A
Dissertation
On

ROUTING AND CONGESTION CONTROL IN OPPORTUNISTIC NETWORKS

Submitted in Partial Fulfillment of the Requirement
For the Award of the Degree of

MASTER OF TECHNOLOGY
in
COMPUTER SCIENCE AND ENGINEERING

by

S.P.AJITH KUMAR
University Roll No.:2K12/CSE/26

Under the Esteemed Guidance of

SH. MANOJ KUMAR
ASSOCIATE PROFESSOR
DEPARTMENT OF COMPUTER ENGINEERING
DELHI TECHNOLOGICAL UNIVERSITY

2012-2015

DEPARTMENT OF COMPUTER ENGINEERING
DELHI TECHNOLOGICAL UNIVERSITY
Delhi-110042, INDIA

ABSTRACT

Opportunistic networks are one of the most interesting evolutions of MANETs. Mobile nodes are enabled to communicate with each other in opportunistic networks even if there is no route to connect them. Also, nodes are not having knowledge about the network topology, which (instead) is necessary in MANET routing protocols. In this network routes are building dynamically, whenever messages are en route between the sender and the destination(s), and any potential node can be opportunistically used as the next hop, provided it is bringing the message nearer to the destination. These necessities make opportunistic networks a challenging and demanding research field.

In this project, a new routing protocol named as Reduced Flooding Epidemic Protocol (RFEP) for infrastructure-less is proposed and is an existing Epidemic routing protocol improvement model. Its objective is to reduce the amount of flooding done in the Epidemic protocol. Therefore it reduces the resource consumption and network bandwidth and as well as power of nodes that helps in maximizing the network lifetime.

Also a method for congestion control is proposed here for opportunistic networks. Congestion is an important problem in this network because some nodes having better connection comparing with other nodes and so the load is unfairly distributed towards them. Therefore, a threshold based packet forwarding scheme is proposed in this work to overcome this issue. Number of nodes is selected as the subsequent hop to forward the packets whose utility metric computed based on its social metrics, delay and packet dropping probability which is higher than the current host by the predefined threshold. The outcome shows that it generated very good results in terms of delivery probability, overhead ratio and reduced number of packets dropped.

ACKNOWLEDGEMENT

First and foremost I would like to thank the **Lord Almighty** for showering his blessing in all endeavours.

With immense pleasure I take this opportunity to express my indebtedness gratitude to our beloved Vice chancellor **Prof. Pradeep Kumar** who is enriching keen interest in academic pursuits.

I convey my sincere thanks to our Honorable HOD **Prof. O P Verma,** Department of CSE for his kind encouragement and motivation to complete this Project successfully.

I profoundly thank our respected Associate Professor **Mr. Manoj Kumar** Department of CSE, for his full fledged support and guidance throughout the Project.

I wish to thank **Mr. Vinod Kumar,** Associate Professor who helped me to learn the basic concepts of Computer Networks and **Mr.R. K. Yadav,** Assistant Professor helped me to learn other related topics which initiated me to do this project.

I would also like to express my sincere thanks to Professor Dr. (Mrs.) **Daya Gupta**, Associate Professor **Dr. Kapil Sharma**, Assistant Professor **Ms. Divyashikha Sethia**, and Programmer **Mr. Manoj Seti** helped and inspired me at several occasions, their supports are highly appreciated.

Last but not least I render my heartiest complements to all my **Staff Members, Librarian, Parents and Friends** for giving their valuable suggestions, encouragement and support for completing my project successfully.

S P Ajith Kumar
University Roll no.: 2K12/CSE/26
M.Tech (Computer Science & Engineering)
Department of Computer Engineering

Department of Computer Engineering
DELHI TECHNOLOGICAL UNIVERSITY
Shahabad Daulatpur, Main Bawana Road,
Delhi-110042.

CERTIFICATE

This is to Certify that the dissertation titled **“Routing and Congestion Control in Opportunistic Networks ”** is a bonafide record of work done by **MR. S P AJITH KUMAR, ROLL NO.: 2K12/CSE/26 at Delhi Technological University** for partial fulfillment of the requirement for the degree of Master of Technology in Computer Science & Engineering. This project was carried out under my supervision and has not been submitted elsewhere, either in part or full, for the award of any other degree or diploma to the best of my knowledge and belief.

Date:____________

Sh. Manoj Kumar
Associate Professor & Project Guide
Department Of Computer Engineering
Delhi Technological University

Table of Contents

Chapter 1

Introduction

Chapter 2

Literature Survey

Chapter 3

Existing Methodology

Chapter 4

Proposed Methodology

Chapter 5

Simulation Result and Analysis

Chapter 6

List of Figures

List of Abbreviations

RFEP	Reduced Flooding Epidemic Protocol
MANETS	Mobile ad-hoc networks
Wi-Fi	Wireless Fidelity
DTNs	Delay Tolerant Networks
ONE	Opportunistic Network Environment
Oppnet	Opportunistic Network
LAN	Local Area Network
PC	Personal Computer
MAPs	Mobile Access Points
PDA	Personal Digital Assistant
GPS	Global Positioning System
RFID	Radio Frequency Identification
IP	Internet Protocol
SWIM	Shared Wireless Info station Model
ICT	Information and Communication Technologies
QoS	Quality of Service
FMLB	Fibonacci Multipath Load Balancing Protocol
PRoPHET	Probabilistic Routing Protocol using History of Encounters and Transitivity
MaxProp	Maximum Probability
Ack	Acknowledgement
TTL	Time to Live

CHAPTER 1

INTRODUCTION

1.1 Opportunistic Network and its challenges

Opportunistic network has been emerging as one of the foremost recent and fascinating evolutions of the MANETs paradigm. They have all the challenges and problems faced by MANETs and they have also some new challenges. Through a common inter-network the nodes which want to communicate are connected with each other. This requirement of connected path is seldom possible in the persistent network scenarios. Mobile devices carried by users are somewhat connected to the network, as users may turn them off to save energy. Due to their high mobility, sometimes the nodes may move out of the radio range of other nodes. The, traditional MANET routing protocols and internet routing protocols based on the concept of establishing a complete path between the starting place and destination before the delivery of the message isn't potential just in case of Opportunistic networks.

Opportunistic networks have both fixed nodes as well as mobile nodes like pedestrian users and vehicles. Generally the nodes are mobile in nature. The nodes can communicate with each other via all types of communication media like Bluetooth, Wi-Fi and other communication-based technologies. Primarily Oppnet might begin operating with single node known as the Seed Oppnet. Then it can grow into a prolonged Oppnet by employing more than a few foreign helper nodes which contribute the messages within the routing and forwarding. This kind of Oppnet is helpful in the events of emergency attentiveness and response actions. Additional types of Opportunistic networks include transportation networks, battlefield networks, autonomic networks, pocket-switched networks, Socio-Aware Community Networks etc.

In Opportunistic networks routing of messages is based on the contact chance between the nodes that arises because of their mobility, technique called Store-Carry-and-Forward and the local forwarding between the nodes. For sending the message to the end node, the protocol moves the message to the intermediate nearest nodes. Due to the light nature of Oppnets, it is possible that the intermediate nodes do not come across other nodes regularly or constantly. If there might not be some proper intermediate node which can be selected as next hop to take the message near to the target or to the target itself, then the message will be directly delivered to the target at any time a direct contact arises with it. When there is no forwarding chances towards the target, then the intermediate nodes must keep the packets in their buffer for a long period of time. The above mentioned Store-Carry-and-Forward method is an extremely good technique to raise the probability to succeed message delivery to the end node in Opportunistic networks. The messages can also bear longer delays as they're buffered within the network. They're anticipating a path to be out there towards the destination. Due to this reason opportunist networks comes under Delay Tolerant Networks (DTNs) sub class. The nodes should have adequate buffer area to store all the messages for less time period therefore on avoid the dropping of packets till subsequent contact happens.

Due to the obscure quality and uneven performance of the nodes, routing and forwarding may be a hard task in opportunist networks. A lot of analysis done in opportunistic networks routing and forwarding region. In Oppnets finding routes towards the desired destination is the most important task. Thus, designing a new routing protocol having forever demand in the Oppnet. The protocol must be energy efficient and consumes less power of nodes in forwarding the message. The aim of the protocol is to decrease the communication delay and increase the successful data delivery rate to the target. The routing protocols used in Opportunistic networks have two categories – infrastructure based protocols and infrastructure-less protocols. In this dissertation, the major focus will be on the infrastructure-less protocols.

The recital of these protocols are based on some additional metrics such as number of messages delivered, delivery probability, average hop count, average delay, average buffer latency.

In opportunistic networks congestion control is an embryonic study topic since the storage space in these devices is inadequate. In this network the load is excessively distributed towards the nodes with better link .This leads to congestion in the network. A number of solitary and manifold copy of packet forwarding schemes that employ congestion control had proposed previously. Single copy based message forwarding schemes have lesser delivery probability. Multiple copy packets forwarding schemes over load the network. Therefore both the schemes are not resource competent. Thus a novel congestion control algorithm is projected that forwards one copy of a message to numerous nodes at a time based on a pre-defined threshold. The forwarding verdict is based on the utility metric of the node. It is computed using common metric, existing storage, delay added to the packet delivery time, probability to drop the packet and the network metrics. If the Packet forwarding scheme is based on utility metric then it leads to a reasonable distribution of the load in the network. By means of a predefined threshold a replica of the message is sent to the entire nodes whose utility metric is larger than the utility metric of the present node. A simulator is used to achieve the simulations. The projected algorithm produces very fine outcome in respect of delivery probability and overhead ratio. The number of packets dropped is also reduced in this algorithm.

1.2 Characteristics of Opportunistic Network

- It is derived from Delay- Tolerant Network (DTN)
- It is a light network
- It has fewer intermittent Contacts
- It has no end-to-end link
- It uses Store, Carry and Forward Mechanism in Routing
- It uses infrastructure less protocols

1.3 Advantages of Opportunistic Network

- Lofty capacity
- Low price
- Restricted & Decentralized operations

1.4 Block Diagram

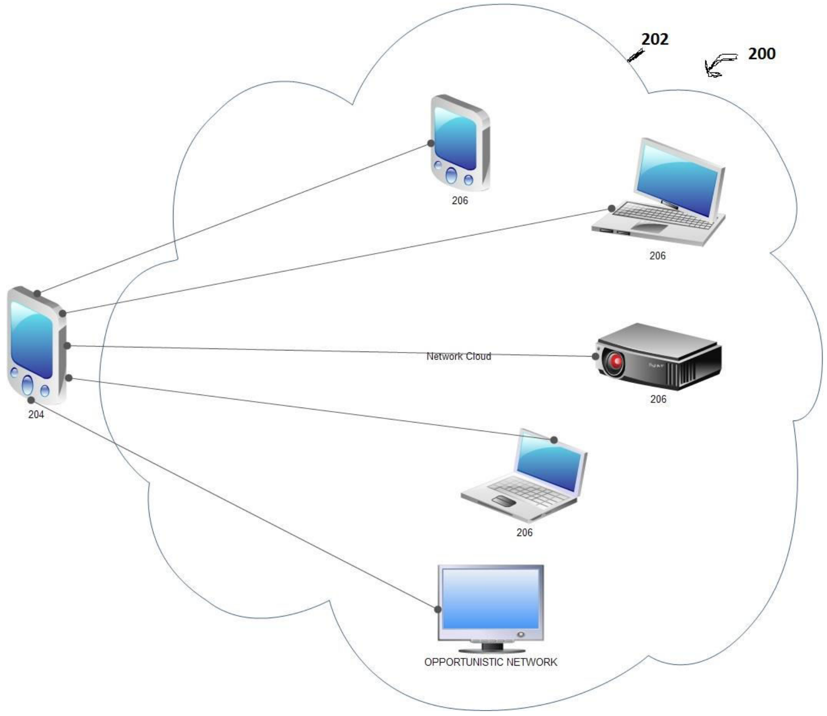


Figure 1.1 Opportunistic-Network-Block Diagram

1.5 Basics of Oppnets

1.5.1 Seed Oppnet & Its Growth

Every Oppnet starts from a seed node. In the starting it consists of one node. The seed breeds into a larger network by extending invitations to link the oppnet to close devices, node clusters or close to systems that is capable to make contact. Any fresh node that turns into a full-fledged oppnet member, precisely a helper, is allowable to call as exterior nodes. By calling "free" joint nodes, the Oppnets are extremely competitive. The issues which can be attended are applicable motivations or enforcements as a result that nodes are keen or required to link, and potently minimum trait of invited collaborators can't be fully believed. Helpers work together on realizing the opportunistic networks objective. They can be deployed to implement the entire tasks although, in common, they are not planned to go with elements of an oppnet that invites to help.

