SIMULATION STUDY OF FEEDBACK BASED TCP PROTOCOL FOR IMPROVING THE PERFORMANCE OF TCP AND VARIOUS DESIGN ISSUES IN MANETS

DISSERTATION

Submitted in partial fulfillment of the

Requirement for the award of the Degree of

MASTER OF TECHNOLOGY

In

(ELECTRONICS & COMMUNICATION ENGINEERING)

By

P. S. B. N. G. RAMESH

Registration No: 11503217

Under the guidance of

Mrs. REENA AGGARWAL

(Assistant Professor)

(School of Electronics and Electrical Engineering)

Lovely Professional University

Phagwara, Punjab

April 2017

CERTIFICATE

This is to certify that the Dissertation entitled **"Simulation study of feedback based TCP protocol for improving the performance of TCP and various design issues in MANETs"** is a record of bonafied work carried out by **P. S. B. N. G. Ramesh (11503217)** under my guidance and supervision for the partial fulfillment of the degree of Master of Technology in Electronics and Communication Engineering at Lovely Professional University, Phagwara.

To the best of my knowledge, the results embodied in this Dissertation work have not been submitted to any university or institute for the award of any degree or diploma.

Dissertation Supervisor
Mrs. Reena Aggarwal
Assistant Professor
Department of ECE
Lovely Professional University
Phagwara

Head of Department
Mr. Lavish Kansal
Assistant Professor
Department of ECE
Lovely Professional University
Phagwara

Examiner I

Examiner II

ACKNOWLEDGEMENT

I take this opportunity to acknowledge the co-operation, good will and both moral and technical support extended by several individuals out of which this Dissertation has evolved. I always cherish my association with them.

I express my sincere and deepest regards to my supervisor **Mrs. Reena Aggarwal** for her valued guidance during this period of my Dissertation. This Dissertation work was enabled and sustained by her vision and ideas. Her scholarly guidance and invaluable suggestions motivated me to complete my Dissertation work successfully.

I owe a great many thanks to **Mrs. Reena Aggarwal** for spending her valuable time. I considered my-self extremely fortunate to have this opportunity of associating with her.

I express my sincere thanks to Dean of Academics, Head of the department (ECE) and the members of Department of Electronics and Communication Engineering, Lovely Professional University for their cooperation.

I would like to express my deep gratitude to my parents. Their continuous love and support gave me strength for pursuing my dream.

Last but not the least, I am thankful to my friends who have been a source of encouragement and inspiration throughout the duration of this Dissertation.

DECLARATION

I here by declare that the work presented in this Dissertation entitled " **Simulation study of feedback based TCP protocol for improving the performance of TCP and various design issues in MANETs** " in partial fulfillment of the requirements of the award of degree of M.Tech (Electronics and Communication Engineering), submitted at department of Electronics and Communication Engineering, Lovely Professional University, Phagwara is an authentic record of my own work under supervision of Mrs. Reena Aggarwal. The matter presented in this report has not been submitted in any other University/Institute for the award of M.Tech Degree or any other Diploma/Degree.

Signature of the Student

This is to certify that the above statement made by the candidate is correct to the best of my knowledge.

Signature of the Supervisor

Mrs. Reena Aggarwal

The M. Tech Viva-Voce Examination of P. S. B. N. G. Ramesh has been held on_________ and accepted.

.

ABSTRACT

The Mobile Ad hoc Networks (MANET) is a set of wireless mobile nodes. These nodes dynamically form spontaneous network which works without centralized administration. Due to this characteristic, there are some challenges that protocol designers and network developers are faced with. These challenges include routing, service and frequently topology changes. Therefore routing discovery and maintenance are critical issues in these networks. There are also limited battery power and low bandwidth available in each node. The Transmission Control Protocol (TCP) was designed to provide reliable end-to-end delivery of data over unreliable networks. In practice, most TCP deployments have been carefully designed in the context of wired networks. Ignoring the properties of wireless ad hoc networks can lead to TCP implementations with poor performance. Indeed, in mobile or static ad hoc networks losses are not always due to network congestion, as it is mostly the case in wired networks. So, by analyzing all these performance degrading issues, a model was developed which introduces feedback in the TCP with the adaptive back-off response. The various factors that influence the performance of the TCP are throughput, end to end delay, routing overhead, packet delivery ratio. This model reduced the performance degradation in TCP by improving the throughput, reducing the packet loss as well as the delay and further classified the feedback based TCP with adaptive back-off response into Full congestion window TCP (Fcwnd-TCP) and Partial congestion window TCP (Pcwnd-TCP) on the basis of the effective utilization of the size of the congestion window. In this report, the comparative analysis of Standard-TCP with the Feedback based TCP with adaptive back-off response was done with various performance parameters and it was found from the analysis that feedback TCP gave the optimized performance with the standard one.

LIST OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

AODV	Ad hoc On Demand Distance Vector (Routing)
AOMDV	Ad hoc On Demand Multiple Distance Vector (Routing)
CGSR	Cluster-head Gateway Switch Routing Protocol
DARPA	Defense Advanced Research Projects Agency
DSR	Dynamic Source Routing
MANET	Mobile Ad hoc network
TCP	Transmission Control Protocol
RADAR	Radio Detecting and Ranging
Wi-Fi	Wireless Fidelity
GSM	Global System for Mobile Communication
WLAN	Wireless Local Area Network
Wi-MAX	Worldwide Interoperability for Microwave Access
PCMCIA	Personal Computer Memory Card International Association
SURAN	Survivable Radio Network
JTRS	Joint Tactical Radio System
NTDR	Near Term Digital Radio
IEEE	Institute of Electricals and Electronics Engineers
CPU	Central Processing Unit
TORA	Temporally Ordered Routing Algorithm
HSR	Hierarchical State Routing
ZRP	Zone Routing Protocol

LMR	Light-Weight Mobile Routing
ABR	Associativity-Based Routing
SSA	Signal Stability-Based Adaptive Routing Protocol (SSA)
SHARP	Sharp Hybrid Adaptive Routing Protocol
LANMAR	Landmark Ad Hoc Routing Protocol
GPS	Global Positioning System
RTT	Round Trip Delay Time
QOS	Quality of Service
RFN	Route Failure Notification
RRN	Route Re-Establishment Notification
FP	Failure Point
TCP-F	Transmission Control Protocol with Feedback
IETF	Internet Engineering Task Force
S-TCP	Standard Transmission Control Protocol
A-TCP	Ad hoc Transmission Control Protocol
ELFN	Explicit Link Failure Notification
SACK	Selective Acknowledgement
IP	Internet protocol
PDU	Protocol Data Unit
NS2	Network Simulator
MH	Mobile Host
ERDN	Explicit Route Disconnection Notification
ERSN	Explicit Route Successful Notification

ICMP	Internet Control Message Protocol
ECN	Explicit Congestion Notification
BER	Bit Error Rate
UDP	User Datagram Protocol
FTP	File Transfer Protocol
HTTP	Hyper Text Transfer Protocol
DNS	Domain Name Server
ARP	Adaptive Routing Protocol
SMTP	Simple Mail Transfer Protocol
TMTP	Trivial File Transfer Protocol
BOOTP	Bootstrap Protocol
DHCP	Dynamic Host Configuration Protocol
RARP	Reverse Address Resolution Protocol
IGMP	Internet Group Message Protocol
OSI	Open System Interconnection
DREAM	Distance Routing Effect Algorithm for Mobility
GPSR	Greedy Perimeter Stateless Routing
IARP	Intra Zone Routing Protocol
DRP	Dynamic Routing Protocol
SST	Signal Stability Table
SRT	Static Routing Protocol
OSPF	Open Shortest Path First
OLSR	Optimized Link State Routing

CHAPTER 1 INTRODUCTION

1.1 Introduction to Wireless Communication

Wireless networks are very important in communication equipment. At present they are used in various industrial, military applications and networks which are personalized. The primary difference between wired network and wireless networks was the channel of communication. In wired networks physical medium is present, where as in case of wireless networks, there is no physical medium. Wireless networks are very popular networks in wide variety of applications by considering some of the following factors like reliability, easy to install, bandwidth, operating cost, security, amount of power required to operate and network performance [1]. All these networks rely on infrastructures which are fixed. Some of the most common wireless networks which are based on infrastructure are cellular networks, RADAR, cordless telephone, Wi-MAX, GSM, WLAN, Wi-Fi, Satellite communication, Microwave communication and Cordless Telephone etc.

