Detection of Selfish Nodes in Manet

By:

Mansingh Rathore

12MCEI41

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

INSTITUTE OF TECHNOLOGY

NIRMA UNIVERSITY

AHMEDABAD-382481

May 20, 2014

Detection of Selfish Nodes in Manet

Major Project

Submitted in partial fulfillment of the requirements

For the degree of

Master of Technology in Computer Science and Engineering

(Information and Network Security)

Prepared By:

Mansingh Rathore

(12MCEI41)

Guided By:

Prof. Pushpak Raval

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

INSTITUTE OF TECHNOLOGY

NIRMA UNIVERSITY

AHMEDABAD-382481

May 20, 2014

Certificate

This is to certify that the Major Project Report entitled "**Detection of Selfish Nodes in Manet**" submitted by **Mansingh Rathore (Roll No: 12MCEI41)**, towards the partial fulfillment of the requirements for the degree of Master of Technology in Information and Network Security of Nirma University, 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. Pushpak Raval
Guide & Assistant Professor,
CSE Department,
Institute of Technology,
Nirma University, Ahmedabad.

Prof. Sharada Valiveti
Associate Professor
Coordinator M.Tech - INS
CSE Department,
Institute of Technology,
Nirma University, Ahmedabad.

Dr. Sanjay Garg
Professor and Head,
CSE Department,
Institute of Technology,
Nirma University, Ahmedabad.

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

Undertaking for Originality of the Work

I, **Mansingh Rathore**, Roll. No. **12MCEI41**, give undertaking that the Major Project entitled "**Detection of Selfish Nodes in Manet**" submitted by me, towards the partial fulfillment of the requirements for the degree of Master of Technology in **Information and Network Security** of Nirma University, Ahmedabad, is the original work carried out by me and I give assurance that no attempt of plagiarism has been made. I understand that in the event of any similarity found subsequently with any published work or any dissertation work elsewhere; it will result in severe disciplinary action.

Signature of Student

Date:

Place:

Endorsed by

Prof. Pushpak Raval

(Signature of Guide)

Acknowledgement

It gives me immense pleasure in expressing thanks and profound gratitude to **Prof. Pushpak Raval**, Professor, Computer Science Department, Institute of Technology, Nirma University, Ahmedabad for his valuable guidance and continual encouragement throughout this work. The appreciation and continual support he has imparted has been a great motivation to me in reaching a higher goal. His guidance has triggered and nourished my intellectual maturity that I will benefit from, for a long time to come.

My deepest thank you is extended to **Prof. Sharada Valiveti**, PG INS - Coordinator, Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmedabad for an exceptional support and continual encouragement throughout the Major Project.

It gives me an immense pleasure to thank **Dr. Sanjay Garg**, Hon'ble Head of Computer Science and Engineering Department, Institute of Technology, Nirma University, Ahmedabad for his kind support and providing basic infrastructure and healthy research environment.

A special thank you is expressed wholeheartedly to **Dr K Kotecha**, Hon'ble Director, Institute of Technology, Nirma University, Ahmedabad for the unmentionable motivation he has extended throughout course of this work.

I would also thank the Institution, all faculty members of Computer Engineering Department, Nirma University, and Ahmedabad for their special attention and suggestions towards the project work.
The blessings of God and family members make the way for completion of Project. I am very much grateful to them.

- Mansingh Rathore

12MCEI41

Abstract

An Ad-hoc network is a collection of mobile nodes without any central authority which forms temporary network dynamically.Because of limited communication range among MANET, several network hopes may be needed to deliver a packet from one node to another node in the wireless network. In Ad-hoc network each node is router as well as the end system which uses services of network.Means each node provide services to other nodes and use services of other nodes.All protocols(AODV,DSR etc) which has designed till now takes ideal condition scenario in which all nodes are well behaved and forward all type of packets comes to them.

But in Real network some nodes may be selfish. such nodes may not cooperate with its neighboring nodes and use their resources and not provide its own resources for them.By this activity selfish node can reserves its CPU power,bandwidth for retransmitting data of others,battery and can use it for themselves only when they needed.For detection of such nodes we can modify existing protocols like DSR, AODV.

In this project we proposed a new neighboring node based mechanism for detection of selfish nodes in MANET and perform the simulation using Network Simulator-2(Version-2.35). Each node of MANET has to be cooperate on continuous basis within a time frame.Behaviour of those nodes which has not cooperated with other nodes treated as suspicious and have to go under test of checking selfiness. Simulation results show that our neighboring node based system can be used for detection of selfish nodes.

Keywords: Network Simulator, Mobile Ad-hoc Network (MANET); Nodes; Selfish Nodes, Misbehaving Nodes.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Background

A Mobile Ad-hoc network (MANET) is a collection of mobile nodes ie. MANET is a network consisting of mobile nodes like PDAs,PCs,Laptops, Tabs, and wireless phones.These devices has properties of self configuration and self organisation, by this property it can form new network very easily. [01].MANET is a new communication paradigm. It consists of a collection of mobile nodes which communicates through a wireless medium. There is no central authority in MANET like infrastructured based network,they communicate directly to destination node.There is no acces point to connet nodes with each other.They connected directly.If a node is not in direct range of destination node then it can connect it with the help of intermediate node which will forward its packet to destination.Due to this activity in MANET each node is work router also.

Dynamic Source Routing [DSR] and AODV are desiged for such network to handle such activity in MANET or any wireless network.[02].Manet require minimum deployment facilities and configuration setup and no need of central authority due to which is is very suitable for emergency condition like natural disaster,in military operations and in medical emergencies.In such condition resources are very limited and time to setup network is also very less due to this manet is suitable for it. Manet will tranfer its masseges by cooperation of each node of the network without infrastucture.

A MANET is a self designing arrangement of mobile nodes joined by wireless connections. In a MANET, the nodes are allowed to move randomly, changing the network topology quickly and erratically. Manets are decentralized, and thusly all network exercises are

completed by the nodes themselves. Every node is an end-system as well as a router to send packets for different nodes. The majority of the steering calculations intended for MANET, for example, DSR and AODV are focused around the assumption that each node forward each and every packet. In any case a portion of the nodes may be selfish. These nodes utilize the network and its resources yet they don't coordinate with other nodes. Such nodes don't consume any energy, for example, battery, CPU power,and likewise data transmission for other nodes and they hold them just for themselves.
In reputation based strategy, network nodes all in all distinguish and announce the misbehavior of a suspicious node. Such a announcement is then proliferated all around the network. Credit based method gives motivating forces to nodes to reliably perform networking functions. Keeping in mind the end goal to attain this objective, electronic credit or comparable installment technique could be set up. Nodes get paid for giving resources to different nodes. Acknowledgement based procedure depend on the acknowledgement receipt to check that a packet has been sent.

1.2 Motivation

Security is main requirement for any wireless network so it is also important for Ad-hoc network.Security is basically devided into three main types which are Confidentiality, integrity of data and availability of services in any network.Ad-hoc network is open in nature ahd has dynamic topology and has no central authority so it has weak defence mechanism.so ad-hoc network are very susceptible to attack.

1.3 Problem Definition

In MANET, each node is depends on others to forward its packets.And as we know nodes are mobile and operated from battery and no continous power supply so they have limited power to use.Due to which nodes may not help other nodes in packet forwarding to save own power.But use network resource for their own data packet forwarding. To avoid forwarding of packets of others selfish node may drop contol packet due to which it will not count as intermidiate node in any routing table for data forwarding.Thus it can reserve its resources,and use it for its own use. here, we propose a new mechanism for detection of such selfish nodes. Every node has to contribute its services and resources for network operations if any node deviates from it, it has to go under test of checking

of selfishness.

1.4 Objectives of the Study

Objectives of this project work are as follows:

- Study of performance of dynamic source routing protocol and its consequences.
- Finding out the performance of DSR protocol under selfish node.
- Simulating the selfish mode using DSR routing protocols.
- Results comparision of DSR protocol with and without selfish node.
- Proposed innovated techniques for detection of selfish node in DSR protocol.

Chapter 2

Literature Survey

2.1 Ad hoc Network

This network is called Independent Basic Service Set (IBSS) Stations in a IBSS communicate directly with each other and do not use an access point. Because of the mobility associated with ad-hoc networks, they are commonly called Ad hoc Network. Ad hoc Networks are self organized networks whose nodes are free to move randomly while being

Figure 2.1: Ad hoc Network Operation

able to communicate with each other without the help of an existing network infrastructure [02]. Ad hoc Networks are suitable for use in situations where any wired or wireless infrastructure is inaccessible, overloaded, damaged or destroyed such as emergency or rescue missions, disaster relief efforts and tactical battlefields, as well as civilian network situations, such as conferences and classrooms or in the research area like sensor networks. Ad hoc Network eliminates this dependence on a fixed network infrastructure where each station acts as a intermediate switch[07].

Networks are formed on-the-fly, devices can leave and join the network during its lifetime, devices can be mobile within the network, the network as a whole may be mobile and the network can be deformed on-the-fly. Devices in mobile ad hoc networks should be able to detect the presence of other devices and perform the necessary set-up to facilitate communications and the sharing of data and services [02].

