Effect of Selfish Behavior on Power Consumption in Mobile Adhoc Network

By

Hemang Kothari

09MCE008

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

AHMEDABAD-382481

May, 2011

Effect of Selfish Behavior on Power Consumption in MANET

Major Project

Submitted in partial fulfillment of the requirements

For the degree of

Master of Technology in Computer Science and Engineering

By

Hemang Kothari

(09MCE008)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

AHMEDABAD-382481

May, 2011

Declaration

This is to certify that

a. The thesis comprises my original work towards the degree of Master of Technology in Computer Science and Engineering at Nirma University and has not been submitted elsewhere for a degree.

b. Due acknowledgement has been made in the text to all other material used.

Hemang Kothari

Certificate

This is to certify that the Major Project entitled "Effect of Selfish Behavior on Power Consumption in Mobile Adhoc Network" submitted by Hemang Kothari (09MCE008), towards the partial fulfillment of the requirements for the degree of Master of Technology in Computer Science and Engineering of Nirma University of Science and Technology, Ahmedabad is the record of work carried out by him under my supervision and guidance. In my opinion, the submitted work has reached a level required for being accepted for examination. The results embodied in this major project, to the best of my knowledge, haven't been submitted to any other university or institution for award of any degree or diploma.

Prof. Manish Chaturvedi
Guide, Assistant Professor,
Department of Computer Engineering,
Institute of Technology,
Nirma University, Ahmedabad.

Dr.S.N.Pradhan
Professor and PG-Coordinator,
Department of Computer Engineering,
Institute of Technology,
Nirma University, Ahmedabad.

Prof.D.J.Patel
Professor and Head,
Department of Computer Engineering,
Institute of Technology,
Nirma University, Ahmedabad.

Dr.K.Kotecha
Director,
Institute of Technology,
Nirma University, Ahmedabad.

Abstract

Wireless Ad Hoc Network has witnessed an explosion of interest from researchers in recent years for its applications in classrooms, battlefields and disaster relief activities. A Mobile Ad hoc NETwork (MANET) is a collection of wireless nodes communicating with each other in the absence of any infrastructure. MANET research is gaining ground due to the ubiquity of small, inexpensive wireless communicating devices. Since, not many MANETs have been deployed, As wireless networks become an integral component of the modern communication infrastructure, energy efficiency will be an important design consideration due to the limited battery life of mobile terminals.

Wireless devices have maximum utility when they can be used anywhere at anytime. One of the greatest limitations to that goal, however, is finite power supplies. Since batteries provide limited power, a general constraint of wireless communication is the short continuous operation time of mobile terminals. Therefore, Energy saving is one of the most challenging problems in wireless communication.

Since the network interface is a significant consumer of power, my research has been devoted to find the effect of selfish behavior on power consumption in wireless networks in an effort to enhance energy efficiency.

This report presents a comprehensive summary of work addressing the effect of selfish behavior on power consumption in wireless network.It shows how much energy we can save by behaving selfishly and which selfish behavior is most effective to save the energy.

Acknowledgements

This thesis arose in part out of one year of research. During that time, I have worked with a great number of people whose contribution in assorted ways to the research and the making of the thesis deserved special mention.

In the first place I would like to record my gratitude to **Prof.Manish Chaturvedi**, Assistant Professor, Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmedabad the Guide of the project for supervision, advice, and guidance through out the work. His truly intuition has made him as a constant oasis of ideas and passion in MANET, which exceptionally inspires and enrich my growth as a student, a researcher and a helpful person want to be. I am indebted to him more than he knows.

I would like to thanks **Prof.Sunil Jardosh**, Assistant Professor, Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmedabad for valuable inputs as and when needed.

My deep sense of gratitude to **Dr.S.N.Pradhan**, Professor and PG-Coordinator of Department of Computer Engineering, Institute of Technology, Nirma University, Ahmedabad for an exceptional support and continual encouragement throughout thesis work.

I would like to thanks **Dr.Ketan Kotecha,** Hon'ble Director, Institute of Technology, Nirma University, Ahmedabad for his unmentionable support, providing basic infrastructure and healthy research environment.

I would also thank my Institution, all my faculty members. Last, but not the least, no words are enough to acknowledge constant support and sacrifices of my family members because of whom I am able to complete my dissertation work successfully.

- Hemang Kothari

09MCE008

Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Problem Statement

A mobile ad hoc network (MANET) is a temporary infrastructure less network, formed by a set of mobile hosts that dynamically establish their own network on the fly without relying on any central administration. Mobile hosts used in MANET have to ensure the services that were ensured by the powerful fixed infrastructure in traditional networks, such as packet forwarding, route update, route request. The resource limitation of nodes used in MANET, particular in energy supply, along with the multi-hop nature of this network may cause a new phenomenon which does not exist in traditional networks. To save its energy node may behave selfishly and uses the services of other nodes without correctly participate in system.

1.2 Objective

- Find the effect of selfish behavior on power consumption of good nodes and selfish nodes.
- Which selfish behavior is more effective in saving energy.
- Find out the effect of selfish behavior on power consumption in dense network.

1.3 Scope Of The Project

We find the selfish behaviors from literature. We implement that behaviors in simulator and find its effect on power consumption. We find the most appropriate energy efficient selfish behavior. We find the effect of selfish behavior on dense network.

1.4 Motivation

Many cooperation enforcement policies are proposed in literature which addresses packet forwarding selfish behavior. We study various types of selfish behavior proposed in literature with respect to energy saving parameter to show that there may be other selfish behavior which saves more energy and are more attractive for nodes.

1.5 Thesis Organization

The rest of the thesis is organized as follows.

Chapter 2 Literature survey on selfish behavior. It also specify the various selfish behavior which has different effect on the network.

Chapter 3 Protocols and Tools describe Network Simulator and gives information about other tools which are used during the work. It also provide brief overview about Dynamic Source Routing Protocol.

Chapter 4 Implementation describe the behaviors which are simulated in this report. It also mention the parameters used for simulation.

Chapter 5 Analysis of power consumption detail for each selfish behavior for different number of number of selfish nodes. Effect of selfish behavior on network throughput and routing overhead.

Chapter 6 Conclusion & Future work concluding remarks and scope for future plan is represented.

Chapter 2

Literature Survey and Important observations

2.1 Literature Survey

The type of wireless networks that is the infrastructure less, mobile and has nodes is known as a Mobile ad hoc network (MANET). Infrastructures less mobile networks have no fixed routers and base stations and the participating nodes are capable of movement. Due to the limited transmission range, multiple hops may be required for nodes to communicate across the Ad hoc network. Routing functionality is incorporated into each host, thus ad hoc networks can be characterized as having dynamic, multi-hop, and constantly changing topologies.

Due to the lack of stationary infrastructure, the participating nodes in the Ad hoc network have to forward traffic on behalf of other nodes that are not in close proximity to the destination node. If they deny participating in the routing process, the connectivity between nodes may be lost and the network could be segmented. Therefore, the functionality of an ad hoc network heavily depends on the forwarding behavior of the participating nodes.

- **A Simulation Analysis of Routing Misbehavior in Mobile Ad hoc Networks**[1]

    a. **Concept:**Mobile Ad hoc Networks (MANETs) rely on the cooperation of all participating nodes to provide the fundamental operations such as routing and

data forwarding. However, misbehaving nodes may not follow the cooperation paradigm and cause a serious affect on network performance. Nodes misbehave because they are malicious, selfish or malfunctioning. Selfish nodes try to save their own resources since resources are very constrained in wireless devices. So selfish nodes may decide to not consume their resource in forwarding data packets for other nodes: this can be achieved in two ways:

(1) **Selfish node type 1:** These nodes participate correctly in routing function but not forward data packets it receive for other node; so data packets may be dropped instead of being forwarded to their destination.

(2) **Selfish node type 2:** These nodes do not participate correctly in routing function by not advertising available routes, for example: in DSR selfish node may drop all RREQ they received or not forward a RREP to some destination. Consequently, this selfish node will not participate in the requested routes.

b. **Conclusion:**They have seen Selfish node type 2 (dropping RREQ) do not cause any damage in network with high nodes density. However, it can really affect the end to end delay and lead to congestion in a low density network.

c. **Open Issue:**Misbehaving nodes presence is one major security threat in MANETs that can affect the performance of the underplaying protocols.

- **Local Detection of Selfish Routing Behavior in Ad Hoc Networks[2]**

a. **Selfish Behavior:**Reputation mechanisms for detecting and punishing free-riders in ad hoc networks depend on the local detection of selfish behavior. Although naive selfish strategies based on dropping data packets are readily detected, more sophisticated strategies that manipulate ad hoc routing protocols present a greater challenge.

b. **Solution:**In this work they develop a method to distinguish selfish peers from cooperative ones based solely on local observations of AODV (Ad hoc On-Demand Distance Vector) routing protocol behavior. Their approach uses the finite state machine model of locally observed AODV actions to build up a statistical description of the behavior of each neighbor[2]. They apply a series of well known

statistical tests to features derived from this description to partition the set neighboring nodes into a cooperative and selfishclass.

c. **Conclusion:**In this work, they hypothesized that selfish behavior can be distinguished from cooperative behavior by comparing the statistical behavior of neighbors across multiple local routing instances.

d. **Open Issue:**They have taken some first steps toward developing a robust detection technique based on this idea and have been able to detect simple strategies of dropping RREQ (Route Request) or RREP (Route Reply) messages while maintaining a low false-positive rate.