A MANET is obtained without the need of centralized structures by a group of mobile nodes which forms an ad-hoc network. These networks are very advantageous for establishment because they are fit in an environment where the loss of infrastructure is acceptable and they are not that much effective in cost. The most famous IEEE 802.11 is a "Wi-Fi" protocol can provide facilities of ad-hoc network at very low level even through when there is no point to access, whereas the mobile nodes were restricted to receive and send information. But, across the network, they does not route anything. These networks can function in a way such that they did not depend on anything else or they will connect to a larger network, e.g. Internet. These networks contains a set of using wireless links in which mobile hosts uses to communicate among them, without using any other support of communication. These can be called as multi-hop wireless networks or mobile radio networks. When two or more Mobile Hosts (MHs) are in the range of each other if one mobile host can receive other mobile host's transmission. Every Mobile Host works in a co-operative manner such that each acts as a router and it allows data packets which are directed towards other Mobile Hosts through which they pass. One of the typical applications is a military operation or a recovering from a disaster [2]. These are not confined to specific kind of situations; in some other locations also the performance of these networks are far much better. The classification of Wireless Ad hoc network is as shown in the figure 1.1. For example, imagine a situation of people in a company with laptops, in a conference meeting in the absence of any kind of network services. They make their machines to work by simply forming an ad hoc network. It is one of the examples where ad-hoc networks were used.

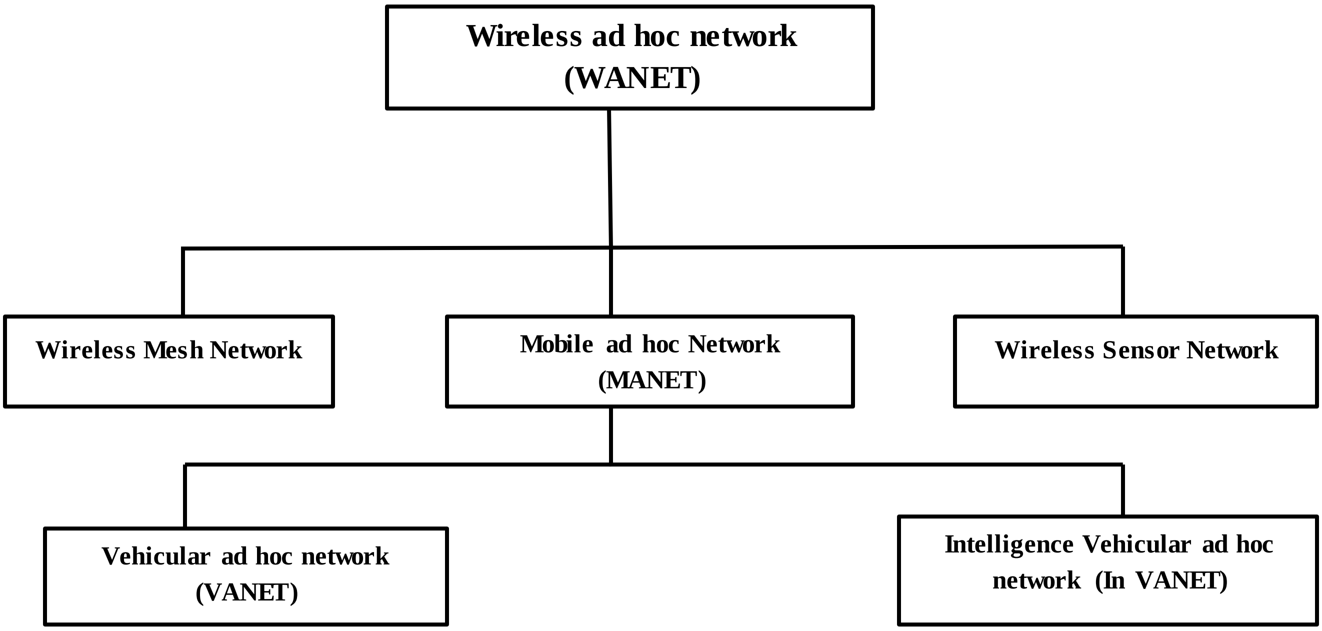

Wireless ad hoc network (WANET)
Wireless Mesh Network
Mobile ad hoc Network (MANET)
Wireless Sensor Network
Vehicular ad hoc network (VANET)
Intelligence Vehicular ad hoc network (In VANET)

Figure 1.1 Classifications of Ad hoc Networks

1.2 Wireless Networks

Wireless networks use some sort of radio frequencies in air to transmit and receive data instead of using some physical cables. The most admiring fact in these networks is that it eliminates the need for laying out expensive cables and maintenance costs. In general, mobile wireless networks can be classified into two types.

1.2.1 Infra-structured Networks

Wireless mobile networks have traditionally been based on the cellular concept and relied on good infrastructure support in which mobile devices communicate with access points like base stations connected to the fixed network infrastructure. Ex: GSM, WLAN, etc