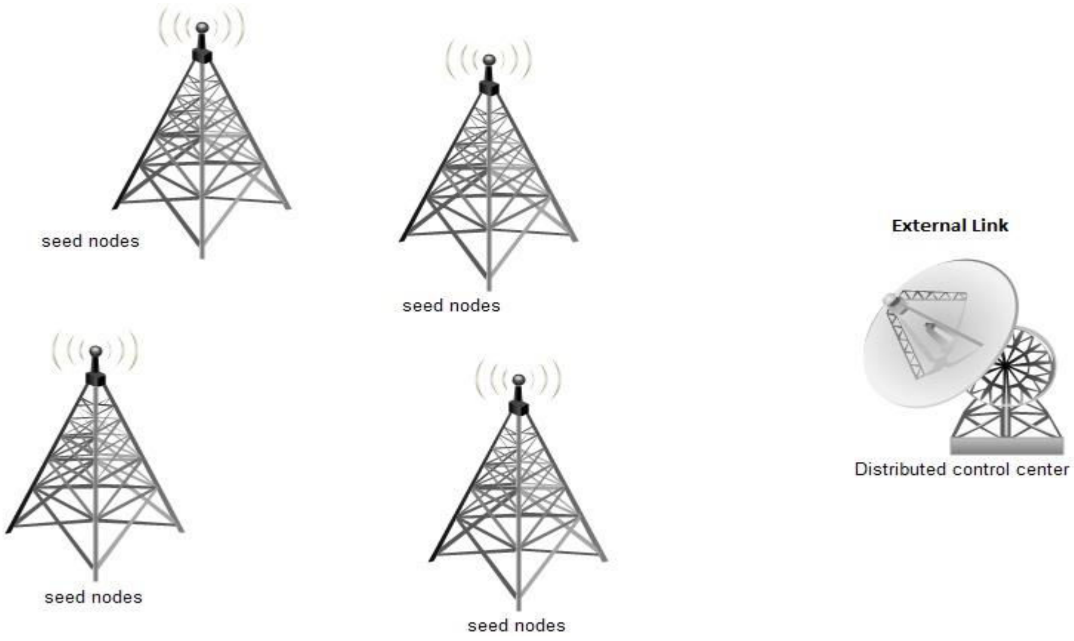


Figure 1.2 OppNet seed

Expanded OppNet

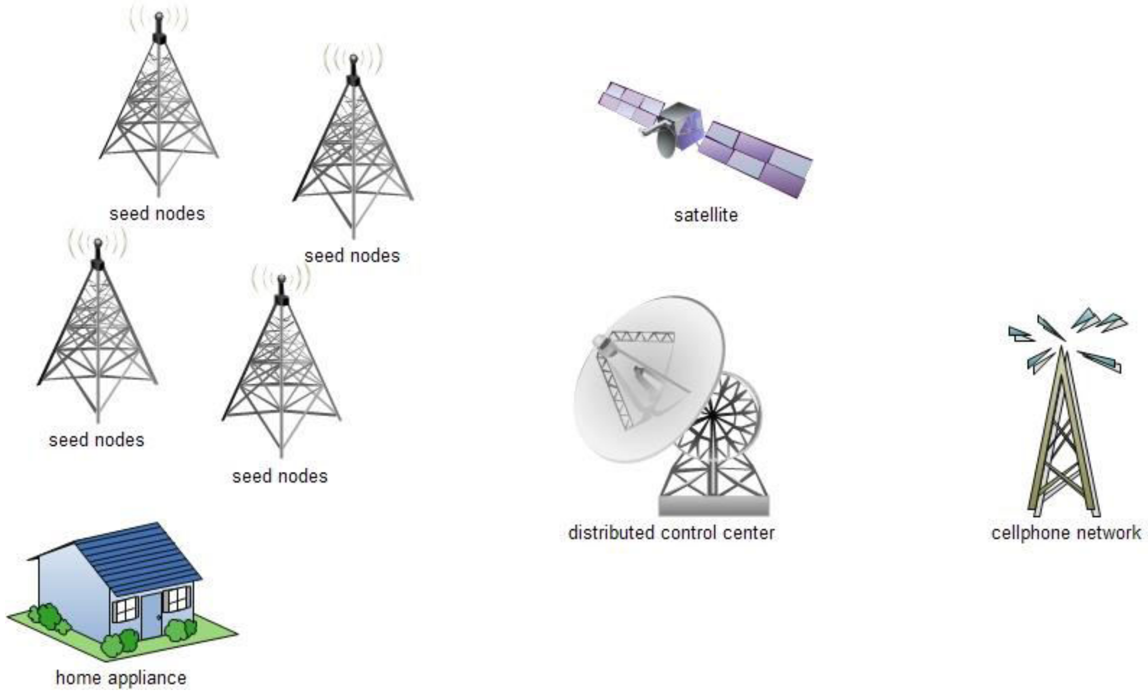


Figure 1.3 Expanded OppNet

1.5.2. Helpers in Oppnet

a) Potential Oppnets Helpers: The helper set in Oppnet includes wireless and wired entities, free-standing and embedded nodes. Constant nodes without sensing capabilities, like networked mainframes or wireless-equipped processors can considerably provide help or having communication capabilities in an Oppnet. The networked processor or embedded processor contains a spread of helpful sensing, processing or communication capabilities. As an example, information regarding user's attendance or nonentity, her job behaviors and internet access patterns available in her desktop and her PDA, information regarding user's place – by his mobile phone; and data regarding food consumed by user's family – by a processor embedded in device and RFID-equipped food parcels and containers. As an example, a portable computer becomes "inevitable" once the seed identifies a division of internet Protocol addresses placed in its nation region and contacts them.

In larger areas, it is not subtle to undertake and do, with Internet Protocol addresses hierarchically planned by internet site.

b) Helper Functionalities: It is common that, in general, functioning inside the "disaster mode" not needed any new practicality from the helpers. As an example, just in case, task of fireplace observation, the climate sensor-net that turn into a helper is entirely told to stop aggregation of precipitation data to build use of the unrestricted resources to strengthen the sampling rates for temperature and speed of wind path. It's possible that more powerful helpers could also be reprogrammed on the fly. In addition, oppnet nodes might even be built with sensing, surplus general communication, calculation, cupboard space and added capabilities are helpful in unpredicted emergencies. Further devices having large sensing capabilities and multisensory devices have come cheaper and cheaper. This shows latest forms of sensors are developed at every instance.

1.6. Applications of Oppnets

Emergency Applications: The significant applications for Oppnets altogether form of pressing things area unit cyclone disaster revival and country protection emergencies. They need the potential to considerably improve effectuality of relief, revival operation and efficiency. For prediction of disasters (like firestorms or hurricanes, its pathway is predicted with a few precision), seed oppnets are set into action and their build-up happened before the disaster, while it's still galore easier to get, add to any nodes and clusters into the oppnet. The initial helpers cited as by the seed can be the sensor-nets organized for structural harm observation and investigation, similar to those embedded in bridges, roads and buildings.

CHAPTER 2

LITERATURE SURVEY

2.1 Classifications of Routing Techniques in Oppnets.

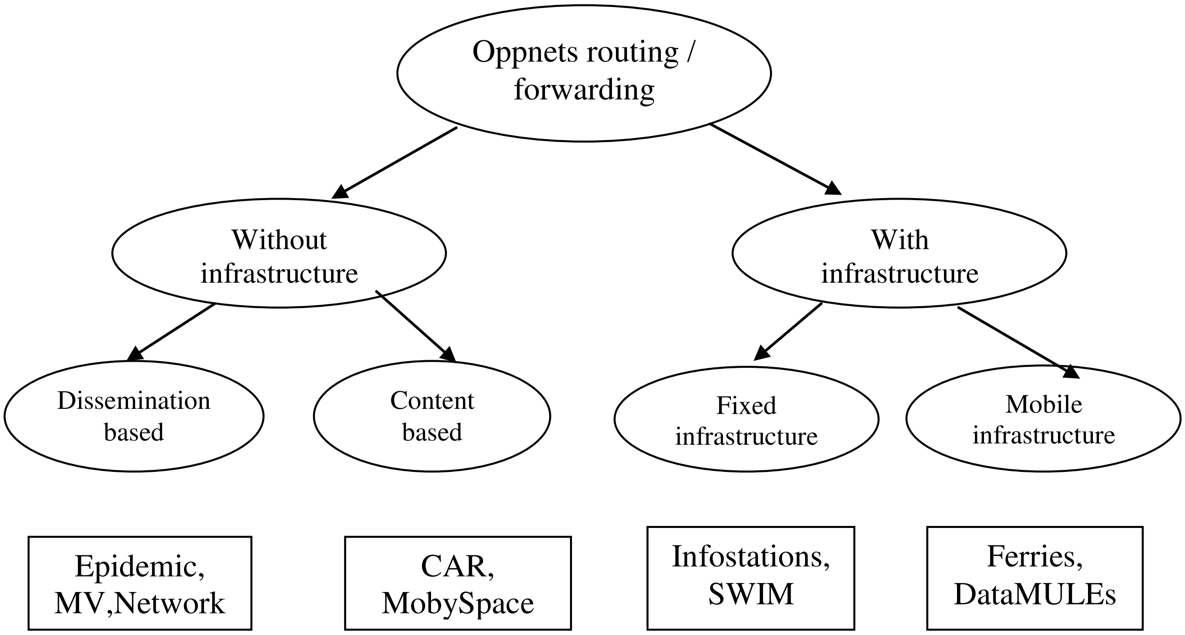


Figure 2.1 Classifications of Routing Techniques in Oppnets.

In the entire case studies we understood that routing is the initial challenge. The designing of better routing ways for oppnets are often a considerable job due to the deep knowledge of dynamic topology used in the network. Routing performance improves once further information regarding which computed topology is used in the network. But, this type of knowledge isn't simply traceable, and a transaction should be reach between information necessity and performance. The fig. 2.1 indicates an achievable terminology of forwarding/ routing algorithms in Oppnets. The samples of all categories unit area listed in foot of figure.

The Oppnet routing and forwarding algorithms in Ad-hoc networks are divided into with-infrastructure and without-infrastructure. In with-infrastructure the routing devices are static and without infrastructure the routing and forwarding devices are dynamic. The without-infrastructure Oppnets are further divided into dissemination based and context based. The dissemination based scheme is used to control flooding of messages in the network, the context based approach will operate to select best next hop in the network to forward the message packet. In both mobile infrastructure and fixed infrastructure network some more powerful node having high storage capacity and high energy. Further they can collect more messages from many nodes which are passed in the route for a long time. The fixed infrastructure network having a fixed geographical area and infrastructure-less network having dynamic random path routing.

2.2 Realistic Case Studies

A special consideration is devoted to practical case studies by opportunistic networks research team. Mobility models are one amongst the necessary elements of practical case studies. Compared to Simulations supported common arbitrary mobility models, simulations supported actual mobility outlines are a lot reliable for testing. Researches implement large number factual application eventualities upon expedient system in addition to practical mobility models. Logically it's not sensible or achievable to offer a new structured system supporting inheritance routing approaches, since these application eventualities are fundamentally opportunistic. The case of wildlife following applications (ZebraNet) designed for observing undomesticated species in unmanned eventualities is one of the examples. The aim of giving Internet connection to developing regions and country side areas where standard and conventional networks can't survive is one more example. Organizing customary networks to wrap these regions isn't profitable, whereas opportunistic networks are an affordable way-out.

2.2.1 Wildlife monitoring: ZebraNet and SWIM

ZebraNet is a knowledge based project at the Princeton campus and its operation is the huge savanna region of the central Kenya beneath the management of Mpala analysis Centre. Zebras wearing unique collars are the animals to be followed. The researchers often move around within the savanna and gathers information from the encountered zebras by using the base station's movable vehicle. For information gathering in ZebraNet two completely different protocols are proposed. The primary protocol is an easy flooding protocol. In this protocol each collar must send the entire information to every neighbor who comes across till it finally reaches the bottom station. The second protocol is known as ancient history based protocol. In this protocol, it is proposed that to relay its information each node chooses simply one amongst its neighbors.

The node having the maximum chance to come across the origin station is to be chosen. A hierarchy level is assigned to each node. It will increment on each instance, if it encounters an origin station and it will decrement if not encounters the origin station for a few instance. The node with the utmost hierarchy rank is designated as a neighbor while transferring information to a relay node. The forwarding protocol is better than direct protocol, in which every collar should straight forwardly communicate with the origin station to transfer the information. This is exposed by the simulation outcomes. In terms of energy utilization and bandwidth, the history based protocol is better than flooding protocol. The ZebraNet system has been put into practice at the Mpala analysis centre following the preliminary study and is presently underneath examination. To check opportunistic forwarding methods the initial outcomes from the actual testing are available readily and been utilized to describe the mobility model used.

Whales are the untamed species that are to be observed in the shared Wireless information Model (SWIM). Irregular information monitoring is achieved from whales having individual tags. Then the information is duplicated and spread at each pair-wise contact among whales. At last the information reaches the particular SWIM stations that can be fixed or mobile. For final processing and utilization, the data is at last forwarded on coastline from SWIM stations. To reveal the effectiveness of SWIM system on actual whales no experimental outcome actually exists. The simulation parameters have been set according to studies and remarks conducted by biologists on whales real behavior. Hence the simulation results are reasonably practical. By raising together the number of SWIM station, number of whales concerned and enhancements are achievable. At last compare to fixed SWIM stations, mobile SWIM stations have superior performance.

2.2.2 Opportunistic networks for developing areas

Irregular internet connectivity can be offered by opportunistic network to country side and growing areas. DakNet project is one of the examples. This project is designed attempt extremely inexpensive infrastructure to give connectivity to villages within India, wherever, it is not profitable to install customary internet access. Kiosks are ready with limited wireless communication and digital storage. These kiosks are built in villages. Mobile Access Points [MAPs] fixed on bicycles, motorcycles and busses bypass the village kiosks. They swap information with them wirelessly. MAPs can upload any kind of information or request stored t the kiosks. Then MAPs can download them from the internet while passing an access point from the near town. Correspondingly MAPs might transfer requested information from the internet and carry it to villages. DakNet has the efficiency to distribute the information, messaging through internet or intranet, voting, census, etc.

2.3 Multiple routing for congestion control and load balancing

Load balancing refers to the method of distributing traffic load equally within the network so as to reduce congestion and to optimize the usage of network resources. In Oppnets, balancing the load would be equally distribute the load according to the existing load of node in the network and avoid near to completion of power of overloaded nodes because of more power consumption in routing/ forwarding packets.

Peter P. Pham & Sylvie Perreau (2002) [10] projected a routing protocol that will increase the network throughput. This scheme projected with a load balancing policy and multi path routing protocol. The analysis unconcealed that load balancing with multipath routing policy gives more performance in respect of congestion and connection throughput comparing with reactive single path routing protocol.

An approach supported an infrastructure-less routing in MANETs strengthen the quality of service has been projected by Gabriel Ioan Ivascu et al (2009) [13]. The developed Infrastructure-less routing path discovery mechanism strength dynamically and distributes the traffic within the network, in step with the present network traffic levels and due to this the nodes process loads. The above said approach improves the network packet delivery ratio and throughput.

Bhavana Sharma, Shaila Chugh, Vishmay Jain (2013) [14] explored that Investigation of Load balancing for MANET in Adaptive Multipath Routing have variety of traffic groups to work out the simplest routing path. This approach calculates the metrics supported to link the loaded nodes. Here communication traffic is considered as high priority traffic and its routing is transmitting by the gently loaded links, unit selected as an alternate to links holding heavier loads.

Yahya M. Tashtoush et al (2012) [12] explored the Fibonacci Multipath Load Balancing Protocol (FMLB) for MANETs. The FMLB protocol distributes transmitted packets over multiple ways in which through mobile nodes, using the Fibonacci sequence. Such distribution can increase the delivery percentage since it reduces the congestion.

2.3.1 Rate based congestion control scheme

In Opportunistic Network the Rate based congestion control techniques measure essential to control the data rate utilized by every sender to avoid overload in the network, wherever multiple senders connect the information measure. The rate control mechanism identifies the approved rate to permit the flows, to retort quickly to modulations in information measure and re-routing events. Rate control is performed at every mobile node to induce the information measure and delay necessities of real time traffic and rate control is performed efforts traffic and provides the specified information measure.

2.3.2 Loss recovery techniques

In Oppnets, Packet losses occur a lot due to mobility. For real time traffic, to mitigate the consequences of data loss, effective loss recovery techniques are needed. Network coding writing is employed to recover pockets that are lost throughout transmission. Initially multiple methods are discovered using ant colony optimization. Then the redundant network coding scheme is applied, received the quantity of packets and also the link failure of a node. Redundant Network code writing avoids the retransmission of missing packets and improves correcting capabilities of the errors due to loss of packets.

Several routing protocols are projected for Opportunistic networks in the past. They vary from epidemic to single copy forwarding. Single copy routing protocols are a lot of resource economical whereas multi- copy replication schemes have the next chance of message delivery. We have a tendency to review these protocols on however they handle congestion and follow congestion avoidance or congestion removal techniques.

