SELFISH NODE AVOIDANCE ROUTING PROTOCOL IN AD HOC NETWORKS

Dissertation submitted to the Jawaharlal Nehru University

in partial fulfillment of the requirements

for the award of the degree of

MASTER OF TECHNOLOGY

IN

COMPUTER SCIENCE AND TECHNOLOGY

By

UPASANA DOHARE

UNDER THE SUPERVISION OF

Dr. D.K. LOBIYAL

SCHOOL OF COMPUTER & SYSTEMS SCIENCES
JAWAHARLAL NEHRU UNIVERSITY
NEW DELHI – 110067, INDIA
JULY, 2011

School of Computer & Systems Sciences
जवाहरलाल नेहरू विश्वविद्यालय
JAWAHARLAL NEHRU UNIVERSITY
NEW DELHI-110067

CERTIFICATE

This is to certify that the dissertation entitled "***Selfish Node Avoidance Routing Protocol In Ad Hoc Networks***", being submitted by **Ms.** ***Upasana Dohare*** to the **School of Computer and Systems Sciences, Jawaharlal Nehru University, New Delhi**, in partial fulfillment of the requirement for the award of the Degree of **Master of Technology in Computer Science and Technology**, is a bonafide work carried out under the guidance and supervision of ***Dr. D. K. Lobiyal***.

The matter embodied in the dissertation has not been submitted for the award of any other Degree or Diploma.

25.7.11

Dr D. K. Lobiyal
(Supervisor),
Associate Professor,
SC&SS, JNU,
New Delhi-110067

Prof. Karmeshu
Dean, SC&SS
Jawaharlal Nehru University
New Delhi-110067

[illegible] meshu
[illegible] संस्थान
S[illegible] ences

School of Computer & Systems Sciences
जवाहरलाल नेहरू विश्वविद्यालय
JAWAHARLAL NEHRU UNIVERSITY
NEW DELHI-110067

DECLARATION

This is to certify that the dissertation entitled "***Selfish Node Avoidance Routing Protocol In Ad Hoc Networks***", being submitted to **the School of Computer and Systems Sciences, Jawaharlal Nehru University**, **New Delhi**, in partial fulfillment of the requirement for the award of the Degree of **Master of Technology in Computer Science and Technology**, is a bonafide work carried out by me.

The matter embodied in the dissertation has not been submitted for the award of any other Degree or Diploma.

Upasana Dohare
Upasana Dohare
M. Tech (2009-2011)
SC&SS, JNU
New Delhi-110067

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to Dr. D. K. Lobiyal, who gave me great intellectual freedom to pursue my interest and provided encouragement and guidance throughout the work. His extraordinary interest and inspiring attitude helped me in solving all the hurdles that cropped up at various stages.

I take this opportunity to convey my sincere thanks to Prof. Sonajharia Minz, Dean of School of Computer & Systems Sciences during my M. Tech. course work, for her endless help in many capacities. I take immense pleasure in thanking all the staff members for providing me necessary facilities in due course of this work.

I wish to give very special thanks to all my fellow and seniors, who share their knowledge with me and timely support throughout M.Tech tenure. I gratefully acknowledge the thoughtful help given to me by them which inspired me greatly through many interesting discussions, support, and feedbacks.

Finally, this work would not have been possible without the confidence, endurance and support of my family. My family has always been a source of inspiration and encouragement. I would like to give my heartiest thanks to my daughter Ekangika for her affection, understanding and patient love that enabled me to complete this work. No words are enough for my husband Sushil Kumar who is always the source of inspiration for all my achievements.

UPASANA DOHARE

ABSTRACT

Forwarding of packets in wireless ad hoc network relies on cooperation of the nodes since these networks are self-organized and distributed. If the nodes become selfish, they try to maximize its benefits by not forwarding the packets for others. This may lead to the inefficient use of network resources. In the work presented in this dissertation, a Game Theoretic Model for selfish node avoidance routing is presented. It is based on two player packet forwarding game which is used for inspiring the cooperation among nodes and avoiding the selfish nodes in the networks. Autonomous Nodes are considered rational acting for their self-interest to maximize their lifetime in order to save energy. The cooperative nodes earn credit for packet forwarding to other nodes. Therefore, a mathematical framework for rational node that maximizes its credits has been developed. Two trigger strategies – game theoretic model with F (forward) and with TFT (Tit For Tat) are used to enforce cooperation among the selfish nodes. Using game theory, it is verified that that this proposed model is robust and can achieve full cooperation among nodes.

The proposed model is simulated using network simulator ns-2. Simulations are carried out to validate the results of game theoretic model and evaluate the performance of this model by integrating it with AODV. The simulation results show that game theoretic model improves packet delivery ratio with the increase in number of the routes in the network. It is shown that game theoretic model with AODV can achieve higher packet delivery ratio for heavy traffic network in the presence of selfish nodes as compared to the original AODV. Further, it is observed that the packet delivery ratio of cooperative nodes decreases proportionally when the number of selfish nodes increases. Furthermore, it is also shown that game theoretic model with AODV gives low routing overheads.

CONTENTS

CHAPTER 1 – AD HOC NETWORKS

CHAPTER 2 – RELATED WORK

CHAPTER 3 – GAME THEORETIC MODEL FOR SELFISH NODE AVOIDANCE

CHAPTER 4 – SIMULATION RESULTS

CHAPTER 5 – CONCLUSION AND FUTURE WORK

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1
AD HOC NETWORKS

1.1 INTRODUCTION

The extensive research and development works on the recent radio frequency devices have been done for the last several years in the wireless environment. Advancements in wireless communications technologies together with the availability of wireless communications devices with major improvement in design, and processing capabilities have enabled wireless connectivity of mobile users to the global internet. In the meantime, a revolution in the computing has been brought with the proliferation of mobile computing devices such as laptop, cell phones, personal digital assistants and portable computers. These new generation computational devices have assisted to improve in working techniques of the users. Technologies trends have thus evolved rapidly from the personal computer age to the ubiquitous computing age in which individual user simultaneously use the multiple electronic platforms through which they access all the required information whenever and wherever needed [1].

The feature of ubiquitous devices offers the simplest solution for their interconnection in wireless networks. Mobile users can use their cellular phone to check e-mail, browse internet, arrange a meeting using video/audio conference, travelers with portable computers can surf the internet from airports, railway stations, and other public locations. Global Positioning System (GPS) terminals can be installed inside rental cars provides the services for tourists as locate driving maps and tourist attractions. The researchers can exchange their files and other information by connecting portable computers via wireless LANs while attending conferences, meeting at office and users can synchronize data and transfer files between portable devices and desktops at home.

The development of mobile technologies made the mobile devices smaller in size, lowering the cost, convenient in use, and more powerful in processing. Mobile user can run more applications and network services in their cellular phone. This is inspiring the explosive growth of mobile computing equipment market. The increasing number of user for Internet, laptop, and portable communication devices motivated this growth further since portability enables users to keep their important information in tools with them.

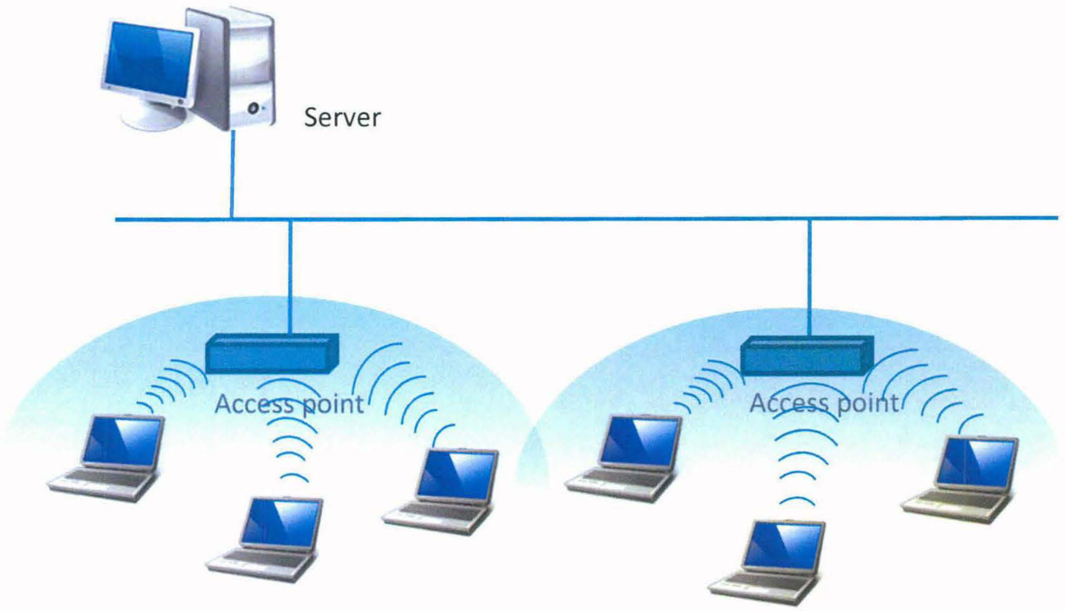

Figure 1.1 Infrastructure-based Wireless LAN

There two different approaches that can be followed to get connection among wireless devices. The connectivity among wireless devices can be achieved via fixed infrastructure-based service provider, or private networks known as Infrastructure-based Wireless LAN. For example, connectivity between two cell phones is setup by mobile switching center in cellular networks; laptops are connected to Internet via wireless access points or router. The infrastructure-based networks are a centrally coordinated and controlled network. The centralized controllers named as access point is connected to the wired network, thus providing Internet access to portable devices. The necessary installation of infrastructure-based networks is time consuming and potentially high cost. There are some circumstances where user required networking connections are not available in a given geographic area. In these inaccessible areas, providing the network connectivity and services to the mobile users becomes a challenging task. While new alternative ways to provide connectivity and deliver the services via Infrastructure-free Wireless LANs known as ad hoc wireless networks. These are focused around having a set of mobile devices connected to each other in the transmission range through freely and dynamically self-configuration and organize themselves to set up a temporary ad hoc network that is both flexible and powerful. In this way, not only mobile nodes can communicate with each other, but can also receive network services through a dynamically elected controller from set of mobile devices.