- **Mitigating Smart Selfish MAC Layer Misbehavior in Ad Hoc Networks[3]**

a. **Selfish Behavior:**A selfish host can deliberately misuse the MAC (Medium Access Control) protocol to gain more network resources than well behaved hosts. For example, IEEE 802.11 requires hosts competing for the channel to wait for backoff interval before any transmissions. A selfish host may choose to wait for a smaller backoff interval, thereby increasing its chance of accessing the channel and hence reducing the throughput share received by well-behaved stations.

b. **Solution:**They propose Predictable Random Backoff (PRB) algorithm that is capable of mitigating the impact of these vulnerabilities[3]. PRB is based on minor modification of IEEE 802.11 binary exponential backoff (BEB) and forces each node to generate "predictable" random backoff intervals.

c. **Conclusion:**Handling MAC layer selfish misbehavior is a fundamental requirement to ensure normal network operation of well behaved nodes in ad hoc networks. Several detection and reaction approaches have been proposed already, however, they could be exploited by some "smart" attackers. In this paper, they first analyzed several selfish attack strategies in MAC layer that can avoid to be detected by the existing detection systems. Then they present PRB, an algorithm based on modifications of BEB in IEEE 802.11 to mitigate the selfish MAC misbehavior, more specifically, the manipulation of the selection of backoff interval. Their simulation results have indicated that PRB outperforms BEB

(binary exponential backoff) in the presence of MAC layer selfish misbehavior especially in a congested network environment.

- **Node Movement Detection to Overcome False Route Failures in Mobile Ad Hoc Networks**[4]

  a. **Selfish Behavior:**The mobile ad hoc network (MANET) is a wireless network without the wired infrastructure such as base stations in which mobile nodes communicate via multiple wireless links. In the MANET, route failures may happen because of node movement or wireless link collisions on routes. Since route failures due to wireless link collisions (i.e., false route failures) are not from network topology changes, they should not trigger route reestablishment; otherwise, the network performance will be aggravated.

  b. **Solution:**In this paper, they propose a node movement detection mechanism that can reduce unnecessary route reestablishment by referring to changes in its neighborhood. This mechanism allows a node to determine its movement based on its neighbor table and decide whether to retransmit a failed packet or to discover a detoring alternate route[4]. For the node movement detection, we add the M flag bit to the HELLO message. In this scheme, each node periodically broadcasts modified HELLO messages to its neighbors via 1-hop flooding. If a node receives a HELLO message with the M flag = 1message), it updates its neighbor table and makes a prediction on its movement by calculating changes in its neighborhood.

  c. **Conclusion:**Packet delivery failures due to wireless link collisions may incur unnecessary route reestablishment. This type of route reestablishment can be prevented if there exists a mechanism that can distinguish packet delivery failures due to wireless link collisions from those due to link disconnections. In this paper, they have proposed a scheme that can determine the cause of a packet delivery failure by referring to the change in a node's neighborhood. If a node experiences a significant neighborhood change, we can deduce that a packet delivery failure is caused by a link disconnection and a route reestablishment is triggered. Otherwise, retransmission of a failed packet is attempted.

- **On Detecting Packets Droppers in MANET: A Novel Low Cost Approach[5]**

  a. **Selfish Behavior:**One of the commonest threats that mobile ad hoc networks are vulnerable to is data packet dropping, which is caused either by malicious or selfish nodes. Most of the existing solutions to solve such misbehavior rely on the watchdog technique, which suffers from many drawbacks, particularly when using the power control technique.

  b. **Solution:**In this paper they introduce a new low cost Session-based Misbehavior Detection Protocol (SMDP) to monitor data forwarding, and detect packet dropping nodes in MANET[5]. Their solution takes advantage of a cross-layer design, and exploits information related to the session layer that makes its control packet transmissions proportional to sessions, which reduces the communication overhead. At the end of a session, each forwarder node shows to its neighbors the number of packets it received from each other during the session, as well as the total sent, by sending a special packet we call Forwarding Approval Packet (FAP). Mechanisms to ensure authentication of such information and to prevent nodes from denying receptions of data packets are used. Nodes then collaboratively analyze the FAPs, and judge one another

  c. **Conclusion:**This paper introduces a new low cost approach for monitoring node misbehavior in MANET. Unlike other monitoring approaches, their approach is able to detect the misbehavior in cases of power control employment. It is also cost effective as it reduces the communication overhead, by using only one hop communication (no flooding), and sending control packets only at the end of sessions, instead of doing so for each packet.

- **New Approach for Selfish Nodes Detection in Mobile Ad hoc Networks[6]**

  a. **Objective:**The resource limitation of nodes used in MANET, particularly in energy supply, along with the multi-hop nature of this network may cause a new phenomenon which does not exist in traditional networks. To save its energy a node may behave selfishly and uses the forwarding service of other nodes without correctly forwarding packets for them. This deviation from the correct behav-

ior represents a potential threat against the quality of service (QoS)Receiver collision, as well as the service availability, one of the most important security requirements.

b. **Selfish Behavior:**

- 1. Partial dropping: node B can circumvent the watchdog by dropping packets at a lower rate than the watchdog's configured minimum misbehavior threshold
- 2. Receiver collision: after a collision at node C, B could skip retransmitting the packet without being detected by A
- 3. False misbehavior accusations: A node may falsely report other innocent nodes in its neighborhood as misbehaving to avoid getting packets to forward
- 4. Insufficient transmission power: B can control its transmission power to circumvent the watchdog. if A is closer to B than C, then B could attempt to save its energy by adjusting its transmission power and makes it strong enough to be overheard by the previous node (A) but less than the required power to reach the true recipient (C)
- 5. Cooperated misbehavior: B and C could collude to cause mischief. In this case, B forwards a packet to C but does not report to A when C drops the packet. C does the same thing when it is B's predecessor in some route.

c. **Solution:**They define a new kind of feedbacks they call two-hop ACK[6], it is an ACK that travels two hops. Node C acknowledges packets sent from A by sending this latter via B a special ACK. Node B could, however, escape from the monitoring without being detected by sending A a falsified two-hop ACK. Note that performing in this way is power economic for B, since sending a short packet like an ACK consumes too less energy than sending a data packet.

- **Secure Cooperation in Autonomous Mobile Ad-Hoc Networks Under Noise and Imperfect Monitoring: A Game-Theoretic Approach[7]**

a. **Selfish Behaviors:**

- **Existence of noise**: In many existing cooperation enforcement schemes,each node decides its next step action based solely on the quality of service it has received in the current and/or previous stages, such as normalized throughput. However, if noise exists, some packets may be dropped unintentionally during the delivery. This can reduce the quality of service experienced by some nodes. As a consequence, these nodes will also lower the service quality provided by them. Such an avalanche effect may quickly propagate through- out the network and after some time, no nodes will forward packets for the others . When designing cooperation stimulation strategies in realistic scenarios, the effect of noise has to be thoroughly considered.

- **Imperfect monitoring**: Since nodes usually base only on what they have observed to make their decisions, imperfect monitoring can always be taken advantage of by greedy or malicious nodes. For example, when the miss detect ratio is high, a node can always drop other nodes' packets but still claim that it has forwarded[7]. None of the existing approaches have been designed with the consideration of noise and imperfect monitoring, which greatly limits their potential applications in realistic scenarios.

- **Topology dependency**:network topology plays an important role when designing cooperation enforcement strategies, and usually it is impossible to find a strategy to enforce all nodes to play fully cooperatively in static adhoc networks. For example, if a user is in a bad location such that no users rely on him or her to forward packets, it is usually impossible for him or her to find other users to help him or her.

- **Variable service request rates**:Similar to changing opponents, we have identified that the variable request rate also plays an important role. For example, if a node has too many packets to send, it is usually impossible to let the other nodes forward all of the packets for it, unless it can return enough favors to the others. Further, due to the topology change, a node that is requested may not need the requester' help immediately, though it may need it late.

- **Selfish Behavior in a Cooperative Commons[8]**

  a. **Selfish Behaviors:**

  - consider a network in which a device establishes a path with rout- ing packets before sending data packets. An effective selfish behavior would be to drop these routing packets or forward with a time-to-live (TTL) of 0 so that no paths can be established. A device could thereby avoid forwarding many subsequent data packets
  - Another selfish behavior would be to make paths that include the selfishly behaving device seem longer than they really are, perhaps by artificially increasing hop counts so the sources are more likely to choose another routes that appear to be shorter[8].
  - Often, part of detecting selfish behavior is requiring devices to watch the transmissions of their neighbors.[10, 11, 12] When devices know that their behavior is observed by neighbors[14, 15, 16], they may still selfishly suppress routing packets and evade detection by transmitting at a power large enough to be seen by the watchdogs[13], but too small to be received by the nominal recipient

- **Detection and Prevention of MAC Layer Misbehavior in Ad Hoc Networks[9]**

  a. **Selfish Behaviors:**

  - A selfish user can disobey the rules to access the wireless channel in order to obtain a higher throughput than the other nodes. A selfish user can also change the congestion avoidance parameters of TCP in order to obtain unfair advantage over the rest of the nodes in the network.
  - MAC layer misbehavior is possible in network access cards that run the MAC protocol in software rather than hardware or firmware, allowing a selfish user or attacker to easily change MAC layer parameters. Even network interface cards implementing most MAC layer functions in hardware and firmware usually provide an expanded set of functionalities which can be exploited to circumvent the limitations imposed by the firmware.