Spray and Wait could be a quota- based mostly replication protocol. During creation of this protocol the upper bound is fixed as its number of permitted replicas of the packet/ message. It suggests that the overloading of one node doesn't imply that the complete network is congested and copies to be created per message should be adaptive.

J. Pujol[11] suggests that using only contact history to compute contact duration, interaction strength and frequency cannot bring home, the bacon a good load distribution which the queue length of a node should even be considered. Another paper proposes a message dropping scheme for congested delay tolerant networks that drops messages on the premise of social relationship of a node so on avoid dropping meaningful messages.

T. Kathiravelu et al.[20] have done work on capabilities a congestion aware adaptive routing protocol wherever selects the next hop of a node on the basis of its predicted connectivity and other factors like available buffer and its willingness to store carry and forward.

A. Grundy et al. [3]-[5] have done a major quantity of work within the field of congestion control in Opportunistic networks. In [5] they proposed a replication based mostly congestion aware forwarding rule that dynamically controls the quantity of replicas of a message supported the extent of expected congestion at the node.

Socially aware node behavior prediction was utilized by R.1. Ciobanu et al. [17] to scale back congestion within the network by forwarding to the nodes that have more chances of delivering the message to the destination.

In conclusion, an approach is needed to avoid congestion that reduces the overhead on the network and maintains a high packet delivery chance to the destination. The approaches introduced earlier were either single copy or multiple copy packet forwarding and largely aimed toward removing congestion. The proposed algorithm could be a congestion control scheme rather than removal, therefore reduces the overhead on the network. Also, it somewhat combines the one and multiple copy approaches by causing one copy of a packet to multiple nodes thereby rising the delivery chance and additional reducing the network overhead.

CHAPTER 3

EXISTING METHODOLOGY

Here, I present the summary of the fundamental concepts of Oppnet routing protocols, namely

- First Contact Routing Protocol
- Direct Delivery Routing Protocol
- Spray and wait Routing Protocol
- PRoPHET Routing Protocol
- MaxProp Routing Protocol
- Epidemic Routing Protocol

3.1. First Contact Routing Protocol

The First contact protocol randomly send the messages to any neighbor node. The path chosen randomly to forward the message from all the available contacts. Suppose no path available to send the message to the neighbor, the message will wait till it gets a path.

The example shows that the aim of this protocol is to send the message from node X1 to node X5. As per the figure 3.1, the node X1 sends the message to X2 or X3 according to its contact. Once it send the message to neighbor node immediately remove the copy of the message from source node. Therefore only one copy of the message exists in the network. Suppose X1 first contact X2 then the message will be forwarded to X2 and X2 will forward to the node X4 or X6. Subsequently X4 or X6 forward the message to the destination node X5. Otherwise if the node X1 forwards the message to X3, X3 send the message to the destination node X5. Due to frequent contact of same nodes, sometime path loop may occur. Because of path loop and keeping single copy of message in the network makes first contact protocol having poor delivery ratio.

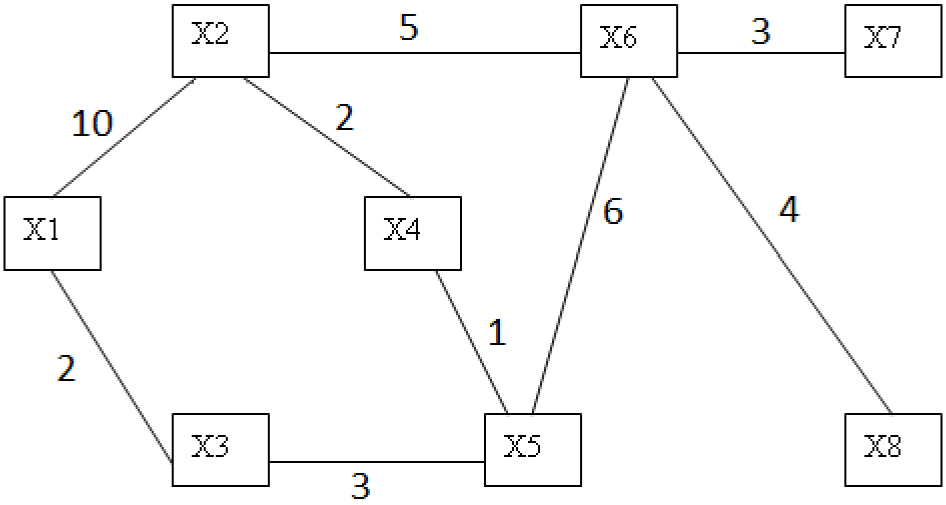


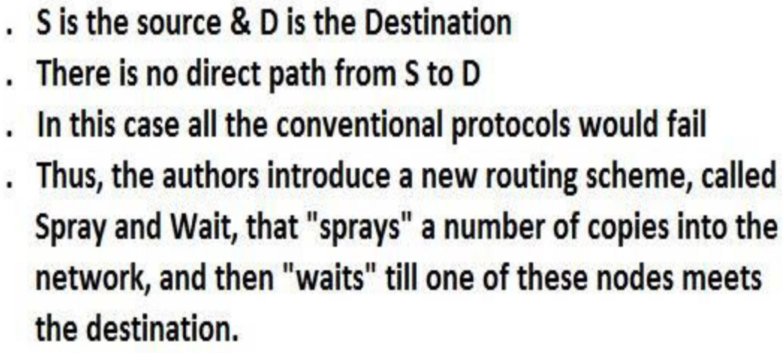
Fig. 3.1 First contact and direct delivery

3.2. Direct Delivery Routing Protocol

Within this routing protocol, the message is not forwarded to the middle nodes by the starting node; instead the starting node holds the message till it makes a direct contact with the ending node. The message directly delivers to the final destination once it comes to the ending node. Hence every message is transmitted only one time. So both the resource utilization and usage of bandwidth are less for message transferring in this protocol method. If the starting node never encounters the ending node at any time then the delivery delay is boundless. Hence this protocol has long delays for delivering the message. In cases where more delivery probability is needed this method is not an optimal technique. Figure 3.1 illustrate that node X1 can deliver messages solely to nodes X2 and X3 provided the edges describe certain cost parameters like distance and delay. Although the route X1-X3-X5-X4-X2 is quicker compare to the direct contact among nodes X1 and X2, the node X1 can’t send a message to X2 through this route.

3.3. Spray and Wait Routing Protocol

This protocol consists two phrases. First one is called spray phrase and second is wait phrase. In spray phase source node transmit message to a fixed number of neighbor nodes and will wait for some time to reach message to the destination node. If the destination was not found in the wait phase then each node having copy of the message will act as a source node. Using fixed number of flooding and wait phase, this protocol limit the flooding level. As compared with epidemic routing protocol, spray and wait protocol has less delivery delay and less number of transmissions.



- S is the source & D is the Destination
- There is no direct path from S to D
- In this case all the conventional protocols would fail
- Thus, the authors introduce a new routing scheme, called Spray and Wait, that "sprays" a number of copies into the network, and then "waits" till one of these nodes meets the destination.

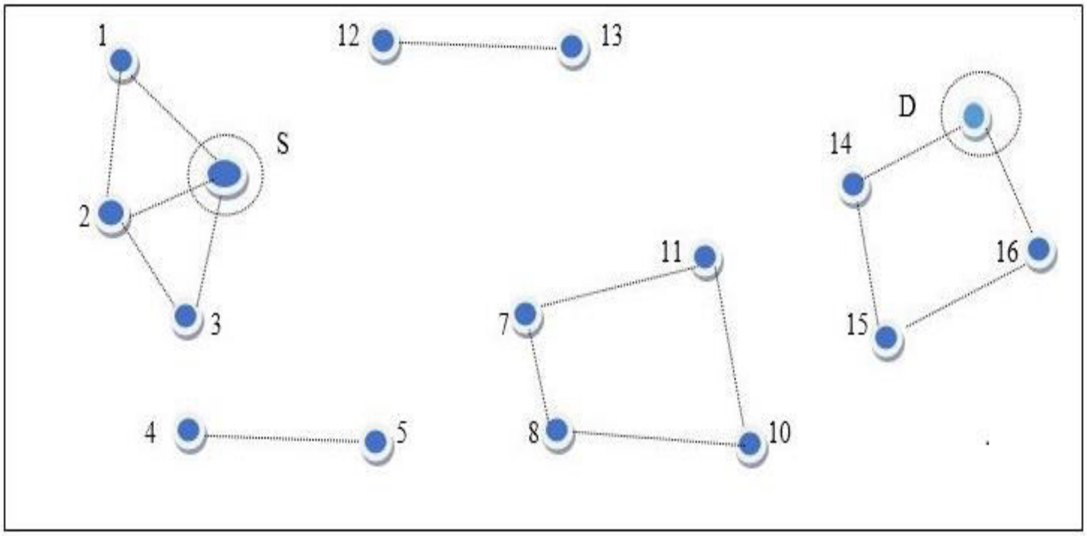


Fig. 3.2 Spray and wait

3.4. PRoPHET Routing Protocol

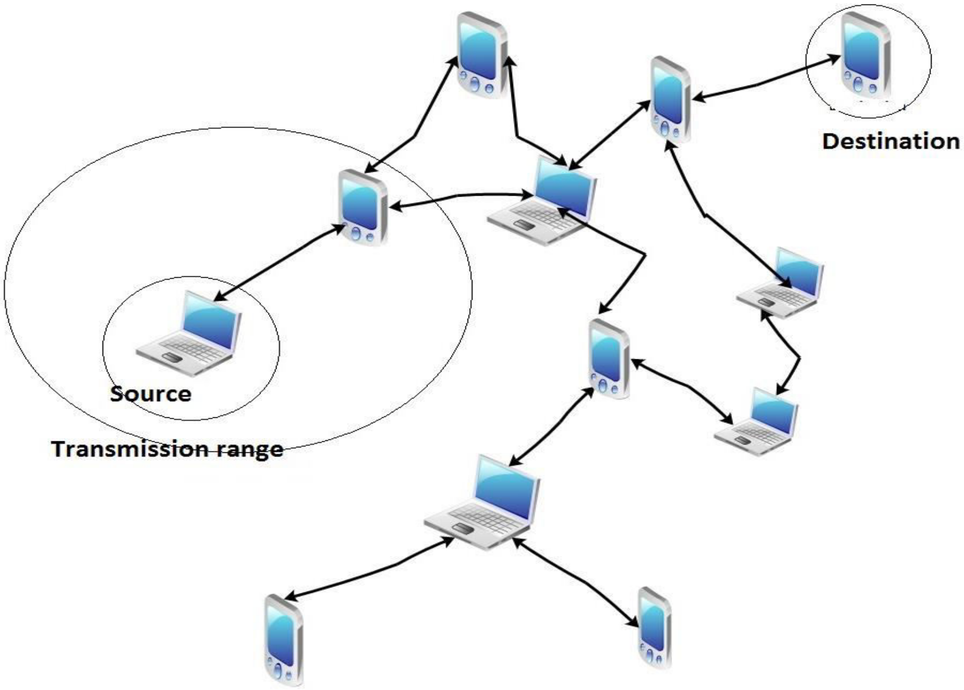


Fig: 3.3 PRoPHET Routing

Each node before send the message in PRoPHET (Probabilistic Routing Protocol using History of Encounters and Transitivity) computes delivery predictability. Delivery predictability between source node and destination node is achieved by estimating probability metric. The delivery predictability is calculated according to the history of visit to particular location or history of encounters between nodes. Each node having summary vector is calculated by applying probabilistic metric used to find delivery predictability. Whenever two nodes meet they exchange their summary vector values. If two nodes meet frequently then these two nodes having higher delivery predictability and both are good forwarder for each other. Therefore a source node is willing to send message to destination will select neighbor node which is having higher delivery predictability. As per the simulation result comparing with epidemic routing protocol PRoPHET having less communication overhead, higher delivery success rate, less delay and less message exchange.

3.5. MaxProp Routing Protocol

Maxprop was designed based on forwarding routing protocol. The messages are forwarded to the peers who are having higher probability to deliver messages in the destination node. Also Using modified Dijkstra algorithm it calculate shortest path to deliver the message to peers. These protocols maintain a queue in a buffer and highest priority given to new messages. If the buffer is almost full then it removes the message which has to travel long distance. It also has facility of message acknowledgement, helps to remove redundant messages in the network. For small buffer size nodes performance is very poor due to adaptive threshold calculation. According to the simulation its overall performance is good comparing with epidemic routing protocol.

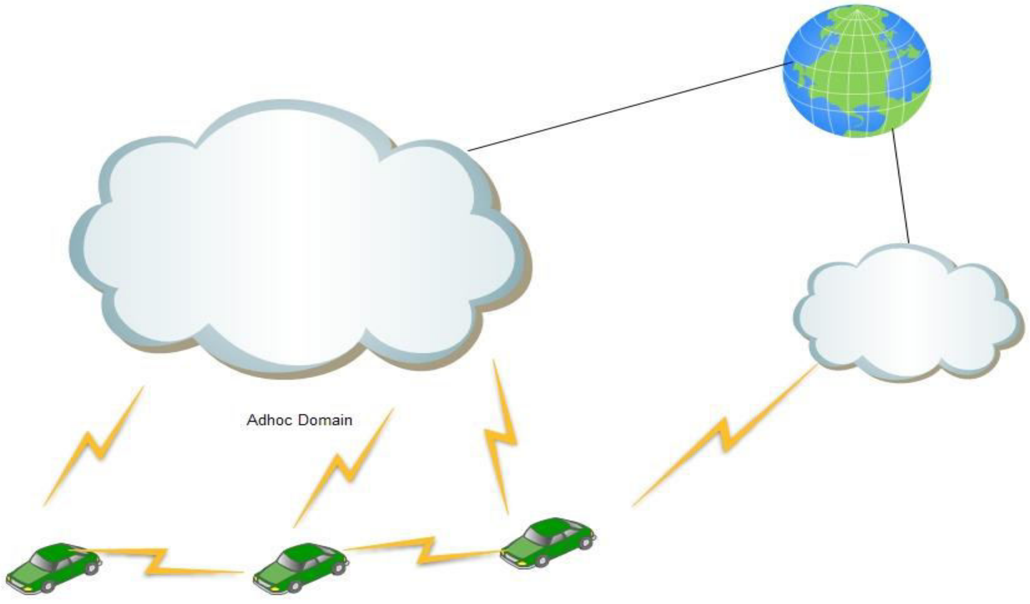
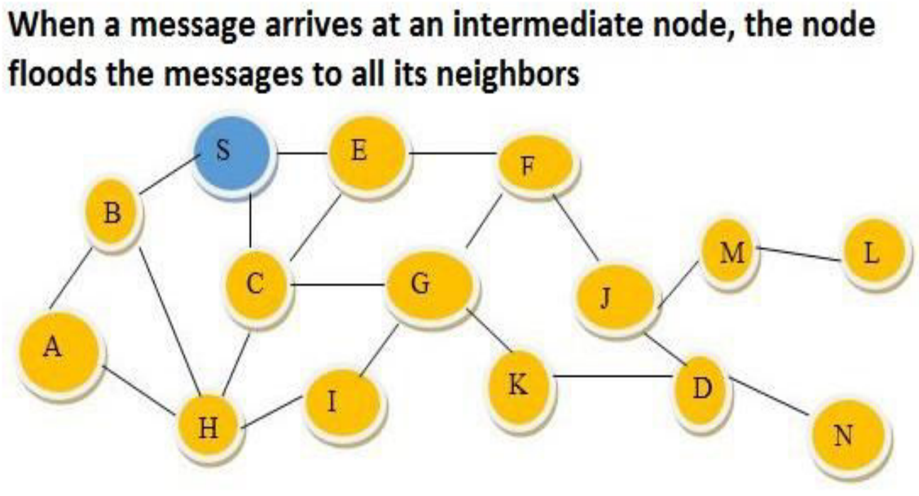


Fig.: 3.4 MaxProp Routing Protocol

3.6 Epidemic routing protocol

This routing protocol comes under the category of infrastructure-less flooding-based method. Two buffers are present in each node. The first buffer is used to store the messages produced by the node itself. The second buffer is used to store the message received from the other remaining nodes. A unique and single identification (ID) is attached to every message. A directory of message IDs which it is presently holding in its buffer is maintained by each node. This list or directory is called the summary vector. As soon as the two nodes gather, they swap their summary vectors among each other. By means of collating the two summary vectors, the nodes collate those messages that they haven't contained with them. Once this process of message collection is finished, the entire nodes have the identical messages in their buffers. This introduces a huge quantity of redundancy in the network. This earns major claim on both bandwidth and buffer power, however, altogether makes it tremendously strong to node and network breakdown. In this epidemic routing protocol, message delivery proportion is incredibly lofty and the message is handover in least amount of time if adequate means resources are existing.