2.1.1 Features

A mobile ad hoc network has following features:

- **Autonomous Terminal**

  In Ad hoc Network, each mobile terminal is an autonomous node, which may function as both a host and a router. In other, since there is no background network works, besides the basic processing ability as a host, the mobile nodes perform switching functions like router. So usually endpoints and switches are indistinguishable in Ad hoc Network.

- **Distributed Operation**

  For the central control of the network operations, the control and management of the network is divided among the terminals. The nodes involved in a Ad hoc Network should collaborate amongst themselves and each node acts as a relay as per requirement, to implement functions like security and routing.

- **Multi-hop Routing**

  Basic types of ad hoc routing algorithms can be single-hop and multi-hop, based on different routing protocols and link layer attributes. Single-hop Ad hoc Network is simpler than multi-hop in terms of structure and implementation, with the cost of lesser functionality and applicability. When delivering data packets from a source to its destination out of the direct wireless transmission range, the packets should be forwarded through one or more intermediate nodes.

- **Light-weight Terminal**

  In most cases, the Ad hoc Network nodes are mobile devices with less CPU processing capability, small memory size, and low power storage. Such devices need optimized algorithms and mechanisms that implement the computing and communicating functions.

2.1.2 Characteristics

Ad hoc Networks are new paradigm of networks, offering unrestricted mobility without any underlying infrastructure. Basically, ad hoc network is a collection of nodes communicating with each other by forming a multi-hop network. Following are the characteristics of a Ad hoc Network.

- **Dynamic Topologies**

  Nodes are free to move arbitrarily. The network topology may change randomly and have no restriction on their distance from other nodes. As a result of this random movement, the whole topology is changing in an unpredictable manner, which in turn gives rise to both directional as well as unidirectional links between the nodes.

- **Energy Constrained Operation**

  Almost all the nodes in an ad hoc network rely on batteries or other exhaustive means for their energy.The battery depletes due to extra work performed by the node in order to survive the network. Therefore, energy conservation is an important design optimization criterion.

- **Bandwidth Constraint**

  Wireless links have significantly lower capacity than infrastructures networks. Throughput of wireless communication is much less because of the effect of the multiple access, fading, noise, interference conditions. As a result of this, congestion becomes a bottleneck in bandwidth utilization.

- **Limited Physical Security**

  Ad hoc Networks are generally more prone to physical security threats than wireless networks because the ad hoc network is a distributed system and all the security threats relevant to such a system are pretty much present, as a result, there is an increased possibility of eavesdropping, spoofing, masquerading, and denial-of-service type attacks.

2.1.3 Applications

Because ad hoc networks are flexible networks that can be set up anywhere at any time, without any infrastructure, including pre-configuration or administration, people have

come to realize the commercial potential and advantages that mobile ad hoc networking can bring.

This section describes some of the most prevalent applications for ad hoc wireless networks. The self-configuring nature and lack of infrastructure inherent to these networks make them highly appealing for many applications, even if it results in a significant performance penalty. The lack of infrastructure is highly desirable for low-cost commercial systems, since it precludes a large investment to get the network up and running, and deployment costs may then varies with network success.

Lack of infrastructure is also highly desirable for military systems, where communication networks must be configured quickly as the requirement occure,generally in remote areas. Other advantages of ad hoc wireless networks include ease of network reconfiguration and reduced maintenance costs. However, these advantages must be balanced against any performance penalty resulting from the multi-hop routing and distributed control inherent to these networks.

- **Data Networks**

  Ad-hoc wireless data networks primarily support data exchange between laptops, palmtops, personal digital assistants (PDAs) and all other information devices. These data networks generally fall into three categories based on their coverage area: LANs, MANs, and WANs. Infrastructure-based wireless LANs are already quite common, and deliver good performance at low cost. However, ad hoc wireless data networks have many advantages over these infrastructure-based networks. First, only single access point is needed to connect to the backbone wired infrastructure: this reduces installation cost requirements. In addition, it can be inefficient for nodes to go through an access point or base station. For example, PDAs that are next to each other can exchange information directly rather than routing through an intermediate node.

  Wireless MANs typically require multi-hop routing since they cover a large area. The challenge in these networks is to support high data rates, in a cost-effective manner, over multiple hops, where the link quality of each hop is different and changes with time. The lack of centralized network control and potential for high-mobility users make this objective complicated. Military programs such as DARPAs GLOMO (Global mobile information systems) have invested much time and money

in building high-speed ad hoc wireless MANs that support multimedia, with limited success [23].

Wireless WANs are needed for applications where network infrastructure to cover a wide area is too costly or impractical to deploy. For example, sensor networks may be dropped into remote areas where network infrastructure cannot be developed. In addition, networks that must be built up and torn down quickly, e.g. for military applications or disaster relief, are infeasible without an ad hoc approach.

- **Home Networks**

  These networks are envisioned to support communication between PCs, laptops, PDAs, cordless phones, smart appliances, security and monitoring systems, consumer electronics, and entertainment systems anywhere in and around the home. Such networks could enable smart rooms that sense people and movement and adjust light and heating accordingly, as well as aware homes that network computers and sensors for assisted living of old people and those with disabilities.

  These networks also encompass video or sensor monitoring systems with the intelligence to coordinate and interpret data and alert the home owner and the appropriate police or fire department of unusual patterns, intelligent appliances that coordinate with each other and with the Internet for remote control, software upgrades, and to schedule maintenance, and entertainment systems that allow access to a VCR, set-top box, or PC from any television or stereo system in the home [08].

- **Device Networks**

  These networks use for short-range wireless connections between devices. Such networks are primarily intended to replace inconvenient cabled connections with wireless connections. Thus, the need for cables and the corresponding connectors between cell phones, modems,headsets, PDAs, computers, printers, projectors, network access points, and other such devices is no more required. The main technology drivers for such networks are low-cost low-power radios with networking capabilities such as Bluetooth. The radios are integrated into commercial electronic devices to provide networking capabilities between devices. Some common uses include a wireless headset for cell phones, a wireless USB or RS232 connector, wireless cards, and wireless set-top boxes.

- **Sensor Networks**

  Wireless sensor networks consist of small nodes with sensing, computation, and wireless networking capabilities, as such these networks represent the convergence of three important technologies. Sensor networks have enormous potential for both consumer and military applications. Military missions require sensors and other intelligence gathering mechanisms that can be placed close to their intended targets. The potential threat to these mechanisms is therefore quite high, so it follows that the technology used must be highly redundant and requires as little human intervention as possible. An apparent solution to these constraints lies in large arrays of passive optical, chemical,electromagnetic, and biological sensors. These can be used to identify and track targets, and can also serve as a first line of detection for various types of attacks. Such networks can also support the movement of unmanned, robotic vehicles. For example, optical sensor networks can provide networked navigation, routing vehicles around obstacles while guiding them into position for defense or attack. The design considerations for some industrial applications are some what similar to those for military applications. In particular, sensor arrays can be deployed and used for remote sensing in nuclear power plants, mines, and other industrial venues.

2.2 Security Goals

In providing a secure networking environment some or all of the following service may be required.

2.2.1 Authentication

It verifies the identity of node or a user, and to be able to prevent impersonation. In wired networks and infrastructure-based wireless networks, implementation of a central authority at a point such as a router, base station, or access point is possible. But there is no central authority in Ad hoc Network, and it is much more difficult to authenticate an entity. Authentication can be providing using encryption along with cryptographic hash function, digital signature and certificates.

2.2.2 Integrity

Ensure that the data has been not altered during transmission. The integrity service can be provided using cryptography hash function with some form of encryption. When dealing with network security the integrity service is often provided implicitly by the authentication service.

2.2.3 Availability

Ensure that the intended network security services listed above are available to the intended parties when required. The availability is typically endure by redundancy, physical protection and other non-cryptographic means, e.g. use of robust protocol.

2.2.4 Non-repudiation

Ensure that parties can prove the transmission or reception of information by another party, i.e. a party cannot falsely deny having received or sent certain data. By assigning signature to the message, the entity cannot later deny the message.
In public key cryptography, a node signs the message by its private key. All other nodes can verify the signed message by using As public key, and A cannot deny that its signature is attached to the message.

2.2.5 Access Control

To prevent unauthorized use of network services and system resources, access control is tied to authentication attributes. In general, access control is the most commonly thought of service in both network communications and individual computer systems.

2.3 Classification of Ad hoc Networks Routing Protocols

Routing protocols in Ad hoc Networks are classified into three different categories according to their functionality [05]

- Reactive
- Proactive
- Hybrid Protocol

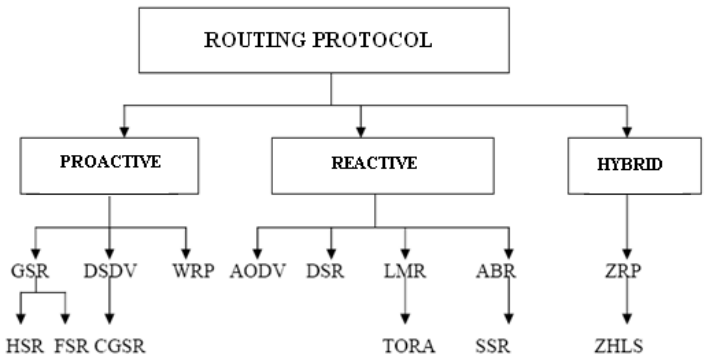

Figure 2.2: Classification of Routing Protocol

In Josh Broch et. al. [02], the area of ad hoc networking has been receiving increasing attention among researchers in recent years, as the available wireless networking and mobile computing hardware bases are now capable of supporting the promise of this technology. Over the past few years, a variety of new routing protocols targeted specifically at the ad hoc networking environment have been proposed, but little performance information on each protocol and no detailed performance comparison between the protocols has been available.