- A selfish user can implement a whole range of strategies to maximize its access to the medium. The most likely strategy that a selfish user will employ is to use different schemes for manipulating the rules of the MAC layer. In 802.11, the attacker can manipulate the size of the Network Allocation Vector (NAV) and assign large idle time periods to its neighbors, it can decrease the size of Interframe Spaces (both SIFS and DIFS), it can select small backoff values, it can unauthenticate neighboring nodes etc.

- **Attack-Resistant Cooperation Stimulation in Autonomous Ad Hoc Networks**

  a. **Selfish Behavior:***Emulate link breakage:* When source node (R) want to transmit packet to next node (R+1) on certain route R, if R+1 is selfish , R+1 can simply keep silent to let R1 believe that R+1 is out of R1's transmission range.[17]

  b. **Open Issue:**Find a scheme which can detect this kind selfish behavior.

- **Cooperation or Not in Mobile Ad Hoc Networks: A MAC Perspective**

  a. **Selfish Behavior:**In wireless network we need to send RTS(Request to send) - CTS(Clear to send) signal before transmission. If selfish node does not reply for RTS signal to save its energy then cooperation can not be achieved. This is one kind of selfish behavior, Another issue is if node does not want to listen any packet from anyone so it can switch off its network card to save its own resources.[18]

  b. **Open Issue:**Find the cooperation scheme to deal with this kind of selfish behavior.

- **IMPORTANT: A framework to systematically analyze the Impact of Mobility on Performance of Routing protocols for Adhoc Networks[19]**

  a. **Concept:** They believe that existing mobility models are not sufficient to capture some important mobility characteristics of scenarios in which MANETs may be deployed. For ex, Random Waypoint is a well designed model but it is insufficient to capture the following characteristics:

- **Temporal dependency:** Due to physical constraints of the mobile entity itself, the velocity of mobile node will change continuously and gently instead of abruptly, i.e. the current velocity is dependent on the previous velocity. However, the velocities at two different time slots are independent in the Random Waypoint model.
- **Spatial dependency:** The movement pattern of a mobile node may be influenced by and correlated with nodes in its neighborhood. In Random Waypoint, each mobile node moves independently of others.
- **Geographic restrictions:** In many cases, the movement of a mobile node may be restricted along the street or a freeway. A geographic map may define these boundaries

b. **Conclusion:**They proposed a framework to analyze the impact of mobility pattern on routing performance of mobile ad hoc network in a systematic manner. In their study, they observed that the mobility pattern does influence the performance of MANET routing protocols.

c. **Open Issue:**To analyze the impact of traffic on performance of routing protocols for Ad hoc Network.

- **Poisson Packet Traffic Generation Based on Empirical Data[20]**

a. **Concept:**Poisson packet traffic can be produced in two steps. Real traffic trace is analyzed in the first step. In second step, A new equivalent synthetic Poisson traffic is generated in such a way that the first order statistical parameters remain unchanged. New packet inter-arrival time series are produced in a random manner using negative exponential probability distribution with a known mean. New packet size series are also produced in a random manner. However, due to specified minimum and maximum packet sizes, a truncated exponential probability distribution is applied.

b. **Open Issue:**With the rise of packet switching it was thought that modeling of connectionless-oriented packet switched data traffic differs from conventional connection-oriented circuit-switched voice traffic in so many fundamental ways

that the same concepts for traffic model would not be applicable.

- **Detecting IEEE 802.11 MAC layer misbehavior in ad hoc networks: Robust strategies against individual and colluding attackers[21]**

  a. **Concept:**Selfish behavior at the Medium Access (MAC) Layer can have devastating side effects on the performance of wireless networks, with effects similar to those of Denial of Service (DoS) attacks. They consider the problem of detection and prevention of node misbehavior at the MAC layer, focusing on the back-off manipulation by selfish nodes.

  b. **Problems:**A selfish user can also change the congestion avoidance parameters of TCP in order to obtain unfair advantage over the rest of the nodes in the network . In devices with limited power resources, certain nodes might refuse to forward packets on behalf of other sources in order to save battery power . In all these cases, the misbehaving nodes will degrade the performance of the network from the point of view of the honest participants.

  c. **Open Issue:**A layered reputation mechanism should be deployed in order to either reward cooperation (e.g., payments) or penalize misbehaving nodes (e.g., revocation). They also propose fair sharing. However, fair sharing also involves the intention of a node to send a packet and therefore it is affected by packet arrivals from higher layers and backlogs at different nodes. This introduces the issue of throughput fairness and throughput benefit.

- **DOMINO: Detecting MAC layer greedy behavior in IEEE 802.11 hotspots[22]**

  a. **Problem:**The proliferation of hotspots based on IEEE 802.11 wireless LANs brings the promise of seamless Internet access from a large number of public locations. However, as the number of users soars, so does the risk of possible misbehavior. They show in this paper that a greedy user can substantially increase his share of bandwidth, at the expense of the other users, by slightly modifying the driver of his network adapter.

  b. **Solution:**They present DOMINO (Detection Of greedy behavior in the MAC layer of IEEE 802.11 public NetwOrks), a piece of software to be installed in

or near the Access Point. DOMINO can detect and identify greedy stations, without requiring any modification of the standard protocol.

DOMINO periodically collects traffic traces of active user stations during short intervals of time called monitoring periods. A series of tests, each aiming at detecting a particular misbehavior technique, determines if the analyzed traffic presents behavior anomalies. The outputs of these tests are then fed into a Decision Making Component (DMC) that decides whether a given station is cheating. If so, the control is passed to the misbehavior handling mechanism that is dependent on the WISP policy.

c. **Open Issue:**A framework that can be adapted to the study of cheating and detection techniques in any network based on a shared medium.

- **Proactive Cooperation Mechanism based on Cooperation Records for Mobile Ad hoc Networks[23]**

  a. **Selfish Behaviors**Different studies assume different types of selfish behavior. One type of selfish behavior involves transmitting only control packets but discarding data packets. Another involves discarding packets selectively or randomly. Still another involves falsifying routing information to disturb the normal operation of the network. These patterns of selfish behavior involve malicious falsification of program codes or routing information. The majority of the third party nodes may not behave in any of these ways. Consequently, these types of behavior represent only a part of the total selfish behaviors. Therefore this paper defines a type of selfish behavior which ordinary people, without the skills to falsify program codes or data maliciously, are likely to exhibit. This behavior involves refusing to forward any control or data packets for others. Selfish people can take such an action easily, for example by turning the power off or by turning off the communication function when they do not need to communicate.

  b. **Solution**PCOM (Proactive Cooperation Mechanism) is effective in preventing selfish nodes (SN) from communicating. In PCOM, each node holds the cooperation records of its adjacent nodes, and forwards only those packets that are generated by nodes with good cooperation records. PCOM thus prevents SNs

from joining the network. Furthermore, PCOM does not increase the processing load of nodes or signaling traffic on the network.

c. **Open Issue**The issues are still to study include the application of PCOM to routing protocols other than AODV, the optimization of PCOM parameters for different traffic patterns, mobility patterns, and node densities, and measures to be taken against SNs that falsify software or data.

2.2 Miscellaneous

- **A Survey of Several Cooperation Enforcement Schemes for MANETs**

a. **Concept:** Key-based schemes are considered computationally hard for MANET, whilst a-priori knowledge of the identities is required for initial key exchange. They efficiently support confidentiality services to prevent passive attacks (e.g., eavesdropping), authentication of nodes to establish end-to-end paths and integrity of messages to avoid fabrications. Where as, reputation-based schemes use the nodes' reputation to forward packets through reliable nodes. The reputation of a node increases when it carries out rightly the packet forwarding task, without altering their fields. The models of this category support effective mechanisms to measure the reputation of other nodes of the network.

CONFIDENT[24] designed as an extension to an on-demand routing protocol, such as the DSR. CONFIDANT facilitates monitoring and reporting for a route establishment that avoids the misbehaving nodes. It is based on the assumption that the packets of misbehaving nodes are not forwarded by fair nodes. If, however, a node was incorrectly accused or turns out to be a repentant and no longer malicious, re-integration into the network is possible.

CORE. This scheme, introduced by Michiardi and Molva in [25], relies on the DSR routing protocol. It stimulates node collaboration through monitoring of the cooperativeness of nodes and a reputation mechanism.

Liu and Issarny introduce a reputation model that incorporates time and context, along with mechanisms to support reputation formation, evolution and propagation [26]. The scheme is not focused only on the network-level functions, but on various types of services, such as a web service (e.g., ad-hoc discussion forums), and, thus, it applies to software agents, as well.

OCEAN. The Observation-based Cooperation Enforcement in Ad hoc Networks, proposed in [27], introduces an intermediate layer that resides between the network and the MAC layers. This layer helps the nodes to make intelligent routing and forwarding decisions. It is designed on top of the DSR, but its principles can be applied to other routing protocols, as well. OCEAN relies only on first-hand observations.

b. **Open Issue:**Although there are many cooperation enforcement schemes are available but no single cooperation scheme solve the all problems.