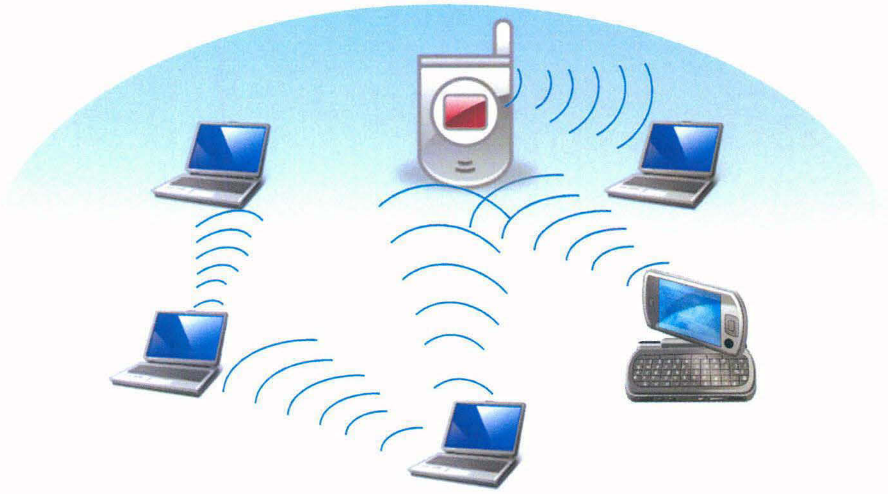

Figure 1.2 Ad Hoc Network

1.2 HISTORY AND DEFINITION OF MOBILE AD HOC NETWORK

Key developments in the history of mobile ad doc network (MANET) involved the tactical network related applications to improve battlefield communications and survivability. The active nature of military operations means that military cannot trust on access to a fixed pre-placed communication infrastructure in battlefield since it cannot be quickly install and starting communication among mobile nodes such as soldiers, tanks, aircraft, etc. Early ad hoc networking applications can be traced back to the DARPA Packet Radio Network (PRNET) project in 1972. The goal of this project was to provide the packet switching networking efficiently in which bandwidth can be shared and uses the store-and-forward routing to transmit information from one node to designated node in mobile wireless environment. The PRNET was asynchronous and can be form with distributed architecture connecting large number of nodes. It used a combination of Aloha and CSMA channel access protocols to support the dynamic sharing of the broadcast radio channel. The limitation of radio coverage can be removed by using multi-hop store-and-forward routing techniques, which effectively enables multi-user communication within a very large geographic area. The main issues of PRNET incorporated in Survivable Radio Networks (SURAN) developed DARPA in 1983, in the area of network scalability, security, processing competency, monitoring capability and energy management. The main objectives were to develop network algorithms to support a network that can scale to tens of thousands of nodes and withstand security attacks, as well as use small, low-cost, low-power radios that could support sophisticated packet radio protocols [2].

A series of new developments inspired a new phase in ad hoc networking in the early 1990. The term "ad hoc networks" adopted in a research paper published in 1994 originated as the idea of an infrastructureless collection of mobile hosts. At the same time, DoD initiated DARPA Global Mobile (GloMo) Information Systems program and the near-term digital radio (NTDR), which aimed to provide office environments ethernet-type multimedia connectivity anytime, anywhere among wireless devices. A two-tier self-organized ad hoc network used by the NDTR. It used clustering and link state routing for packet delivery [1].

Mobile Ad-hoc Networks (MANET) are infrastructureless networks. These networks have no fixed routers, every node could be router. All nodes are capable of movement and can be connected dynamically in arbitrary manner. The responsibilities for organizing and controlling the network are distributed among the terminals themselves. The entire network is mobile, and the individual terminals are allowed to move freely. In this type of networks, some pairs of terminals may not be able to communicate directly with each other and have to relay on some terminals so that the messages are delivered to their destinations. These terminals as an evolution of current mobile phones, laptops, iPAD and emerging PDAs equipped with wireless interfaces. The only external resource needed for their successful operation is the bandwidth. Terminals can communicate directly by using the wireless LAN technologies. The nodes may be located in or on airoplanes, ships, trucks, cars, perhaps even on people or very small devices. The set of applications for mobile ad hoc networks is diverse, ranging from small, static networks that are constrained by power sources, to large-scale, mobile, highly dynamic networks.

The design objectives of ad hoc networks include the speedup of connection setup, the ease of removal of services and users, and the any-time, anywhere network services access on handheld devices. The ad hoc networking offers unique benefits and flexibility for certain environments and applications. They can be created and use anytime, anywhere. Such networks can be intrinsically fault tolerance since they do not operate under the limitations of a fixed topology. Since all the nodes of such networks are allowed to be mobile, the composition of such networks is necessarily time varying. The removal of nodes does only by communicating with others nodes [1].

MANETs are becoming popular since they help realizing network services for mobile users in areas with no pre-existing communications infrastructure, or when the use of such infrastructure requires wireless extension. Internet services can be provided in such area via ad hoc nodes connected to a fixed backbone network through a dedicated gateway device enabling IP networking services. All these advantages make ad hoc networking attractive option in future wireless networks [2].

In the early days, the military, police, and rescue agencies prompted to use such types of network especially in under hostile conditions, including isolated scenes of natural disaster or armed conflict. Soldiers carried the mobile communicator can now talk in ad hoc manner without the need for base stations. The vehicle equipped with audio sensors and cameras can be deployed at targeted regions to gather the important information which can be forwarded back to a sink node via mobile ad hoc communications. Ship-to-ship mobile ad hoc networking is also required since there is no alternative communication paths exit in the absence of ground. In the recent days, home and office networking and collaborative computing with laptop have appeared as other major area of applications. Participants are attending the conferences, meeting can freely use their laptop, iPAD and others handheld devices to form instant ad hoc network for sharing the file and others important information with need of fixed infrastructure base stations and network administrator [1].

1.3 ISSUES AND CHALLANEGS IN AD HOC NETWORKS

In general, mobile ad hoc network is an autonomous collection of mobile devise (laptops, phones, sensor, iPAD etc) that are connected via wireless links and cooperate in a distributed manner and need to organize themselves dynamically in order to provide the necessary network services without using the existing network infrastructure or centralized administration. Nodes are free to join or leave the network. The networks topology may change rapidly and unpredictably since the node move randomly. Nodes that belong within each other's transmission range can communicate directly and are responsible for dynamically discovering each other. For communicating with nodes that reside beyond this range, the node needs to use intermediate nodes to relay the messages hop by hop. Such network may include multiple hops, and hence it is appropriate to call such networks as ''multi-hop wireless ad hoc networks''. Ad hoc wireless networks inherit the traditional problems of wireless communications and wireless networking such as the Link layer design, Channel access and frequency reuse,, Reliability, Routing, Resource Allocation, Network Capacity, Cross Layer Design, Power/energy management, Internet connectivity, security and node cooperation problems. Besides these problems and complexities, the multihop nature, and the lack of fixed infrastructure add a number of characteristics, complexities, and design constraints that are specific to ad hoc networking [3][2].

Autonomous and infrastructure-less: MANET does not rely on any pre-exist fixed infrastructure or centralized administration. Each node operates in distributed peer-to-peer mode, may be worked as an independent router and generates independent information. Since the network management has to be distributed across different nodes, which brings more difficulty in fault detection and management [2].

Multi-hop routing: in the MANET, the key issue of any routing algorithm is that every node acts as a router and a route may be created with intermediate node. Therefore a route may change not only because of end-host mobility but also because of intermediate router mobility.

Mobility issues: The routers are free to move randomly and organize themselves arbitrarily; thus, the topology of network may change quickly and arbitrarily resulting in route changes, frequent network partitions, and possibly packet losses. Such a network may operate in distributed and standalone manner.

Variation in communication link capabilities: The communication capabilities of each node may be varying and operate across different frequency bands. This heterogeneity in node radio capabilities can result in possibly asymmetric links.

Computational capabilities of nodes: Each mobile node may be equipped with a different hardware configuration and embedded with different version of software. These are resulting in variability in computational capabilities. Architecting and designing network protocols and algorithms for these heterogeneous networks cannot be easy task, thus requiring dynamic adaptation to the changing conditions.

Resource Management issue: The available computing and networking resources should be utilized by application in efficient manner. Many applications estimate the best use of these resources using one or more environment parameters to perform their adaptation. The ad hoc networks have the broader range of environment parameters; therefore resources allocation becomes more difficult.

Energy constrained operation: Mobile nodes are equipped with batteries having limited power. This in turn limits network services and applications that can be supported by each node. The application with complex routing algorithms cannot be supported. This becomes a bigger issue in mobile ad hoc networks since, each mobile node function as a router, additional energy is required to forward packets from other nodes [2].

Network security: The openness of the channel channels, any nodes can join and leave the network, absence of infrastructure and dynamically and rapidly changing topology, make ad hoc networks security a challenging task.

Cooperation enforcing: The mobile node involvement is needed to retain an ad hoc network operational to provide the basic network services such as packet forwarding and routing. One or more intermediate nodes between the source and destination cooperate in the forwarding the packet along the route to the destination. The intermediate autonomous nodes may refuse to use their limited resources to forward the packet to other nodes. This can lead to inefficient use of the network resources since messages may have to be rerouted through different paths to the destination node. A node that does not participate in routing is called a misbehaving node. The misbehaviors in packet forwarding can be caused by nodes that are malicious or selfish. A malicious node participates in routing but it is intentionally damage network functioning by dropping packets. Selfish nodes may not wish to consume their resources to carry the source's traffic. Such a node uses the network services but does not cooperate [4].

1.4 ROUTING IN AD HOC NETWORKS

Routing in mobile ad hoc networks faces additional problems and challenges, when compared to routing in traditional wired networks with fixed infrastructure since the nature of ad hoc network is highly dynamic results in rapid and unpredictable changes in network topology. The challenges and complexities, together with critical importance of routing protocol in establishing the communication among mobile nodes make active area of research. Ah hoc routing algorithms organize the network by automatically discovering the topology of the connectivity among constituent nodes. The collection of interconnected nodes serves as the network's communications infrastructure. MANETs are nonhierarchical systems, with each node (mobile router) serving identical roles as a source, sink, and pass-through for data.

Protocols	Example
Proactive protocols	Destination-sequenced Distance- Vector (DSDV) Optimized Link- State Routing (OLSR) Topology dissemination Based on Reverse Path forwarding (TBRPF)
Reactive protocols	Ad Hoc On-Demand Distance-Vector (AODV) Dynamic Source Routing (DSR) Temporally Ordered Routing Algorithms (TORA) Associativity Based Routing (ABR)

Table 1.1 CLASSIFICATION OF ROUTING PROTOCAL

Most of the existing routing protocols follow two different design approaches in MANET shown in table 1.1: the *tabledriven (*Proactive protocols*)* and the *source-initiated on-demand (*Reactive protocols*)* approaches. In table driven routing protocols, the protocols consistent and up-to-date routing information to all nodes is maintained at each node whereas in on-demand routing the routes are created only when desired by the source host [5].

The Destination-Sequenced Distance-Vector Routing (DSDV) protocol is explained in [6] is a distance vector routing protocol based on the classical Bellman-Ford routing algorithms. Every node maintains a routing table with one route entry for each destination in which the shortest path route (based on number of hops) is computed. Routing table updates are periodically transmitted throughout the network in order to maintain table consistency. A destination sequence number is used to remove the loops in routes. Sequence number is used to choose an alternative path between source and destination. It is incremented whenever a change occurs in its neighborhood. The route labeled with the most recent sequence number is always used.