When a message arrives at an intermediate node, the node floods the messages to all its neighbors

Fig. 3.5 Epidemic Routing protocol - Message arrival at node

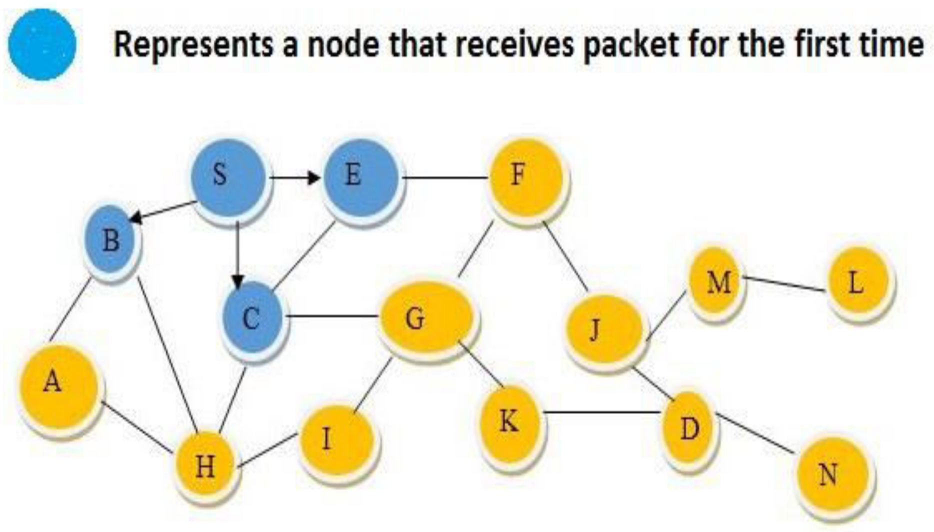


Fig. 3.6 Epidemic Routing protocol - Message arrival and flooding

The purpose of this protocol is to dispense application messages to host, named as carriers inside linked parts of ad_hoc networks. Like this, the message is rapidly dispensed via linked parts of the network. This routing depends upon carriers approaching to make contact with a further mobility. At this instant, the message scatters to an extra island of nodes. During such transmit communication of data; messages having high possibility finally attain their target.

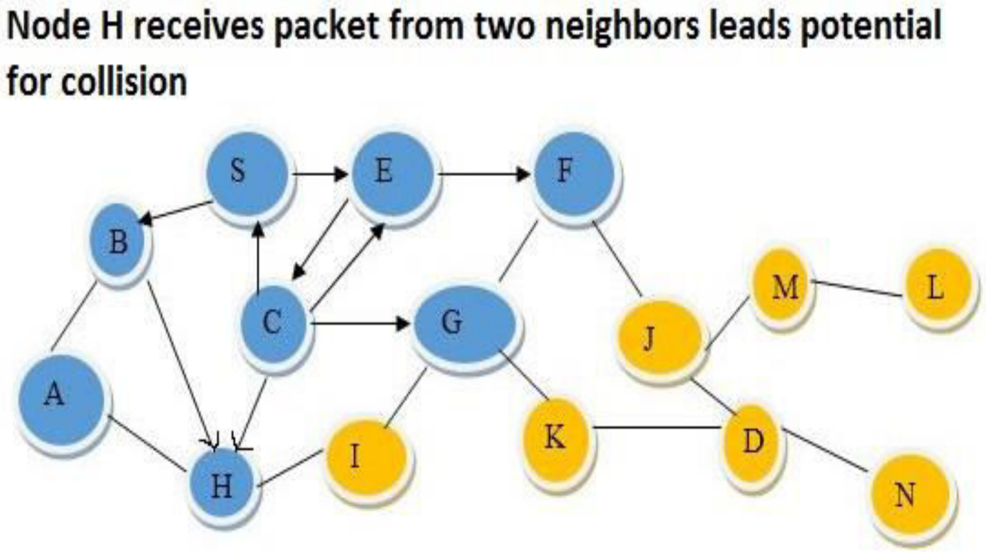

Node H receives packet from two neighbors leads potential for collision
S
E
F
B
C
G
J
M
L
A
K
D
N
H
I

Fig. 3.7 Epidemic Routing protocol - Message arrival flooding and collision

The given figure 3.7 explain epidemic routing at the lofty stage, by means of symbolizing moveable nodes as murky circles and whose wireless communication area exposed as speckled circle expanding from the starting place.

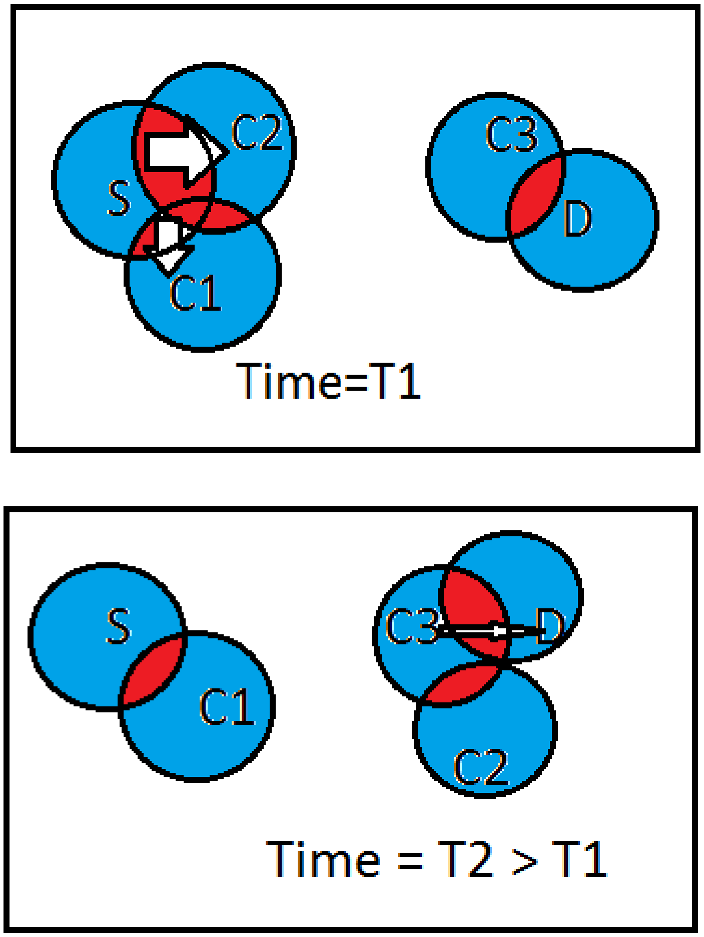


Figure 3.8   Epidemic routing at a High Level

The goals of Epidemic Routing are to:

i) To raise message delivery speed

ii) To reduce message latency, and

iii) To reduce the whole resources inspired in message delivery.

The figure 3.9 displayed above portrays the massage swap in this protocol. Host X make a contact with host Y and starts an anti-entropy session. During the first pace, the summary vector SVx of X is transmitted to Y. The summary vector

SVx is a compressed representation of the entire messages buffered at X. Then in the second pace a logical AND function is performed by Y between the repudiation of its summary vector SVy (the negation of y's summary vector) and SVx. To be precise, Y resolves the set dissimilarity between the messages buffered X and the massages buffered nearby Y. After that, it transmits a vector soliciting these messages from X. During the third pace X transmits the solicited messages to Y. This process is repetitive as soon as Y makes a contact with a novel neighbor. With specified adequate buffer space and time, these anti_entropy sessions assure ultimate messages deliverance via such pair_wise message swap.

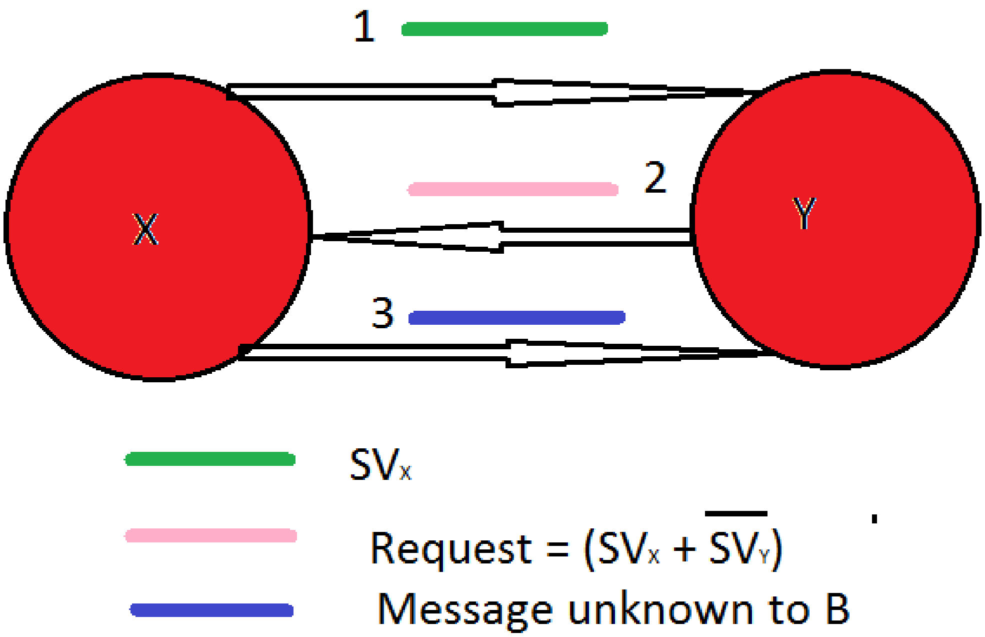


Figure 3.9   Exchange of Summary Vectors

This plan for epidemic routing links a sole and an unique message identifier, a hop count and a non-compulsory acknowledge request with every message. The highest number of epidemic swaps that a distinct message is exposes is determined by the hop count pasture. Though the hop count is alike to the TTL pasture in IP packets, message having a hop count of one would be delivered to their final destination. A message is distributed rapidly through the network, if the hop count values are higher. Normally, this will minimize average delivery time and maximize the entire resource utilization. Therefore message having a lofty priority may be noted with a lofty hop count. To diminish resource utilization, majority message may near to anticipated number of hops for a specified network pattern.

It is specified that message are delivered likelihood in epidemic routing, but certain applications must need acknowledgements of message deliverance. The acknowledge request (ack. request) field directs the final destination of a message to give an acknowledgement of message deliverance. These acknowledgements are sampled as easy go back messages from recipient rear to the dispatcher. Moreover, the acknowledgement can be allied with some other message intended rear to the dispatcher after the message is effectively of delivered. The quantity of memory and network resource inspired during epidemic routing is restricted by the buffer size.

CHAPTER 4

PROPOSED METHODOLOGY

4.1 Problem Identification

The Epidemic routing protocol creates an oversized quantity of redundancy within the network attributable to the excessive flooding of messages within the network. This incurs considerable demand on together bandwidth and buffer capacity. It additionally consumes lots of battery power of the nodes that will increase the dead nodes within the network and reduces the network time period. These limitations of Epidemic routing protocol motivated to intend new routing protocol that decreases the number of message flooding within the Oppnet, messages relayed within the network thus on minimize the bandwidth usage, power consumption of nodes, Network resource usage, whereas keeping the quantity of messages delivered, latency, buffer time comparable to the epidemic protocol.

Further, an approach is needed to avoid congestion that reduces the overhead on the network and maintains a high packet delivery chance to the destination. The approaches introduced earlier were either single copy or multiple copy packet forwarding and principally aimed toward removing congestion. The proposed algorithm may be a congestion avoidance scheme rather than removal, so reduces the overhead on the network. Also, it somewhat combines the single and multiple copy approaches by causation one copy of a packet to multiple nodes thereby rising the delivery chance and reducing the network overhead.

4.2 Reduced Flooding Epidemic Protocol [RFEP]

In this chapter the proposed Reduced Flooding Epidemic Protocol [RFEP] is described in detail. For the proposed of RFEP protocol, the following three improvement factors such as Stability factor, Random-neighbor-selection factor, and Delivery-probability-factor, has added in the already existing Epidemic protocol to decrease the quantity of message flooding in the network. The Random-neighbor-selection factor reduces the number of neighboring nodes that can be selected as a potential next hop. The Stability factor and Delivery-probability-factor are further used to calculate a Utility Metric that is used to select a neighboring node as a next hop in the routing. These improvements will decrease the number of copy of message relayed in the Oppnet by selecting a proper next hop node instead of flooding the message copy to each node in the oppnet. This results in smaller usage of network bandwidth and resource consumption, as well as power of nodes which helps in increasing the network lifetime. This new protocol is expected to reduce the overheads seen in the previous protocols. All other parameters are kept same as that of Epidemic protocol. The aforementioned three factors are described below.