- **MANET: Selfish Behavior on Packet Forwarding[28]**

  a. **Concept:** They present and discuss reactive solutions that aim at detecting selfish misbehavior on packet forwarding when it appears in the network. The detection may be limited to the route including the selfish node, or may give deeper information and identify the selfish. Upon the detection of a selfish, routing through this node will be avoided. One of the main class of reactive solutions is monitoring based solution.The monitoring class includes basic approaches that focus on the monitoring phase and suggest techniques to control the forwarding process.

  b. **Monitoring-based Approach:**There are mainly four monitoring approaches, two of them are based on the promiscuous mode monitoring, while the others rely on the employment of acknowledgments (ACKs). The advantage of the promiscuous monitoring compared with ACKs employment is that the first one requires no overhead for monitoring, and allow to monitor both directed and broadcast

packets (packets sent to one neighbor and to all neighbors respectively). However, the promiscuous mode monitoring has many troubles regarding the accuracy on detections, especially when employing the power control technique.

- End-to-end ACKs mechanism consists of monitoring the reliability of routes by acknowledging packets in an end-to-end manner, to render the routing protocol reliable (like TCP). That is, the destination node acknowledges the successfully received packets by sending a feedback to the source. A successful reception implies that the corresponding route is operational, while a failure in the ACK reception after a timeout may be considered as an indication that the route is either broken, compromised, or includes selfish nodes.
- Watchdog is a basic technique on which many further solutions rely. It aims to detect misbehaving nodes that do not forward packets, by monitoring neighbors in the promiscuous mode. Suppose node S sends packets to D using a route including (possibly amongst others) respectively three intermediate nodes: A, B, and C. When A transmits a packet to B to forward to C, A can check whether B forwards each packet by analyzing packets it overhears during a given timeout. If A overhears a packet it is monitoring during the fixed timeout then it validates its forwarding, otherwise it raises a rating regarding B, and will judge that B is misbehaving and notify S as soon as the rate exceeds a given threshold. The solution also includes the path-rater component, that selects routes based on the link reliability knowledge.

Chapter 3

Protocol & Tools

3.1 Dynamic Source Routing Protocol

3.1.1 Introduction

The Dynamic Source Routing protocol (DSR)[29] is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. Using DSR, the network is completely self-organizing and self-configuring, requiring no existing network infrastructure or administration. Network nodes (computers) cooperate to forward packets for each other to allow communication over multiple hops between nodes not directly within wireless transmission range of one another. As nodes in the network move about or join or leave the network, and as wireless transmission conditions such as sources of interference change, all routing is automatically determined and maintained by the DSR routing protocol. Since the number or sequence of intermediate hops needed to reach any destination may change at any time, the resulting network topology may be quite rich and rapidly changing.

The DSR protocol allows nodes to dynamically discover a source route across multiple network hops to any destination in the ad hoc network. Each data packet sent then carries in its header the complete, ordered list of nodes through which the packet must pass, allowing packet routing to be trivially loop-free and avoiding the need for up-to-date routing information in the intermediate nodes through which the packet is forwarded. By including this source route in the header of each data packet, other nodes forwarding or overhearing

any of these packets may also easily cache this routing information for future use.

3.1.2 Overview and Important Properties of the Protocol

The DSR protocol is composed of two mechanisms that work together to allow the discovery and maintenance of source routes in the ad hoc network:

- *Route Discovery* is the mechanism by which a node **A**wishing to send a packet to a destination node **E** obtains a source route to **E**. Route Discovery is used only when **A** attempts to send a packet to **E** and does not already know a route to **E**.

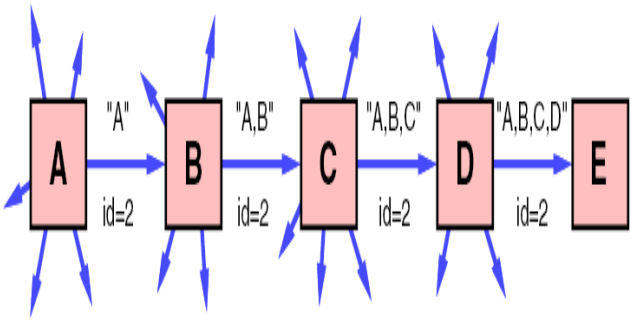

Figure 3.1: Route Discovery example

- *Route Maintenance* is the mechanism by which node **A** is able to detect, while using a source route to **E**, if the network topology has changed such that it can no longer use its route to **E** because a link along the route no longer works. When Route Maintenance indicates a source route is broken, **A** can attempt to use any other route it happens to know to **E**, or can invoke Route Discovery again to find a new route. Route Maintenance is used only when **A** is actually sending packets to **E**.

Route Discovery and Route Maintenance each operate entirely on demand. In particular, unlike other protocols, DSR requires no periodic packets of any kind at any level within the network. For example, DSR does not use any periodic routing advertisement, link status sensing, or neighbor detection packets, and does not rely on these functions from any underlying protocols in the network. This entirely on-demand behavior and lack of

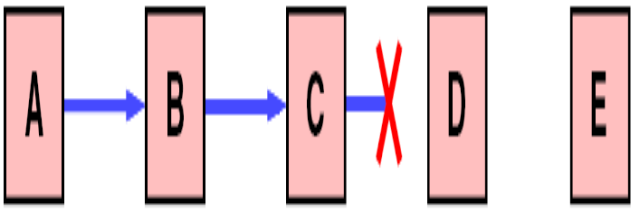

Figure 3.2: Route Maintenance example: Node C is unable to forward a packet from A to E over its link to next hop D.

periodic activity allows the number of overhead packets caused by DSR to scale all the way down to zero, when all nodes are approximately stationary with respect to each other and all routes needed for current communication have already been discovered. As nodes begin to move more or as communication patterns change, the routing packet overhead of DSR automatically scales to only that needed to track the routes currently in use.

3.2 Tools

3.2.1 Network Simulator

Network simulator is tool used to stimulate different network scenarios. We can build ns either from the the various packages (Tcl/Tk, otcl, etc.), or We can download an 'all-in-one' package. I start with the all-in-one package, especially if we're not entirely sure which packages are installed on your system, and where exactly they are installed. The disadvantage of the all-in-one distribution is the size, since it contains some components that we don't need anymore after we compiled ns and nam. It's still good for first tests, and we can always switch to the single-package distribution later.

- Run the **./install** to install ns.
- Set the environment variable as per the ns directory.
- Run **./configure** to configure various parameters.

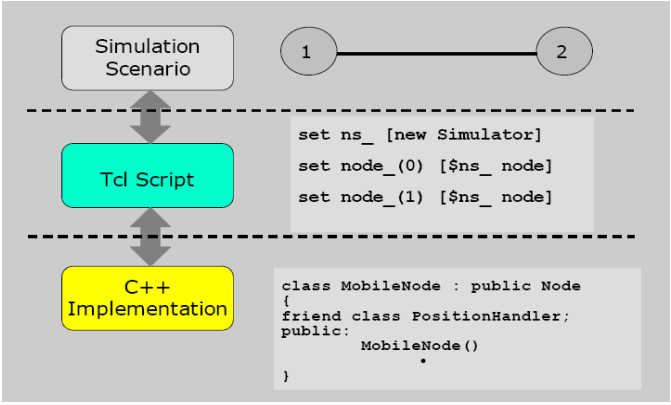

Figure 3.3: NS2-Overview

3.2.2 GNUPlot

Gnuplot is a command-driven interactive function plotting program. It can be used to plot functions and data points in both two- and three-dimensional plots in many different formats. It is designed primarily for the visual display of scientific data. gnuplot is copyrighted, but freely distributable; you don't have to pay for it. GNUPlot provides following functionalities.

a. Plotting two-dimensional functions and data points in many different styles

b. Plotting three-dimensional data points and surfaces in many different styles

c. Algebraic computation in integer, float and complex arithmetic

d. Support for a large number of operating systems, graphics file formats and output devices

e. TEX-like text formatting for labels, titles, axes, data points

f. Extensive on-line help

3.2.3 Awk

Awk has two faces: it is a utility for performing simple text-processing tasks, and it is a programming language for performing complex text-processing tasks.The two faces are really the same, however. Awk uses the same mechanisms for handling any text-processing

task, but these mechanisms are flexible enough to allow useful Awk programs to be entered on the command line, or to implement complicated programs containing dozens of lines of Awk statements. The Awk text-processing language is useful for such tasks as:

- Tallying information from text files and creating reports from the results.
- Adding additional functions to text editors like "vi".
- Translating files from one format to another.
- Creating small databases.
- Performing mathematical operations on files of numeric data.

Awk statements comprise a programming language. In fact, Awk is useful for simple, quick-and-dirty computational programming. Anybody who can write a BASIC program can use Awk, although Awk's syntax is different from that of BASIC. Anybody who can write a C program can use Awk with little difficulty, and those who would like to learn C may find Awk a useful stepping stone.