Optimized Link- State Routing (OLSR) protocol [7] is a link state protocol and intended to reduce duplicate retransmission in the same area. The routes are immediately available when needed. Forwarding of packet is done using hop by hop routing. Each node identifies its MPRs for forwarding the control traffic that causes reducing the size of control message and minimizing the overhead from flooding control traffic.

TBRPF is described in paper [8] is a link-state routing protocol that uses a different technique to reduce the routing overhead. It provides a complete topology link-state routing protocol in that each node is provided with the state of each link in the network. TBRPF is extremely active to detect a change in the status of links and alternate routes are immediately computed whenever a link in the path is down. The TBRPF protocol consists of two phases: (I) Neighbor Discovery, and (II) Broadcasting of link-state updates. The purpose of the neighbor discovery is to allow each node in the network to quickly detect the neighboring nodes with which the node has a bi-directional link.

The Ad Hoc On-Demand Distance Vector (AODV) routing protocol described in [9] is an improved version of the DSDV algorithm. The intention behind to develop the AODV protocol is that it typically minimizes the number of required broadcasts by creating routes on a demand basis, as opposed to maintaining a complete list of routes as in the DSDV algorithm. The route finding process is initiated on on-demand, since nodes that are not on a selected path do not maintain routing information or participate in routing table exchanges. The AODV work as follows: When a source has packet to transmit to an unknown destination, it broadcasts a Route Request (RREQ) using flooding in the network. At each intermediate node, when it received a RREQ, a route to form intermediate node to the source is created. If the receiving not the destination then it rebroadcasts the RREQ otherwise it send a unicast Route Reply (RREP) to the source.

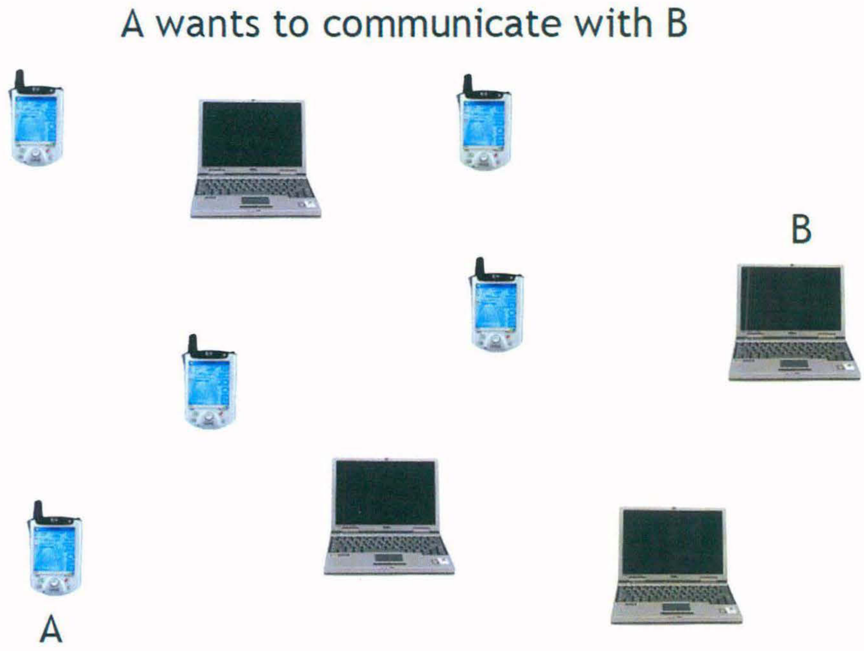

Figure 1.3 Two nodes A and B want to communicate in AODV

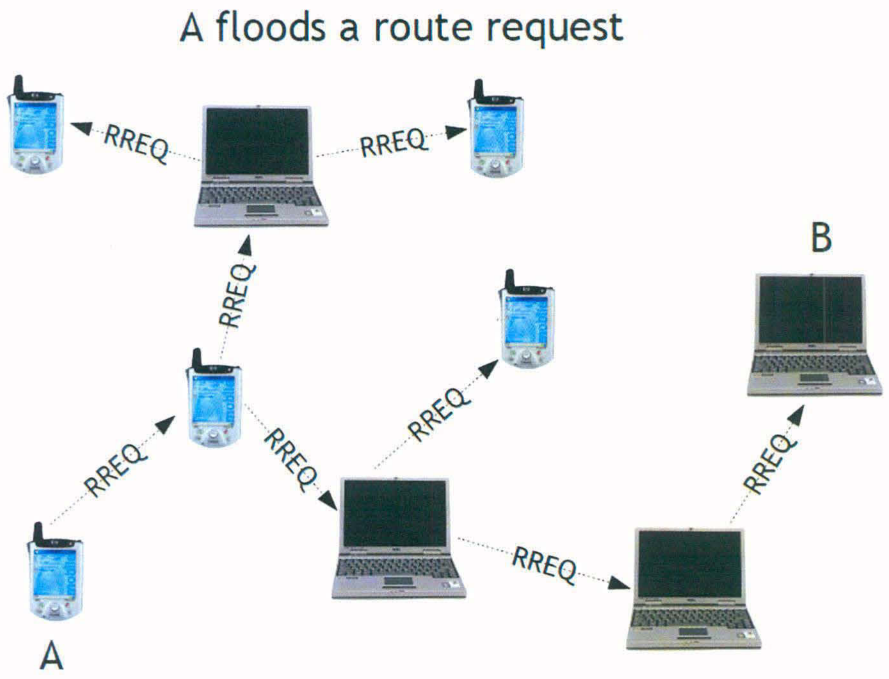

Figure 1.4 Route Request in AODV

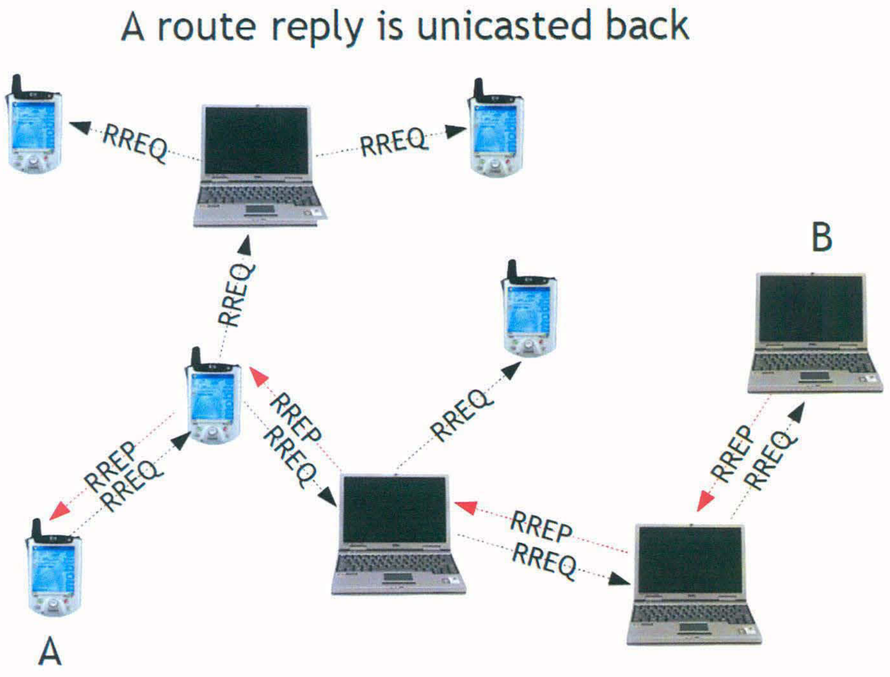

Figure 1.5 Route Reply in AODV

DSR is a loop-free, source initiated on demand routing protocol proposed in [10]. DSR algorithm makes for operation are that the network diameter is relatively small and that the mobile nodes can enable a promiscuous receive mode, whereby every received packet is delivered to the network driver software without filtering by destination address [5]. DSR allows nodes to keep multiple routes to a destination in their cache. Hence, when a link on a route is broken, the source node can check its cache for another valid route. If such a route is found, route reconstruction does not need to be reinvoked. Packet contains all routing information, reduce the bandwidth and others resources computation.

Temporally Ordered Routing Algorithms (TORA) routing protocol is source-initiated on-demand routing protocol that is best suited for a network with a highly changing topology of large dense population nodes. It is built on the concept of link reversal of the Directed Acyclic Graph (ACG) [11]. It is bandwidth efficient since its support for multiple routes. This protocol retains multiple route possibilities for a single source/destination pair. Route reconstruction is not necessary until all known routes to a destination are deemed invalid.

Associativity Based Routing (ABR) is ABR protocol is also a loop and deadlock free protocol. It defined a new routing metric termed degree of association stability in selecting routes, so that route may exist for longer, thus more stable and requiring less updates subsequently. Hence, although the resulting path does not necessarily result in the smallest possible number of hops, the path tends to be longer lived than other routes. A long-lived route requires fewer route reconstructions and therefore yields higher throughput [12].

The reactive protocols are more efficient in term of control overhead and power consumption, since routes are only established on demand basis. While in proactive protocols, routes are updated periodically to keep information up-to-date and consistent. In each nodes cache, multiple routes are update also that might never be needed, adding unnecessary routing overheads. Proactive routing protocols have less end-to-end delay since routing information is constantly updated and, routes to every destination are always available [2].

Authenticated Routing for Ad-hoc Networks (ARAN) detects and protects against malicious actions by third parties and peers in Ad-hoc environment. ARAN requires that nodes keep one routing table entry per source-destination pair that is currently active[15].

Secure Efficient Ad hoc Distance vector routing protocol (SEAD) is robust against multiple uncoordinated attackers creating incorrect routing state in any other node, in spite of active attackers or compromised nodes in the network [15].

Secure Routing Protocol, in which, the use with DSR to design SRP as an extension header that is attached to ROUTE REQUEST and ROUTE REPLY packets. SRP requires a security association only between communicating nodes, it uses extremely lightweight mechanisms to prevent other attacks [15].

The Secure AODV implements two concepts secure binding between IPv6 addresses and the independent of any trusted security service, Signed evidence produced by the originator of the message and signature verification by the destination, without any form of delegation of trust [15].