Josh Broch et. al [02], defines a new simulation environment which provides a powerful tool for evaluating ad hoc networking protocols and other wireless protocols and applications. Using this simulation environment, present the results of a detailed packet-level simulation comparing four recent multi-hop Wireless ad hoc network routing protocols. These protocols, DSDV, TORA, DSR, and AODV, cover a range of design choices, including periodic advertisements vs. on demand route discovery, use of feedback from the MAC layer to indicate a failure to forward a packet to the next hop, and hop-by-hop routing vs. source routing. Paper defined simulation of each protocol in ad hoc networks of 50 mobile nodes moving about and communicating with each other, and presented the results for a range of node mobility rates and movement speeds. In comparing the protocols, author choose to evaluate them according to these three metrics:

- **Packet delivery ratio:**

  The ratio between the number of packets originated by the application layer CBR sources and the number of packets received by the CBR sink at the final destination.Packet delivery ratio is important as it describes the loss rate that will be seen by the transport protocols, which in turn affects the maximum throughput

that the network can support. This metric characterizes both the completeness and correctness of the routing protocol.

- **Routing overhead:**

  The total number of routing packets transmitted during the simulation. For packets sent over multiple hops, each transmission of the packet (each hop) counts as one transmission.

  Routing overhead is an important metric for comparing these protocols, as it measures the scalability of a protocol, the degree to which it will function in congested or low bandwidth environments, and its efficiency in terms of consuming node battery power. Protocols that send large numbers of routing packets can also increase the probability of packet collisions and may delay data packets in network interface transmission queues.

- **Path optimality:**

  The difference between the numbers of hops a packet took to reach its destination and the length of the shortest path that physically existed through the network when the packet was originated.

  In the absence of congestion or other noise, path optimality measures the ability of the routing protocol to efficiently use network resources by selecting the shortest path from a source to a destination.

  Josh Broch et. al [02], calculate it as the difference between the shortest path found internally by the simulator when the packet was originated, and the number of hops the packet actually took to reach its destination. Each of the protocols studied performs well in some cases yet has certain drawbacks in others.

Some Basic Protocol Algorithms:

- **DSDV (Destination-Sequenced Distance Vector) Algorithm**

  This algorithm performs quite predictably, delivering virtually all data packets when node mobility rate and movement speed are low, and failing to converge as node mobility increases. DSDV 18 is a hop-by-hop distance vector routing protocol requiring each node to periodically broadcast routing updates. The key advantage of DSDV over traditional distance vector protocols is that it guarantees loop-freedom.

- **TORA (Temporally-Ordered Routing Algorithm) Algorithm**

  This algorithm, although the worst performer in performed experiments in terms of routing packet overhead, still delivered over 90 percent of the packets in scenarios with 10 or 20 sources. At 30 sources, the network was unable to handle all of the traffic generated by the routing protocol and a significant fraction of data packets were dropped.

  TORA [14][15] is a distributed routing protocol based on a link reversal algorithm. It is designed to discover routes on demand, provide multiple routes to a destination, establish routes quickly, and minimize communication overhead by localizing algorithmic reaction to topological changes when possible. Route optimality (shortest-path routing) is considered of secondary importance, and longer routes are often used to avoid the overhead of discovering newer routes.

  The actions taken by TORA can be described in terms of water flowing downhill towards a destination node through a network of tubes that models the routing state of the real network. The tubes represent links between nodes in the network, the junctions of tubes represent the nodes, and the water in the tubes represents the packets flowing towards the destination. Each node has a height with respect to the destination that is computed by the routing protocol. If a tube between nodes A and B becomes blocked such that water can no longer flow through it, the height of A is set to a height greater than that of any of its remaining neighbours, such that water will now flow back out of A (and towards the other nodes that had been routing packets to the destination via A).

- **AODV (Ad Hoc On-Demand Distance Vector) Algorithm**

  Finally, this algorithm performs almost as well as DSR at all mobility rates and movement speeds and accomplishes its goal of eliminating source routing overhead, but it still requires the transmission of many routing overhead packets and at high rates of node mobility is actually more expensive than DSR.

  AODV [17] is essentially a combination of both DSR and DSDV. It borrows the basic on-demand mechanism of Route Discovery and Route Maintenance from DSR, plus the use of hop-by-hop routing, sequence numbers, and periodic beacons from DSDV.

  AODV is a purely reactive routing protocol. In this protocol, each terminal does

not need to keep a view of the whole network or a route to every other terminal. Nor does it need to periodically exchange route information with the neighbour terminals. Furthermore, only when a mobile terminal has packets to send to a destination does it need to discover and maintain a route to that destination terminal. In AODV, each terminal contains a route table for a destination. A route table stores the following information: destination address and its sequence number, active neighbours for the route, hop count to the destination, and expiration time for the table. The expiration time is updated each time the route is used. If this route has not been used for a specified period of time, it is discarded.

- **Basic Mechanism:**

  When a node S needs a route to some destination D, it broadcasts a ROUTE REQUEST message to its neighbours, including the last known sequence number for that destination. The ROUTE REQUEST is flooded in a controlled manner through the network until it reaches a node that has a route to the destination. Each node that forwards the ROUTE REQUEST creates a reverse route for itself back to node S.

  When the ROUTE REQUEST reaches a node with a route to D, that node generates a ROUTE REPLY that contains the number of hops necessary to reach D and the sequence number for D most recently seen by the node generating the REPLY. Each node that participates in forwarding this REPLY back toward the originator of the ROUTE REQUEST (node S), creates a forward route to D. The state created in each node along the path from S to D is hop-by-hop state; that is, each node remembers only the next hop and not the entire route, as would be done in source routing.

  In order to maintain routes, AODV normally requires that each node periodically transmit a HELLO message, with a default rate of once per second. Failure to receive three consecutive HELLO messages from a neighbour is taken as an indication that the link to the neighbour in question is down. Alternatively, the AODV specification briefly suggests that a node may use physical layer or link layer methods to detect link breakages to nodes that it considers neighbours [17]. When a link goes down, any upstream node that has recently forwarded packets to a destination using that link is notified via an UNSOLICITED ROUTE REPLY containing an infinite

metric for that destination. Upon receipt of such a ROUTE REPLY, a node must acquire a new route to the destination using Route Discovery as described above.

Chapter 3

Related Work

3.1 Node Misbehaviours in MANET

Like DSR, all other routing protocols designed for MANET naively assume that all the nodes in the network are cooperative in performing the networking tasks. This can be guaranteed if all of the nodes belong to a single authority where all of them have the same common objective. However that is not the case such as in civilian applications, some of the nodes may behave selfishly and only act towards those that add to their own benefits. Providing network services such as forwarding packets and detecting routes consumes network bandwidth, local CPU time, memory and battery power which are limited in MANET nodes[05].

For example, simulation studies by Buttyan and Hubaux [6] show that when the average numbers of hops from a source to a destination is around 5, then almost 80 percent of the transmission energy will be devoted to packet forwarding. By denying services for others, a node could reserve its resources for its own use and stay longer in the network. So there is a strong motivation for the nodes not to cooperate and misbehaving. In general, there are two types of node misbehaving: misleading and selfish.

3.1.1 Misleading Nodes

A misleading node is selective in choosing which packet it wants to respond. It behaves like an honest node, responding to all control packets during route discovery process. However when the node receives a data packet to be further forwarded, the misleading node silently drops it. The reasons for choosing data packets for dropping is because data packets are generally greater in term of size and number than the control packets and

thus consumes more energy to forward. This type of behaviour is also called Gray Hole Attack [07].

3.1.2 Selfish Nodes

The second type of node misbehaving is selfish. Selfish node aims to save its resources to the maximum. This type of misbehaving node discards all incoming packets (control and data) except those which are destined to it. By dropping control packets, the nodes would not be included in the routing and then be released from being requested to forward data packets.

The similarity of these two types of misbehaving is that they both use the network to forward their own packets but refuse to provide the same services back. Misbehaving nodes can significantly degrade the performance of a MANET. Simulation done by Babakkhouya et al.[08] shows that the percentage of misleading nodes can decrease the number of packets that are successfully delivered in the network. When 50 percent of the nodes of the network become misleading, the packet delivery ratio (PDR) degrades by 55 percent. Selfish nodes on the other hand, have no big impact on PDR. However, this type of misbehaving can increase the average end to end delay.

As the number of selfish nodes been increased, the source node will have less option on which route the data packets should travel. As a result, less attractive route will be selected which means longer delays. It also means that the remaining cooperative nodes have to take the extra burden of forwarding packets. If 50 percent of the nodes become selfish, the average end to end delay increases by 60 percent. In this paper, we present a system to detect selfish nodes in a MANET.