Awk is not really well suited for extremely large, complicated tasks. It is also an "interpreted" language – that is, an Awk program cannot run on its own, it must be executed by the Awk utility itself. That means that it is relatively slow, though it is efficient as interpretive languages go, and that the program can only be used on systems that have Awk. There are translators available that can convert Awk programs into C code for compilation as stand-alone programs, but such translators have to be purchased separately

Chapter 4

Implementation

4.1 Selfish Behavior Implementation

4.1.1 Forwarding Node Selfish Behavior

Mobile Ad Hoc Network (MANET) is a collection of mobile nodes (hosts) which communicate with each other via wireless links either directly or relying on other nodes as routers. The operation of MANETs does not depend on pre-existing infrastructure or base stations. A mobile node can become a failed node for many reasons, such as moving out of the transmission ranges of its neighbors, exhausting battery power, malfunctioning in software or hardware, or even leaving the network. Besides these failed nodes, based on the behavior, the mobile nodes are classified into:

- Cooperative Nodes are active in route discovery and packet forwarding, but not in launching attacks
- Failed Nodes are not active in route discovery
- Malicious Nodes are active both in route discovery and launching attacks

Selfish Nodes do not forward packet for others. They tend to drop data packets of others to save their energy so that they could transmit more of their own packets. This type of attack comes under denial-of-service (DoS) category. Selfish nodes, on the other hand, which cooperate during route discovery and defer during packet forwarding, need to be explored.

4.1.2 Effect

One immediate effect of node misbehavior and failures in wireless ad hoc networks is the node isolation problem due to the fact that communications between nodes are completely dependent on routing and forwarding packets. In turn, the presence of selfish node is a direct cause for node isolation and network partitioning, which further affects network survivability.

4.1.3 Wireless Network Card On/OFF Selfish behavior

Different studies assume different types of selfish behavior. One type of selfish behavior involves transmitting only control packets but discarding data packets. Another involves discarding packets selectively or randomly. Still another involves falsifying routing information to disturb the normal operation of the network. These patterns of selfish behavior involve malicious falsification of program codes or routing information. The majority of the nodes may not behave in any of these ways.

Consequently, these types of behavior represent only a part of the total selfish behaviors. Therefore this report defines a type of selfish behavior which ordinary people, without the skills to falsify program codes or data maliciously, are likely to exhibit. This behavior involves refusing to forward any control or data packets for others. Selfish people can take such an action easily, for example by turning the power off or by turning off the communication function when they do not need to communicate.

In this report, the behavior of the selfish neighbors is modeled and the objective is to study the impact of selfish behavior on the power consumption. In particular, it is to analyze the nodes behavior while forwarding packets for other nodes. Energy saving is the only reason assumed for a node being selfish.

4.2 Simulation Setup

we conducted exhaustive simulations in the simulation tool NS-2.34. The number of nodes (network size N) is 50. The mobility model chosen is the Random Way Point Model, which is general in nature and provides the uniform node distributions. Unless otherwise indicated, the speed is uniformly distributed between 0 and 20 ms. We used Random Way Point

model because we were not targeting particular application. Constant Bit Rate (CBR) and Poisson Traffic Model are chosen for generating data packets. We used poisson traffic because it is more realistic and to make analysis more complete. In each traffic pattern, 50 sessions are constantly maintained to keep every node involved in networking.

The results are averaged over multiple simulation rounds conducted with various random seeds. The simulation time is set to 1000s so that the system can reach steady states. We set maximum number of packet as 10000 which is large enough to continue session till end of the simulation time. Physical layer parameters are taken according to wavelan card. The default network parameters are listed in Table 1

Type	**Value**
Transmit Power	1.65 W
Receiving Power	1.40 W
Sleep Mode	0.045 W
Idle Mode	0.843 W
Traffic Model	CBR & Poisson
Packet Size	512 Bytes
Interval	1 Sec
Maximum Packet	10000
Initial Energy	1500
Simulation Time	1000 Sec

Table I: Simulation Parameter

4.3 Result

We generate traces for dynamic as well as static topology with CBR as well as poisson traffic.Each result is average of 10 traces. Following table summarize the detail of trace.

Topology	**Traffic Model**	**Num of Nodes**	**Num of Selfish Node**
Static	CBR	50	2,4,6,8,10,12
Dynamic	CBR	50	2,4,6,8,10,12
Dynamic	Poisson	50	2,4,6,8,10,12

Table II: Trace Detail

Chapter 5

Analysis

5.1 Forwarding Node Selfish Behavior

In this behavior, selfish node do not forward packet for others to save its resources.

5.1.1 Static Topology with Constant Bit Rate Traffic

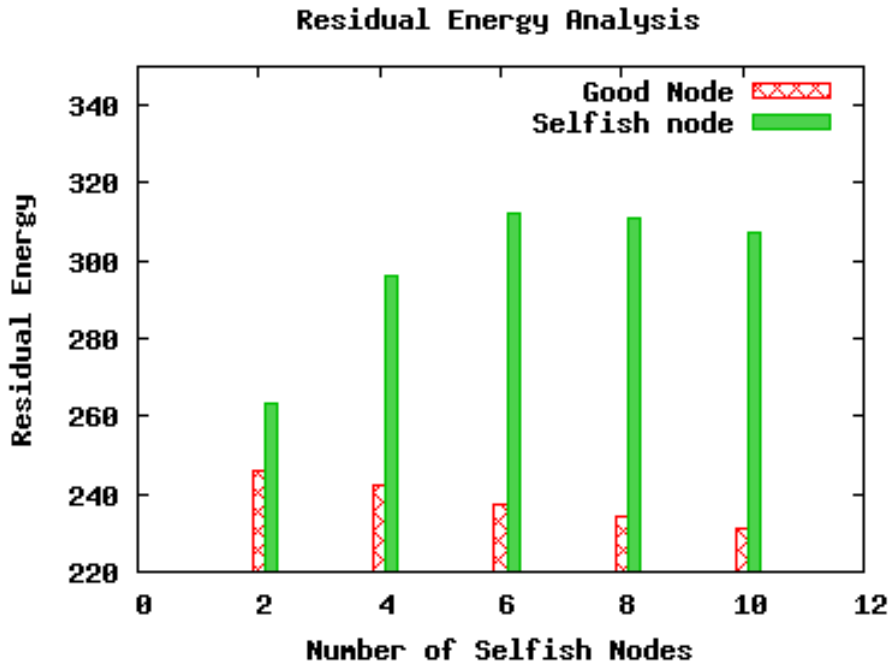

Figure 5.1: Residual Energy Vs Num. of Selfish Node for Static Topology

In static topology, routes are established at the beginning of session and remains valid throughout the session. So route overhead is low compare to dynamic topology and do not consume more energy. From Figure 5.1 we can say that as number of selfish node increase in network, good node need to do more work to compensate the selfish node work. So good node need to spend more energy to complete the work. Simulation result show that selfish nodes save more energy as number of selfish node increase in network.

5.1.2 Dynamic Topology with Constant Bit Rate Traffic

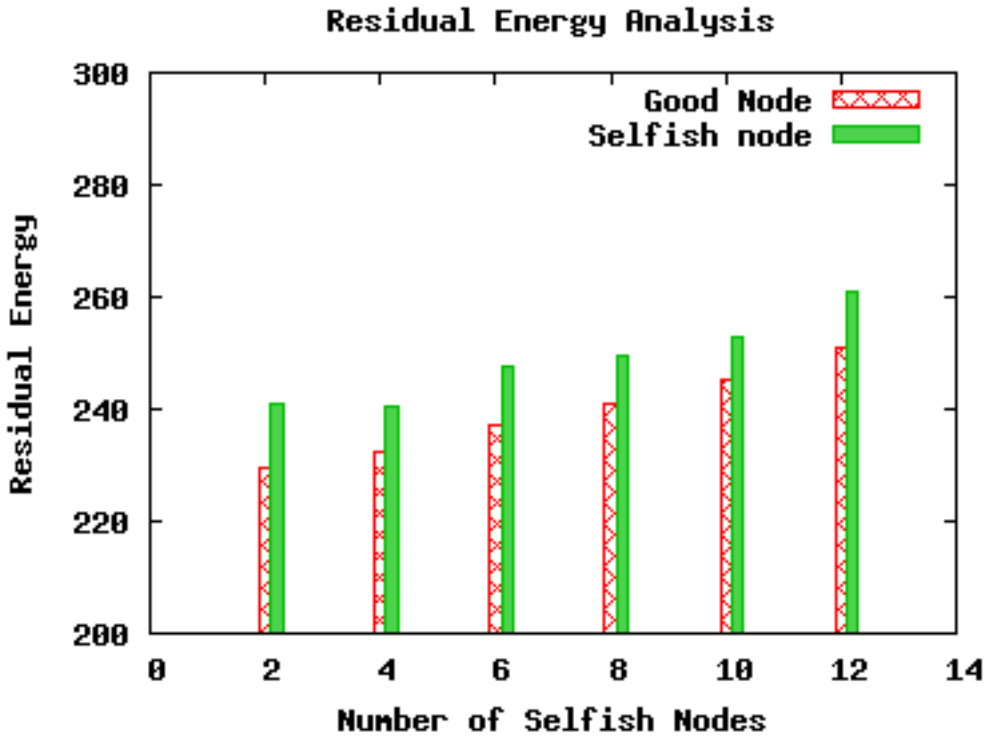

Figure 5.2: Residual Energy Vs Num. of Selfish Node for CBR Traffic

Figure 5.2 shows the simulating result of dynamic topology where nodes tend to move form one place to another place at different time frame. So links may break and re-route discovery required. It is required to establish lots of connection because of this movement. From graph we can say that as number of selfish node increase in network, good nodes as well as selfish nodes saves energy. We identified following reasons for it:

- In mobile network scenario, routes may break frequently and routing overhead is a large component in energy consumption.
- When node density is high and all the nodes participate in flooding based route discovery done by DSR, nodes consume more energy. This in turn means that density play important role in dense network.
- When some nodes behave selfishly, they prune all route request coming to them. So they reduce the number of control packet in network hence reduce energy consumption of good nodes as well as selfish nodes.