Routing protocols for fixed networks usually collect the information about the network topology and select routing paths locally based on this information. In addition, in fixed networks the paths do not need to be optimal as there resource constraints do not play an important role. However, in ad hoc networks the situation differs significantly and this forces the routing protocols to choose paths so that resource usage is optimized and to take into account consistency problems arising from the dynamically changing topology. Routes should be advertised and set up obeying to the chosen routing protocol and should truthfully reflect the knowledge of the topology of the network. To get information necessary for successful malicious behavior, nodes can attract traffic to

themselves or their machinating nodes by means of false routing advertisements. Denial-of-service attacks can be achieved by fake routing information (injecting of incorrect routing information or replay of old routing information or 'black hole routes' [13].
The following types of misbehavior can be indicated:

- No forwarding of data and control packets.
- Offer unusual traffic attraction (advertises many very good routes or advertises routes very fast, so they are deemed good routes),
- Route salvaging (i.e. rerouting to avoid a broken link), although no error has been observed,
- Lack of error messages, although an error has been observed,
- Changing error messages, although no error has been observed,

1.5 COOPERATION IN AD HOC NETWORKS

In the absence of a fixed infrastructure, the basic network operations of wireless ad hoc network rely on cooperation of the nodes. The delivery of packets from source node to destination node relies on the several others nodes to help in forwarding the packets since destination is the beyond the transmission range of a source node. To increase the life time and energy efficiency of the network, it is allowing packets to be delivered over several short transmission links rather than one long transmission link. If the destination node is not directly approachable, the intermediate nodes between the source and destination make mutual contribution in the transmission by forwarding or relaying the packet along the route to the destination. However, the nodes in the ad hoc network may belong to different organization, company and person, so these nodes are autonomous and functioning for their own self-interest to minimize the use of their limited resources like energy, may refuse to forward packets for other nodes. This is the fundamental problem of the ad hoc network in which nodes are participating with selfish behavior. Selfishness of nodes may lead to inefficient use of the network resources since packets may have to be rerouted through alternative paths to the destination node or retransmitted when nodes dropped packets [4][23].

The researchers have addressed the several problems of inspiring the cooperation among node which promise to forward the packets but do not termed as misbehaving. They proposed many game theoretic solutions to enhance the efficiency of the networks with autonomous nodes acting on their self-interest to minimize the use of their limited resources. These solutions assumed to give nodes credit for packet forwarding or relaying for others node. The cooperative nodes earn credit through its behavior and use the accumulated credit to buying cooperative behavior from other nodes [17], [19] [21].

Another approach to inspiring the cooperation among nodes which agree to forward the packets based on the reputation of nodes gathered from neighboring nodes. These neighboring nodes continue to monitor the behavior the node whether it forwarding the packets or they are dropping /misbehaving with the packets [16], [18]. While the researcher provided many solutions to encourage the cooperation among nodes, however there are several possible drawbacks with of these solutions. The monitoring nodes may be misinterpreting the behavior of nodes, increased the computation to monitor the misbehaviors for other nodes, increase the overhead on the network by consuming the channel capacity, forwarding the reputation information gathered from others nodes, and use the its limited resources like energy for monitoring the misbehavior for others.

1.5.1 REPUTATION SYSTEM FOR AD HOC NETWORKS

Energy consumption is one of the most important performance metrics for wireless ad hoc networks because it directly relates to the operational lifetime of the network. Since energy is a valuable resource, intermediate nodes may not wish to consume their energy to carry the source's traffic. This is called "Selfish" of the node. However, if every node behaves 'Selfish' and refuse to cooperate, network throughput may be drastically reduced [16][17]. The use of reputation systems to decide who to trust, and to encourage trustworthy behavior and to remove selfish nodes. Three goals for reputation systems [16][18]:

- To provide information to distinguish between a trustworthy principal and an untrustworthy principal.
- To encourage principals to act in a trustworthy manner.
- To discourage untrustworthy principals from participating in the service the reputation mechanism is present to protect.

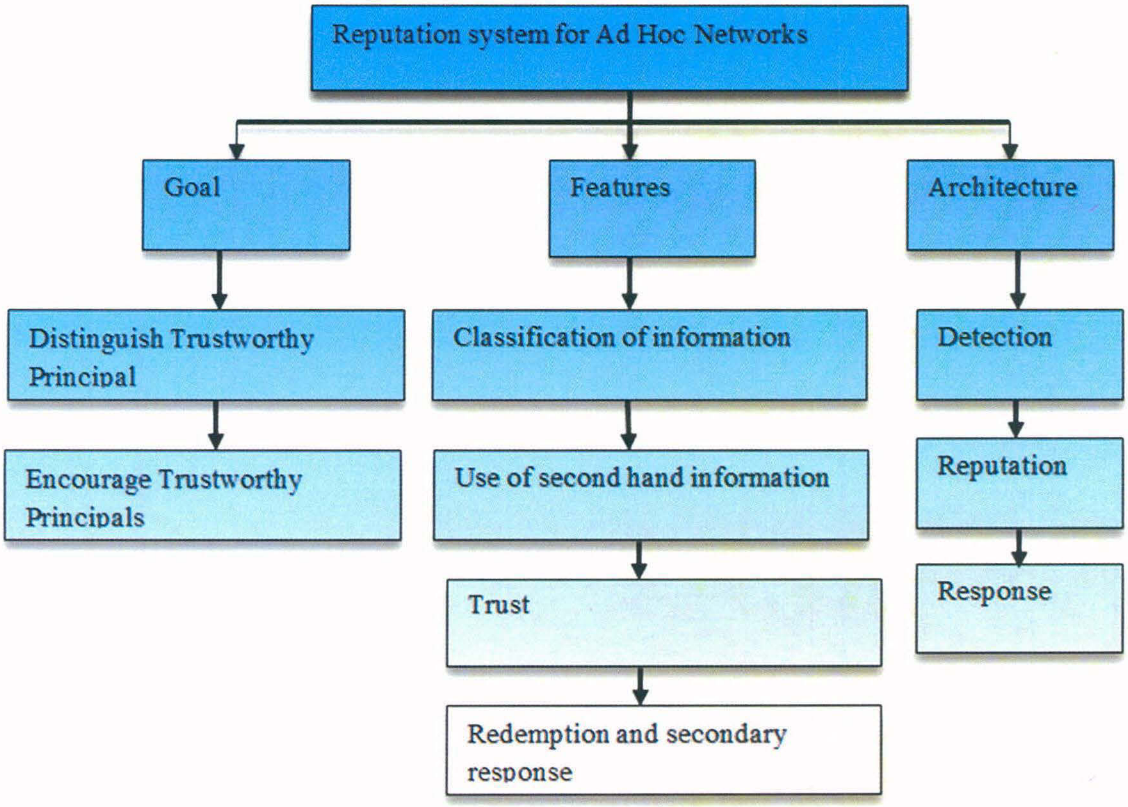
Reputation system for Ad Hoc Networks
Goal
Features
Architecture
Distinguish Trustworthy Principal
Classification of information
Detection
Encourage Trustworthy Principals
Use of second hand information
Reputation
Trust
Response
Redemption and secondary response

Figure 1.6 Reputation System for Ad Hoc Networks

The features of a reputation system [16][18]:

- **Representation of information and classification:** These determine how monitored events are stored and translated into reputation ratings, and how ratings are classified for response.

- **Use of second-hand information**: Reputation systems can either rely exclusively on their own observations or also consider information obtained by others. Secondhand information can, however, be spurious, which raises the questions of how to incorporate it in a safe way and whether to propagate it.

- **Trust**: The use of trust influences the decision of using second-hand information. The design choices are about how to build trust, out-of-band trust versus building trust on experience, how to represent trust, and how to manage the influence of trust on responses.

- **Redemption and secondary response:** When a node has been isolated, it can no longer be observed. The question of how those nodes should be rated over time is addressed by these two features. If the misbehavior of a node is temporary, a redemption mechanism ensures that it can come back to the network.

To enable nodes to adapt to changes in the network environment caused by misbehaving nodes, a reputation system consists of three modules, monitoring, reputation and response modules. The goal of monitoring is to gather first-hand information about the behavior of nodes in a network. The two main ideas behind reputation that it is used as an incentive for good behavior and provides a basis for the choice of transaction partners. The response aims at isolating misbehaving nodes. In the wireless ad hoc networks one way to incentive nodes to forward other's nodes' packet is through the use of reputation schemes where cooperation is induced by the threat of partial or total network disconnection if a node acts selfish [19]. The reputation is very useful to design secure routing protocols for Wireless Ad Hoc Networks.

1.5.2 APPLICATION OF GAME THEORY TO AD HOC NETWORKS

Game theory is a field of applied mathematics that describes and analyzes the ways in which strategic interaction among the rational entities produce the outcome with respect to the utilities of those rational entities. The game theory has been applied in the area of economics, political science, biology, and sociology, engineering and computer science. In the past few years, the different aspects of computer networks have been studies using game theory as a tool. There has been shown the interest in developing networking games to analyze the performance of wireless ad hoc networks. Since the game theoretic models developed for ad hoc networks focus on the networks services provided for others, resolve contentions among nodes, routing decision, packet forwarding and issues related to transport layer etc. of the networks. This model is also used to explore how selfishness of the individual nodes may affect the performance of the whole network. Table 1.1 showing how to the different components of a game map to the elements of a ad hoc network [20].

Components of a game	**Element of an ad hoc network**
Players	Nodes in the network
Strategy	Action related to the functionality being explored (e.g., the decision to forward packets or not, the setting of power levels, access the channel)
Utility function	Performance metrics (Packet deliver ratio, throughput, delay, target signal-to-noise ratio, energy)

Table 1.1 Mapping of games components to elements of an ad hoc network.

1.6 MOTIVATION

An interested problem is that how to provide the appropriate incentives to discourage selfish behavior of the node. The overall performance of the network is suffered by selfishness. Examples include a node may be increasing its transmission power which leads to interference at its neighbors, a node start immediately retransmitting a frame in case of collisions without going through a backoff phase or a node is refusing to forward packets for others.[20]

1.7 PROPOSED WORK

In this work, we proposed to use game theoretic approach to increase life time of nodes and to identify and avoid selfish node from participating in routing. To achieve this aim we have set the following objectives:

✓ To design a selfish node avoidance routing protocol that detects and isolates selfish nodes by making routing decisions based on past experience, observation, and collecting the forwarding behavior of the selfish nodes.

✓ A Game theoretic model may be proposed to extend the life of the nodes by energy conservation but also preventing node from being selfish in the network and enhancing the cooperation among the mobile nodes.

✓ To integrate the proposed model with AODV protocol and analyze the packet delivery ratio of cooperative nodes and selfish nodes, routing overhead by simulating it using network simulator ns-2.

1.8 ORGANIZATION OF DISSERTATION

The rest of the dissertation is organized as follows: in chapter 2, the works related to the topic of the dissertation are presented. In chapter 3, the proposed work entitled *"Game Theoretic Model for Selfish Node Avoidance"* is being studied. The simulation results of the proposed work are presented in the chapter 4. Finally, we conclude the work in the chapter 5.

TH-20625

Jawaharlal Nehru Library

CHAPTER 2
RELATED WORK

In the ad hoc networks, solutions for the problems of selfish nodes have been studied either using game theory or reputation systems. Recently there have been a sequence of research papers [4], [16], [17], [18], [19], [21], [23], [25], and [26] published in the area of communication and ad hoc networks that made efforts to solve various problems introduced by selfish nodes.. A node tries to select a strategy that maximizes its own gain called rational node. Some of these studies have a common approach of incurring the credits if they are considered to provide the service for others. For example, in ad hoc network, nodes earn credits for packet forwarding or relaying for other nodes. The cooperative nodes earn credit through its behavior and use the accumulated credit to buying cooperative behavior from other nodes. While others have a common approach to motivate the cooperation among nodes by gathering secondhand information. Based on this information of neighboring nodes, a source node decides to forward packets through a node having good reputation.