A simple Infra-structured Network is shown in the figure 1.2

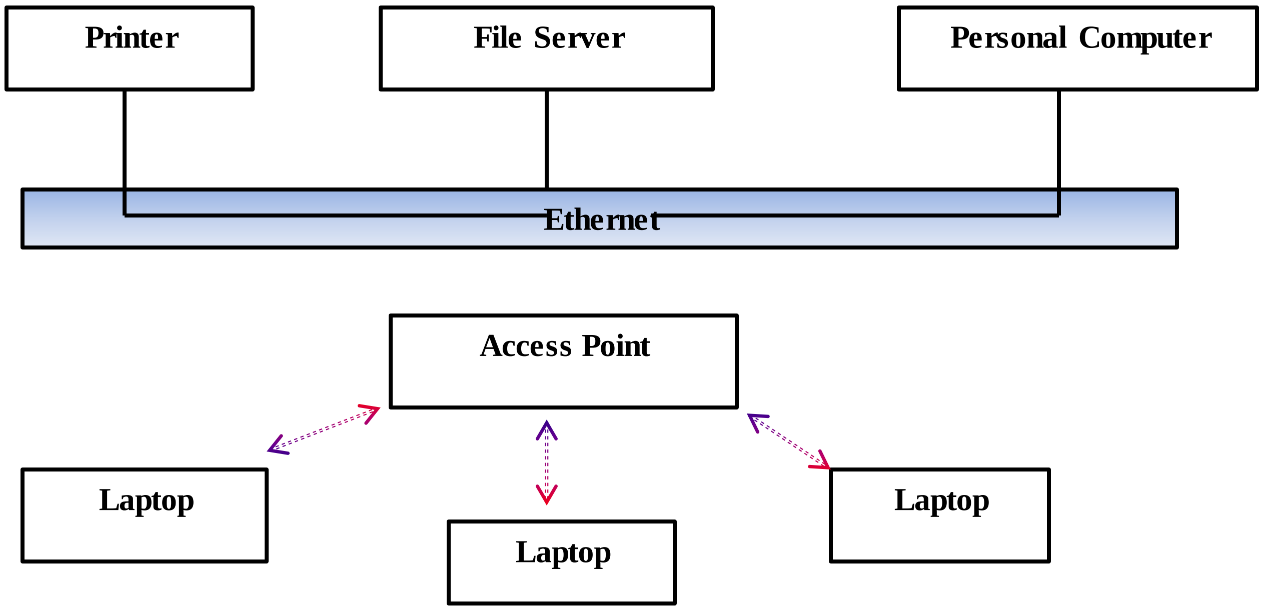


Figure 1.2 Infra-structured Network

1.2.2 Infrastructure less network (Ad-hoc networks)

Wireless nodes can dynamically form a network to exchange information without using any pre-existing fixed network infrastructure [3]. A simple Infra-structure less network is shown in the figure 1.3. This is a very important part of communication technology that supports truly pervasive computing, because in many contexts information exchange between mobile units cannot rely on any fixed network infrastructure, but on rapid configuration of a wireless connections on-the-fly.

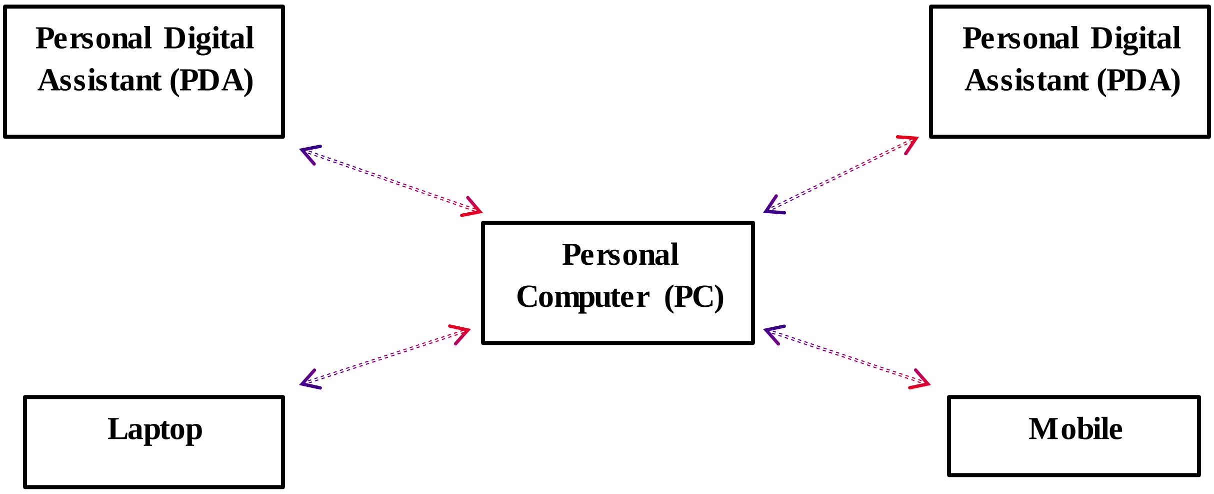

Personal Digital Assistant (PDA)
Personal Digital Assistant (PDA)
Personal Computer (PC)
Laptop
Mobile

Figure 1.3 Infra-structure less Network

Advantages of Wireless Networks

- Setting up a wireless system is easy and fast and it eliminates the need for pulling out the cables through walls and ceilings.
- Network can be extended to places which cannot be wired.

Disadvantages of Wireless Networks

- Interference due to weather, other radio frequency devices, or obstructions like walls.
- The total throughput is affected when multiple connections exists.

1.3 Problems in Wireless communications

Some of the problems related to wireless communication are multipath propagation, path loss, interference, and limited frequency spectrum. Multipath propagation is when a signal travels from its source to destination, in between there are obstacles which make the signal propagate in paths beyond the direct line of sight due to reflections, refraction and diffraction and scattering [4]. Path loss is the attenuation of the transmitted signal strength as it propagates away from the sender. Path loss can be determined as the ratio between the powers of the transmitted signal to the receiver signal. This is mainly dependent on a number of factors such as radio frequency and the nature of the terrain. It is sometimes important to estimate the path loss in wireless communication networks.

Due to the radio frequency and the nature of the terrain are not same everywhere, it is hard to estimate the path loss during communication. During communication a number of signals in the atmosphere may interfere with each other resulting in the destruction of the original signal. Limited Frequency Spectrum is where, frequency bands are shared by many wireless technologies and not by one single wireless technology.

1.4 About MANET

MANET is a collection of wireless mobile nodes, which dynamically form a temporary network, without using any existing network infrastructure or centralized administration. These are often called infrastructure-less networking since the mobile nodes in the network dynamically establish routing paths between themselves. Current typical applications of a MANET include battlefield coordination and onsite disaster relief management.

Ad hoc is a Latin phrase which means “for this purpose”. It generally signifies a solution designed for a specific problem or task. Mobile ad hoc network, known as MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. A simple Ad hoc Network containing Laptops and Mobiles connected is shown in the figure 1.4. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activity including discovering the topology and delivering messages must be executed by the nodes themselves, i.e. routing functionality will be incorporated into mobile nodes.