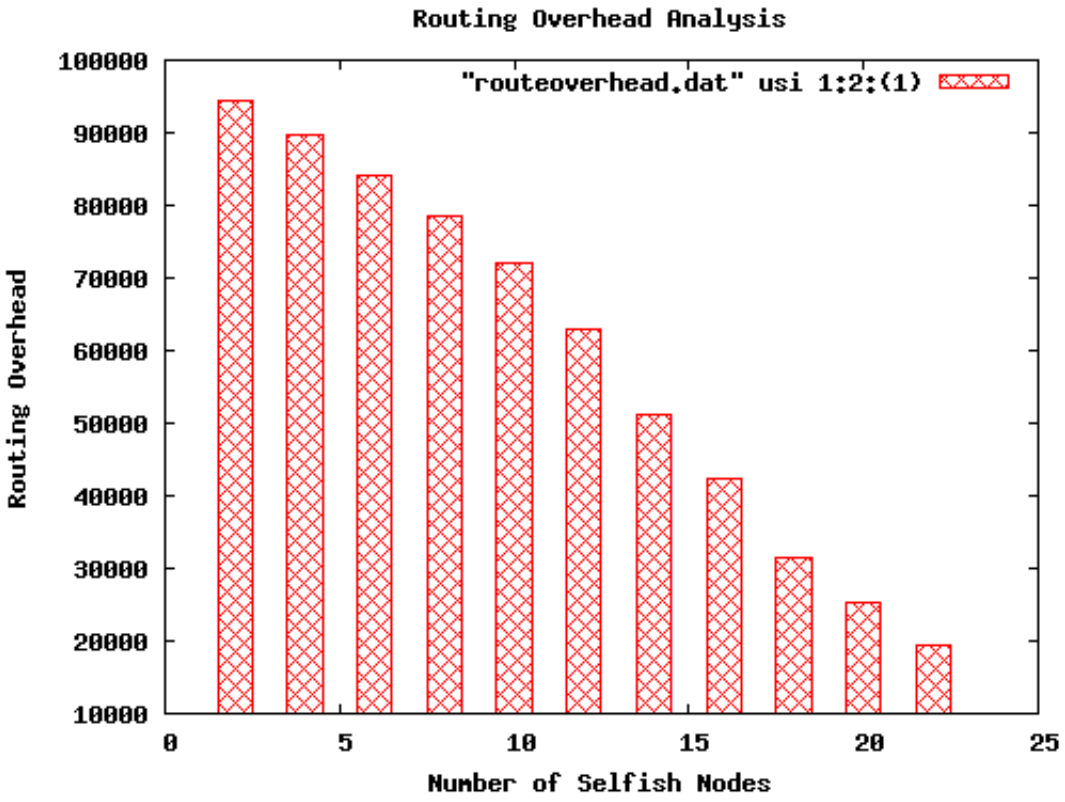

Figure 5.3: Route overhead Vs Num. of Selfish Node for CBR Traffic

From Figure 5.3, We can say that when some node behave selfishly, they prune control packets and reduce the routing overhead. As number of selfish nodes increase, Routing overhead of overall network decrease drastically. Due to drastic decrement in routing overhead, overall network become efficient and good nodes as well as selfish nodes saves energy.

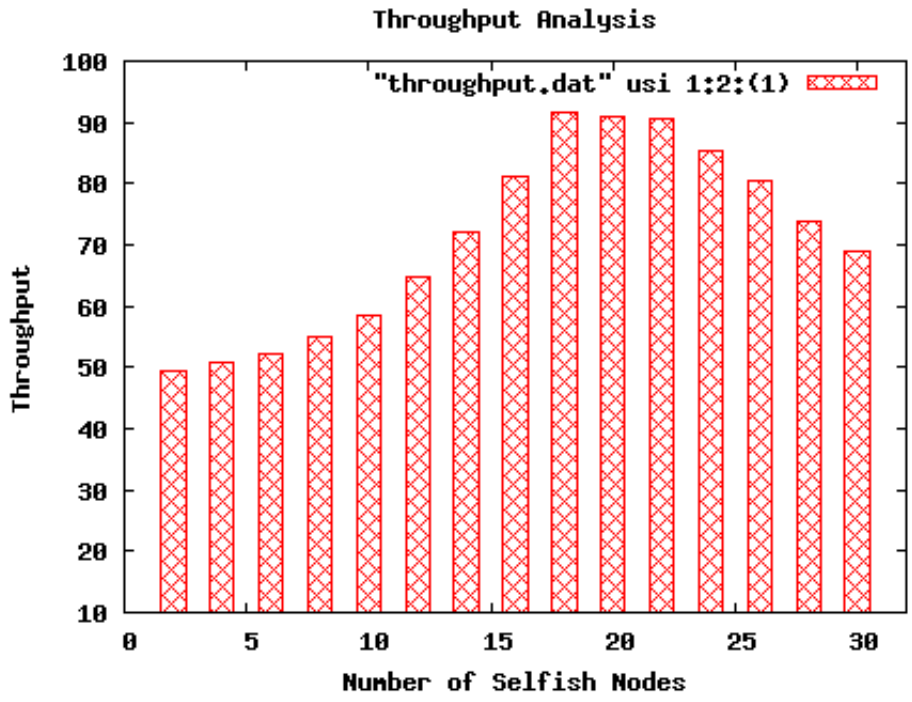

Figure 5.4: Throughput Vs Num. of Selfish Node for CBR Traffic

Figure 5.4 shows the throughput of network with varying number of selfish nodes. Simulation result suggest that certain number of selfish nodes are good for network. It also improves network throughput and make network efficient. When initially density is high, the probability of collision increase. As more number of node behave selfishly, network density decreases which in turn decrease the probability of packet collision. So up to certain limit, selfish nodes are good for network.

5.1.3 Dynamic Topology with Poisson Traffic

Simulating result shows that as number of selfish node increase in network, good nodes as well as selfish nodes saves energy(shown in fig.5.5). In mobile network scenario, routes may break frequently and routing overhead is a large component in energy consumption. When node density is high and all the nodes participate in flooding based route discovery done by DSR, nodes consume more energy. When some nodes behave selfishly, they prune all route request coming to them. So they reduce the number of control packet(shown in fig.5.6) in network hence reduce energy consumption of good nodes as well as selfish nodes.