2.1 GAME THEORETIC MODELS

Authors in [4] provided an introduction to neutral cooperation in the ad hoc network which is based on game theoretic analysis of selfishness of the nodes with a focus on the packet forwarding and relaying scenarios. Authors explained the two-player packet forwarding scenario and three-player packet forwarding scenario as follows:

Two players (nodes) p1 and p2 are considered to forward packet for each other's. Two set of actions a= {FORWARD (F), DOES NOT FORWARD (DNF)} assumed to be picked simultaneously by the source player. Both sources are assumed to have an identical fixed cost $c \in (0,1)$ to forward a packet for the other source and a fixed unit reward for having a packet successfully delivered to its destination. The four action profiles are possible as given below: $a_1^* = (DNF, DNF)$, $a_2^* = (F, DNF), a_3^* = (DNF, F)$, and $a_4^* = (F, F)$. The payoff for both sources is denoted by (π_1, π_2) where $\pi_i(\alpha)$ the payoff of the i^th^ source, as function of the actions that both sources choose and $\alpha \in (a_1^*, a_2^*, a_3^*, a_4^*)$. If the action profile a_1^* is chosen, then player p1 receive a payoff of $\pi_1(a_1^*) = 0$ and p2 receive a payoff $\pi_2(a_1^*) = 0$. Similarly $\pi_1(a_2^*) = -c$, $\pi_2(a_1^*) = -1$, $\pi_1(a_3^*) = 1$, $\pi_2(a_3^*) = -c$, and $\pi_1(a_4^*) = 1 - c$, $\pi_2(a_4^*) = 1 - c$. Rational sources always choose their actions in order to maximize their own payoffs. The only rational action for both sources is to choose DNF since $\pi_1(a_1^*) = 0 > \pi_1(a_2^*) = -c$ and $\pi_1(a_3^*) = 1 > \pi_1(a_4^*) = 1 - c$. Therefore, the only rational action profile is a_1^* which the Nash equilibria. In the repeated game, the strategy is as follows: initially each source start playing with F and continue to play F until the other player chooses DNF. If the player p1 chooses to play DNF in the nth stage, the total discounted payoff is

$$\prod_1 = \left(\sum_{k=0}^{n-1} \omega^k\right)(1-c) + \omega^n.1$$

where 0<ω<1.

For the three players forwarding game, the action profile set is represented by $\{a_1^*, a_2^*, a_3^*, a_4^*, a_5^*, a_6^*, a_7^*, a_8^*\}$

where

$a_1^* = (DNF, DNF, DNF)$,

$a_2^* = (F, DNF, DNF)$,

$a_3^* = (DNF, F, DNF)$,

$a_4^* = (F, F, DNF)$,

$a_5^* = (DNF, DNF, F),$

$a_6^* = (F, DNF, F),$

$a_7^* = (DNF, F, F),$

$a_8^* = (F, F, F).$

The respective payoff of these action profile are (0,0,0), (-c,0,1), (1,-c,0),(1-c,-c,1), (0,1,-c), (-c,1,1-c), (1,1-c,-c) and (1-c,1-c,1-c). The only rational action profile is a_1^* which the Nash equilibria. For same strategy, if the player p1 chooses to play DNF in the nth stage, the total discounted payoff is

$$\prod_1 = \left(\sum_{k=0}^{n-1} \omega^k\right)(1-c) + (\omega^n + \omega^{n+1}).1$$

In [16], the local reputation information is used to decide the reputation value of nodes. Author suggested that every node have knowledge of the reputation value $R\in [R_{min}, R_{max}]$ of all its neighbor nodes. Three thresholds are given as: i) R_1, ii) R_2, iii) R_3, where $R_{\min} < R_1 < R_2 < R_3 < R_{\max}$. A node can be categorized as follows: if node is said to be good if its reputation$R \in [R_{3,}R_{\max})$; It is misleading if $\in [R_{3,}R_2)$, it is selfish if $R \in [R_{2,}R_1)$. Otherwise it is unable to determine whether N is selfish or not if $R \in [R_{min,}R_1)$. At the beginning, all nodes have good reputation. The reputation of node is increased if it forwards a packet otherwise it is decreased. When the route is initiated, a node with good reputation is chosen. Otherwise, if no node is available with good reputation, it prefers to choose misleading node.

In [17] Wireless nodes are considered with the energy constraints. Nodes are assumed to rational. A rational node means that its actions are strictly determined by self-interest. Each node is associated with a minimum lifetime constraint. The throughput of each node is measured in terms of the ratio of the number of successful rely requests generated by the node. The optimal tradeoff between the throughput and lifetime of nodes are studied using the game theory. A distributed Generous TFT (tit for tat) algorithms was introduce which decides whether to accept or reject a rely request.

In [19] a game theoretic reputation mechanism is introduced to incentivize nodes which forward the packet for others, where cooperation is induced by the threat of partial or total network disconnection if a node acts selfishly. It is shown that a node which is perceived as selfish node due to the problem of packet collisions and interference can be avoided. A method named as DARWIN (Distributed and Adaptive Reputation mechanism for Wireless ad hoc Networks) has been introduced to avoid retaliation situations after a node is falsely perceived as selfish to help restore cooperation quickly.

In [21] a game theoretic model to investigate the conditions for cooperation in wireless ad hoc networks, without incentive mechanisms has been presented. Several theorems for the strategy always defects (AIID) are stated and proved for cooperation, considering the topology of the network and the existing communication routes. It is concluded that with a very high probability, there will be some nodes that have AIID as their best strategy.

2.2 REPUTATION SYSTEM BASED MODELS

In [18] a reputation-based system as an extension to source routing protocols for detecting and punishing selfish nodes has been introduced. It is shown that by punishing these nodes will not benefit them. Instead, being cooperative has a better chance to increase their benefit.

In [23] a context-free (COFFEE) protocol is presented that does not rely on past experience and selfish behavior detection. This protocol can send packets through a route without knowing whether the intermediate nodes are selfish or not. The information about route and destination is removed from packets by originating node to hide the identity of the destination. The encrypted packets with a secret key and the encrypted key are sent by the originating nodes and key can only be revealed when the entire transmission process is over. Since the identity of the destination is hidden, when a node receives any packet, it may think that the packet could be destined to it; therefore, it will forward the packet to others nodes to get the answer.

In [25], an approach for detection of selfish behavior in the wireless mobile ad hoc networks is presented. This approach is based on Dempster-Shafer theory (DST) named as Dempster-Shafer theory based selfishness detection framework (DST-SDF). SDT-SDF trusts on the end-to-end packet acknowledgments. The acknowledgment is expected for each packet send to destination node with a pretended time. If it arrives within the predefined time, the source node has reason to claim that all intermediate nodes on the route are cooperative. Otherwise the source node believes that some of the intermediate nodes are not cooperating and showing selfishness in forwarding the packets on the route. After the timeout, a special recommendation message is broadcast to inform the other nodes about its behavior. This recommendation messages is used to evaluate the selfishness of each node using DST algorithms. The resulting values can be used for routing decision.

In [26], the CORE mechanism is proposed based on the reputation concept to enforce cooperation among the nodes of a MANET and to prevent passive denial of service attacks due to node selfishness. CORE calculates the reputation of a node using its own experience and experience of other nodes as well. Both experiences can be combined to form a function. The Watchdog (WD) uses this function for evaluating the behavior of the other nodes. If the observed behavior is the same as the outcome of this function, the rating of the observed node remains the same, otherwise it is altered.

After reviewing the related work, it is observed that game theory can be used as the tools for analyzing selfishness and complex interactions between nodes in ad hoc network. Above techniques can be combined with other schemes, algorithms and analytical tools to derive a new framework for routing in wireless ad hoc networks.

CHAPTER 3

GAME THEORETIC MODEL FOR SELFISH NODE AVOIDANCE

Wireless ad hoc network uses the multihop transmission to allow the delivery of packets to destination node since it is the beyond the transmission range of an originating source node. To increase the life time and energy efficiency of the network, it is allowing packets to be delivered over several short transmission links rather than one long transmission link. If the destination node is not directly approachable, the intermediate nodes between the source and destination make mutual contribution in the transmission by forwarding or relaying the packet along the route to the destination. For the case of military network, it is reasonable to assume that intermediate nodes will always forward packets for other nodes when requested to do so. However, this assumption may not be valid since nodes are autonomous and functioning for their own self-interest to minimize the use of their limited resources like energy, may refuse to forward packets for other nodes. Selfish behavior of nodes of can lead to inefficient use of the network resources since packets may have to be rerouted through alternative paths to the destination node or retransmitted when nodes dropped packets [4].

The researchers have studied the several problems of inspiring the cooperation among nodes and avoid the selfish node in the ad hoc networks. They proposed many game theoretic solutions to enhance the efficiency of the networks with autonomous nodes acting on their self-interest to minimize the use of their limited resources. These solutions assumed to give nodes credit for packet forwarding or relaying for other nodes. The cooperative nodes earn credit through its behavior and use the accumulated credit to buying cooperative behavior from other nodes [19] [21]. Another approach to inspiring the cooperation among nodes and avoid selfish nodes in the ad hoc network based on the reputation information of nodes gathered from neighboring nodes. These neighboring nodes continue to monitor the behavior of the nodes whether it is forwarding the packets or they are dropping /misbehaving with the packets [16], [18]. While the researcher provided many solutions to encourage the cooperation among nodes, however there are several possible drawbacks with of these solutions. The monitoring nodes may be misinterpreting the behavior of nodes, increased the computation to monitor the misbehaviors for other nodes, increase the overhead on the network by consuming the channel capacity, forwarding the reputation information gathered from others nodes, and use its limited resources like energy for monitoring the misbehavior for others.

In this chapter, we introduce the basics of game theory [20],[22]that is used in design of model for proposed work since the game theory aims to effectively use in modeling the interaction among independent nodes in an ad hoc network.

3.1 Basics of Game Theory

Game theory is discipline of applied mathematics that models and analyzes interactive decision situations. The main areas of application of game theory are mathematics, economics, political science, biology, and sociology. It was founded by the great mathematician John von Neumann.

Games are models for the collaboration among individual rational decision makers. The rational decision makers are called to as players of the games. These players choose a single action from a set of possible actions. Each player get the resulting outcome after performing their chosen actions, the outcomes influence the players is called interaction. Each player evaluates the resulting outcome through a payoff or "utility" function representing their objectives.

Mathematically, a general form of a game G is represented by $G = \{N, A,, <u_i>\}$ where

$N = \{1, 2, \ldots, n\}$ is the set of players.

$A = A_1 \times A_2 \times \ldots \times A_n$ is the Cartesian product of the sets of actions available to each player and A_i represented the action set for player i.

$<u_i> = \{u_1, \ldots, u_n\}$ is the set of utility functions that each player i wants to maximize, where $u_i: A \rightarrow R$.