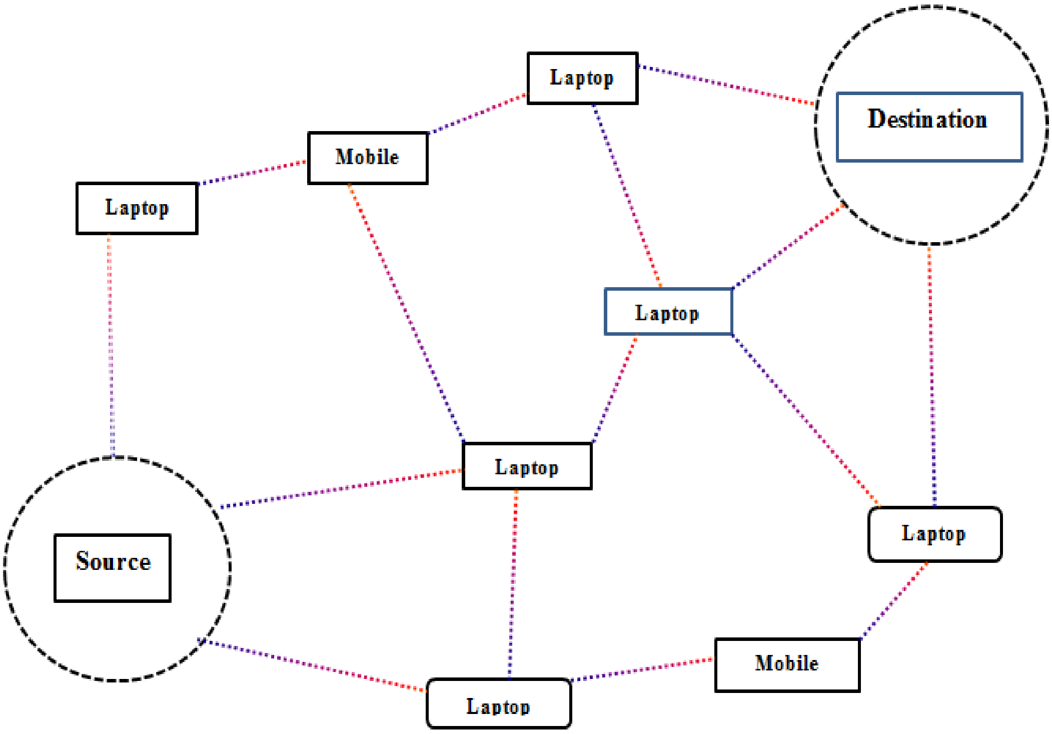


Figure 1.4 Ad hoc Network

1.5 The background of Mobile ad hoc network

Mobile ad hoc networking is a technology under development for the last 20 years principally through research funding sponsored by the U.S Government. It is somewhat synonymous with mobile packet radio networking (a term coined via during early military research in the 70's and 80's), Mobile mesh networking (a term that appeared in an article in The Economist regarding the structure of future military networks) and Mobile, Multi-hop, Wireless, Networking (perhaps the most accurate term, although a bit cumbersome). In the 1990s, the concept of commercial ad-hoc networks arrived with notebook computers and other viable communications equipment [5]. At the same time, the idea of a collection of mobile nodes was proposed at several research conferences. The IEEE 802.11 subcommittee had adopted the term "ad-hoc networks" and the research community had started to look into the possibility of deploying ad-hoc networks in other areas of application. Meanwhile, work was going on to advance the previously built ad-hoc networks.

Later on in mid-1990s, within the Internet Engineering Task Force (IETF), the Mobile ad hoc networking working group was formed to standardize routing protocols for ad-hoc networks. The development of routing within the working group and the larger community resulted in the invention of reactive and proactive routing protocols [6]. Soon after, the IEEE 802.11 subcommittee standardized a medium access protocol that was based on collision avoidance and tolerated hidden terminals, making it usable for building mobile ad hoc networks prototypes out of notebooks and 802.11 PCMCIA cards. Hyper LAN and Bluetooth were some other ad-hoc network standards that addressed and benefited ad-hoc networking.

The earliest MANETs were called "packet radio" networks, and were sponsored by DARPA in the early 1970s. BBN Technologies and SRI International designed, built, and experimented with these earliest systems. Experimenters included Jerry Burchfield, Robert Kahn, and Ray Tomlinson of later TENEX, Internet and email fame. It is interesting to note that these early packet radio systems predated the Internet, and indeed were part of the motivation of the original Internet Protocol suite. Later DARPA experiments included the Survivable Radio Network (SURAN) project, which took place in the 1980s. Another third wave of academic activity started in the mid-1990s with the advent of inexpensive 802.11 radio cards for personal computer. Current MANETs are designed primary for military utility; examples include JTRS and NTDR. The popular IEEE 802.11 ("Wi-Fi") wireless protocol incorporates an ad-hoc networking system when no wireless access points are present, although it would be considered a very low grade ad-hoc protocol by specialists in the field. The IEEE 802.11 system only handles traffic within a local "cloud" of wireless devices. Each node transmits and receives data, but does not route anything between the network's systems. However, higher-level protocols can be used to aggregate various IEEE ad-hoc networks into MANETs.

The MIT Media Lab $100 laptop program hopes to develop a cheap laptop for mass distribution (>1 million at a time) to developing countries for education. The laptops will use ad hoc wireless mesh networking to develop their own communications network out of the box.

As a new technology for information acquisition, the mobile ad-hoc network is of high research value and wide application prospects. It has become hot off the press in the last ten years in the globe. Owing to its mobility, dynamic topology, equivalence, self-organizing and other unique features, it has great advantages in emergency communications and military mobile communications. Routing is one of the core issues in mobile ad-hoc network. An effective routing mechanism will be helpful to extend the successful deployment of mobile ad-hoc network. In this thesis, a brief introduction of the mobile ad-hoc network definition, main features, network structure and applications will be given in the first place.

1.6 Characteristics of MANETs

A MANET consists of mobile platforms (e.g., a router with multiple hosts and wireless communications devices)—here in simply referred to as "nodes"--which are free to move about arbitrarily. The nodes may be located in or on airplanes, ships, trucks, cars, perhaps even on people or very small devices, and there may be multiple hosts per router.

A MANET is an autonomous system of mobile nodes. The system may operate in isolation, or may have gateways to and interface with a fixed network. In the latter operational node, it is typically envisioned to operate as a "stub" network connecting to a fixed internet work. Stub networks carry traffic originating at and/or destined for internal nodes, but do not permit exogenous traffic to "transit" through the stub network. MANET nodes are equipped with wireless transmitters and receivers using antennas which may be omnidirectional (broadcast), highly-directional (point-to-point), possibly steerable, or some combination thereof [7]. At a given point in time, depending on the nodes' positions and their transmitter and receiver coverage patterns, transmission power levels and co-channel interference levels, a wireless connectivity in the form of a random, multi-hop graph or "ad hoc" network exists between the nodes. This ad hoc topology may change with time as the nodes move or adjust their transmission and reception parameters.

1) Dynamic topologies: Nodes are free to move arbitrarily; thus, the network topology which is typically multi-hop--may change randomly and rapidly at unpredictable times, and may consist of both bidirectional and unidirectional links.

2) Bandwidth-constrained: Wireless links will continue to have significantly lower capacity than their hardwired counterparts. In addition, the realized throughput of wireless communications--after accounting for the effects of multiple access, fading, noise, interference conditions, etc is often much less than a radio's maximum transmission rate.

One effect of the relatively low to moderate link capacities is that congestion is typically the norm rather than the exception, i.e. aggregate application demand will likely approach or exceed network capacity frequently. As the mobile network is often simply an extension of the fixed network infrastructure, mobile ad hoc users will demand similar services. These demands will continue to increase as multimedia computing and collaborative networking applications rise.

3) Energy: Some or all of the nodes in a MANET may rely on batteries or other exhaustible means for their energy. For these nodes, the most important system design criteria for optimization may be energy conservation.

4) Limited physical security: Mobile wireless networks are generally more prone to physical security threats than are fixed-cable nets [8]. The increased possibility of eavesdropping, spoofing, and denial-of-service attacks should be carefully considered. Existing link security techniques are often applied within wireless networks to reduce security threats. As a benefit, the decentralized nature of network control in MANETs provides additional robustness against the single points of failure of more centralized approaches.

In addition, some envisioned networks (e.g. mobile military networks or highway networks) may be relatively large (e.g. tens or hundreds of nodes per routing area). The need for scalability is not unique to MANETS.

These characteristics create a set of underlying assumptions and performance concerns for protocol design which extend beyond those guiding the design of routing within the higher-speed, semi-static topology of the fixed Internet.

1.7 End-to-End service over Hop-by-Hop infrastructure

Current trend in networking shows a paradigm shift towards end-to-end service. Given the plethora of network services either implemented or in the stage of development, it is nearly impossible to design a networking infra-structure keeping all of them in mind. Such an attempt will result in huge information being stored per hop to understand and route traffic and this will result in an explosion of state information per hop. The right way to approach the problem is to concentrate on designing a networking infrastructure which will satisfy a few basic requirements and constraints. Then various end-to-end services can then be built over that infrastructure.