4.2.1 Random-neighbor-selection factor

This factor is used to limit the number of potential neighboring nodes selected as next hop of a sender or an intermediate node. Before forwarding every node's message to its near nodes first calculates a random number say x, suppose x is greater than the numbers of near nodes, the message is forwarded to x neighbor nodes. If x is bigger than the number of near nodes of a node, then the message is transmitted to all the neighbor nodes. In this way this algorithm minimises the spreading of the number of copies of message in the opportunistic network.

4.2.2 Stability factor

To find out the stability of node's movement represented by S, a table referred to as the Speed Table is employed. When the node travels, the coordinate values recorded in the table. After, the node will utilize this coordinate values and calculate its average speed between two different positions. This average speed data will be available within the Speed Table. Using this table, the algorithm will analyze whether or not the modification in average speeds is incredibly enormous or nominal. A big difference indicates unstable movement and nominal modification indicates as a stable node. On Beginning all the nodes having stability value zero. For every two successive speeds if the variation is bigger than 10 units per second, the stability decreased using the formulae, then New S value is computed as

$$S = S_{old} – (1-S_{old})*S_{init} \qquad (1)$$

Otherwise it is increased using the formula, the New S value is

$$S = S_{old} + (1-S_{old})*S_{init} \qquad (2)$$

Here S_{init} is an initialization constant whose value can be taken in between 0 and 1. In this work, it is taken to be 0.5 which can be modified accordingly as per the need.

4.2.3 Delivery-probability-factor

RFEP uses this delivery-probability-factor to calculate the delivery probability of any two nodes in the network. To deliver the messages this utilizes the transitivity and history of encounters by assuming that nodes move in a very foreseeable fashion and not at random. The delivery predictability P(a,b) tells that node ‘a’ having chances to meet ‘b’ in future. If the neighbor has plenty of chances to meet the end node, the intermediate node moves the message to the neighbor. So as to seek out the delivery chance of a node, the RFEP protocol uses the same equation as defined in PRoPHET Protocol. The aforementioned Stability factor and Delivery-probability-factor parameters are used to calculate the Utility Metric represented by U(a) of the a^{th} node using the formula:

$$U(a) = \sum_{b=1}^{b=2} W(b) * Va(b) \qquad (3)$$

where W(b) is the load of the b^{th} constraint and $V_a(b)$ is that the value of the b^{th} constraint for a^{th} node i.e. $V_a(1)$ is the Stability factor value, $V_a(2)$ is the Delivery-probability-factor value for node a. Then U(a) is computed based on the value for node ‘a’ and a threshold T will decide its option for the next hop for the message. The message is send to near by node which is having higher value compared to T. Thus, T is further used to manage the quantity of flooding within the network.   Then T is used to maintain flooding quantity in the network.

4.3 Threshold Based Congestion Control Algorithm

An approach to control congestion within the oppnets is proposed here. Once 2 nodes meet, they exchange their handiness data and other metrics together with social, resource and network metrics. Every node then updates its native table containing these metrics. Forwarding decisions are made based on these metrics which distributes the load fairly within the network therefore avoiding congestion. The metrics used are: social metrics, node's resource metrics and network metrics.

4.3.1 Social metrics

Utility of the nodes are calculated based on smoothed centrality, similarity with a neighbor and tie strength.

Centrality is computed as the count of a node neighbors as shown in equation (1). A node with more number of neighbor nodes is more central as compared to others.

$$\text{Centr (i) = Number of i's neighbors} \qquad (1)$$

Then the centrality is smoothed by taking some time, resulting in an even good load spreading.

$$\text{SCent (i)} = \alpha * \text{Centr (i)}_t + (1 - \alpha) * \text{Centr(i)}_{t-1} \qquad (2)$$

In equation (2), SCent(i) is the smoothed centrality, α is a constant, its value lies between 0 and 1, Centr(i)_{t-1} is the centrality computed previously and Centr(i), is the current centrality value.

Similarity is the count of common neighbors between the two nodes.

$$\text{Sim}_i(J) = |C_i \cap C_j| \qquad (3)$$

In equation (3), $\mathrm{Sim}_i(J)$ is the similarity of a node i with node j, C_i and C_j are the set of neighbors corresponding to i node and j node respectively.

The Tie Strength is a combination of contact frequency, recency and duration. Equation (4) is given as:

$$\mathrm{TS}_{\mathrm{i}}(j) = \frac{f(j)}{F(i) - f(j)} + \frac{d(j)}{D(i) - f(j)} + \frac{r(j)}{R(i) - r(j)} \qquad (4)$$

As per the above equation, frequency of contact denoted as f(j) for node j, entire frequency of contacts denoted by F(i) for the of node i with other nodes, the time taken to contact is denoted by d(j) for node j, the total time-span denoted by D(i), r(j) is the recency of contact with j and R(i) is the total time the node is part of the oppnet. Social Utility have been the combination of all the above defined metrics as shown in equation (5):

$$\mathrm{SocialUtil}_i(J) = \mathrm{SCent}(i) + \mathrm{Sim}_i(j) + \mathrm{TS}(j) \qquad (5)$$

4.3.2 Node's resource metrics

A node with more available storage is preferred for packet forwarding, as the chances of a packet being dropped are lesser, as compared to a node with lesser available buffer.

$$Av(i) = Bi - \sum_{a=1}^{N} M_a(i) \qquad (6)$$

In equation (6), Av(i) is the available storage at node i, B(i) is total buffer capacity and $M_a(i)$ is the total space occupied by a message i in the buffer.

Delay metric calculates the total delay a node adds to packets travelling through it.

$$D(i) = \sum_{a=1}^{N} (T_{now} - T_{Mi}(i)) \qquad (7)$$

Equation (7) calculates the delay metric D(i), where T_{now} is the current time and $T_{Mi}(i)$ is the message received time.

Dropping probability (Dp) metric calculates the probability of a message that will be dropped at a node. A node with a lesser value is preferred.

$$Dp(i) = \frac{D(i)}{D(i) + T} \qquad (8)$$

D(i) is the delay metric & T is the Time to live of a message(s) as calculated in equation (7)

Congestion rate (Cr) metric could be used to avoid the parts of the network that congested at a faster rate.

$$Cr(i) = \frac{T_{full}(i)}{T_{at}(i)} \qquad (9)$$

Equation (9) computes CR as the ratio of the time a buffer is full (T_{full}(i)) and the time a buffer is available (T_{at}(i)).

Then Node's Utility is computed as:

$$\mathrm{NodeUtil}(i) = \frac{\mathrm{Av(i)}}{(\mathrm{D}(i) + \mathrm{Dp(i)} + \mathrm{Cr(i)}} \qquad (10)$$

Equation (10) shows that the utility of the node was directly proportional to its availability metric and was inversely proportional to the congestion rate metric, dropping probability and delay.

4.3.3 Network metrics

It is important to consider network with utility metrics of a node. This enables the sender to avoid forwarding the message to a part of the network that is expected to be congested in the future, leads avoiding congestion. Network metric of a node is computed by considering network with availability and delay metrics.

Network buffer availability metrics are computed by considering a mean of the availability metric of all the neighbors of the node i, as shown in equation (11).

$$EN_{Av}(i) = \frac{1}{N}\sum_{a=1}^{N} Av_i(i) \qquad (11)$$

Network delay metric can be calculated by considering a mean of the delay metric of all the neighbors of the node i, as illustrated in equation (12).

$$EN_D(i) = \frac{1}{N}\sum_{a=1}^{N} D_a(i) \qquad (12)$$

Total network utility metric is calculated as:

$$ENUtil(i) = \frac{EN_{AV}(i)}{EN_D(i)} \qquad (13)$$

Equation (13) tells that a node's network utility metric is directly proportional to network availability metric and is inversely proportional to network delay metric, as the aim is to select a part of the oppnet that has higher buffer availability and adds less delay to the packets travelling through its aid.

Then the total utility of every node is computed by taking a weighted summation of the social, node and network metrics.

TotalUtil(i) = (s * SocialUtil$_x$(J))+ (n * NodeUtil(i))+ (en * ENUtil(i)) (14)

In equation (14), s, n and en were constants that could be varied according to the requirements to give more weight to one metric or another.

4.3.4 Forwarding policy

A congestion avoidance forwarding policy is proposed based on the sum of the utility metrics of the nodes. If a node willing to send/ forward a packet, selects multiple nodes, its total utility metric is greater than predefined threshold, as the next hop. By using this metric it shows that the network is not congested and the probability of delivery is high and the packets are not dropped.

CHAPTER 5

SIMULATION RESULT AND ANALYSIS

5.1 Simulation Setup

5.1.1 The ONE Simulator

The Opportunistic Network Environment simulator.

Information

The Opportunistic Network Environment simulator [ONE] is an Environment for simulation and capable to do

- Creating node movement with the help of number of movement models.
- Connecting the messages between each node with the use of different Delay Tolerant Network algorithms.
- Seeing all the movements and passing message in real time on its own interface.

ONE can get the mobility data from real-world traces or other mobility generators. ONE can also generate number of reports from node movement to message passing and general statistics.

Every simulation run uses the settings from default_settings.txt, if one exists. We will be able to offer an additional configuration file(s) as a parameters to outline new settings or override those outlined in default settings. For example: epidemic_settings.txt.

5.1.2 RFEP default setup

The ONE simulator is used to calculate the performance of Reduced Flooding Epidemic Protocol.. The nodes are movable in nature and have divided into groups of six and every group consists of 40 nodes. The nodes having I and III groups are walkers with a speed of 0.5 – 1.5 m/sec. The II node groups of cyclists with different speeds of 2.7 – 13.9 m/sec. The nodes of three groups (IV, V and VI) are cars/trams with different speeds from 7 – 10 m/s. In the simulations we selected the shortest path map based movement model. Here, as per the description of map the nodes will move from one place to another place. For finding the shortest path from starting to ending place simulator use the map path. The mobile nodes have a transmit speed of 2 Mbps & communication range of 10 meters. Every time the simulation will run 43000 secs. The world size is 4500m x 3400m meters for the movement model. Every 25 – 35 seconds a new message is generated and the size is between 500 KB to 1 MB. The following values assigned for parameters for generating the result. W (b) represents two different parameters. Here the value of T is taken to be 0.6, the Delivery-probability-factor weight W (2) = 0.5, The Stability factor weight W(1) = 0.5.

The Following energy settings have been applied for all group nodes.

Table 5.1: Energy default-settings

Group.initialEnergy	5000 units
Group.scanEnergy	0.1 units
Group.transmitEnergy	0.2 units
Group.scanResponseEnergy	0.1 units
Group.baseEnergy	0.01 units

Before start of the simulation the node having a value is the initial energy. The energy usage per scanning is known scan Energy. Scans Response Energy means energy usage per scanning response. The energy usage per second while sending is known as transmits Energy. The quantity of power consumed when the node is idle is called base Energy, The simulation used the following configurations/ settings:

Changing the number of nodes in the simulation: To compare Reduced Flooding Epidemic Protocol against the Epidemic routing protocol the total no of nodes are taken as 120, 150, 180, 210 and 240 in this simulation

The performance metrics are:

a) ***Overhead ratio:*** This is for each messages total number of copies forwarded. It is calculated as (NumberOfRelayedMessages – NumberOfDelivered Messages)/ (NumberOfDeliveredMessages).

b) ***Message delivery probability:*** In a particular time period how many messages received by the end node.

c) ***Number of total messages delivered:*** This is how many messages received by end node.

d) ***Average Delay****:* It is the average of difference with the message delivery time and message creation time.

e) ***Dead nodes count****:* This is that the number of nodes whose energy becomes almost zero i.e. less than 50 units after simulation.

f) ***Residual energy average****:* This is the average energy left after the simulation is over.

g) ***Average-buffer-time****:* Message creation time and message delivery time difference.

h) ***Average Hop-count****:* It is the average number of nodes in-between travelled by a message to arrive at its destination.

5.1.3 Congestion control default setup

The proposed congestion control algorithm is experimented using ONE simulator. Following metrics are used to find out the performance of the proposed algorithm:

a) ***Overhead ratio:*** This is the variation among the number of messages delivered and the number of packets relayed.

b) ***Average latency***: This is the average variation among the message delivery time and message creation time. It measures the delay a node adds to a message travelling via it.

c) ***Delivery probability***: This is the amount of probability of message delivered to the destination in a fixed period of time.

The following table defines the congestion control simulation configuration of the Network.

TABLE 5.2: SIMULATION SPECIFICATION

Simulation time	43200 seconds
Number of host in each groups	40
Number of host	5
Buffer Size	5MB
Message time to live	300 Minutes
Message size	500KB – 1MB
Message creation interval	25 – 35 seconds
Scenario update interval	0.1 seconds

5.2 Performance Evaluation - RFEP

The results produced in this effort are shown in Figures 5.1 to 5.9. We studied from these figures that Buffer time, Residual Energy, the number of nodes, Hop count, number of delivered messages, Delay, number of copy of forwarded messages, Probability of received messages, relayed messages force the performance of the Reduced Flooding Epidemic routing protocol [RFEP] of Oppnets.

5.2.1 Average Residual Energy

Average energy left after simulation is over is called average Residual Energy.

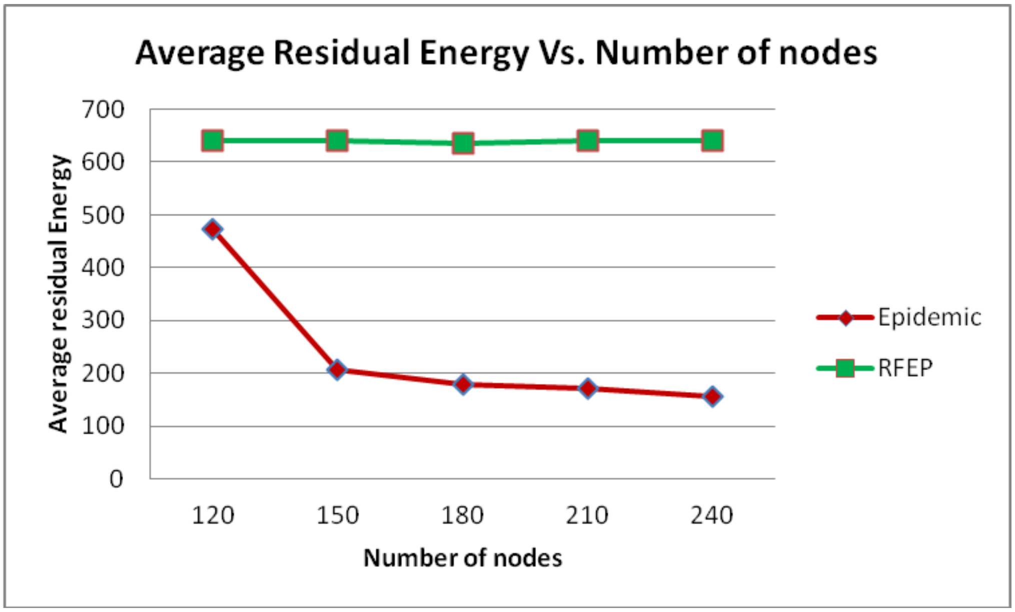


Fig. 5.1 - Average Residual Energy

From figure 5.1, this is clear that when the number of nodes number increases, the nodes average residual energy decreases for Epidemic Protocol and the nodes number increases RFEP protocol Residual Energy value remains constant or small variation. This is due to the fact that the nodes number gets increases and the number of delivered messages decreases which effects in lot of transmits and scans of nodes. The rate of decrease is bigger in the Epidemic routing protocol as comparison with the RFEP protocol. The Direct Delivery protocol having maximum average residual energy comparing with all the protocols. The difference in the amount of nodes had not affected the residual energy of RFEP. This shows that flooding is more or less constant and not depending on number of nodes.