The *action tuple* can define as together a_i and a_{-i} where the action a_i chosen by i^th^ player, and the actions chosen by all others the players in the game denoted as a_{-i}.

The *best reaction* define as an action chosen by a player that maximizes his utility function for a given action tuple of the other players. Mathematically, r is a best reaction by player i to a_{-i} if

$$r \in \{argmax\, u_i(a_i, a_{-i})\}$$

Definition 1: ***Nash equilibrium (NE)*** is an action tuple that corresponds to the mutual best reaction. In other words, NE is an action tuple $\mathbf{a}^* = (a_1 ^* \ldots a_n ^*)$ where no individual player can benefit from unilateral changing its action, that is,

$$u_i(a_1^*, \ldots, a_{i-1}^* a_i^* a_{i+}^*, \ldots, a_n^*) \geq u_i(a_1^*, \ldots, a_{i-1}^* a_i a_{i+}^*, \ldots, a_n^*)$$

for all a_i in the possible action set of player i and for all i=1,..,n.

Definition 2: ***Pareto optimal*** is a set of actions a = $(a_1,\ldots,a_n)$ is Pareto optimal if there exists no other set of actions for which one or more players can improve their payoff without reducing the payoff of other players.

Definition 3: The Prisoner's Dilemma is a fundamental problem in game theory that demonstrates why two players might not cooperate even if it is in both their best interests to do so. The generalized form of game between two players is use is known as prisoner's dilemma. Both players have two possible pure strategies: Cooperate (C) or Defect (D) and payoff for their actions are shown in table-1. Each of the player P1 and P2 have two possible choices to play C or D is called strategies space S_i={C, D} for i={1,2}. The action profile can be defined as the element of the product-space of the strategy space of each player. If the P1 play D and the P2 play C, the P1 gets the temptation to defect payoff of 5 points while the P2 receives the payoff of 0 points. If both cooperate they get the reward for mutual cooperation payoff of 3 points each, while if they both defect they get the punishment for mutual defection payoff of 1 point.

Table-3.1 payoff metrics of the Prisoner Dilemma

P2 **P1**	**Cooperate**	**Defect**
Cooperate	3 3	0 5
Defect	5 0	1 1

Only a stable solution of this game is that both players cooperate. Therefore the action profile a={C, C} is the only NE of this example of the Prisoner Dilemma.While in three others cases, at least one player can switch from C to D and improve his own payoff. On Other hand, much better outcome for both players happens when neither of them cooperates. The action profile other than a={C, C} is Pareto optimal of this example of the Prisoner Dilemma.

3.2 Game Theoretic Model of Packet Forwarding

In this section, a game theoretic model for analyzing the selfishness in forwarding packets is presented. Application of Game theory in this model is based on the hypothesis that node forward the packets rationally, in the sense that each node has an utility function that a node tries to maximize its utility function with imposed constraints on its choices of actions in the game.

3.2.1 Preliminaries

It is assumed that an ad hoc network consists of two types of nodes - non-selfish node and selfish node but not malicious. These nodes are equipped with a limited power battery. A selfish node is a rational user that wants to save its energy by not forwarding the packet for others. The packet forwarding through multi-hop routes from the originating node to destination node relies on the intermediate nodes. Wireless links are bidirectional. The node listens to all the transmitted packets from their neighbors. The dynamic nature of ad hoc networks leads to imperfection or noise in transmission observed by a node.

The nodes resources are consumed by packets forwarding for others. It is defined that the forwarding/relaying cost to be β where $\beta \geq 1$. A node received the reward α when it's a packet is relayed where $\alpha \geq 1$. Any two neighbor nodes desired to send the packets to each other and they forward each other's packet. We can identify such pair of nodes and analyzed the interaction between them as a two-player game. It is reasonable to expect that the packet forwarding game between two players play several times since they decide whether to drop or forward their respective packets. It also assumes that time is divided into slots and a node is able to send sufficiently large number of packets in each slot. At the end of the each slot, the node monitors the throughput of its neighbor by overhearing. If throughput is below a certain threshold, it stops the transmitting packet. The node is denoted by a subscript *i* and its neighbor by a subscript $-i$.

3.2.2 Forwarding game formulation

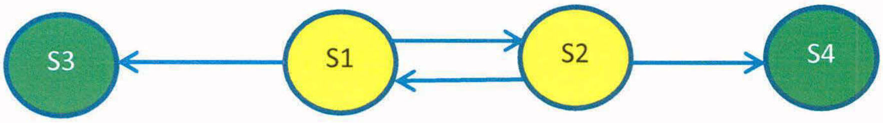

Figure 3.1 a two player packet forwarding game scenario

This section describe a two player packet forwarding scenario for natural cooperation and how the natural cooperation between a pair of nodes is affected by different assumptions about the selfishness in packet forwarding and noise observed while overhearing.

In figure 3.1, there are four nodes S1 to S4. S1 and S2 are willing to send packets to their destination S4 and S3 respectively. Without cooperation of S1, S2 is not able to send its packets to S3 and similarly, S1 can't send packets to S4. The set of actions are available to each player are as "forward" or "Do not forward" the packet of the other source. The payoff is defined as the difference between the reward of successfully deliver packet minus the cost of the forwarding a packet for the other sources. In this scenario, the payoff matrix of two player forwarding game is give in Table-2.

***TABLE-2* PAYOFF MATRIX OF TWO PLAYER FORWARDING GAME**

	S2 DOES NOT FORWARD(DNF)	S2 FORWARD(F)
S1 DOES NOT FORWARD(DNF)	(0, 0)	(α, -β)
S1 FORWARD(F)	(-β, α)	(α-β, α-β)

Packet drop due to selfishness in packet forwarding: - The packet forwarding through multi-hop routes from the originating node to destination node relies on the intermediate nodes. However, the intermediate nodes provide the packet forwarding, consume their limited energy resources. Therefore they, in order to conserve its limited energy resources could decide not to cooperate in the packet forwarding by switching off its interface. If many of them are acting selfishly by changing their behavior in this way, may lead to the collapse of the network. Nodes may choose to participate in packet forwarding but uses the minimum transmission power to deliver a packet acting as selfishly. Source node may not overhear this transmission, assumed that the packet is dropped by relay node.

We define a drop probability $p_{-i}^{(t)}$ of node –*i* as

$$p_{-i}^{(t)} = \begin{cases} 0 \quad if \ \frac{E_c}{E_f} < \theta_{E,}, & Packet\ is\ dropped \\ \frac{E_c - \theta_{E,}E_f}{E_f - \theta_E E_f} \quad if \ \frac{E_c}{E_f} \geq \theta_{E,}, & packet\ is\ forwarded \end{cases} \tag{1}$$

where E_c is the residual energy, E_f is the full energy and θ_E is threshold energy ratio. The relay nodes monitor its energy level before forwarding a packet, if it is below θ_E then relay node drop the packet otherwise forward a packet. The θ_E may not be the same for all nodes.

Packet perceived to drop due to noise observed in overhearing:- The nodes overhear all the transmitted packets from their neighbors. Due to noise in transmission, it is not always possible to detect whether a relay node forwarded a packet or not. A packet may be perceived to drop by -*i* since node *i* is not completely overhear the packet transmission but it is not dropped. Let us assume that length of a packet is *L* bits. If node *i* did not overhear all *L* bits of a packet, it is assumed to be dropped by –*i*. it is assumed that the loss probability of a bit is $p_b = 10^{-4}$.

Probability that node *i* overhear forwarded packet is $(1 - p_b)^L$.

Probability that node -*i* drops a packet at time slot *t* is $p_e = 1 - (1 - p_b)^L$. (2)

A packet may be dropped either selfishness in packet forwarding or noise observed in overhearing. By overhearing the transmission, node *i* then estimates the perceived dropping probability $\hat{p}_{-i}^{(t)}$ of its neighbor at time slot t≥0. Further, It is assuming that in each slot *t*, node *i* wishes to send *N* packets through node *–i* to its destination. The throughput of node *–i* estimated by node *i* in time slot *t* is can be expressed as

$$\tau_{-i}^{(t)} = N\hat{p}_{-i}^{(t)}$$
$$= N[p_{-i}^{(t)} + \left(1 - p_{-i}^{(t)}\right)p_e]$$

Substituting p_e form (2) in above expression, we get

$$\tau_{-i}^{(t)} = N\ \left[\left(p_{-i}^{(t)} + \left(1 - p_{-i}^{(t)}\right)\right)(1 - (1 - p_b)^L)\right] \tag{3}$$

We defined the normalize throughput of node *–i* as

$$\hat{\tau}_{-i}^{(t)} = \frac{node\ i\ estimate\ number\ of\ packet\ forwared\ by - i}{actul\ number\ of\ packet\ send\ to - i}$$

$$\hat{\tau}_{-i}^{(t)} = \frac{\tau_{-i}^{(t)}}{N} = \left[\left(p_{-i}^{(t)} + \left(1 - p_{-i}^{(t)}\right)\right)(1 - (1 - p_b)^L)\right] \tag{4}$$

The normalize throughput $\hat{\tau}_{-i}^{(t)}$ will be used as input to strategies function of node *i*.

The average payoff of the node *i* at time slot *t* using the table -2 can be expressed as:

$$\pi_i^t = (\alpha - \beta)\left(1 - p_i^{(t)}\right)\left(1 - p_{-i}^{(t)}\right) + \alpha\left(1 - p_i^{(t)}\right)p_{-i}^{(t)} - \beta\left(1 - p_{-i}^{(t)}\right)p_i^{(t)}$$

By simplifying:

$$\pi_i^t = (\alpha - \beta)\left[1 + \frac{\beta}{\alpha-\beta} p_i^{(t)} - \frac{\alpha}{\alpha-\beta} p_{-i}^{(t)}\right] \tag{5}$$

A player wishes to maximize its total discount payoff and is given by [4]

$$U_i = \sum_{n=0}^{\infty} \delta^n \pi_i^t \tag{6}$$

where $0 < \delta < 1$ is the discount factor. Substituting the π_i^t from (5), the total discount payoff of node *i* can be expressed as

$$U_i = \sum_{n=0}^{\infty} \delta^n (\alpha - \beta)\left[1 + \frac{\beta}{\alpha-\beta} p_i^{(t)} - \frac{\alpha}{\alpha-\beta} p_{-i}^{(t)}\right] \tag{7}$$

The payoff of node *i* can be calculated by using the actual value of $p_{-i}^{(t)}$from equation (1). If the node *i* supposed to have many chances for future interaction, then δ will be close to one.