3.2 Classification of Techniques

Several techniques have been proposed to detect misbehaving nodes in mobile ad hoc network. These techniques can be classified into following three categories:

3.2.1 A Reputation-Based Technique

Reputation based technique on the other hand rely on building a reputation metric for each node according to its behavioral pattern. A monitoring method used by most systems in this category is called a watchdog. Watchdog was proposed by Marti et al. [04] to detect data packet non forwarding by overhearing the transmission of the next node.

[05][06][07] use similar monitoring technique but then propagate collected information to nearby nodes and are susceptible to false praise and false accusation attacks.
Mr. Bansal and Mr. Baker proposed a system called OCEAN [08] where the reputation of a neighbor is evaluated using only locally available information and thus avoid sophisticated and potentially vulnerable techniques of reputation propagation throughout the network. It is reported that even with direct observations of the neighbor; OCEAN performs almost as well and sometimes even better compared to schemes that share second-hand reputation information.

3.2.2 Credit Based Technique

The basic idea of credit based technique is to provide incentives for nodes to faithfully perform networking functions. In order to achieve this goal, virtual (electronic) currency or similar payment system may be set up. Nodes get paid for providing services to other nodes. When they request other nodes to help them for packet forwarding, they use the same payment system to pay for such services. Credit based schemes can be implemented using two models:
1) The Packet Purse Model (PPM) and
2) The Packet Trade Model (PTM) [03].

- **The Packet Purse Model**

  In this model, the originator of the packet pays for the packet forwarding service. The service charge is distributed among the forwarding nodes. The originator loads it with the number of beans sufficient to reach the destination. Each forwarding node acquires one or several beans from the packet and thus, increases the stock of its beans. If packet does not have enough beans to be forwarded, the packet is discarded. The basic problem with this approach is that, it might be difficult to estimate the number of beans that are required to reach a given destination [03].

- **The Packet Trade Model**

  In this model, packet does not carry beans but it is traded for beans by intermediate nodes. Each intermediary buys it from previous one for some beans and sells it to the next one for more beans. The total cost of forwarding the packet is covered by destination of the packet. An advantage of this approach is that the originator does not have to know in advance the number of beans required to deliver a packet

[03].

3.2.3 Acknowledgement Based Technique

The last category is acknowledgment based technique, it rely on the reception of a acknowledgment to verify that a packet has been forwarded. Liu et al. [09] proposed the 2ACK system where nodes explicitly send acknowledgment two hops upstream to verify co-operation. This system is susceptible to collusion of two or more consecutive nodes. Furthermore, colluding nodes can frame honest ones by claiming not to receive the acknowledgment. All of the mechanisms mentioned above are designed to detect and handle misleading nodes.

There are a few systems that have been proposed to detect selfish nodes in a MANET. One example is Context Aware Scheme [10] introduced by Mr. Paul and Mr. Westhoff. This system uses un-keyed hash chains and a promiscuous mode to detect the misbehaviour during route discovery phase. The observers of misbehaviour independently communicate their accusation to the source. To convict a culprit, more than three accusations are needed. If there is only one accusing node, the accusing node itself will be considered to be an attacker.

The drawback of this system is that it is more beneficial for a node not to send the alarm message to avoid the risk being the only accuser and regarded as attacker. In [11], Djenouri et al. propose two different techniques to detect two different types of control packet droppers. They suggest the use of two-hop ACK approach for monitoring directed packets (RREP, RRER) and promiscuous-based overhearing technique for monitoring broadcast packets (RREQ). Huang et al. [12] suggest that the monitoring node simply compares the ratio of relay RREQ number between its neighbour and itself. If the ratio is smaller than a threshold, the neighbour is regarded as selfish and its packet is dropped as the punishment.

3.3 Other Proposed Techniques

3.3.1 Brain Mapping Function Scheme

- **Overview of the Proposed Architecture**

  In Abhishek et. al [23], proposed a scheme on the real fact that everyone want to live and struggle for its existence if anyone is sure that he will not going to die

because of deficiency of resources then it will be more chances that he will not cheat others for resources . The same concept is used in the core of proposed theoretical model.

- **The Brain Mapping Function Node**
  (BMFN): These nodes perform Brain Mapping functions for all nodes present in ad hoc network. The important parts of Brain Mapping nodes are
  - **IDPS module:**This Module has the capability of detection and prevention of selfish node.
  - **Turi machine:**It comprises of infinite memory capability to store virtual node.
  - **Virtualization Layer:**This Layer is used for creating virtual node.
- **Working of proposed model**
  The working of model is very simple the Brain Mapping Function Nodes (BMFN) are created in ad hoc network the number of BMFN depends on factors like area, radio range strength, data importance etc. The BMFN is very robust and effective because it takes concepts of various fields like theory of computation (TOC), neural network, artificial intelligence, and many more so it has advantages of all these fields. The paper proposed a new technique to detect and prevent selfish node furthermore it could be possible for some networks this scheme provide fully freedom from selfish nodes and increases throughput and performance that could not be achieved till yet.

3.3.2 Cache Scheme

Basic Cache Scheme

In Hongxun Liu et. al [24], proposed a technique in which, hardware assisted detection scheme, the hardware is responsible to detect the misbehavior of the software and report such misbehavior to other nodes. In the cache based detection scheme, there is a cache unit as well as a few counters. The cache stores the identity information of the recently received packets and is used to differentiate original packets from duplicate packets received by wireless node.

A mobile node could receive the same route request multiple times due to the broadcast effect during the route discovery process. When node A receives a route request

packet and broadcasts that packet, its neighbor B will receive and broadcast the route request packet. Due to the nature of broadcast, node A will receive the same route request packet again from node B. If node A has a few neighbors within its transmission range, it is likely that A will receive a few duplicate route requests. The cache can help the detection hardware recognize the original route request from the duplicate route requests.

There are four counters used in the cache based detection scheme: TC (Total Counter), DC (Drop Counter), TDC (Total Data Counter) and DDC (Data Drop Counter). The first two counters are used to detect simple dropping while TDC and DDC are used to detect selective dropping. TC is used to record the total number of unique packets received, while DC is used to record how many unique packets are dropped by this node. TDC is used to record how many data packets are received by the node while DDC records the number of data packets dropped.

Mobile ad hoc networks are more vulnerable to misbehaving activities than the wired networks, which makes securing the mobile ad hoc networks very promising and enormously important. This paper presents a hardware based cache scheme to detect the misbehaving nodes. The features of the proposed scheme are:

1) High detection of misbehaving nodes.

2) Zero false positive.

3) Minor changes to software layer.

The simulation results also show that the cache scheme seems to have low detection effectiveness in the case of selective dropping scenario. But we should not count the misbehaving nodes which never commits data packet dropping as misbehaving. Thus, the right calculation of detection effectiveness should only count the nodes which commits data packet dropping as misbehaving. Now, the detection effectiveness will be nearly 100 percent. The cache scheme can detect the misbehaving nodes accurately in terms of detection effectiveness and false positive in both the simple dropping and the selective dropping scenarios.

3.3.3 2ACK Scheme

In Manvia et. al [25], proposed a system which is used to detect the misbehavior routing using 2ACK and also check the confidentiality of the data message in

MANETs environment. Here, author used a scheme called 2ACK scheme, where the destination node of the next hop link will send back a 2 hop acknowledgement called 2ACK to indicate that the data packet has been received successfully. The proposed work (2ACK with confidentiality) is as follows.

1) If the 2ACK time is less than the wait time and the original message contents are not altered at the intermediate node then, a message is given to sender that the link is working properly.

2) If the 2ACK time is more than the wait time and the original message contents are not altered at the intermediate node, then a message is given to sender that the link is misbehaving.

3) If the 2ACK time is more than the wait time and the original message contents are altered at the intermediate node, then message is given to sender that the link is misbehaving and confidentiality is lost.

4) If the 2ACK time is less than the wait time and the original message contents are altered at the intermediate node then, a message is given to sender that the link is working properly and confidentiality is lost.

At destination, a hash code will be generated and compared with the senders hash code to check the confidentiality of message. Hence, if the link is misbehaving, sender to transmit messages will not use it in future and loss of packets can be avoided.

3.3.4 Two-Timer Scheme

In Hongxun et. al [21], proposed a hardware assisted detection scheme which can be used to detect routing attacks and packet forwarding attacks. In this scheme, the hardware monitors the upper and software layers of its own node. The hardware consists of two logical components. One component contains tamper-resistance mechanisms, protecting the hardware from hardware attacks and logical attacks. With the help of tamper-resistance component, each wireless node could be easily identified. The other component is responsible for detecting misbehavior of the upper layer.

The hardware detection unit is the foundation of defending MANET. When the software of the node is compromised or is mounting attacks, the hardware can

detect the misbehavior of the software layer and report it to the network [21].

Chapter 4

Project Design

4.1 DSR (Dynamic Source Routing) Algorithm

At any mobility rate and movements of node this DSR protocol perform good.It uses source routing due to which in such condition routing overhead increases.

DSR [09][10][02] uses source routing instead of hop-by-hop routing,means each packet routed in the network carry a header which contains information about nodes in sequence it should pass through during traversing due to which intermediate node has no need to maintain up to date routing information about the network.Packet contains all routing decisions it eliminates all requirement of route advertisment periodically.