5.2.2 Average Buffer Time

Message creation time and message difference time difference is called average buffer time.

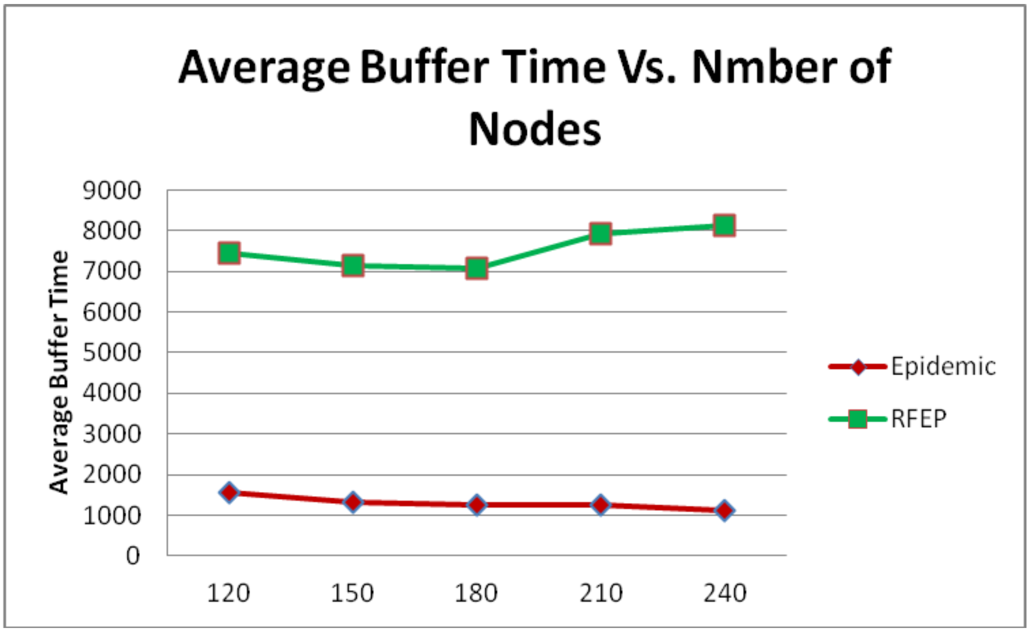


Figure 5.2 Average Buffer Time

From Figure 5.2, this is clear that the Epidemic Routing Protocol average buffer time is less compared to RFEP Protocol. Therefore the message flooded in all nodes with in the radio frequency range has less buffer time. Variation in number of nodes does not affect more the average buffer time.

5.2.3 Average Hop Count

This is the average number of nodes in-between travelled by a message to arrive to its destination.

From Figure 5.3, it is clear that in Epidemic Routing Protocol number of in-between nodes pass through a message to arrive to its destination increased when number of nodes increased. Hence it consumed more energy. But in RFEP Protocol there is small variation in number of in-between nodes travelled by a message to arrive at its destination when number of nodes increased. This shows that RFEP Protocol uses less number of intermediate nodes to reach messages in destination and energy consumption is less.

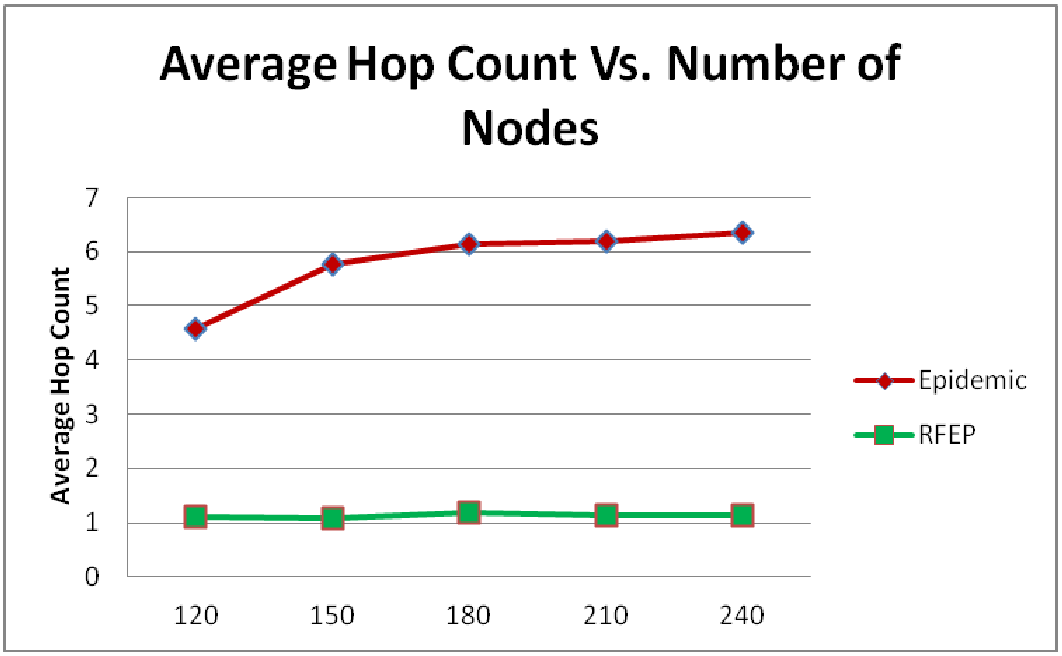


Figure 5.3 Average Hop Count

5.2.4 Number of dead nodes

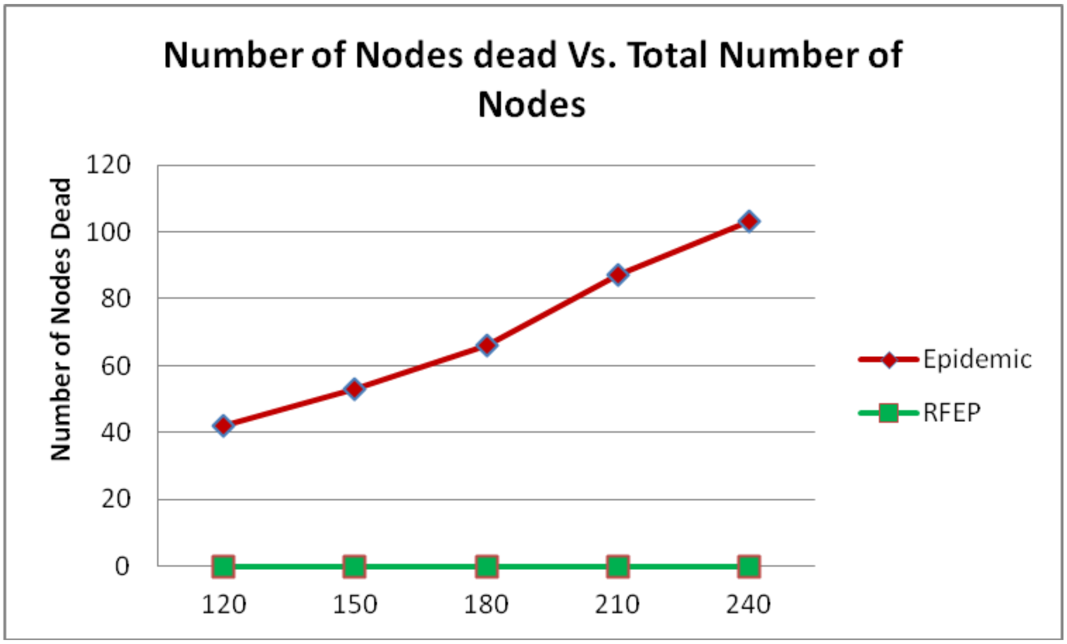


Figure 5.4 Number of dead nodes

If energy of a node becomes nearly zero i.e. less than 150 units after the simulation is called dead node. The Figure 5.4 shows that in the epidemic protocol if the number of nodes increases as well as the number of dead nodes also increases. Fact is more number of scans and transmits between nodes. But in RFEP Protocol when number of nodes increases there is no change in number of dead nodes. This is due to less number of transmit and scans between nodes take place, causes less energy consumption. In Epidemic Protocol dead node rate is increasing and there are no dead nodes while increasing number of nodes in RFEP Protocol.

5.2.5 Average Delay

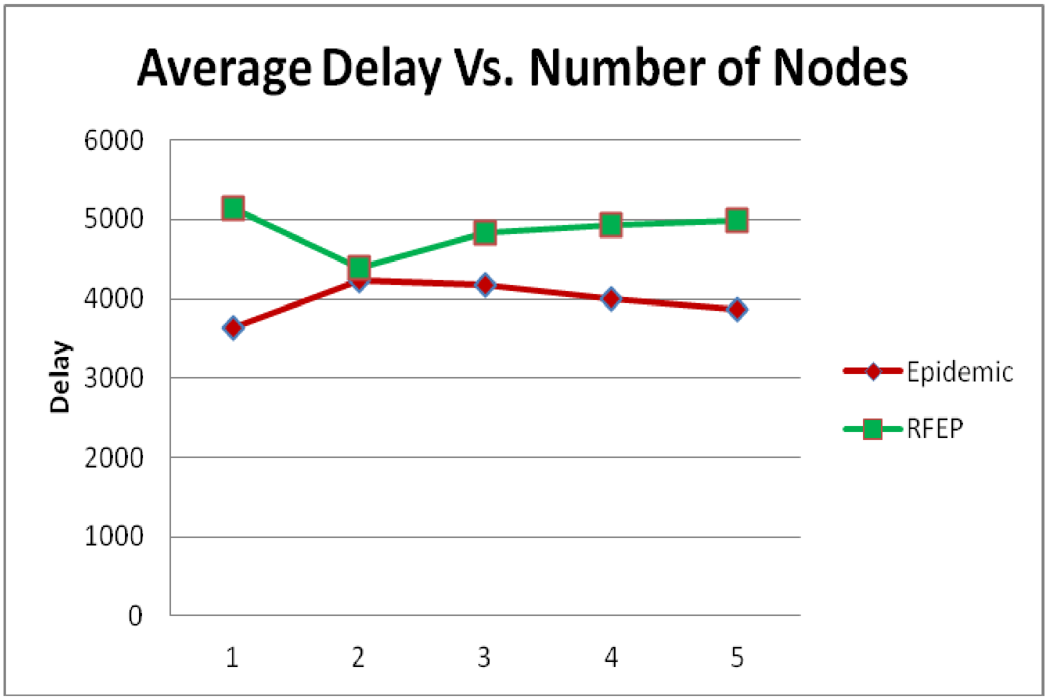


Figure 5.5 Average Delay

This is the average variation among the message creation and message delivery time. From Figure 5.5, this is understood that the number of nodes increases, the average delay initially increases and from a particular place onwards decreases in Epidemic routing protocol. Alternatively in RFEP protocol initially average delay decreases then from particular point onwards started increasing. This shows that average delay is less in Epidemic Protocol and more in RFEP Protocol.

5.2.6 Probability of Messages received

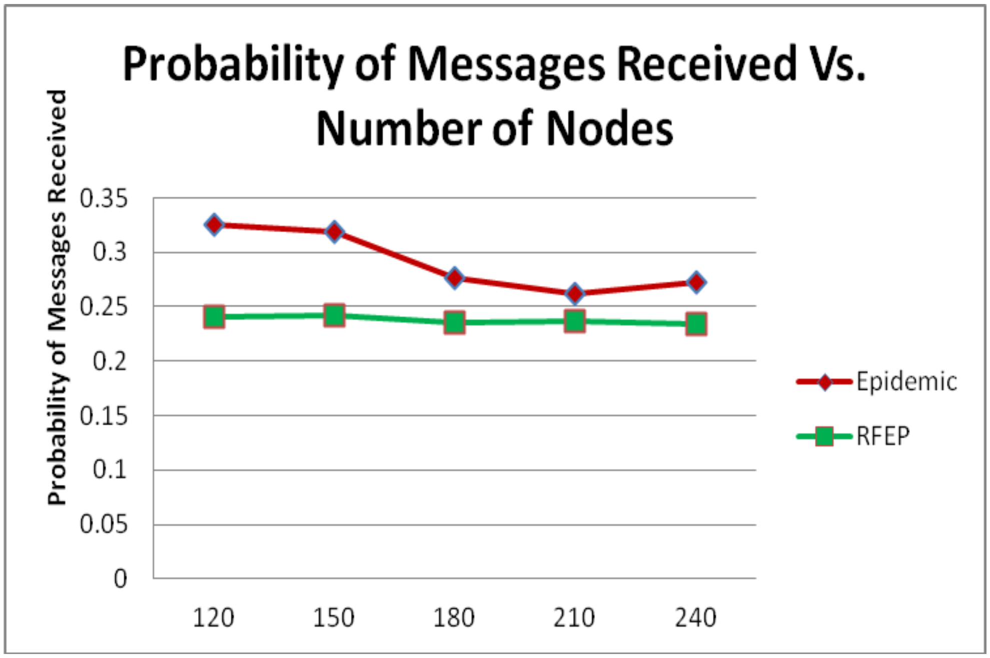


Figure 5.6 Probability of Messages received

This is within a given period of time probability of the messages properly received by the destination node. From Figure 5.6 it is understood that Probability of messages received decreased when number of node increased in Epidemic routing protocol. But at particular point once again probability of messages received started increasing in Epidemic routing protocol. In RFEP probability of messages received decreases when number of node increases. By comparing Epidemic and RFEP protocols probability of messages received high in Epidemic routing protocol and less in RFEP protocol.

5.2.7 Number of Messages Delivered

Total messages received by the destination node are called number of messages delivered. From Figure 5.7, we came to know that in epidemic protocol as the number of nodes increases, the number of delivered message to the destination also increases. But in RFEP Protocol as the nodes count increases there is a small variation in number of messages delivered. In Epidemic Protocol message delivery rate is high and RFEP Protocol message delivery rate is low.