3.2.3 Trigger Strategy

In the repeated game, each player is permitted to use a strategy to deicide its action "do not forward" or "forward" packets for others on the information collected in past. We define the trigger strategy in the two player repeated packet forwarding game to provide cooperation $\bar{\bar{P}}_i^t$ of a node *i* in time slot *t* such that the cooperation of a node -i is estimated based on normalized throughput $\hat{\tau}_{-i}^{(t)}$ in the time slot t-1. If the normalized throughput of a node is below a threshold τ_{th}, it is consider a selfish node and node *i* decided to not forward the packet of node –i. Mathematically the trigger strategy is defined as:

$$\bar{\bar{P}}_i^t = f_i\left(\hat{\tau}_{-i}^{(t-1)}\right) \qquad (8)$$

where $f_i(.)$ is a strategy function of node i. There are many strategies possible. Few of them are given below:

$\bar{\bar{P}}_i^0 = f_i\left(\hat{\tau}_{-i}^{(0)}\right) = 0$, Use this function if node-i playing DNF in the first time slot

$$f_i\left(\hat{\tau}_{-i}^{(t-1)}\right) = \begin{cases} 0 \quad if\ \hat{\tau}_{-i}^{(t-1)} \leq \tau_{th}, & use\ this\ if\ Node - i\ playing\ DNF \\ 1 \quad if\ \hat{\tau}_{-i}^{(t-1)} = 1\,, & use\ this\ funtion\ if\ Node - i\ playing\ F \\ \hat{\tau}_{-i}^{(t-1)}\ if\ 1 < \hat{\tau}_{-i}^{(t-1)} < \tau_{th}, & use\ this\ TFT \end{cases}$$

where DNF means “DO NOT FORWARD”, F means “FORWARD” and TFT (Tit-For-Tat). It is defined as a node i is playing this strategy start with F and then playing with the same throughput as of node-i in the previous time slot.

The strategy profile (DNF, DNF) is the only Nash equilibrium of the forwarding game with uncertain ending since neither player stands to improve their payoff from cooperation with an opponent that always do not forward. The dilemma of this game is that both players could receive a better payoff of α-β > 1 if they selected the strategy profile (F, F). This strategy profiles is Pareto optimal.

CHAPTER 4
SIMULATION RESULTS

In the simulations, our focus is to study the performance of proposed game theoretic model for selfish node avoidance using the AODV protocol. The model developed is simulated in network simulator ns-2.

4.1 SIMULATION SETUP

We used the two rays ground radio-propagation model for wireless channel. The bandwidth of the wireless channel is 2 Mbps. To propagate the signal in all direction, Omni directional antenna has been used. The multiple access with collision avoidance protocol (802.11) was used at the MAC layer. The physical radio range of node is 200 meters. Routing was performed using the AODV protocol with selfish node. The simulation parameters used in the work are shown in table-4.1.

Initially, in the simulation, 10 nodes are randomly placed in an area of 500×500 m^2. We have implemented the proposed game theoretic model. During the simulation run we randomly selected 2 nodes that do not implement game theoretic model and behave selfishly by dropping all packets that are destined for others. A selfish node means a node that drop the packet to save its energy by not forwarding packet for others. A cooperative node is one which forwards the packets. Thereafter 20, 30, and up to 80 cooperative nodes are randomly selected and same number of selfish nodes are also selected for the simulation.

Table-4.1 Simulation parameter and its value

PARAMETER	**VALUE**
Number of node	100
Number of selfish node	10%-90%
Cooperative node	10%-90%
Area	500x500 m^2
Packet size	512 bytes
CBR	5-30 packets/sec
Initial Energy E_f	1000 Joules
Threshold Energy ratio θ_E	.40
Threshold Normalize throughput τ_{th}	.60
Simulation time	500 s

To evaluate the performance of the network in which nodes implement two players game theoretic model, the number of forwarded packet are measured. We measured the following evaluation metrics - number of routes versus packet delivery ratio, CBR versus packet delivery ratio, and percentage of selfish nodes versus packet delivery ratio. Further, we also measured the metrics and percentage of selfish nodes versus routing overhead. *Packet Delivery Ratio* is defined as the ratio of the number of packet received at the destination node to the number of packets sent by the source node. *Routing Overhead is* defined as the ratio of the amount of routing related control packet in bytes (RREQ, RREP, RERR and Game Theoretic AODV) to the amount of data packet sent in byte in the network.

4.1 SIMULATION RESULTS

Figure 4.1 shows the simulation results obtained for Packet delivery ratio as the number of routes varies in the network where 10% nodes are selfish and 90% are cooperative nodes. It is observed that the packet delivery ratio increases with the increase of the routes. This is due to fact that when there are more active routes, a node does not listen since it is busy in forwarding the increased number of packet. This is leading to consume more energy of node. Therefore cooperative nodes are supposed to be acting as selfish. This increases the level of retaliation situations in TFT strategies. When the number of route is more than 16, the packet delivery ratio starts decreasing since the packets are being forwarded by the originating node. But the packets are not overheard by the originating node due to bit error in packet overhearing which increases selfishness

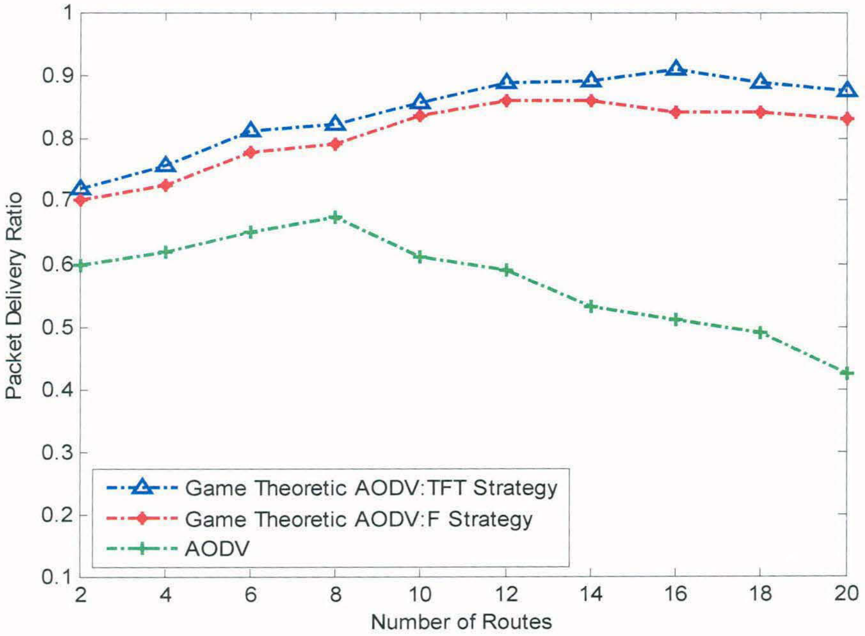

Figure 4.1 Packet delivery ratio for the different numbers of routes.

among the cooperative nodes. Further, packet delivery ratio of AODV with selfish nodes falls drastically since nodes do not implement the game theoretic model for avoiding the selfishness.

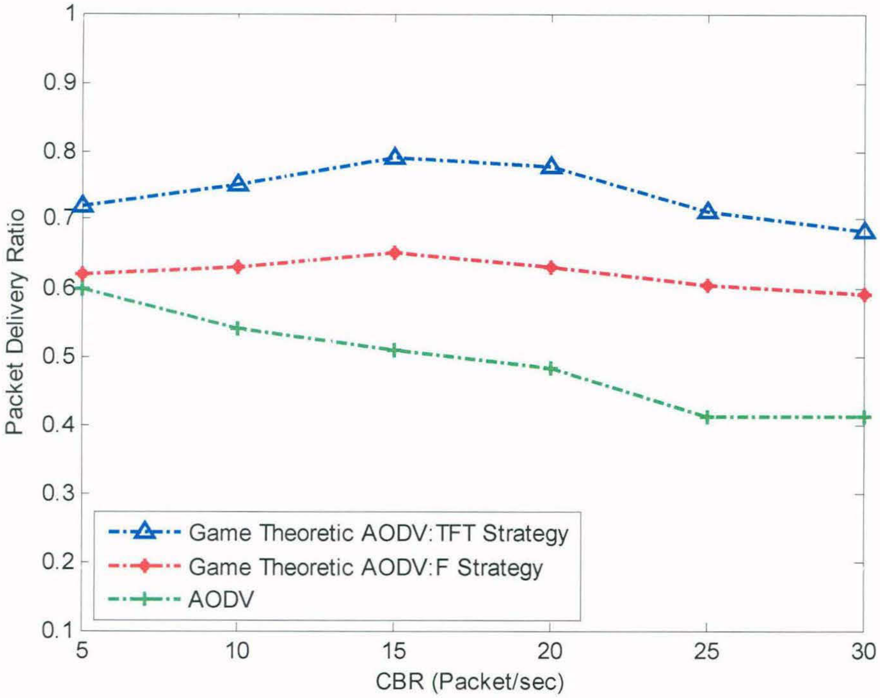

Figure 4.2 Packet delivery ratio for the different packets rates.

Figure 4.2 shows the simulation results for packet delivery ratios as the rate of CBR traffic of source nodes varies. It is observed that when CBR source generates more than 15 packets in one second, the packet delivery ratio start decreasing. . This is due to fact that when there are more cooperative nodes they might deviate from strategy F to strategy TFT to save their energy since forwarding of more packets consume more energy. Therefore cooperative nodes are supposed to be acting as selfish. Further, Packet delivery ratio for AODV decreases faster as the CBR increases compared to AODV with game theoretic model. It works efficiently in the heavy loaded network as compared to the original AODV in the presence of selfish nodes.

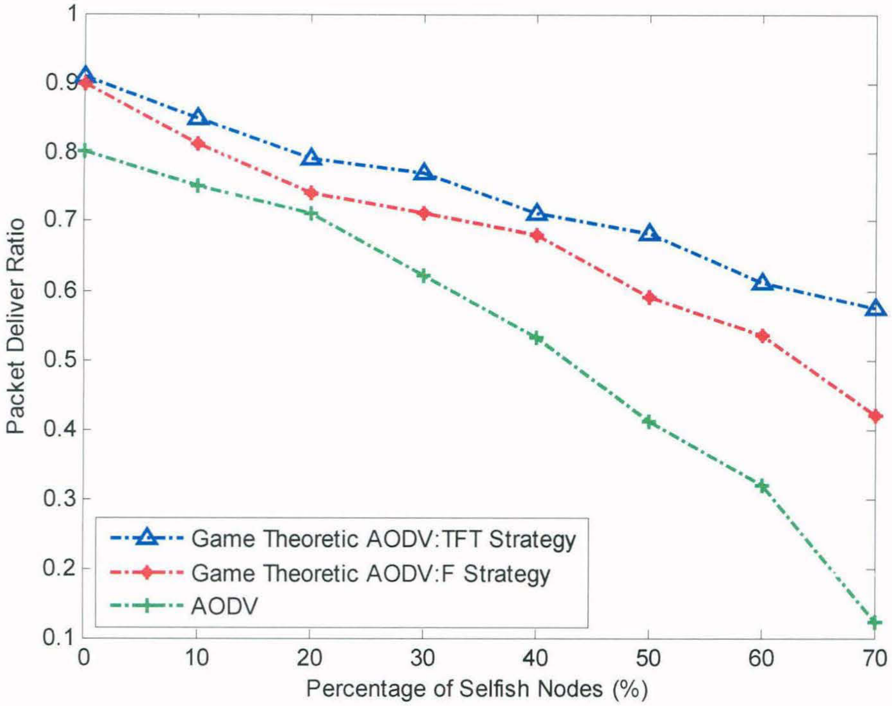

Figure 4.3 Packet delivery ratio for the different number of selfish nodes.

