEEE Infocom, March 2004.

[24] M. Felegyhazi, J.-P. Hubaux, and L. Buttyan, "Nash Equilibria of Packet Forwarding Strategies in Wireless Ad Hoc Networks," IEEE Trans. on Mobile Computing, vol.5, no.4, April 2006.

[25] A. Garyfalos and K.C. Almeroth, "Coupon Based Incentive Systems and the Implications of Equilibrium Theory," Prof. of 2004 IEEE International Conference on E-Commerce Technology, March 2004.

[26] P. Golle, K. Leyton-Brown, I. Mironov, and M. Lillibridge, "Incentives for sharing in peer-to-peer networks," Proc. 2nd International Workshop on Electronic Commerce, November 2001.

[27] A. Heinemann, J. Kangashrju, F. Lyardet and M. MAuhlhAauser, "Ad Hoc Collaboration and. Information Services Using Information Clouds," Proc. of the International Workshop on Applications and Services in Wireless Networks, July 2003.

[28] D. B. Johnson, D. A. Maltz, and J. Broch, "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks," Ad Hoc Networking, edited by Charles E. Perkins, Chapter 5, pp.139-172, Addison-Wesley, 2001.

[29] F.Kelly, "Charging and rate control for elastic traffic," Eur.Trans.Telecommum. – Focus on Elastic Services Over ATM networks, vol.8, no.1, pp.33-37, 1997.

[30] R.J.La and V. Anantharam, "Utility-Based Rate Control in the Internet for Elastic Traffic" IEEE Tran. on Networking, vol.10, no.2, 2002.

[31] R.B.Myerson, "Game Theory Analysis of Conflict," Cambridge, MA: Harvard University Press, 1991.

[32] P. Michiardi and R. Molva, "Simulation-based Analysis of Security Exposures in Mobile Ad Hoc Networks", European Wireless Conference, February 2002.

[33] P. Michiardi and R. Molva, "Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," Proc. of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security: Advanced Communications and Multimedia Security, pp.107-121, September 2002.

[34] S. Marti, T.J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. of Mobicom, August 2000.

[35] P. Michiardi and R. Molva, "A game theoretical approach to evaluate cooperation enforcement mechanisms in mobile ad hoc networks," Proc. of Modeling and Optimization in Mobile Ad Hoc and Wireless Networks, March 2003.

[36] A. Mok, B. Mistry, E. Chung and B. Li, "FAIR: Fee Arbitrated Incentive Architecture in Wireless Ad Hoc Networks," Proc. of the 10th IEEE Real-Time and Embedded Technology and Applications Symposium, May 2004.

[37] P. Nicopolitidis, G. Papadimitriou, M. S. Obaidat, and A. S. Pomportsis, "the economics of wireless networks," communications of the ACM, vol.47, iss.4, April 2004.

[38] C. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers," Proc. of ACM SIGCOMM Conference, pp.234-244, August 1994.

[39] V. Park and S. Corson, "Temporally-Ordered Routing Algorithm (TORA) Version 1 Functional Specification," Internet Draft, November 1997.

[40] C.E. Perkins and E.M. Belding-Royer,"Ad-hoc On Demand Distance Vector Routing," Proc. of 2nd IEEE Workshop on Mobile Computing Systems and Applications, February 1999.

[41] K. Paul and D. Westhoff, "Context Aware Detection of Selfish Node in DSR based Ad-hoc Network," Proc. of IEEE GLOBECOM 2002, November 2002.

[42] J.B.Rosen, "Existence and uniqueness of equilibrium points for concave n-person game," Econometrica, vol.33, pp.520-534, July 1965.

[43] F. Rosenkranz, "Deterministic solution and stochastic simulation of a simple production-inventory model," Mathematical Methods of Operations Research, vol.17, no.4, pp.141-152, August 1973.

[44] M.J.B. Robshaw,"Stream Ciphers," RSA Laboratories Technical Report TR-701 Version 2.0, July 1995.

[45] O.V. Ratsimor, T. Finin, A. Joshi, and Y. Yesha, "eNcentive: A Framework for Intelligent Marketing in Mobile Peer-To-Peer Environments," Proc. of the 5th International Conference on Electronic Commerce, October 2003.

[46] F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues for Ubiquitous Computing," first Security and Privacy supplement to IEEE Computer, April 2002.

[47] N.B. Salem, L. Buttyyan, J.P. Hubaux, and M. Jakobsson, "A Charging and Rewarding Scheme for Packet Forwarding in Multi-hop Cellular Networks," Proc. of MobiHoc, June 2003.

[48] N. B. Salem, L. Buttyan, J.P. Hubaux, and M.Jakobsson, "Node Cooperation in Hybrid Ad Hoc Networks," IEEE Trans. Mob. Comput. vol.5(4), pp.365-376, 2006.

[49] K.Sanzgiri, D.LaFlamme, B.Dahill, B.N.Levine, C.Shields, and E.M.Belding-Royer. "Authenticated Routing for Ad hoc Networks," IEEE Journal on Selected Areas in Communications vol.23, iss.3, pp.598-610, 2005.