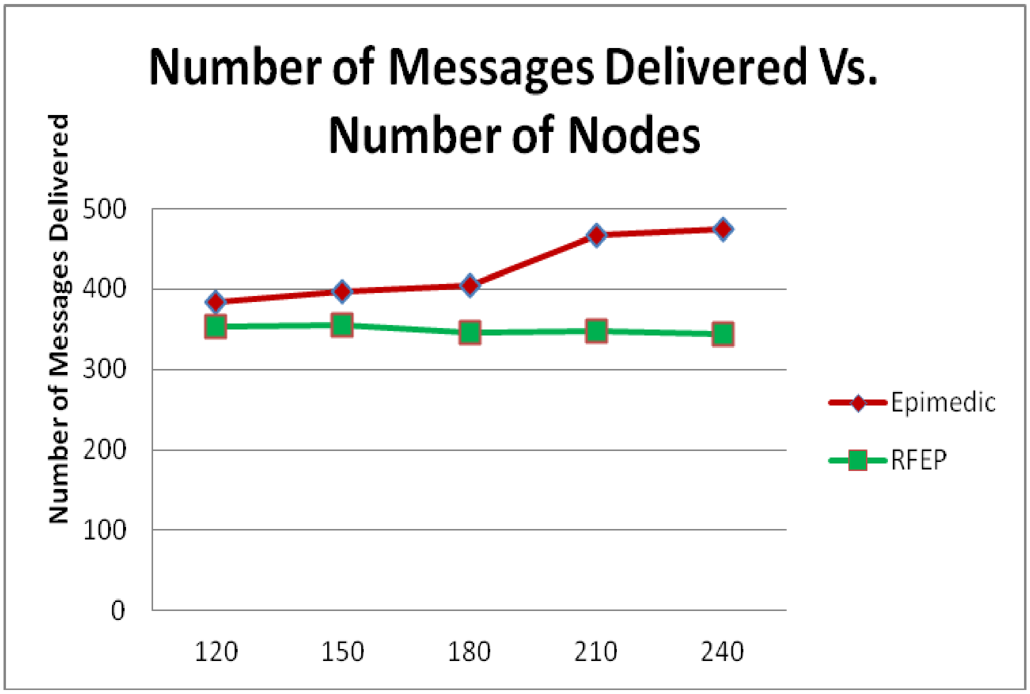


Figure 5.7 Number of Messages Delivered

5.2.8 Overhead ratio

Copies per message forwarded in this network are known as overhead ratio. It is calculated as (NumberOfRelayedMessages – NumberOfDelivered Messages)/ (NumberOfDeliveredMessages). From Figure 5.8, it is clear that when no. of nodes increases, average no. of copy of messages forwarded also increases in Epidemic Routing Protocol. But in RFEP when number of nodes increases then a small difference in copy of messages forwarded. Therefore Epidemic routing protocol for Forward more number of copy of messages and RFEP forwarded less number of copy of messages.

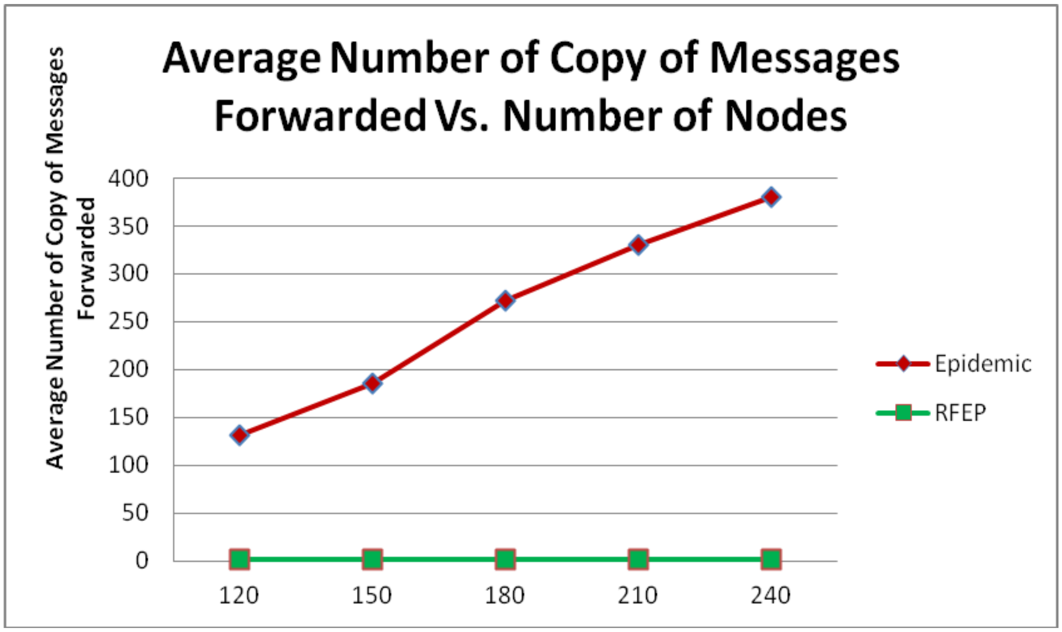


Figure 5.8 Over head ratio

5.2.9 Relayed Messages

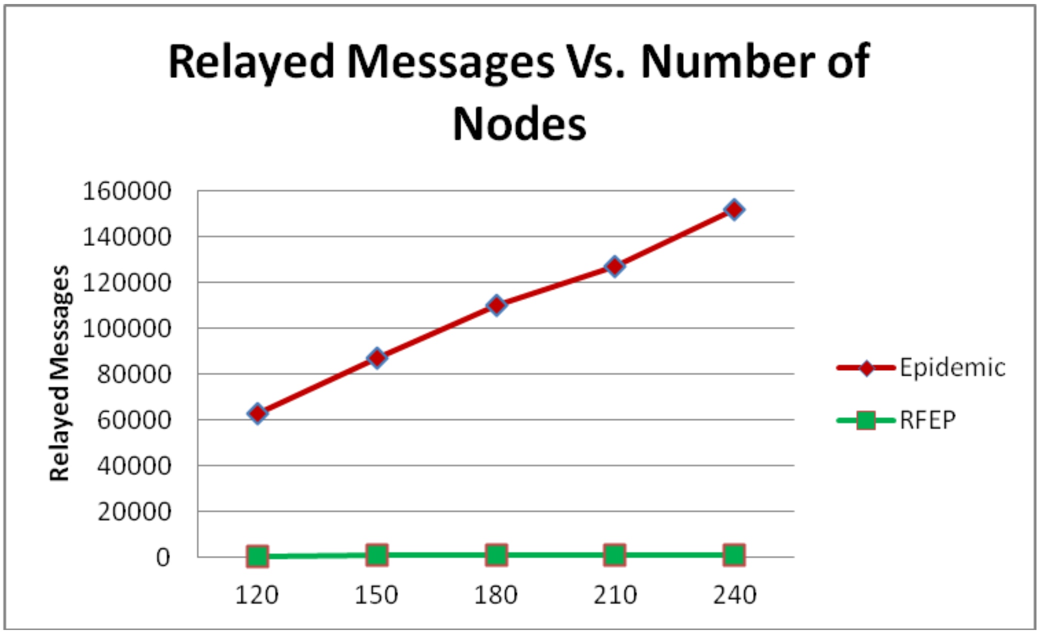


Figure 5.9 Relayed Messages

Figure 5.9 show that when number of nodes increases relayed messages also increases in Epidemic routing protocol. But RFEP protocol there is small variation while increasing number of nodes. Therefore flooding is more in Epidemic and controlled in RFEP.

Figure 5.1 to 5.9 shows the outcome performance of RFEP and Epidemic protocol by varying number of nodes. This could be observed that with increase in number of nodes, messages delivered percentage also increases. This result indicates increase in quantity of nodes will increase amount of flooding and the number of message carriers in the network. This result higher rate of message delivery. RFEP has lesser number of messages delivered as match with the Epidemic because of more flooding in case of Epidemic protocol, that increases the chance of a message getting delivered.

The overhead ratio increases as the quantity of nodes are also increased. This result indicates that while increasing the quantity of nodes, the quantity of messages flow also in the network (i.e. number of relayed messages) increases. This results in the increased overhead ratio. It can be observed that RFEP has less overhead ratio as compared to the Epidemic protocol due to major reduction in the amount of flooding.

The average latency is slightly more than the Epidemic protocol. This is because RFEP takes more time due to the limited flooding in deciding to select the best suitable node as next hop for carrying the message. The average buffer time of RFEP is high as compared with the Epidemic protocol. It is validated with the fact that in case of Epidemic a node floods the message to the neighbors from its buffer as soon as it comes into the network boundary. But in RFEP, a node keeps it in its buffer until it finds a better node that can be selected as next hop which in turn increases its average buffer time. When the quantity of nodes increased accordingly the average residual energy decreases. It seems that an increase in the quantity of nodes will increase the transaction between the network nodes, which ultimately decreases the average residual energy. RFEP has more value of average residual energy than the Epidemic protocol because of the reduced flooding and optimization done for next hop selection.

It is further noted that when the quantity of nodes are increased, the quantity of dead nodes even increases. Due to this effect an increasing the quantity of nodes will also raise the interactions among the nodes in the network, which eventually decreases their residual energy, and hence there will be more dead nodes in the network. RFEP has less number of dead nodes ((in fact 0 dead nodes) present in the network because of the reduction in flooding. It shows that the application of RFEP protocol in Opportunistic networks can increase the network lifetime by decreasing the consumption of power of the nodes.

5.3 Performance Evaluation - Congestion Control

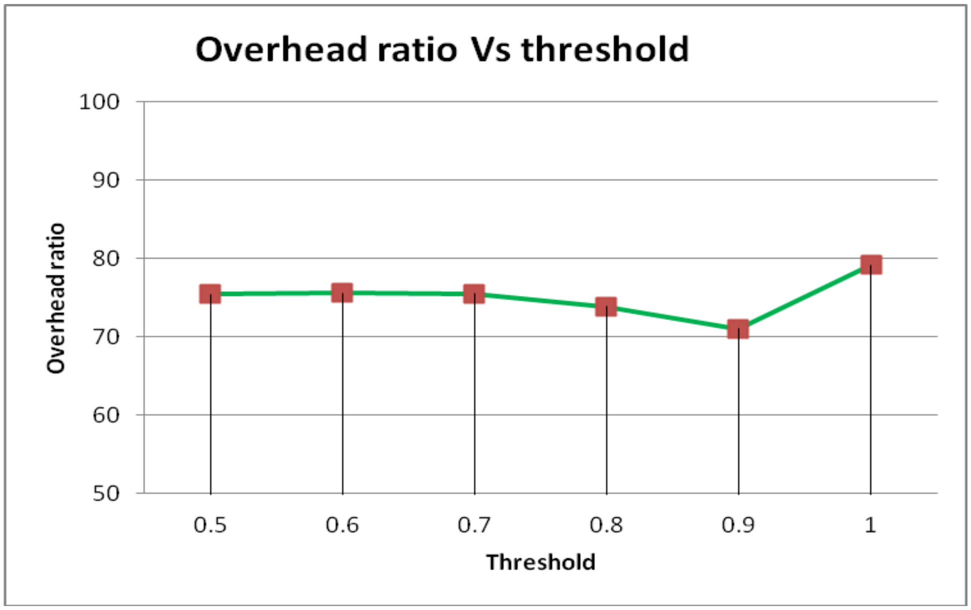


Fig. 5.10 Overhead ratio versus Threshold

After conducting more simulations, the value of threshold and constants were set as: α = 0.8 and threshold=0.9. The chosen values produces the better results in terms of all performance metric used: overhead ratio= 71.0056, delivery probability= 0.2454 and the number of packets dropped= 25890. Figure 5.10 illustrates a plot of the threshold values vs. the overhead ratio.

The weighing constant values are s, n and en are: s= 0.4, n= 0. 3 and en= 0.3.

5.3.1 Overhead ratio

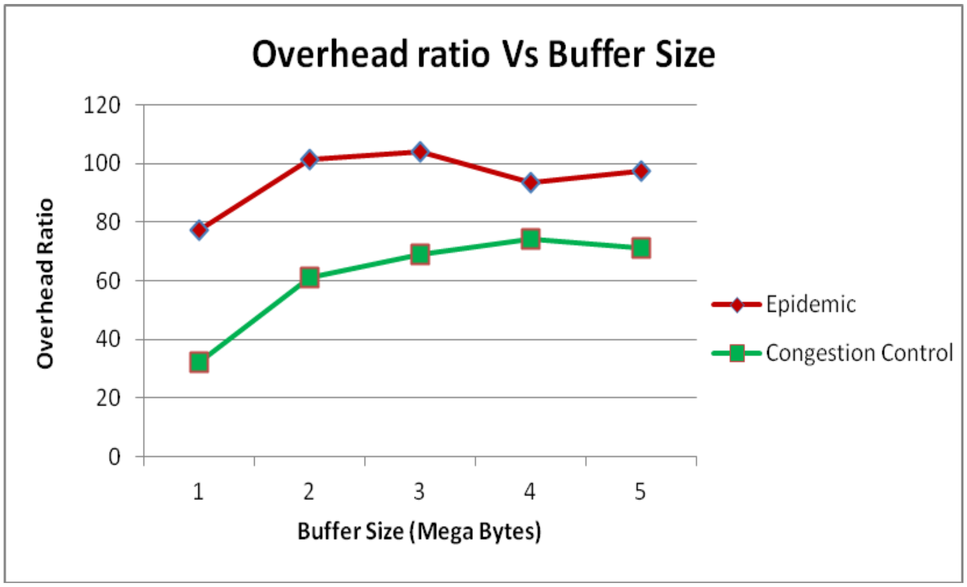


Fig. 5.11. Overhead ratio versus Buffer size

The projected algorithm compares the epidemic routing protocol in terms of the overhead ratio. Fig. 5.11 shows that the congestion control algorithm has less overhead ratio comparing with epidemic routing protocol. The congestion control algorithm's average overhead ratio is 61.47984 and that of epidemic is 94.76122. At the buffer size of 1 MB, the overhead value is 77.4894 and 32.2316 for epidemic protocol and congestion control respectively which are less.

5.3.2 Number of Packets dropped

Fig. 5.12 shows a plot of the buffer size vs. the number of packets dropped. The congestion control and epidemic average number of packets drop are 19826.6

and 26357.4 respectively. The projected algorithm is least number of packets dropped as comparing with other protocol.