Figure 4.3 shows the simulation results for packet delivery ratio as the percentage of selfish nodes and cooperative nodes varies in a network. The percentage of selfish nodes in the network is varied from 0 to 70%. The CBR for this simulation is 10 packets. It is observed that the packet delivery ratio for both strategy F and TFT is 0.90 and for AODV is 0.80 when none of the node is acting as a selfish node. Further, the packet delivery ratio of cooperative nodes decreases proportionally when the number of selfish nodes increases. This is happening because of two facts. First, as the number of selfish nodes increases, the total number of packets being dropped increases proportionally. Second, it decreases as the repeated route request is fired and the overheads for searching the alternative route are increased. Compared with the original AODV, the game theoretic modeled AODV protocol works better in situations where the selfishness among nodes is increasing. For example, there are 70% nodes are selfish, the game theoretic modeled AODV protocol delivers about 58% of the data traffic, while the original AODV protocol can only deliver 12%.

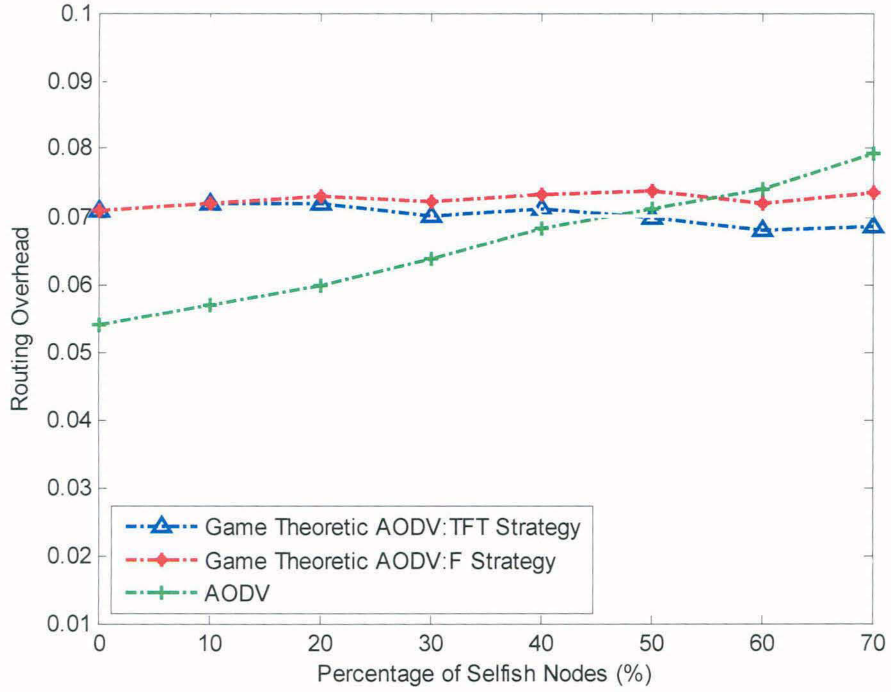

Figure 4.4 Routing overhead for the different number of selfish nodes.

Figure 4.4 shows the simulation results for the routing overhead of the game theoretic modeled AODV for the different percentage of selfish nodes and cooperative nodes in the network. The percentage of selfish nodes in the network is varied from 0 to 70%. The CBR for this simulation is 10 packets. It is observed that the routing overhead increases to 7% approximately for the game theoretic modeled AODV while in the case of original ADOV it is 5.5% when no node is acting as selfish node. The routing overheads for the game theoretic modeled AODV increases very slowly with the increase of selfish nodes. While the routing overheads for the original AODV increases faster.

This is due to fact that repeated route request are fired for route establishment and overheads are incurred in searching the alternative routes. For example when there are 70% selfish nodes, the overheads for the original AODV are 8.0%. While for the game theoretic modeled AODV protocol, it is only 7.5% since in the original AODV, the nodes do not implement the cooperation mechanisms.

CHAPTER 5

CONCLUSION AND FUTURE WORK

5.1 CONCLUSION

We have studied how game theoretic model can help for selfish node avoidance routing by enforcing cooperation among selfish nodes. A mathematical framework for rational node that maximizes its credits has been presented. To enforce cooperation among the selfish nodes, two trigger strategies are used; game theoretic model with F (forward) and with TFT (Tit For Tat). Further, to explore the usability of this model simulations are carried out using NS-2. From the simulation results, the following observations are made:

- The gap between packet delivery ratio of the two cooperative nodes strategies increases with the increase in number of routes. This is happening since increase the level of retaliation situations in TFT strategies.

- The game theoretic modeled with AODV achieves higher packet delivery ratio for heavy traffic network in the presence of selfish nodes as compared to the original AODV.

- The packet delivery ratio of cooperative nodes decreases proportionally when the number of selfish nodes increases. This is happening because of two facts - first, the number of selfish nodes increases as the total number of packets being dropped increases, and second, firing of repeated route requests and overheads for searching the alternative route.

- The implementation of game theoretic modeled with AODV results in low routing overheads.

5.2 FUTURE WORK

In the current work, we have applied only two player game theoretic model. Further, the model has not been tested for mobile environment. Therefore, this work can be extended to explore the followings issues in the future course of research:

- Three player packet forwarding game or more player packet forwarding game can be studied to provide better the cooperation among selfish nodes.

- Cooperation among selfish nodes in mobile environment can be investigated since mobility increases mutual dependency between nodes.

REFERENCES

[1] George Aggelou, “Mobile Ad Hoc Networks: from wireless LANs to 4G networks”, Tata McGraw-Hills,ed 2009.

[2] Imrich , Marco ,Jennifer and Lui, “Mobile ad hoc networking: imperatives and challenges”, Ad Hoc Networks: Elsevier vol. 1, (2003) pp. 13–64

[3] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester, “An Overview of Mobile Ad Hoc Networks: Applications and Challenges”, Journal of the Communications Network, Vol. 3, No. (July 2004), pp. 60-66

[4] Jie Yang, Andrew G. Klein, and D. Richard Brown III, “Natural Cooperation in Wireless Networks”, IEEE signal processing magazine vol.26, issue 5, September 2009. pp. 98-106

[5] Royer, E.M., Chai-Keong Toh, “A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks”, IEEE Personal Communications,. Vol. 6 issue 2 April 1999, pp. 46-55

[6] C.E. Perkins, P. Bhagwat, “Highly dynamic destination sequenced distance-vector routing (DSDV) for mobile computers”, Computer Communications Review (October 1994) pp.234–244

[7] Jacquet, P., Muhlethaler, P., Clausen, T., Laouiti, A., Qayyum, A., Viennot, L.,” Optimized link state routing protocol for ad hoc networks, In Multi Topic Conference, 2001. IEEE INMIC 2001. Technology for the 21st Century. Proceedings. IEEE International, 2001, pp. 62 – 68

[8] B. Bellur, R.G. Ogier, F.L. Templin, “Topology broadcast based on reverse-path forwarding (TBRPF)”, IETF Internet Draft, draft-ietf-manet-tbrpf-01.txt, March 2001.

[9] C. E. Perkins and E. M. Royer, "Ad Hoc On Demand. Distance Vector (AODV) Routing", draft-ietf-manet-. aodv-02.txt, Nov. 1998

[10] D.B. Johnson, D.A. Maltz, Dynamic source routing in ad hoc wireless networks, in: T. Imielinski, H. Korth (Eds.),Mobile Computing, Kluwer Academic Publishers, Dordrecht, 1996, pp. 153–181

[11] V. Park and S. Corson, Temporally Ordered Routing Algorithm (TORA) Version 1, Functional specification IETF Internet draft (1998)

[12] R. Dube, C. Rais, K.-Y. Wang, S. Tripathi, "Signal stability based adaptive routing for ad hoc mobile networks", IEEE Personal Communications, February 1997, pp. 36–45

[13] E.VENKAT REDDY, "Trustworthy Robust Routing Protocol for Mobile Ad Hoc Network", International Journal of Engineering Science and Technology, Vol.2 (2), 2010

[14] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu, And Lixia Zhang, "Security in mobile ad hoc networks:challenges and solutions", IEEE Wireless Communications, Volume: 11 Issue:1 february 2004

[15] karan singh, r. S. Yadav, ranvijay, "A review paper on ad hoc network security", international journal of computer science and security, volume (1): issue (1), May/June, 2007

[16] Fang Liu Rongsheng Dong Jianming Liu Xuliang Xu, "A Reputation Mechanism to Stimulate Node Cooperation in Ad Hoc Networks", Third International Conference on Genetic and Evolutionary Computing, 2009

[17] Vikram Srinivasan, Pavan Nuggehalli, Carla F. Chiasserini, Ramesh R, Rao "Cooperation in Wireless Ad Hoc Networks", IEEE INFOCOM 2003

[18] Tiranuch Anantvalee and Jie Wu, "Reputation-based System for Encouraging the Cooperation of Nodes in Mobile Ad Hoc Networks", IEEE International Conference on Communications, 2007.

[19] Juan José Jaramillo and R. Srikant, "A game theory based reputation mechanism to incentivize cooperation in wireless ad hoc networks", Elsevier :Ad Hoc Networks, Volume 8, Issue 4, June 2010

[20] Vivesk S, James N., Allen B. Rekha M., Luiz A., James E., Jeferey H., and Robert P., "Using game theory to analyze wireless ad hoc networks", IEEE communication surveys and tutorials, fourth quarter, 2005, pp. 46-56.

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

[22] Noam Nisan, Tim R, Eva, and Vijaya V.V., "Algorithmic Game theory", Cambridge university press, 2007.

[23] Chengqi song and Qian zhang, "Protocol for stimulating packet forwarding in wireless ad hoc networks", IEEE wireless communication, oct. 2010, pp. 50-55.

[24] Kim hyun jin and Jon M. Peha, "Detecting selfish behavior in a cooperative commons", Proceedings of the IEEE International Dynamic Access Spectrum Access Networks Symposium (DySpan) , Chicago, Illinois, October 2008, pp.1-22.

[25] Jerzy K and Rafal O., "A framework for detection of selfishness in multihop mobile ad hoc networks", Journal of telecommunications and information technology", feb, 2009, pp. 34-40.

[26] P. Michiardi and R. Molva. "CORE: a collaborative reputation mechanism to enforce node cooperation in mobile ad-hoc networks". In Proceedings of the 6th IFIP Conference on security communications, and multimedia, CMS2002, pp.1-15

aharlal Nehru Univer
Library