1.8 Applications

Ad-hoc networks are suited for use in situations where an infrastructure is unavailable or to deploy one is not cost-effective. One of many possible uses of mobile ad-hoc networks is in some business environments, where the need for collaborative computing might be more important outside the office environment than inside, such as in a business meeting outside the office to brief clients on a given assignment.

A mobile ad-hoc network can also be used to provide crisis management services applications, such as in disaster recovery, where the entire communication infrastructure is destroyed and recovering communication quickly is crucial. By using a mobile ad-hoc network, an infrastructure could be set up in hours instead of weeks, as is required in the case of wired line communication [9]. Another application example of a mobile ad-hoc network is Bluetooth, which is designed to support a personal area network by eliminating the need of wires between various devices, such as printers and personal digital assistants. The famous IEEE 802.11 or Wi-Fi protocol also supports an ad-hoc network system in the absence of a wireless access point.

Similar but more constrained applications are also found in the military domain. Search and rescue missions, potentially in a hostile environment, not only require networking of troops to assure command and control and to avoid friendly fire even in heterogeneous coalition environments but also add concerns about emanation security, jamming, and compromised nodes to the threat environment to be considered.

1.9 Routing in MANET

Mobile Ad-hoc networks are self-organizing and self-configuring multi-hop wireless networks, where the structure of the network changes dynamically. This is mainly due to the mobility of the nodes. Nodes in these networks utilize the same random access wireless channel, cooperating in an intimate manner to engage them in multi-hop forwarding. The node in the network not only acts as hosts but also as routers that route data to/from other nodes in network. In mobile ad-hoc networks there is no infrastructure support as is the case with wireless networks, and since a destination node might be out of range of a source node transferring packets, so there is need of a routing procedure. This is always ready to find a path so as to forward the packets appropriately between the source and the destination. Within a cell, a base station can reach all mobile nodes without routing via broadcast in common wireless networks. In the case of ad-hoc networks, each node must be able to forward data for other nodes. This creates additional problems along with the problems of dynamic topology which is unpredictable connectivity changes.

1.9.1 Properties of Ad-Hoc routing protocols:

The properties that are desirable in Ad-Hoc Routing protocols are:

i. Distributed operation: The protocol should not depend on centralized controlling node and should be in a distributed manner which is the case for stationary networks. Due to mobility the network can be partitioned, as a result of dissimilarity, the nodes in an ad-hoc network can enter or leave the network very easily

ii. Loop free: To improve the overall performance, the routing protocol should assurance that the routes supplied are loop free. This avoids any misuse of bandwidth or CPU consumption.

iii. Demand based operation: To minimize the control overhead in the network and thus not misuse the network resources the protocol should be reactive [10]. This means that the protocol should react only when needed and should not periodically broadcast control information.

iv. Unidirectional link support: The radio environment can cause the formation of unidirectional links. Utilization of these links and not only the bi-directional links improves the routing protocol performance.

v. Security: The radio environment is especially vulnerable to impersonation attacks so to ensure the wanted behavior of the routing protocol some sort of security measures is necessary. Authentication and encryption is the way to go and problem here lies within distributing the keys among the nodes in the ad-hoc network.

vi. Power conservation: The nodes in the ad-hoc network can be laptops and thin clients such as PDAs that are limited in battery power and therefore uses some standby mode to save the power. It is therefore very important that the routing protocol has support for these sleep modes.

vii. Multiple routes: To reduce the number of reactions to topological changes and congestion multiple routes can be used. If one route becomes invalid, it is possible that another stored route could still be valid and thus saving the routing protocol from initiating another route discovery procedure.

viii. Quality of Service Support: Some sort of Quality of service is necessary to incorporate into the routing protocol. This helps to find what these networks will be used for. It could be for instance real time traffic support.

1.10 Problems in Mobile Ad hoc Networks

i. Asymmetric links: Most of the wired networks rely on the symmetric links which are always fixed [11]. But this is not a case with ad-hoc networks as the nodes are mobile and constantly changing their position within network. The three types of asymmetric links are Bandwidth Asymmetry, Loss rate asymmetry and route asymmetry.

a) Bandwidth asymmetry: One of the networks which experience bandwidth asymmetry of highest value are Satellite networks which was due to different engineering tradeoffs like mass, volume and power. For majority of the space applications, the data will be transmitted from satellite to the earth station. But the link from the earth station to the satellite will not be used frequently for transferring of data. In case of broadcast satellites the ratio of the satellite to earth link bandwidth to the earth to satellite link bandwidth is approximately 1000. In Ad hoc networking, the value of asymmetric nature of bandwidth is not huge value. In majority of the ad hoc networks, the ratio of the bandwidth will be between 3 and 54. The causes of this asymmetric nature are due to transmission rates of different values. Due to different rate of transmissions, even though the paths are symmetric from source to destination, the links will experience bandwidth asymmetry.

b) Loss rate asymmetry: Loss rate asymmetry occurs when the backward path is having more lossy nature when compared to forward path. In Ad hoc networking, this asymmetric nature occurs due to packet losses and this changes from location to location. It is found that loss rate asymmetry is one cause of bandwidth asymmetry. In case of multi-rate IEEE 802.11 protocols, senders will use the algorithm of Auto-Rate-Fallback (ARF) algorithm for selecting the rate of transmission. With the help of Auto-Rate-Fallback algorithm, senders will try to utilize more rate of transmission after the successful consecutive transmissions and will go back to lesser rate of transmissions after observing the failure of transmission. Lower rate of transmission will be used when the loss rate is high.

c) Route asymmetry: Route asymmetry is different from other two forms of asymmetry like Bandwidth Asymmetry and Loss rate Asymmetry, even the path from sender to receiver and the receiver to the sender is same, and in case of route asymmetry different paths can be used for sending TCP data and receiving the TCP Acknowledgements. If the rate of mobility of nodes is very high, then Route asymmetry will increase the routing overheads and loss of packet [12]. When nodes are moving and utilizing different forward and reverse routes, it will increase the failure of routes. But in static networks or networks having less mobility rate, the lifetime of the routes in the network is high. The protocols of routing have to select the symmetric paths if those routes are available in Ad hoc networks having high rate of mobility.

ii. Routing Overhead: In wireless ad hoc networks, nodes often change their location within network. So, some stale routes are generated in the routing table which leads to unnecessary routing overhead.

iii. Interference: This is the major problem with mobile ad-hoc networks as links come and go depending on the transmission characteristics, one transmission might interfere with another one and node might overhear transmissions of other nodes and can corrupt the total transmission.

iv. Dynamic Topology: Since the topology is not constant; so the mobile node might move or medium characteristics might change. In ad-hoc networks, routing tables must somehow reflect these changes in topology and routing algorithms have to be adapted. For example in a fixed network routing table updating takes place for every 30sec. This updating frequency might be very low for ad-hoc networks.

v. Lossy Channels: The main reasons for the occurrence of errors in wireless channel are Signal attenuation, Doppler Shift and Multipath fading.

a) Signal Attenuation: When electromagnetic waves are travelling in free space from transmitter to receiver the strength of the electromagnetic signals decreases with respect to increase in distance away from the transmitter and intensity electromagnetic radiation is very low at the receiver, which gives rise to lower signal-to-noise ratio (SNR) at the receiver.

b) Doppler shift: Doppler shift occurs as a result of the relative motion of the transmitter and the receiver [13]. Doppler shift results in frequency shifts of the arriving signal, so it is difficult for the signal to reach successfully at the receiver without changing the frequency values of the signal.

c) Multipath fading: Multipath fading occurs when the electromagnetic waves which are traveling from transmitter to receiver in free space over multiple paths undergo reflection and diffraction from various objects like tall buildings, mountains and heavy structural constructions and it results in fluctuations of signals in the phase, amplitude and geographical angle of the signal which is received at the receiver.

vi. Hidden and Exposed stations: In Ad hoc networking, stations depend on the mechanism of physical carrier-sensing to find the idle channel. This kind of sensing mechanism will not solve the hidden and exposed station problems.