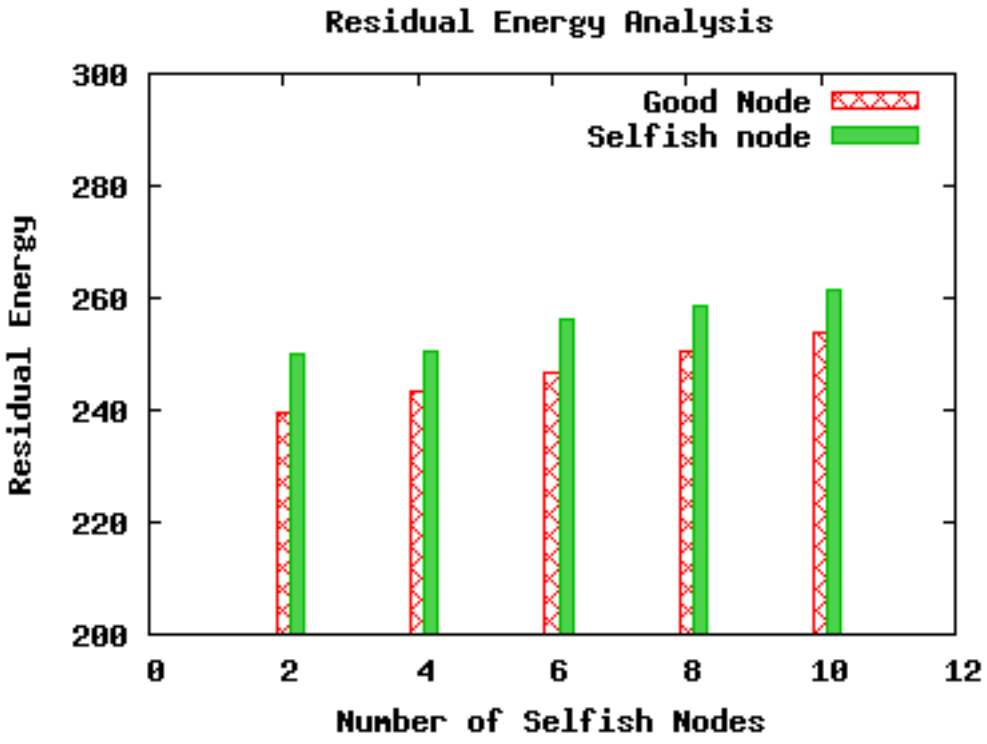

Figure 5.5: Residual Energy Vs Num. of Selfish Node for Poisson Traffic

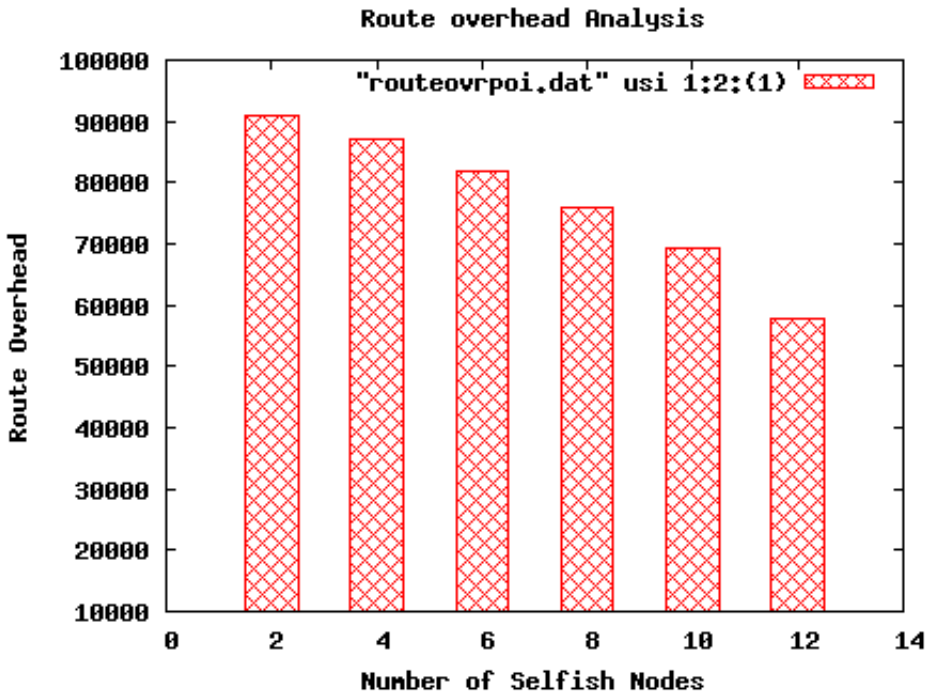

Figure 5.6: Route overhead Vs Num. of Selfish Node for Poisson Traffic

5.2 Wireless Network Card On/OFF Selfish behavior

This type of selfish behavior can easily deployed by layman user. This behavior saves highest energy compare to other selfish behavior available in literature. This behavior involves refusing to forward any control or data packets for others. Selfish people can take such an action easily, for example by turning the power off or by turning off the communication function when they do not need to communicate[23].

5.2.1 Static Topology with CBR Traffic

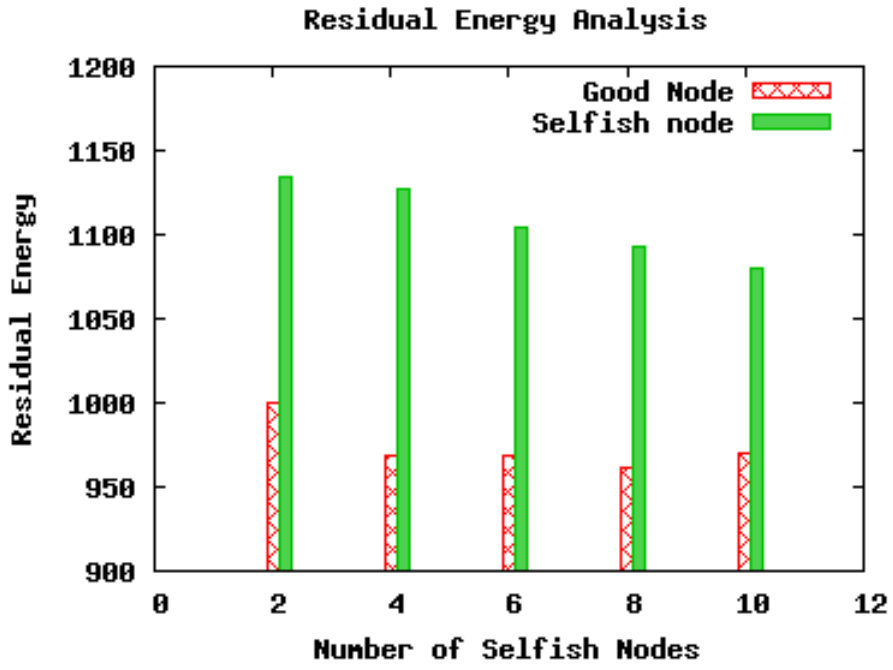

Figure 5.7: Residual Energy Vs Num. of Selfish Node for On/OFF Behavior in Static Topology

In static topology, routes are established at the beginning of session and remains valid throughout the session. In this behavior, node switch on their network card only when they need to communicate. This behavior is easy to implement and saves more energy compare to other behavior.

5.2.2 Dynamic Topology with CBR Traffic

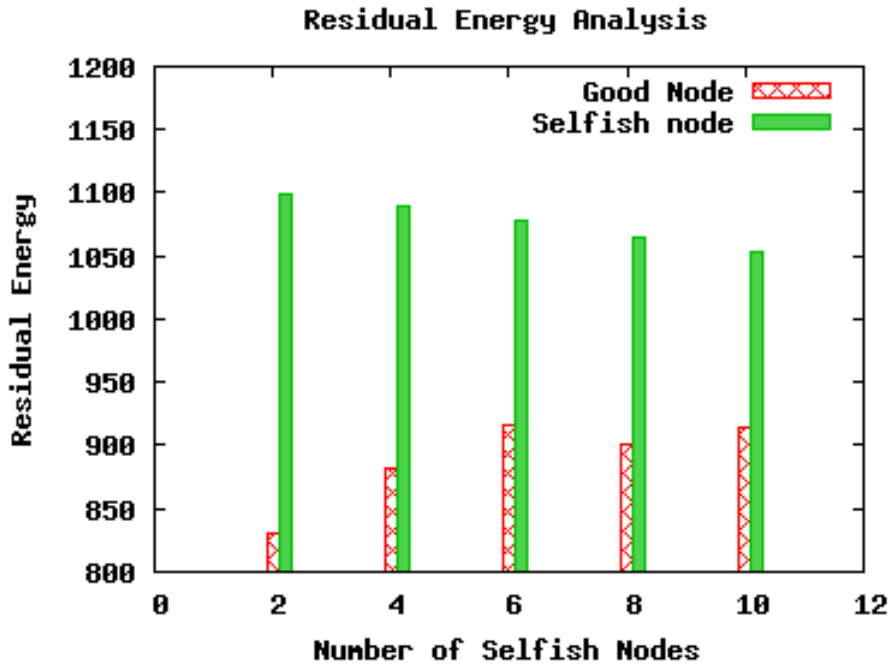

Figure 5.8: Residual Energy Vs Num. of Selfish Node for On/OFF Behavior in Dynamic Topology

Figure 5.8 shows the simulating result of dynamic topology where nodes tend to move form one place to another place at different time frame. So links may break and re-route discovery required. So nodes save less energy compare to static topology.

5.3 Comparison of Selfish Behaviors

In this report, we implemented two different selfish behavior and find their effect on power consumption. One of our selfish behavior targets the forwarding function of Dynamic Source Routing protocol. Other behavior targets the power function of wireless network card. Following graph shows the comparison of two behavior. Simulating result shows that Network Card On/Off selfish behavior saves more energy compare to Forwarding Packet Misbehavior.