Basic Mechanism:

DSR is one of routing protocols proposed with MANET working group of the Internet Engineering Task Force (IETF) [02]. The protocol has two main functions:

1) Route Discovery

2) Route Maintenance,

these two working on-demand. A source node which want to communicate with destination node first search its own route cache table. If no route foundfor the destination, it will initiate Route Discovery by broadcasting a RREQ (Route Request) packet to its neighbors. Each intermediate node receiving the RREQ, and adds its address to the RREQ and then rebroadcast the modified RREQ.

If the destination node receives the RREQ, it constructs a RREP (Route Reply)

packet and sends the RREP back to the source node using the reverse path. Upon receiving the RREP, the source node updates its route cache table with an entry for the destination node and can start sending the data packet. Route maintenance on the other hand is used to handle link break. If a node detects there is a link break from data link layer, it will generate a RERR (Route Error) packet and send back to the source node using the part of the route traversed so far. The notified source node must delete the broken link from its route cache table. If the source node has another packet to send to the same destination, it must try another route or invoke route discovery process again if it does not have any other routes.

Basic Process:

1) **Route Discovery** is the mechanism by which a node S wishing to send a packet to a destination D obtains a source route to D. To perform a Route Discovery, the source node S broadcasts a ROUTE REQUEST packet that is flooded through the network in a controlled manner and is answered by a ROUTE REPLY packet from either the destination node or another node that knows a route to the destination. To reduce the cost of Route Discovery, each node maintains a cache of source routes it has learned or overheard, which it aggressively uses to limit the frequency and propagation of ROUTE REQUESTs.

2) **Route Maintenance** is the mechanism by which a packets sender S detects if the network topology has changed such that it can no longer use its route to the destination D because two nodes listed in the route have moved out of range of each other. When Route Maintenance indicates a source route is broken, S is notified with a ROUTE ERROR packet. The sender S can then attempt to use any other route to D already in its cache or can invoke Route Discovery again to find a new route.