1.11 Congestion control in MANET

To maintain and allocate network resources effectively and fairly among a collection of users is a major issue. The resources shared mostly are the bandwidth of the links and the queues on the routers or switches. Packets are queued in these queues awaiting transmission. When too many packets are contending for the same link, the queue overflows and packets have to be dropped. When such drops become common events, the network is said to be congested. In Ad-hoc networks, since there is no fixed infrastructure there are no separate network elements called routers and hence the mobile nodes themselves act as the routers (i.e. they are responsible for routing the packets). Congestion control methods can be router centric or host/node centric. In existing congestion control methods, the source is informed about the congestion in the network so that either it may slow down the packet transmission rate or find an alternate route which may not necessarily be an optimal route. It must be pointed out that all the congestion control methods are able to inform the source about the congestion problem because they use Transmission Control Protocol (TCP).

1.12 Effect of Mobility and Topology Change

In mobile ad hoc networks (MANETs), the movement of node changes the network topology in an unpredictable manner. As the change in the topology of the network is sensitive to frequent link failures and partitioning of the network which causes overhead in routing, more delay in the transmission and loss of packets in mobile nodes [14]. Hence, in order to design a Mobility resilient MANET, an intuitive solution is to enlarge the transmission range of the mobile wireless devices for reducing the network topology change rate. However, by this way, the mobile nodes would suffer more radio interference, channel contention, and energy consumption, which may seriously degrade the utilization of the network resources. An example of topology change in ad hoc network is as shown in figure 1.5. To obtain the enhanced performance of the network, it is mandatory to know the properties of mobility of nodes and its effect on topology change in MANETs.

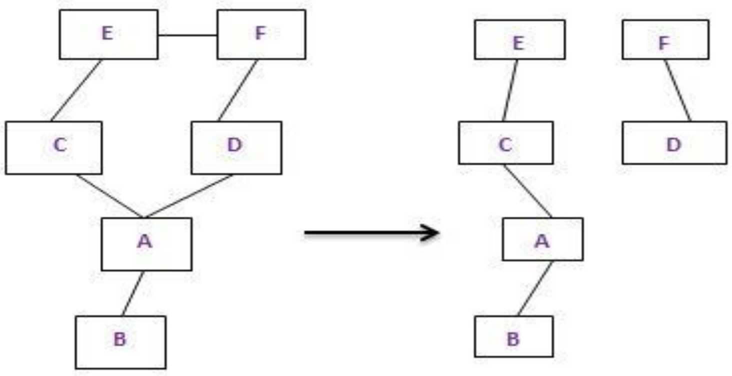


Figure 1.5 Topology Change in Ad Hoc network

CHAPTER 2 LITERATURE SURVEY

Most TCP deployments have been carefully designed in the context of wired networks. In wired networks the loss of the data is always due to the network congestion. But in Ad hoc networks the losses is not always due to network congestion. *Ahmad Al Hanbali [1]* presented in his paper about various reasons for the loss of data in Ad hoc networks like lossy channels, Hidden and exposed stations, Path Asymmetry, Network Partition, Routing Failure and Power Constraints.

To make the mobile ad hoc network more robust a scheme called HEAD (a hybrid mechanism to enforce node cooperation in mobile ad hoc networks) was presented by *GUO Jianli [2]* to over-come the misbehavior. It employs only first-hand information and works on the top of Dynamic source Routing protocol. By interacting with the DSR, HEAD can detect the misbehavior nodes in the packet forwarding process.

In order to increase the network lifetime of the MANET a new power aware Efficient Power Aware Routing is proposed by *Shivashankar [3]*. EPAR identifies the capacity of a node not just by its residual battery power, but also by the expected energy spent in reliably forwarding data packets over a specific link. Using a min-max formulation, EPAR selects the path that has the largest packet capacity at the smallest residual packet transmission capacity.

In Mobile ad hoc networks, to reduce the influence of interference between the selected node-disjoint multipath scheme two on-demand multipath routing protocols. Efficient, Stable, Disjoint Multipath Routing protocol (ESDMR) and Efficient, Disjoint Multipath Routing protocol (EDMR) was presented and designed by *Eman S. Alwadiyeh [4]*. The proposed routing protocols have a higher delivery rate and higher throughput.

To get increased network utility and reduced power, *Songtao Guo [5]* proposed a cross-layer rate-effective network utility maximization (RENUM) framework by taking into account the lossy nature of wireless links, constraints of rate outage probability and average delay. The proposed algorithm is shown through numerical simulations to outperform other network utility maximization algorithms without rate outage probability/average delay constraints. The Proposed algorithm has higher effective rate, lower power consumption and delay.

To reduce unnecessary transmissions and loss of throughput in MANETs a feedback scheme was introduced by *Kartik Chandran [6].* When a route is disrupted, the source is sent a Route Failure Notification (RFN) packet, allowing it to freeze its timers and stop sending packets. When the route from intermediate nodes to destination node is again established, the intermediate nodes will inform the source node with a notification of route re-establishment packet, after that it continues transmitting the packets by unfreezing timers. Feedback based TCP gives best performance for simulated results.

Gavin Holland [7] presented that how TCP performance is affected due to link breakage. Through simulation it is shown that TCP throughput drops significantly when nodes move due to TCPs inability to recognize the difference between link failure and congestion. It introduced a new metric expected throughput for the comparison of throughput in multi-hop networks. This metric showed how the use of explicit link failure notification (ELFN) techniques can significantly improve TCP performance.

In Long Term Evolution (LTE) network. Handover may cause sudden degradation of the quality of the communication if the process is not correctly controlled. To alleviate these problems, three solutions are proposed by *D. Pacifico [8]* fast path switch, handover prediction, and active queue management. The first two solutions avoid excessive delay in the packet delivery during the handover, whereas the third solution acts at the transport network with an active queue management. Simulation results showed that the proposed solutions present advantages. The handover prediction used with the active queue management increases TCP performance.

Prediction based link availability estimation models for MANET has been proposed by *Shengming Jiang [09].* This model predicts the probability of an active link between two nodes being continuously available for a predicted period based on the movement of current nodes. For predicting the availability of the link they used the exponential distribution.

To increase packet delivery ratio in dynamic source routing a model has been proposed by *Liang Qin [10].* They have used the model for link prediction based on received signal strength, which is the function of distance between two nodes. A link between two nodes is available as long as the distance between the two nodes is smaller than the transmission range or the received signal strength is above a threshold.

Adrin [11] proposed Link Cache Extension for Predictive Routing. They adopt the mobility model, which assumes a free space propagation model where the received signal strength is a function only of the distance to the transmitter assuming a fixed radiated power from each node. They assumed that all nodes are capable of determining a position either through GPS or some other positioning system and that these positions are time stamped so that a velocity and bearing can be computed.