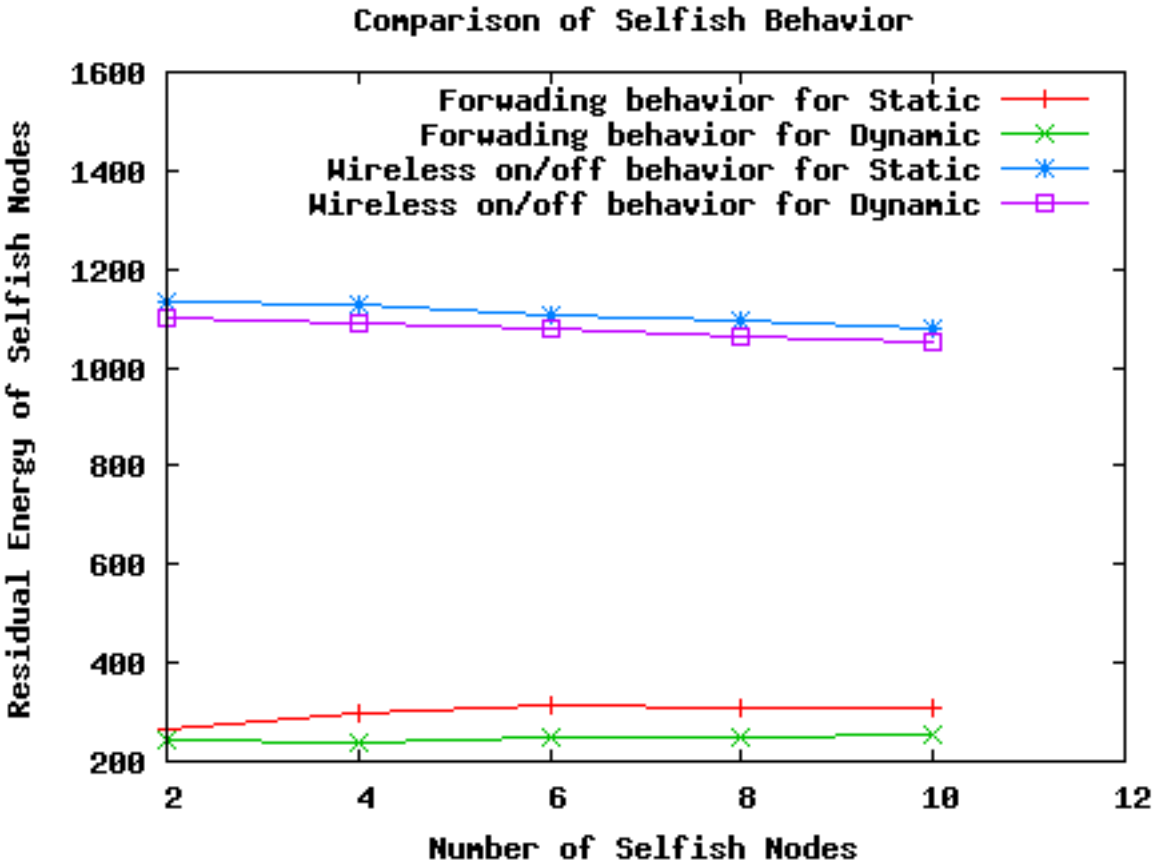

Figure 5.9: Comparison of Selfish Behavior

In this report, the behavior of the selfish neighbors is modeled and the objective is to study the impact of their selfish behavior on the power consumption. Energy saving is the only reason assumed for a node being selfish.

Chapter 6

Conclusion & Future Work

6.1 Conclusion

In this report, we implemented two different selfish behavior and find their effect on power consumption. One of our selfish behavior targets the forwarding function of Dynamic Source Routing protocol. Other behavior targets the power function of wireless network card. Our conclusion can be summarized with following points.

a. Forwarding Packet Misbehavior

- In static topology network scenario, selfish nodes save more energy than good nodes. As number of selfish node increase, residual energy of good node decrease. This shows that good nodes require to do more work in presence of selfish nodes in network.
- In dynamic topology network scenario, routing overhead plays major role in energy consumption. As number of selfish nodes increase, node density decrease which in turn reduce routing overhead and energy consumption of nodes.
- Residual energy of good nodes as well as selfish node increase with number of selfish nodes. Selfish nodes save more energy in this case as well .

b. Network Card On/OFF Misbehavior

- In static and dynamic topology network scenario, selfish nodes save more energy than good nodes. Selfish node switch on their network card only when they need to communicate.

c. Network card on/off behavior saves more energy then forwarding packet misbehavior.

6.2 Future Work

a. The next step is to study Topology Control Protocols to determine network density and adjust network card parameters accordingly.

b. Currently, We have simulation results satisfy the fact that certain number of selfish nodes are good in network. We aim to find the analytical expression for the same.

References

[1] Abdelaziz Babakhouya, Yacine Challal, Abdelmadjid Bouabdallah,"A Simulation Analysis of Routing Misbehavior in Mobile Ad Hoc Networks". 2008 IEEE, DOI 10.1109/NGMAST.2008.56.

[2] B.Wang ,Sohraab Soltani, Jonathan K. Shapiro,"Local Detection of Selfish Routing Behavior in Ad Hoc Networks".in International Symposium on Parallel Architectures, Algorithms and Networks(I-SPAN),Las Vegas, December 2005

[3] Lei Guang and Chadi Assi, "Mitigating Smart Selfish MAC Layer Misbehavior in Ad Hoc Networks,"wimob,pp.116-123,2006 IEEE International Conference on Wireless and Mobile Computing, Networking and Communication,2006

[4] Hyun Yu, Sanghyun Ahn "Node Movement Detection to Overcome False Route Failures in Mobile Ad Hoc Networks", in International Conference on Information Science and Security, Seoul 2008

[5] Tarag Fahad, Djamel Djenouri, Robert Askwith "On Detecting Packets Droppers in MANET: A Novel Low Cost Approach " in IAS'07 Proceedings of Third International Symposium on Information Assurance and Security.pp.56-64.2007

[6] Djamel Djenouri , Nadjib Badache. Two Hops ack: "New Approach for Selfish Nodes Detection in Mobile Ad hoc Networks". Technical report LSI-TRO704, University of Science and Technology houari boumediene, Algeria, April 2003.

[7] Wei Yu and K. J. Ray Liu "Secure Cooperation in Autonomous Mobile Ad-Hoc Networks Under Noise and Imperfect Monitoring: A Game-Theoretic Approach ",IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 3, NO. 2, JUNE 2008

[8] Hyun Jin Kim and Jon M. Peha "Detecting Selfish Behavior in a Cooperative Commons",in Proceedings of IEEE DySPAN,pp. 1-12,2008.

[9] A. A. Cardenas, S. Radosavac, and J. S. Baras, Detection and prevention of MAC layer misbehavior in ad hoc networks, in Proceedings of the 2nd ACM Workshop on Security of ad hoc and Sensor Networks, SASN, Washington, DC, USA. ACM, 2004, pp. 1722

[10] S. Marti, T. J. Guili, K. Lai, M. Baker. Mitigating Routing Misbehavior in Mobile Ad Hoc Networks. Proc. of MOBICOM 2000, pp.255-65, 2000.

[11] P. Michiardi, 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, pp.107-21, 2002.

[12] S.Buchegger, J.-Y. Le Boudec. Nodes Bearing Grudges: Towards Routing Security, Fairness, and Robustness in Mobile Ad Hoc Networks. Proc. of the Tenth Euromicro Workshop on Parallel, Distributed, Networkbased Processing, pp.403-10, Jan. 2002.

[13] S.Buchegger, C. Tissieres, J.-Y. Boudec. A Test-Bed for Misbehavior Detection in Mobile Ad-hoc Networks - How Much Can Watchdogs Really Do? Proc. of the Sixth IEEE Workshop on Mobile Computing Systems and Applications, 2004.

[14] Y. Rebahi, V. Mujica, D. Sisalem. A Reputation-Based Trust Mechanism for Ad hoc Networks. Proc. of the 10th IEEE Symposium on Computers and Communications, pp.37-42, 2005.

[15] Q. He, D. Wu, P. Khosla. SORI: A Secure and Objective Reputationbased Incentive Scheme for Ad-hoc Networks. Proc. of IEEE WCNC2004, Mar. 2004.

[16] S. Bansal, M. Baker. Observation-based Cooperation Enforcement in Ad-hoc Networks. Technical Report, Stanford University, 2003.

[17] Wei Yu, K. J. R. Liu,Attack-resistant cooperation stimulation in autonomous ad hoc networks,Selected Areas in Communications, IEEE Journal on, Vol. 23, No. 12. (05 December 2005), pp. 2260-2271.

[18] Hangguan Shan, Weihua Zhuang, Zongxin Wang, Cooperation or not in mobile ad hoc networks: a MAC perspective ICC'09 Proceedings of the 2009 IEEE international conference on Communications.

[19] F. Bai, N. Sadagopan, A. Helmy, "IMPORTANT: A framework to systematically analyze the Impact of Mobility on Performance of RouTing protocols for Adhoc NeTworks", IEEE INFOCOM, pp. 825-835, April 2003.

[20] Andrej KOS, Janez BASTER, "Poisson Packet Generation based on Empirical Data",systmics,cybernetics and informatics, volume-1, number-5,2006.

[21] S. Radosavac, Alvaro A. Cardenas, John S. Baras and George V. Moustakides,"Detecting IEEE 802.11 MAC layer misbehavior in ad hoc networks: Robust strategies against individual and colluding attackers" Journal of Computer Security 15 (2007) 103128.

[22] M. Raya, J.-P. Hubaux and I. Aad, DOMINO: a system to detect greedy behavior in IEEE 802.11 hotspots, in: Proc. of the Second International Conference on Mobile Systems, Applications and Services (MobiSys2004), Boston, MA, 2004.

[23] Toshihiro Suzuki, Motonari Kobayashi, Ashiq Khan, and Masanori Morita,"Proactive Cooperation Mechanism based on Cooperation Records for Mobile Ad hoc Networks",IEICE Transactions on Communication vol E90 BNo. 10.

[24] S. Buchegger and J.-Y. Le Boudec, "Performance Analysis of the CONFIDANT Protocol ", in Proc. 3rd ACM Intl. Symp., on Mobile Ad Hoc Networking and Computing, Jun 02

[25] P. Michiardi and R. Molva, CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks, In Proc. 6th IFIP Commun. and Multimedia Security Conf., Sept. 02

[26] J. Liu and V. Issarny, "Enhanced Reputation Mechanism for Mobile Ad Hoc Networks", in Proc. 2nd Intl. Conf. on Trust Management, Mar.04

[27] S. Bansal and M. Baker. "Observation-Based Cooperation Enforcement in Ad-hoc Networks", Techical Report, Stanford University, 03

[28] Djamel Djenouri , Nadjib Badache "MANET: Selfish Behavior on Packet Forwarding" at Encyclopedia of Wireless and Mobile Communications,2008.

[29] David B.,Johnson David A.,Maltz Josh Broch "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks", Ad Hoc networking, vol 5, pp 139-172,2001.

Index