[50] C. Saraydar, N. Mandayam, D. Goodman, "Efficient power control via pricing in wireless data networks," IEEE Trans. on Communications, vol.50, no.2, pp.291-303, February 2002.

[51] V. Srinivasan, P. Nuggehalli, C. F. Chiasserini, R. R. Rao, "Cooperation in Wireless Ad Hoc Networks," Proc. of IEEE INFOCOM, March 2003.

[52] V.Srinivasan, P. Nuggehalli, C.F. Chiasserini, and R. R. Rao, "An analytical Approach to the Study of Cooperation in Wireless Ad Hoc Networks," IEEE Trans. on Wireless Comm., vol.4, pp.722-733, March 2005.

[53] A.Urpi, M.Bonuccelli, and S.Giordano, "Modeling cooperation in mobile ad hoc networks: A formal description of selfishness," Proc. of Modeling and Optimal in Moile, Ad Hoc and Wireless Networks, April 2003.

[54] K. Wrona and P. Mahonen, "Analytical Model of Cooperation in Ad Hoc Networks," Telecommunication Systems, Springer vol.27, pp.347-369, No.2-4, October 2004.

[55] H. Yaiche, R. R. Mazumdar, C. Rosenberg,"A game theoretic framework for bandwidth allocation and pricing in broadband networks," IEEE/ACM Trans. on Networking, vol.8, pp.667-678, October 2000.

[56] S. Zhong, J. Chen, and Y.R. Yang, "Sprite: A Simple, Cheat-Proof, Credit-Based System for Mobile Ad-Hoc Networks," Proc. of IEEE INFOCOM, April 2003.

[57] F.Zheng, B.Gleeson, and J.Nelson, "Performance analysis and design: Power saving backoff algorithm for IEEE 802.11 DCF", Proc. Networking, May 2006.

[58] S. Zhong, L. E. Li, Y. G. Liu, and Y. R. Yang, "On Designing Incentive-Compatible Routing and Forwarding Protocols in Wireless Ad-Hoc Networks-An Integrated Approach Using Game Theoretical and Cryptographic Techniques," to appear in ACM Wireless Network (WINET) journal, 2007.

[59] http://en.wikipedia.org/wiki/Bugatti_Veyron

[60] http://orcmid.com/BlunderDome/clueless/2004_12_05_clu-chive.asp

[61] Economics and Liberty. http://www.econlib.org/library/Marshall/marP.html.

[62] Gnutella. http://gnutella.wego.com/.

[63] KaZaA. http://www.kazaa.com/.

[64] The Network Simulator NS-2. http://www.isi.edu/nsnam/ns/.

[65] Random Waypoint Model http://www.netlab.tkk.fi/ esa/java/rwp/rwp-model.shtml

[66] Supply and Demand. http://en.wikipedia.org/wiki/Supply_and_demand.

[67] http://w3.antd.nist.gov/wahn_mahn.shtml.

[68] http://winet-coop.epfl.ch/

List of Publications

Referred Publications and Transactions

Transactions and Journals

1. Mingmei Li, Eiji Kamioka, and Shigeki Yamada, "Pricing to Stimulate Node Cooperation in Wireless Ad Hoc Networks," IEICE Transactions on Communications, July 2007 (in press).

Conference Proceedings

1. Mingmei Li, Eiji Kamioka, Shigeki Yamada, and Yang Cui, "Efficient Node Forwarding Strategies via Non-cooperative Game for Wireless Ad Hoc Networks," Proc. of ICCNMC, Networking and Mobile Computing, LNCS Vol.3619, Springer-Verlag, pp. 334-343, August 2005.

Technical Reports

1. Mingmei Li, Eiji Kamioka, and Shigeki Yamada, "Pricing to Improve Cooperation in Wireless Ad Hoc Networks," Proc. of MoMuC2006-19, pp.103-107, May 2006.

2. Mingmei Li, Eiji Kamioka, and Shigeki Yamada, "Modeling Incentive for Cooperation in Wireless Ad Hoc Networks," Proc. of the 2005 IEICE society Conference, Network Planning, Control and Management BS-10-18, pp.44-45, September 2005.

3. Mingmei Li, Eiji Kamioka, and Shigeki Yamada, "Efficient Node Forwarding Strategies via Pricing for Wireless Ad Hoc Networks," Proc. of ubiCNS 2005, pp.37-42, May 2005.

4. Mingmei Li, Shigeki Yamada, and Eiji Kamioka, "Enhancing the Trustability of

Mobile Nodes in Ad Hoc Networks," Proc. of the IEICE Society Conference, Network Planning, Control, and Management BS-9-11, pp.21-22, September 2004.
5. Mingmei Li, Eiji Kamioka, and Shigeki Yamada, "A Game Theorem-Based Approach to Avoid Malicious Nodes in Mobile Ad Hoc Networks," Proc. of IEICE, Vol.104 No.189, MoMoC2004-35, pp.13-18, July 2004.