A predictive preemptive Ad hoc On-Demand distance Vector Routing (PPAODV) has been proposed by *Sofiane Boukli Hacene [12]*, which predicts the link failure using the received signal strength (RSS). This method of prediction uses the interpolation of Lagrange, which evaluates the Received Signal Strength with the help of function and previous information of Received Signal Strength. Predictive Preemptive AODV discovers a new route before the active route breaks and changes the route smoothly by predicting a RSS of data packets at the predict time t, from the past information of RSS.

S. Crisostomo [13] have presented a proposal for link expiration time computation using GPS (Global Positioning system) equipped receiver. Though, no results and analysis were presented. It utilizes mobility information and geographical location of the neighbors which includes longitude, latitude which will be propagated with the help of Hello messages.

For the calculation of velocity and thus link break time computation based on distance and velocity, a scheme have been proposed by *P. Mani [14]*. The simulation results and analysis show that there is improvement in the end-to-end delay. For CBR traffic, there is reduction in packet delivery ratio using this model as compared to AODV. For TCP type of traffic, it will not give much raise in throughput for AODV.

A prediction based link availability estimation model for TCP has been proposed by *Prashant Singh [15]*. This model predicts the probability of breakup an active link between two nodes based on the node movement. It uses distribution for prediction of link availability to represent the pdf of epoch length. Epoch length is 46 defined as the length of interval for which a node moves in a constant direction at a constant speed.

As the mechanisms of TCP for controlling congestion are introducing the very high flow of traffic on present communication networks which degrade the performance of the network. To overcome this problem, *Amit Aggarwal [16]* proposed a technique which space the data evenly and send that data into the network in the complete Round trip delay time (RTT), by sending the data in this way will leads to reduction in burst flow of traffic. With Pacing of the data, better throughputs, less packet loss and enhanced performance can be achieved.

To improve the performance of TCP in multi-hop mobile ad hoc networks, *Chandran [17]* has performed simulation using NS2. The author has worked on various parameters like how TCP throughput is affected by size of the window, size of the packet, size of the buffer, length of path in case of full duplex link as well as half-duplex link, Unfairness by varying the size of the window and size of the packet and results are plotted by making the comparative analysis.

For improving the performance of the network of TCP in a lossy wireless networks *Thomas [18]* has introduced various models for effective throughput and utilization of bandwidth. The author has simulated on multi-stream bandwidth, throughput and packet loss. The TCP connections which are connected in parallel is having effective throughput and utilization of the bandwidth. It is proved by the author that if the congestion is not present, the usage of parallel connections of TCP is equal to that of single connection of Multi stream source.

Anantharaman [19] studied the TCP performance of MANETs and showed a set of outcomes of simulation and found the major issues which impact TCP performance in MANETs. They used multiple parameters for link failure detection, route latency evaluation, packet level route index unavailability and flow level route to find the mobility effect. By evaluating the rate of loss, throughput and timeout values of retransmission in the layer of TCP, the mobility effect on various parameters to TCP performance will be related. It is concluded from the simulation outcomes that the previous approaches was adapted to improve TCP performance in MANET. It was observed that the author improved the throughput in stack of default protocol by around 75%.

In hybrid MANET, certain aspects regarding the TCP performance was described by *Karlsson [20]* with extensive simulation. In their work, for connecting to public internet unfixed nodes adopt paths of multi hop. Such vision has very interest in 4G operations as hotspot coverage will be extended.

To examine the cross layer based techniques of TCP for controlling the congestion in MANET, *Shukla [21]* has carried out extensive survey in MANETs. The basic assumption of TCP is that the packet loss due to errors in the network is not acceptable in the unfixed network. If interruption does not occur during communication in the network then the performance of the TCP will be better. In this research work, the main reason for the degradation of the performance of TCP communication in MANET is found. In particular there are some factors like mobility, wireless channels, frequent changes of routes; link breakages are taken which degrade TCP performance. It is concluded that if there is no interruption in the network during communication then TCP performs better.

The network congestion is the main reason for the loss of packets is not completely acceptable in case of wireless networks stated by *Xiang[22]*. The major factors which degrade the performance of TCP are erroneous in wireless communication, handoffs in case of single-hop networks, medium access contention, changing the routes frequently and breaking of the routes in case of multiple-hop networks. The performance is less in multiple-hop networks when compared to single-hop networks. TCP should be able to differentiate congestion and route/link breakages.

The various types of Transmission Control Protocols are proposed by *Feng Wang [23]* in order to improve the performance when compared to standard TCP. The various types are Feedback based TCP (TCP-F), TCP Explicit Link Failure Notification (TCP-ELFN), Ad hoc TCP (ATCP), TCP-Bus, Fixed Retransmission time out (RTO), TCP-Out of order delivery (DOOR). The performance of these techniques differentiated by comparing the various performance parameters like throughput, delay, packet delivery ratio, bandwidth utilization and power consumption.

The degradation of TCP performance due to the effect of asymmetric network nature of the TCP is by introduced by *Hari Balakrishnan [24]*. In this, the author has explained how the various network asymmetric parameters like Bandwidth Asymmetry, Media-Access Asymmetry and Loss rate Asymmetry will affect the performance of the TCP. The various techniques like TCP header compression, Acknowledgement filtering, Acknowledgement congestion control, Acknowledgement first scheduling is implemented and the simulation results showed the enhanced performance of TCP.

A mechanism based on signal strength was proposed by *Fabius [25]* in order to decrease the loss of packets because of the mobility nature of the ad hoc network as the packet loss causes the unnecessary retransmissions and this leads to consumption of limited battery power. The techniques are the main reason for link failure is if the neighboring nodes are out of the range, in this case transmission power will be increased to make link active and another technique is the discovery of the new route before the link is likely to fail in order to maintain the link.

To improve the TCP performance, a technique was proposed by *Renaud [26]* which enlarge the Initial size of the window of TCP. This will leads to decrease in the amount of Round trip delay time in transferring the data. The larger initial window of TCP will impair the performance. This is achieved by spacing the initial window into ‘n’ number of segments along the Round trip delay.

The modification of the congestion control algorithm is achieved with adapting the congestion window to the feedback of explicit bottleneck which is called as TCP having Rate adaptive nature is proposed by *Aditya Karthik [27]*. The comparison of Rate adaptive form of Transmission protocol and basic Transmission control protocol is performed to understand the way of giving the feedback in implicit form. Under the simulation, the results have shown that the performance is improved by around 18% when compared to normal TCP.

A technique was proposed by *Youssef [28]* in order to control the congestion in TCP which is more reliable for both wired and wireless network environments. It is mainly based on utilizing the one of the reserved bits of the header of TCP to determine whether connection type of TCP is either wired or wireless i.e, for wireless connection it is ‘0’ and wired connection it is ‘1’. Along with these, Signal to Noise Ratio is used to determine the reliability of the link as well as the congestion loss. Upon simulation the results have shown the performance improvement in TCP.

The indirect-TCP which is a changed version of the standard TCP was proposed by *Badrinath [29]* to improve the TCP performance by portioning the connection of network into sender and receiver. In this scenario, the basic/standard TCP is used by the wired connection and changed version is utilized by the wireless connection. By establishing the wired type of connection between middleware station and the host and establishing wireless connection between mobile hosts and proxy, the errors can be prevented in propagating in the network.