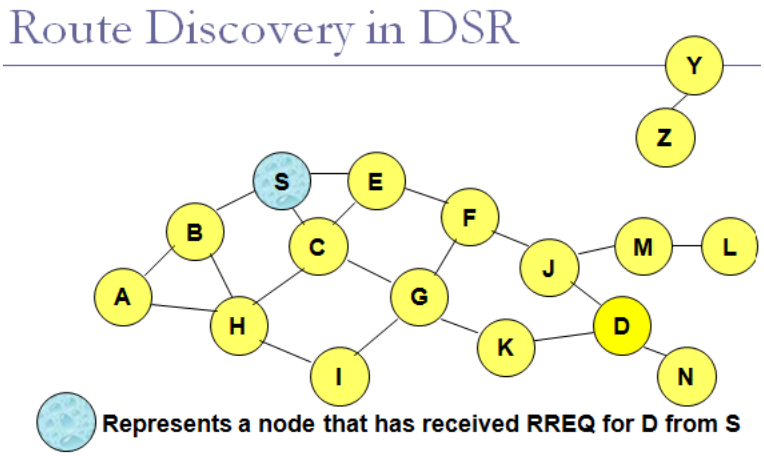

Figure 4.1: Phase-1 of route discovery in DSR

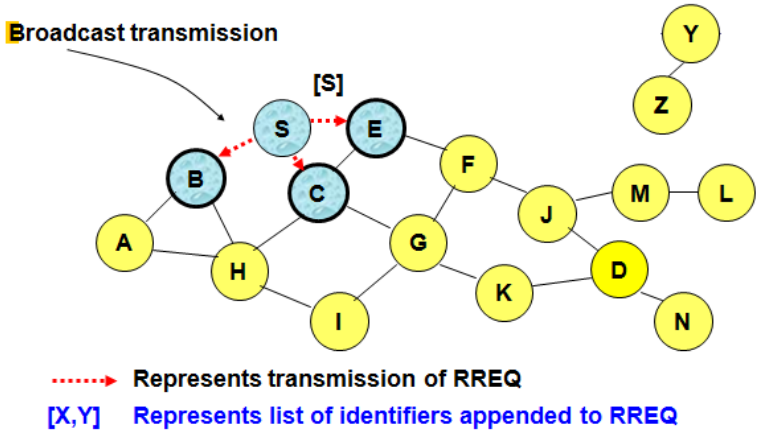

Figure 4.2: Phase-2 of route discovery in DSR

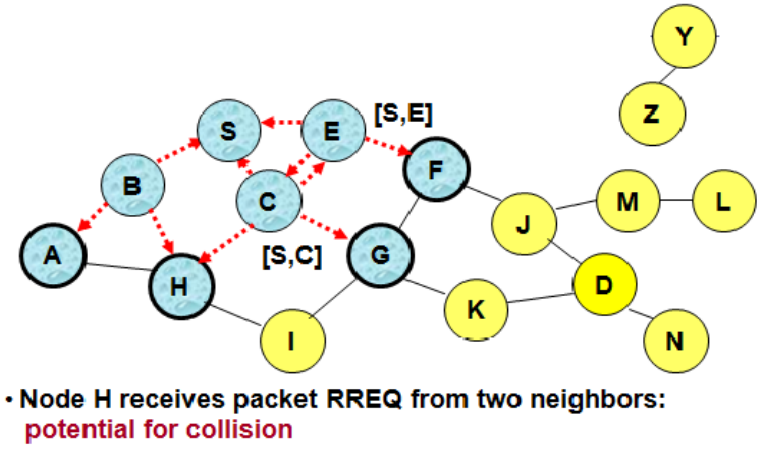

Figure 4.3: Phase-3 of route discovery in DSR

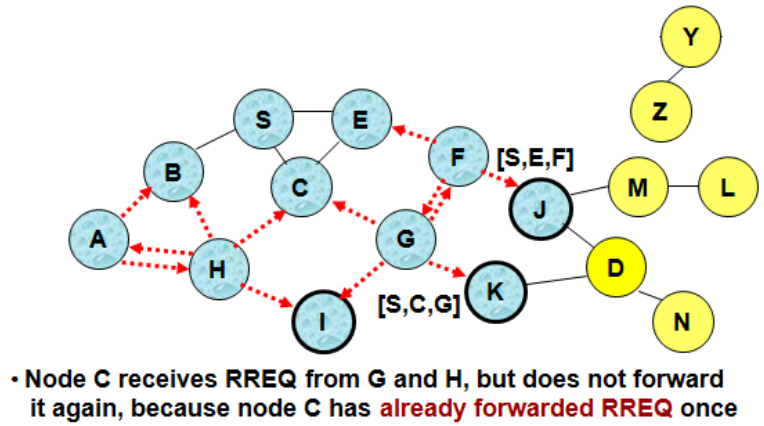

Figure 4.4: Phase-4 of route discovery in DSR

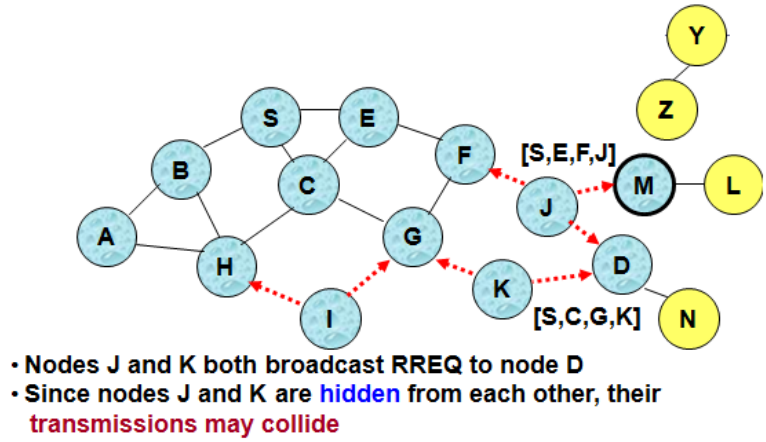

Figure 4.5: Phase-5 of route discovery in DSR

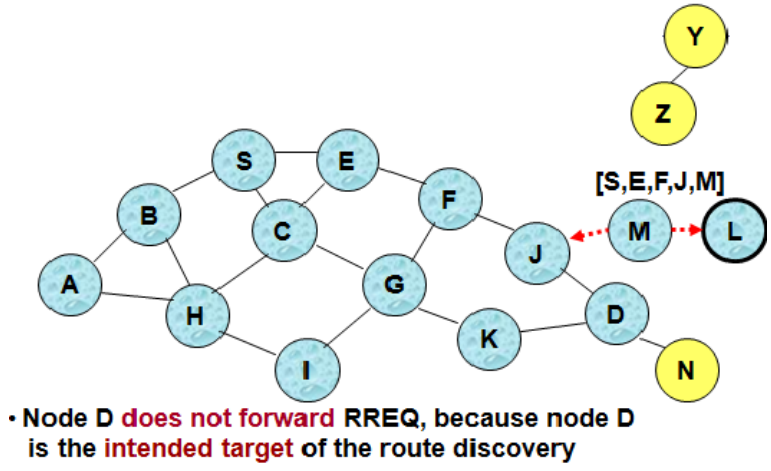

Figure 4.6: Phase-6 of route discovery in DSR

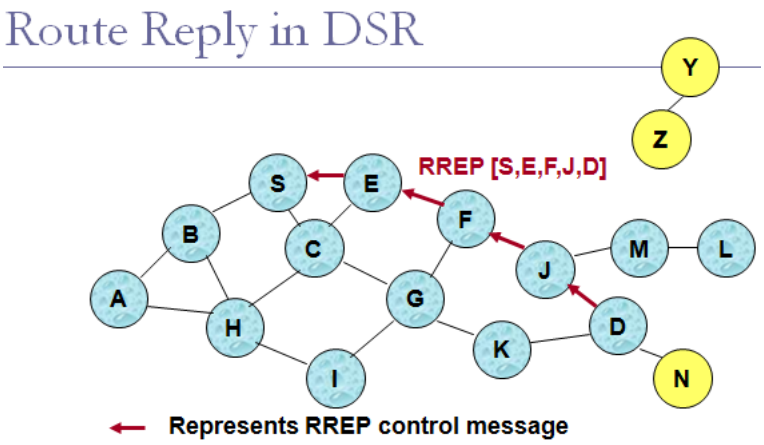

Figure 4.7: Route Reply in DSR

Chapter 5

Proposed Work

Implementation encompasses all the processes involved in getting new software or hardware operating properly in its environment, including installation, configuration, running, testing, and making necessary changes. As such, implementation is the action that must follow any preliminary thinking in order for something to actually happen.

In a survey paper, Survey of innovated techniques to detect selfish nodes in MANET in International Journal of Computer Networking, Wireless and Mobile Communications (IJCNWMC) TJPRC Pvt. Ltd [x], they descibe that if a node want to save its resources for its own purpose then it is a selfish node.They drops all pakets which comes to it for forwarding to other nodes.Monitoring for Data forwarding techniques used in misleading nodes but is is not suitable for selfish node detection. It is due to non-participation of of selfish node in route request process,so it will not use for data forwarding. Furthermore, many nodes may not need data forwarding.e.g. such condition are given below-

1) If a node located at the end of network and have no more nodes after that then in this condition it has no need to forward data packets.

2) When a new node entered in a already established network where all routing is already defined.If there is no link error, routing table will not update and new node can not get RREQ packet.And if new node want to use network for communication it has to get RREQ packet till that it can not forward packet.

In our technique, each observing node works in unbridled mode and might screen

both information and control bundles that are send around inside its receiving range. Each observing node will keep a record for each of its neighboring node. In the INETMANET [02] skeleton, there is as of now a particular table to store the data about the neighboring nods. We add additional fields to the table as the accompanying.

- **Last Action of Neighbouring Nodes :** It is the time when neighboring node provide or contribute service for the network most recently.
- **Last Request of Neighbouring Nodes:** It is the time when neighbouring node request for service from the network.
  this two field will always change due to unbridled mode monitoring.
- **Current Status of Neighbouring Nodes :** Status of neighboring node decided by the monitoring node according to above two parameters. Firstly status will be set to Zero means well behaved and later it can be changed to one means malicious or selfish.

Mechanism:

For selfish node detection we can consider type of action which is utilizing,contributing or none of that as describe in figure

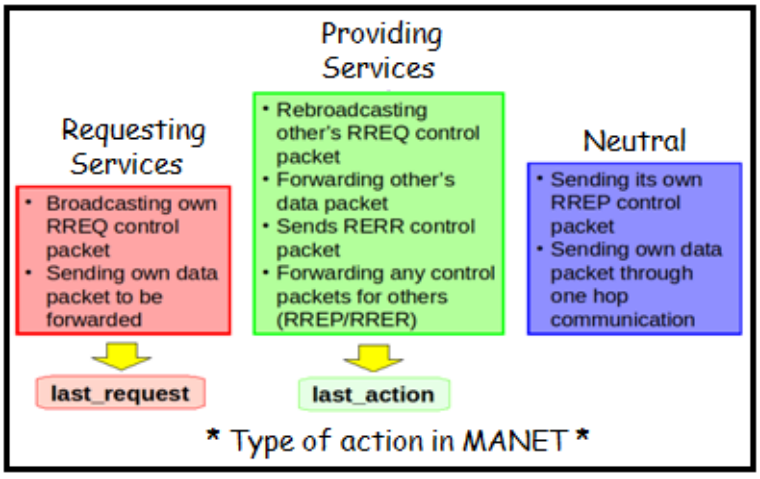

Figure 5.1: Type of action in MANET

At whatever point an observing node hears an request from its neighboring node to send an data packet, it will first check the time distinction between neighboring nodes last ask for and neighboring node last activity of the requesting node. On the off chance that it is still inside threshold as indicated in figure, the status for the node is set to behave. Threshold Time is known as activity hold off time.

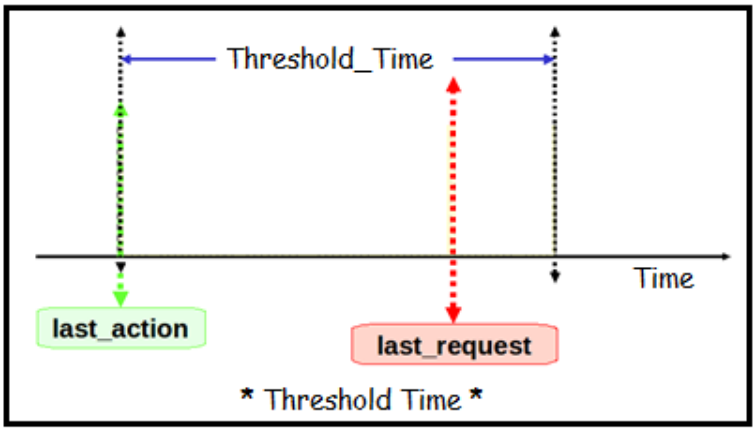

Figure 5.2: Threshold Time

In the event that the time distinction surpasses the threshold, the status for the node will be set to suspicious and further testing might be led as this suspicious node may be wrongly charged because of the uncommon situations as clarified previously. To perform testing, a fake RREQ packet will be telecasted into the MANET. To minimize activity flooding in the system, just the node that accepts the request packet from the suspicious node might lead this testing. Likewise, this fake RREQ packet ought to be just permitted to pass through one hop (TTL=1).

All checking nodes in the area that identify this potential mischief might sit tight for the suspicious node to rebroadcast the fake RREQ bundle inside a certain time-out. On the off chance that it reacts to the RREQ packet, the status of the node is situated to carry on and the time of its neighboring nodes last activity will be redesigned. In the event that it drop the packet and does not react, the checking nodes will name the suspicious node as selfish.

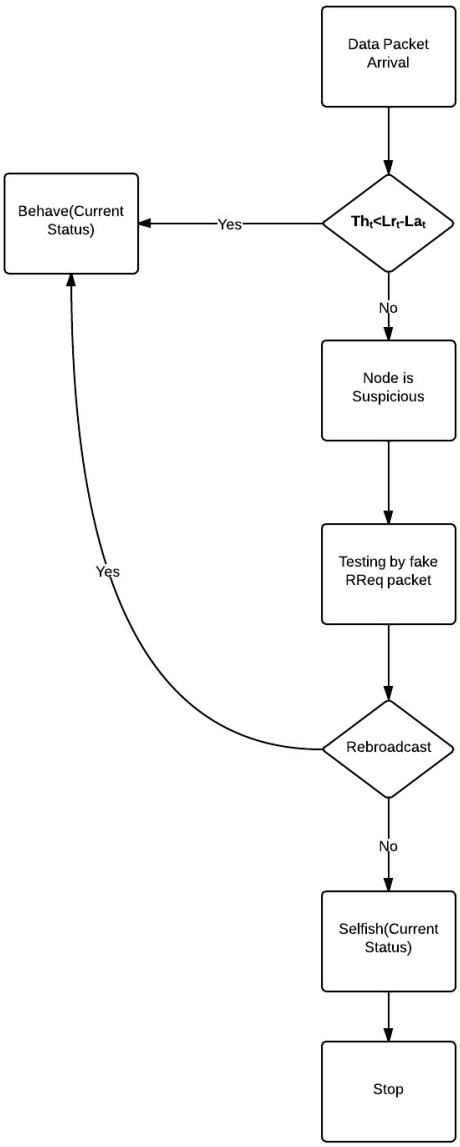

Figure 5.3: Flow Chart for Proposed Design

Chapter 6

Implementation Details

We used Network Simulation-2 (Version-2.35) tool with some nodes and selfish nodes of MANET to simulate our proposal. This network simulation-2 contain following some performance factor which makes its very useful.
1) Real-system not available, it is complex/costly or dangerous.
2) Quickly evaluate design alternatives.
3) Evaluate complex functions for which closed form formulas or numerical techniques not available.
4) NS version2 is a discrete-event driven and object-oriented network simulator.
5) A package of tools that simulates behavior of network

- Create Network Topologies
- Log events that happen under any load
- Analyze events to understand the network behvior.