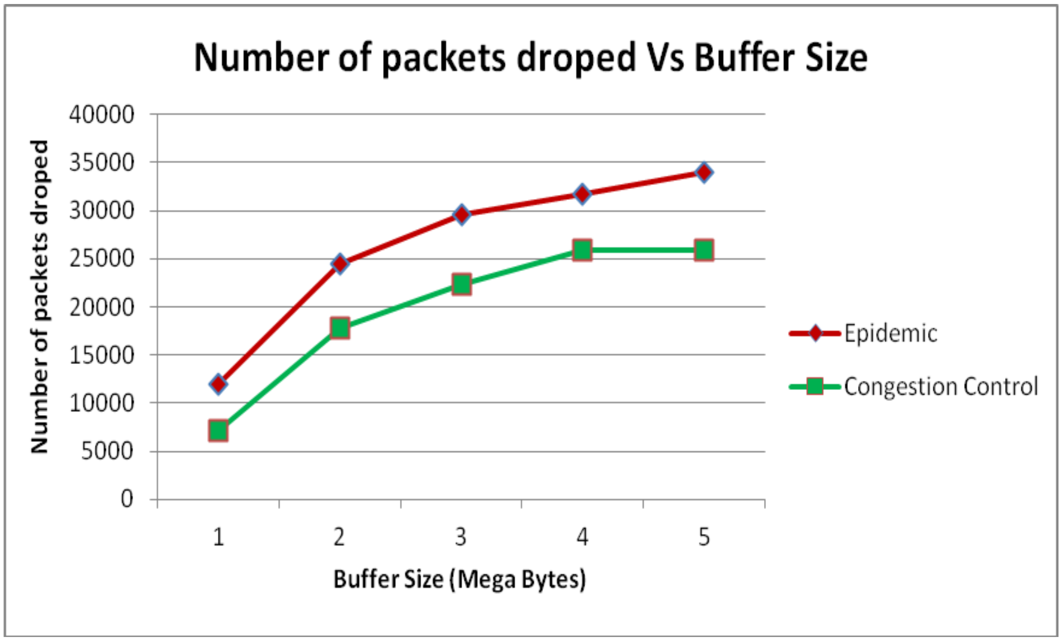


Fig. 5.12 Number of packets dropped versus Buffer size

5.3.3 Average latency

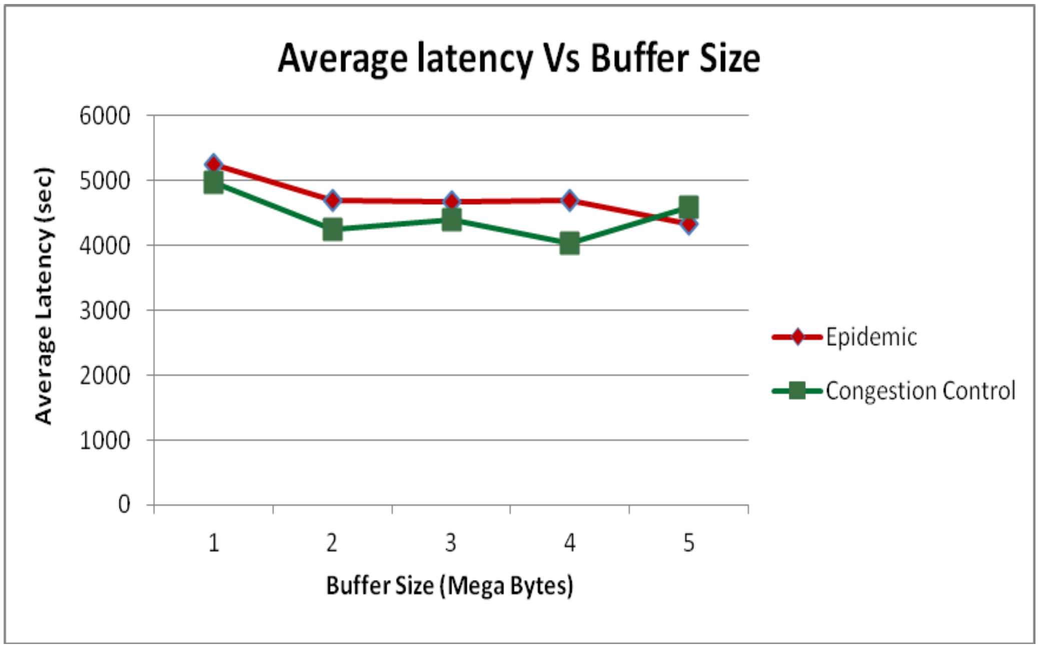


Fig. 5.13. Average latency versus Buffer size

Fig. 5.13 describes a plot of the buffer size vs. the average latency. The epidemic and congestion control average latency values are 4722.06122 and 4443.70164 seconds respectively. The projected algorithm gives average low delay in congestion control protocol compared to epidemic protocol. In between 4MB to 5MB buffer size these protocols produce nearly equal delay in seconds.

5.3.4 Delivery Probability

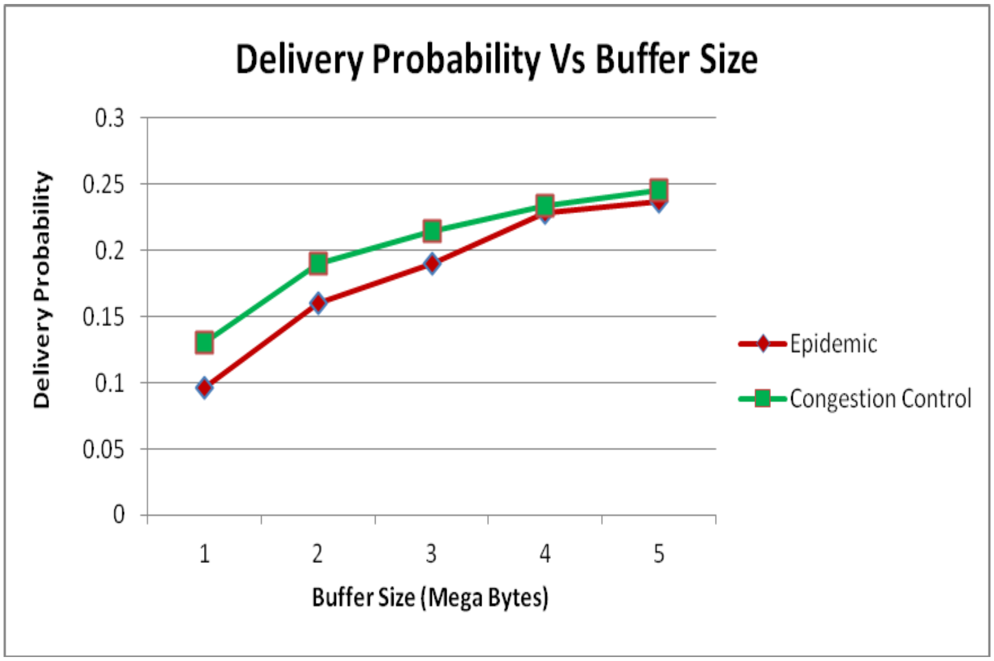


Fig. 5.14. Delivery Probability versus Buffer size

Fig. 5.14 describes a plot of the delivery probability vs. the buffer size. Size of buffer is directly proportional to the delivery probability, the buffer size increases and the packet delivery probability also increases. Epidemic and congestion control average delivery probabilities are 0.18236 and 0.2026 respectively. The projected algorithm shows that congestion control having probability of higher average delivery as compare with the epidemic protocol.

CHAPTER 6
CONCLUSION AND FUTURE WORK

6.1 Conclusion

Opportunistic network is an interesting technology for realising the ubiquitous vision. In this project, a new routing protocol named as RFEP has been projected for Oppnets which is an improvement of Epidemic routing protocol. This protocol tries to decrease the amount of flooding done as in the Epidemic protocol. RFEP performs significantly good with respect to the overhead ratio and the number of message(s) delivered. A congestion awareness forwarding scheme is proposed here that proves the performance of the routing protocol is further improved when the congestion in the oppnet is also considered. Packets forwarding based the social metric, node resources metric and network consideration leads to a fairer distributions of the load all through the network. It is used to Select multiple nodes on the basis of utility metrics and threshold lead to very less overhead ratio, high delivery probability, smaller number of packets dropped, and low delay.

6.2 Future Work

In future work, message acknowledgements may be introduced in the RFEP routing protocol and compare this with already existing routing protocol such as ProPhet, Spray and wait etc. Further evaluate the performance of RFEP protocol by varying parameters like Time to Live and speed of the nodes. The performance of the congestion control router is further improved by considering the probability of the next node meeting the packet at destination node. Work is to be done on further reducing to control overhead by keeping the high delivery probability.

References

[1] S. K. Dhurandher, D. K. Sharma, I. Woungang, and H.C. Chao, “Performance Evaluation of Various Routing Protocols in Opportunistic Networks”, *in Proceedings of IEEE GLOBECOM Workshop 2011*, Houston, Texas, USA , 5-9 December, 2011, pp. 1067-1071.

[2] Z. Zhang, “Routing in Intermittently Connected Mobile Ad Hoc Networks and Delay Tolerant Networks: Overview and Challenges”, *IEEE Communications Surveys and Tutorials*, Vol: 8, Issue: 1, 2006, pp. 24-37.

[3] M. Radenkovic, A. Grundy, "Decongesting Opportunistic Social-based Forwarding", IEEEIIFJP WONS - Iile Seventh International Conference on Wireless On-demand Network Systems and Services, p. 82- 85, February 20 I O.

[4] M. Radenkovic, A. Grundy, "Congestion Aware Forwarding in Delay Tolerant and Social Opportunistic Networks", Proc. 8th Inti. Conf. on Wireless On-Demand Network Systems and Services, Bardonecchia, Italy, p. 60-67, January 2011.

[5] M. Radenkovic, A. Grundy, "Framework for Utility Driven Congestion Control in Delay Tolerant Opportunistic Networks", 7th Inti. Conf. on Wireless Communications and Mobile Computing, Istanbul, p. July 201, 448-454

[6]. Sanjay K. Dhurandher, CAITFS, Netaji Subhas Institute of Technology, Sudip Misra Indian Institute of Technology, Kharagpur, India Harsh Mittal, Anubhav Agarwal, Netaji Subhas Institute of Technology: Ant Colony Optimization-Based Congestion Control, in Ad-hoc Wireless Sensor Networks, 978-1-4244-3806-8/09/$25.00 © 2009 IEEE.

[7] L-J. Chen, C. Hung Yu, C. Tseng, H. Chu, and C. Chou, “A Content-Centric Framework for effective Data Dissemination in Opportunistic networks”, *IEEE Journal on selected Areas in Communications*, vol: 26, Issue: 5, June 2008, pp. 761-772.

[8] Chung-Ming Huang, Kun-chan Lan and Chang-Zhou Tsai, Department of Computer Science and Information Engineering, National Cheng Kung University, Tainan, Taiwan, R.O.C., A Survey of Opportunistic Networks -
978-0-7695-3096-3/08 $25.00 © 2008 IEEE, DOI 10.1109/WAINA.2008.292

[9] Sanjay Kumar Dhurandher, Information Technology, NSIT, Deepak Kumar Sharma, Computer Engineering, NSIT, Isaac Woungang_ Computer Science, Ryerson University - Energy-based Performance Evaluation of Various Routing Protocols in Infrastructure-less Opportunistic Networks. Journal of Internet Services and Information Security (JISIS), volume: 3, number: 1/2, pp. 37-48

[10] Peter P. Pham, Sylvie Perreau Increasing the network performance using multi-path routing mechanism with load balance Ad Hoc Networks, 2 (4)

[11] J. Pujol, A. Toledo, and P. Rodriguez, "Fair Routing in Delay Tolerant Networks", IEEE INFO COM, p. 837-845, 2009.

[12] A Novel Multipath Load Balancing Approach Using Fibonacci Series for Mobile Ad Hoc Networks*Yahya M. Tashtoush and Omar A. Darwish*IJCTE 2012 Vol.4(2): 220-225 ISSN: 1793-8201 DOI: 10.7763/IJCTE.2012.V4.455

[13] QoS routing with traffic distribution in mobile ad hoc networks Gabriel Ioan Ivascu, Samuel Pierre, Alejandro Quintero * Mobile Computing and Networking Research Laboratory (LARIM), Department of Computer Engineering, École Polytechnique de Montréal,

[14] Investigation of Adaptive Multipath Routing For Load Balancing In MANET Bhavana Sharma, Shaila Chugh, Vishmay Jain: International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-5, June 2013

[15] S.c. Nelson, M. Bakht, R. Kravets, S. HarrislII: "Encounter: based routing in DTNs", IEEE Infocom, p. 846-854, April 2009.

[16] P. Hui, J. Crowcroft, and E. Yoneki, "Bubble rap: social-based forwarding in delay tolerant networks," in ACM MoblHoc, p. 241-250, 2008.

[17] R.L Ciobanu, "Reducing Congestion for Routing Algorithms in Opportunistic Networks with Socially Aware Node Behavior Prediction", IEEE 27th International Conference on Advanced InformatIOn Networkmg and ApplicatIOns (AlNA), Barcelona, p. 554-551,2013

[18] A. Vahdat, D. Becker. “Epidemic routing for partially connected ad hoc networks”. *Technical Report CS-2000-06, Dept. of Computer Science, Duke University*, Durham, NC, 2000.

[19] A.S. Tenanbaum, Computer networks, *3rd edition, patiance-Hall interantional,* 1996.

[20] T. Kathiravelu, N. Ranasinghe, and A. Pears, *Towards designing a routing protocol for opportunistic networks*, in Proceedings of the International Conference on Advances in ICT for Emerging Regions (ICTer2010), Colombo, Sri Lanka, September 2010, pp. 56–61.

[21] E. Daly and M. Haahr, "Social network analysis for information flow in disconnected Delay-Tolerant MANETs," IEEE Trans. Mob. Comp, vol. 8, no. 5, pp. 606–621, 2009.

[22] Nikhil Khichariya,2Neha Choubey, M.Tech.Scholar, Computer Technology (CSE), RCET, BHILAI, C.G., India, Asst.Professor, CSE Department, RCET, BHILAI, International Journal of Advanced and Innovative Research Designing an Efficient Routing Protocol for Opportunistic Network (2278-7844) / # 89 / Volume 3 Issue 8.

[23] Luciana Pelusi, Andrea Passarella, and Marco Conti *Pervasive Computing and Networking Laboratory (PerLab),* IIT-CNR, Via G. Moruzzi, *Opportunistic Networking: Data Forwarding in Disconnected Mobile Ad hoc Networks,–* 56124 Pisa, Italy, This work was partially funded by the Information Society Technologies program of the European Commission under the HAGGLE (027918) FET-SAC project.

[24] Thabotharan Kathiravelu, Nalin Ranasinghe, Arnold Pears 2011 6th International Conference on Industrial and Information Systems- An Enhanced Congestion Aware Adaptive Routing, Protocol for Opportunistic Networks, ICIIS 2011, Aug. 16-19, 2011.

[25] Tossaphol Settawatcharawanit∗, Shigeki Yamada†, Md. Enamul Haque‡, Kultida Rojviboonchai, ∗§Department of Computer Engineering, Chulalongkorn University, National Institute of Informatics (NII), Tokyo - Message Dropping Policy in Congested Social Delay Tolerant Networks - Japan 2013 10th International Joint Conference on Computer Science and Software Engineering (JCSSE).

[26] Apu Kapadiay, MIT Lincoln Laboratory, Lexington, MA USA, David Kotz
Institute for Security, Technology, and Society, Dartmouth College
Hanover, NH USA.Opportunistic Sensing: Security Challenges for the New Paradigm.