6.1 Simulation Tools

NS-2 is a network simulator. It is event driven simulation tool. Is is used to study dynamic networks and its communication pattern.Is is basically combination of two languages: one is C++ and other is object oriented tool command language(OTcl).C++ is for background activity and OTcl for setting up simulation in which it assemble and configure objects and schedule discrete events.

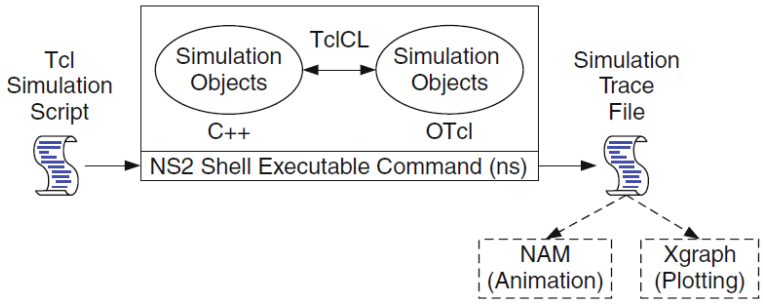

Figure 6.1: Basic Architecture of NS-2

6.2 Modeling of Network

At the firstt network is made with a clear situation utilizing startup wizard. Beginning topology is chosen by making the unfilled situation and network scale is picked by selecting the network scale. For our situation we have chosen campus as our network scale. Size of the network scale is specified by selecting the X compass and Y compass in given units. We have chosen 500 * 500 meters as our network size. Further innovations are specified which are utilized as a part of the reenactment. We have chosen Ad hoc Network show in the advances. After this manual setup different topologies could be created by dragging items from the palette of the task editorial manager workspace. After the outline of network, nodes are legitimately designed physically.

6.3 Simulation Setup

Table-I and II shows the parameters of the Ns2 simulation. We design a network with a field size of 500m x 500m and 20 nodes. The nodes will move inside the network space as per the random way point mobility model [20]. In random way point mobility model, every node will moves to an irregular area inside the specified network territory. Once the node touches base at the target area, it will stays in the position for a period (pause time) before moving to an next random area. In our design, the pause time is set to 0.3 second. The correspondence designs which will utilize will have constant bit rate (CBR) association with a data rate of 3 packets

for every second. 20 connection will make at random so that every node might opportunity to connect with each other node. We simulate our framework utilizing two configuration of selfish nodes in the network:

– For-No Selfish Node

Table-I, shows the parameters requires to perform our simulation with no selfish node

Simulator	NS-2(Version-2.35)
Simulation Time	100(s)
Number of Mobile Nodes	20
Number of Selfish Nodes	00
Topology	500*500(m)
Routing Protocol	DSR
Traffic	Constant Bit Rate(CBR)
Pause Time	03(m/s)
Max Speed	20(m/s)

Table I: Parameters for No Selfish Nodes

– For-Four Selfish Nodes

Table-II, shows the parameters requires to perform our simulation with four selfish node.

Simulator	NS-2(Version-2.35)
Simulation Time	100(s)
Number of Mobile Nodes	20
Number of Selfish Nodes	04
Topology	500*500(m)
Routing Protocol	DSR
Traffic	Constant Bit Rate(CBR)
Pause Time	03(m/s)
Max Speed	20(m/s)

Table II: Parameters for Four Selfish Nodes

For every setup, we will assesses the framework by changing the node's speed 0ms to 4ms and the window size of Threshold Time. We additionally need to test our framework in situations where the selfish nodes utilize distinctive rate of selfishness 0 to 100 percent. So as to assess the recognition ability of our

framework in a moderately little period, we just set the simulation time to 100 seconds.

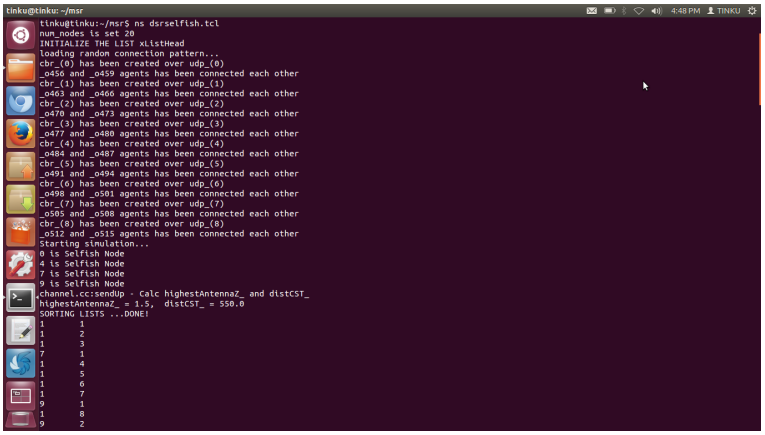

Figure 6.2: Execution of tcl script with malicious node

6.4 Simulation Performance

We choose packet delivery ratio and packet end-to-end delay as performance metrics for evaluating our simulation of selfish attack .

Packet Delivery Ratio: PDR is the ratio of no. of packet sent from the sender(transmitting node) and no. of packet received from receiver(receiving node).These packets are generated by CBR at application layer.

Packet end-to-end delay: It is the average time taken by any packet sent by sender inside the network to reach the receiver in may be in second or in milliseconds.It is some of all type of delays like transmission time,buffering time,induced delay etc.Real time communication should have minimum e2e delay it has very little tolerance for example voice call and video conferencing.

Chapter 7

Simulator Result

After performing proposed system using network simulation-2 with required tools and environment, we can run animator. The animator is a screen which performs all completed work.

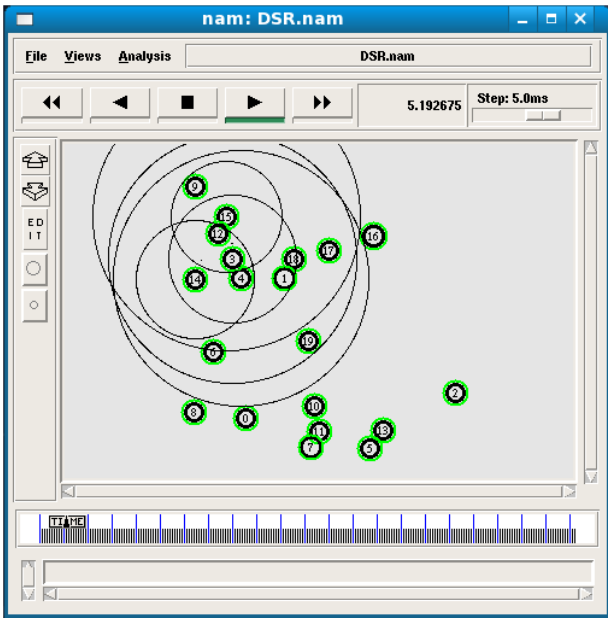

Figure 7.1: Execution of animator with 20 nodes

Where we simulate our system using two configurations of selfish nodes in the network:

Figure 7.2: Nodes transmitting packets in the network

∗ For- No Selfish Node

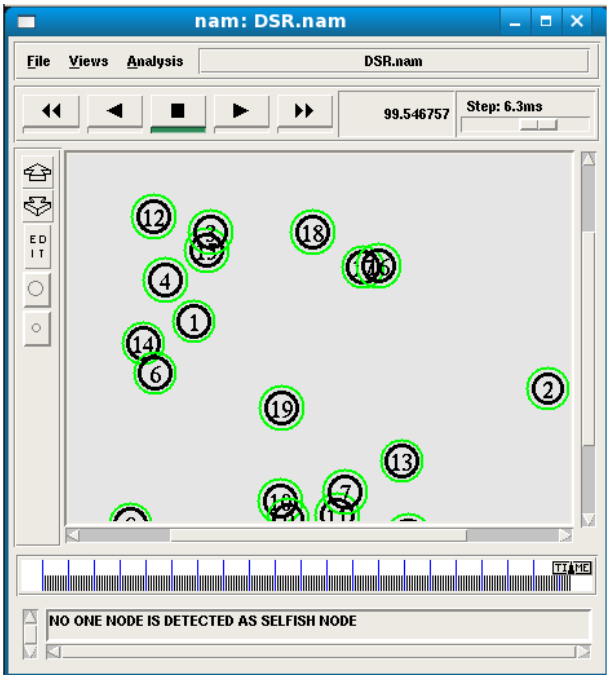

Figure 7.3: NS Animator: Normal DSR (No selfish node)

∗ For- Four Selfish Nodes:

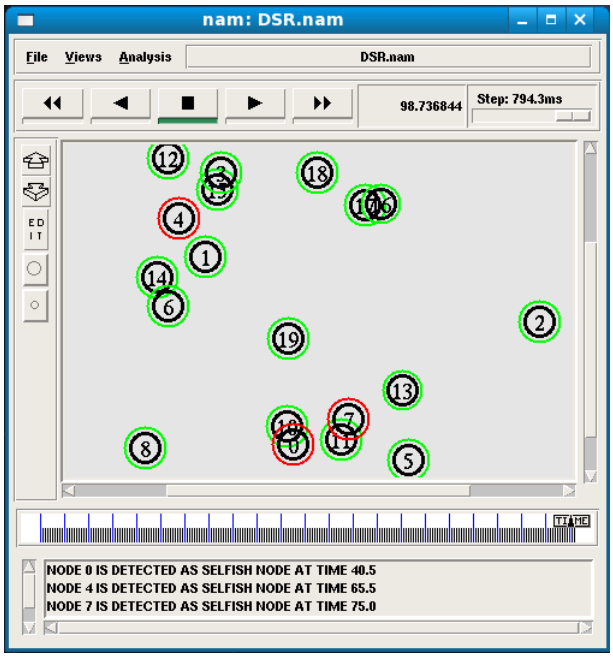

Figure 7.4: NS Animator: Selfish DSR (Four Selfish nodes)

The results were collected as comparison of Packet Delivery Ratio (PDR) for Selfish DSR (four nodes acts as selfish) and Normal DSR (No selfish node). Graph for Normal DSR shows that there is no any loss of data packets (100 percent PDR) i.e. No one node act as a selfish node. While graph for Selfish DSR shows that there is loss of some packets, all packets are not delivered. ie. Some nodes act as selfish nodes which are find out by using our neighboring node based system for MANET to detect selfish node.

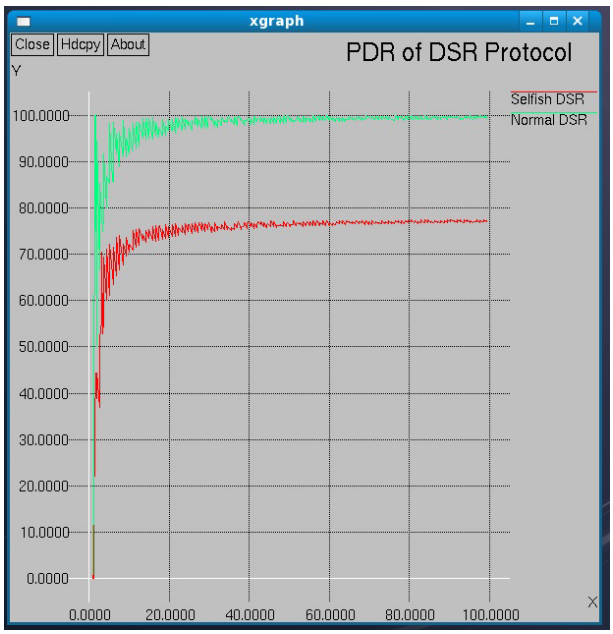

Figure 7.5: Packet delivery ratio for normal and malicious nodes

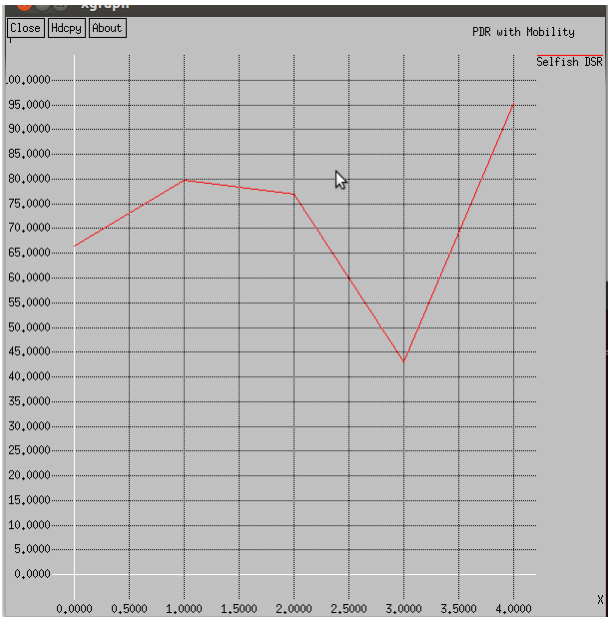

Figure 7.6: Packet delivery ratio for different mobilities for Selfish nodes

Chapter 8

Conclusion and Future Work

In this report, we propose and simulate a new mechanism for detection of selfish node for MANET. Selfish nodes generally use network resources when required but does not provide its own resources for other nodes e.g. data and control packet forwarding to next node.It accept only those packet who has destined to it and drop all other packet destined for other nodes.By this it reserves its resource like energy which it can use in future for its own purpose.Because all nodes have enegy limitation as they are mobile and there is no regular energy supply.For detection of selfish nodes in MANET our system performs significantly well.

For Future work we can evolve such technique which after detection of selfish node can block such nodes so performance of network can be enhanced.

References

[01] Parker J, Undercoffer J, Pinkston J, Joshi A. (2004). On intrusion Detection and Response for Mobil Ad Hoc Networks, in Proceeding IEEE International Conference on Performance Computer and Communications, Workshop on Information Assurance, pp 747-52.

[02] Khairul Azmi Abu Bakar and James Irvine Contribution Time-based Selfish Nodes Detection Scheme ISBN: 978-1-902560-24-3 2010 PGNet

[03] Dipali Koshti, Supriya Kamoji Comparative study of Techniques used for Detection of Selfish Nodes in Mobile Ad hoc Networks, (IJSCE) ISSN: 2231-2307, Volume-1, Issue-4, September 2011

[04] S. Marti, T. Giuli, K. Lai, and M. Bakar, Mitigating routing misbehaviour in mobile ad hoc networks, in Proc. 6th Annual Int. Conf. on Mobile Computing and Networking (MobiCom00), August 2000, pp. 255265.

[05] Q. He, D. Wu, and P. Khosla, Sori: A secure and objective reputation-based incentive scheme for ad-hoc networks, in WCNC 2004.

[06] S. Buchegger and J. L. Boudec, Performance analysis of the confidant protocol: (cooperative of nodes - fairness in dynamic ad hoc networks), in Proc. IEEE/ACM Workshop on (MobiHoc02), June 2002, pp. 226336.

[07] P. Michiardi and R. Molva, Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks, in (CMS02), September 2002.

[08] S.Bansal and M.Baker, Observation-based cooperation enforcement in ad hoc networks Stanford University, Tech. Rep., 2003.

[09] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, An acknowledgment-based approach for the detection of routing misbehavior

in manets, in IEEE Transactions on Mobile Computing, 2006, pp. 536550.

[10] K. Paul and D. Westhoff, Context aware detection of selfish nodes in dsr based ad-hoc networks, in proceedings of IEEE Vehicular Technology Conference 02, 2002.

[11] D. Djenouri, O. Mahmoudi, M. Bouamama, D. Llewellyn-Jones, and M. Merabti, On securing manet routing protocol against control packet dropping, in The 4th IEEE (ICPS2007), Istanbul, July 2007, pp. 100108.

[12] L. Huang, L. Li, L. Liu, H. Zhang, and L. Tang, Stimulating cooperation in route discovery of ad hoc networks, in Proceedings of the 3rd ACM Workshop on (Q2SWinet07), October 2007.

[13] Farzaneh Pakzad and Marjan Kuchaki Rafsanjani Intrusion Detection Techniques for Detecting Misbehaving Nodes, in Computer and Information Science Vol. 4,-1; January 2011.

[14] Kachirski O, Guha R. (2003). Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks, in Proceeding IEEE, (HICSS03), pp 57.1.

[15] Hasswa A, Zulkernine M, Hassanein H. (2005). Routeguard: an intrusion detection and response system for mobile ad hoc networks, in Proceeding IEEE (WiMob2005).

[16] Caballero E J. (2006). Vulnerabilities of intrusion detection systems in mobile ad hoc networks- the routing system, Seminar on Network security, Helsinki University of Technol.

[17] Nasser N, Chen Y. (2007). Enhanced intrusion detection system for discovering malicious nodes in mobile ad hoc network, in Proceeding IEEE (ICC07), pp 1154-9.

[18] Buchegger S, Le Boudec J. (2002). Performance analysis of the CONFIDANT protocol (Cooperation of nodes fairness in dynamic ad-hoc network), in Proceeding 3rd ACM (MobiHoc02), pp 226336.

[19] Michiardi P, Molva R. (2002). Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks, in International Conference on (CMS02).

[20] Bansal S, Baker M. (2003). Observation-based cooperation enforcement in ad hoc networks, in Technical Paper on Network and Internet Architecture (cs.NI / 0307012).

[21] Huang Y, Lee W. (2003). A Cooperative Intrusion Detection System for Ad Hoc Networks, in Proceeding of the ACM Workshop on SASN'03, pp 135-47.

[22] Abhishek Gupta and Amit Saxena Detection and Prevention of Selfish Node in MANET using Innovative Brain Mapping Function: Theoretical Model in IJCA, Vol. 57/12, Nov-12.

[23] Hongxun Liu, Jos G. Delgado-Frias, and Sirisha Medidi USING A CACHE SCHEME TO DETECT SELFISH NODES IN MOBILE AD HOC NETWORKS in Proceeding of the sixth IASTED July 2-4, 2007

[24] Sunilkumar S. Manvia, Lokesh B. Bhajantrib, and Vittalkumar K. Vaggac Routing Misbehaviour Detection in MANETs Using 2ACK, in 4/2010 JTIT.

[25] Hongxun Liu, Jos G. Delgado-Frias, and Sirisha Medidi USING A TWO-TIMER SCHEME TO DETECT SELFISH NODES IN MOBILE AD-HOC NETWORKS in Proceeding of the sixth IASTED July 2-4, 2007.