For preventing the data loss due to congestion, a technique was proposed by *Hari Balakrishnan [30]* by employing the agent of snoop type between the wireless network as well as the wired network. In this method, after the reception of packet by snoop agent from wired network, the agent will store that packet and transfer to mobile host. After the reception of acknowledgement by the agent, the agent will verify the status of the packet and retransmit the packet, if the packet is lost, it is transmitted to destination without intervening with wired network.

As the bit error rates is one of the main reason for the data loss in TCP. To achieve the low bit error rate, a scheme called multicast TCP is proposed by *Brown [31]* in order to decrease the bit error rate in wireless links. To achieve the low bit error rate, the connection of TCP is partitioned into two parts. The standard TCP is used for connecting the supervisor host and the sender host. The TCP adapted type is used for connecting the mobile host and supervisor. When the size of the very large then the supervisory host will freeze the timers and window size was adjusted.

To avoid the performance degradation due to congestion in the network, Explicit Congestion Notification technique was proposed by *Ramakrishnan [32]* to utilize the bits of IP header and bits of TCP header in order to monitor the network status. During the occurrence of the congestion, the Explicit Congestion Notification bits are maintained at true values in the transmitted packet. The coherence of congestion is one of the improvements for Explicit Congestion Notification to reduce the packet loss in the process of transmission.

One of the mechanisms to differentiate the packet loss and congestion is introduced by making a comparison with the arrival time of the packet and the departure time of the packet called as Wireless TCP was proposed by *Venkataraman [33]*. This scheme utilizes the delay between the two packets as a performance parameter to evaluate adapting the rate at the end of the receiver. By estimating the reason behind the loss of packets, it will make the receiver to retransmit the lost packet. So, by transmitting the packets on the basis of rate instead of window size gave good results.

By differentiating the loss due to packets, a scheme was proposed by *Saverio [34]* estimating the available bandwidth called TCP Westwood. This technique will estimate the acknowledgements arriving rate and utilized the feedback acknowledgements as well as the size of the packet to determine the capacity of the network. With this technique, the bandwidth was approximated to determine the size of the congestion window. It will estimate the bandwidth availability by making the wireless link throughput relatively slow.

TCP Vegas was proposed by *Lawrence [35]* for estimating the TCP link capacity by determining the minimum value of Round trip delay time called Base Round trip delay time. The TCP vegas scheme will try to keep the size of the queue by adjusting the size of TCP window, this prevents the loss of packets due to congestion. Upon the occurrence of loss of packets, the connection will be in bad status and this loss will be considered as loss due to congestion. On the other hand, it will be considered as the loss due to errors in the link.

To identify the packet loss due to congestion or bit error rate, Jitter TCP or JTCP was proposed by *Mei-Zhen Chen [36]*. It is mainly on the basis of ratio of the Jitter and the delay between two packets which are found with the help of gap between the packets at the sender side and the gap between the packets at receiver side. Jitter TCP can be having long packet transmission time and it was delayed in the queue of the router till the congestion is rectified. Jitter TCP will be performing better than the other mechanisms of the TCP.

To improve the performance in TCP various solutions was proposed by *Tie-Jun Wu [37]* in order to overcome the drawbacks which cause less performance in TCP. The main drawbacks of TCP are Wireless channels constraints like doppler shift, interference, fading, attenuation of signals, excess contention and unfair access of MAC layer, mobility of the nodes, choosing the best routing protocol, size of the congestion window and asymmetric nature of the path. These are overcomed by detecting the errors in the channels, decreasing the contention at the MAC layer.

To alleviate the problems in TCP, various techniques are proposed at every layer of the TCP by *Sofiane [38]*. The various problems in TCP are the effects due to high bit error rate, mobility of the nodes, network partitioning, multi-path routing, and competition from neighbors for accessing the wireless channel. The solutions for these problems are control protocol for wireless congestion, differentiation algorithm for packet loss, managing links based on the signal strength of the received signal, routing based on path backup, path selection on basis of contention.

To enhance the performance of TCP in mobile networks in case of nodes having high speed mobility, several techniques has been proposed by *Qingyang [39]*. These techniques involve improving the performance of network in terms of throughput, traffic load, delay, packet delivery ratio and latency. The author has studied the main reasons for the performance degradation during hand-off and mobility and found the optimized solutions by classifying the hand-off as the intra-system handoff and intersystem handoff.

The backup path routing was introduced by *Haejung [40]* in order to improve the performance of TCP even though the mobility is very high. In generally, the multiple routes actually degrade the performance of the TCP. Using this scheme, TCP has improved against multipath routing. Here, author has implemented backup path routing using various methods like selection the optimal number of backup paths, selecting the primary and alternative paths and selecting the path having shortest delay. This improved TCP performance by 30%.

To distinguish the losses due to the congestion and the losses due to errors, a scheme was proposed by *Pavel [41]*. This scheme is based on utilizing the TCP header reserved field to know whether the connection is of wired type or wireless type. This scheme will determine the Signal to Noise Ratio to determine the link reliability and it is giving a solution either to decrease the bursts of the packets or to retransmit the lost packets. The simulation results have shown that this scheme was efficient when the errors are due to time-out.

A technique was developed by *Aniket [42]* which combines the feedback based approach as well as the adaptive approach to improve the performance of TCP. To get enhanced performance of TCP, it was proposed to change the existing behavior of standard TCP to either HS-TCP or MX-TCP. The author has concluded that MX-TCP is more suitable for lossy-links such as highway driving and low availability of 2G bandwidth and public hotspots accessing as well as internet and HX-TCP for High bandwidth usage.

For improving the performance of the TCP, the congestion in the network is handled in a efficient manner by comparing the two variants of the TCP which are HS-TCP and TCP Reno by *Gururaj [43]*. The author has performed the simulation in NS2 as well as the mathematical calculation for both HS-TCP and TCP Reno and proved that HSTCP is better.

As the routing protocols are very important to forward or transmit/ route the data from source nodes to intermediate nodes as well as the destination nodes. *Dhenekaran [44]* has made a survey on various routing protocols with their advantages as well as the disadvantages and applications based on the various parameters of those protocols. Further, the author sub-classified the pro-active, reactive and hybrid routing protocols and described which protocol is best suitable for which application.

For improving the performance of the TCP, the congestion in the network is handled in a efficient manner by comparing the two variants of the TCP which are HS-TCP and TCP Reno by *Gururaj [45]*. The author has performed the simulation in NS2 as well as the mathematical calculation for both HS-TCP and TCP Reno and proved that HSTCP is better.

CHAPTER 3 MANET ROUTING PROTOCOLS

As the Mobile Ad hoc Networks (MANETs) are having dynamic nature, the design of communication and networking protocols for networking of these kind of networks one of the very challenging issues. The major important aspects of the process of communication are designing the protocols for routing which will be using to maintain and establish routes of multi-hop to permit the data communication among the nodes [15]. A significant research has been carried out in this domain, and many multi-hop protocols of routing have been developed from past few years. Majority of these protocols are Destination Sequence Distance Vector (DSDV), Ad-hoc on-Demand Distance Vector routing protocol (AODV), Dynamic Source Routing protocol (DSR), Temporally Ordered Routing Protocol (TORA). The classification of routing protocols is shown in the figure 3.1. As these are sufficient for a particular class of applications of Mobile Ad hoc Network (MANET), these are not sufficient for supporting the application having huge demand such as video and audio processing. These applications need the network to provide Quality of Service (QoS).

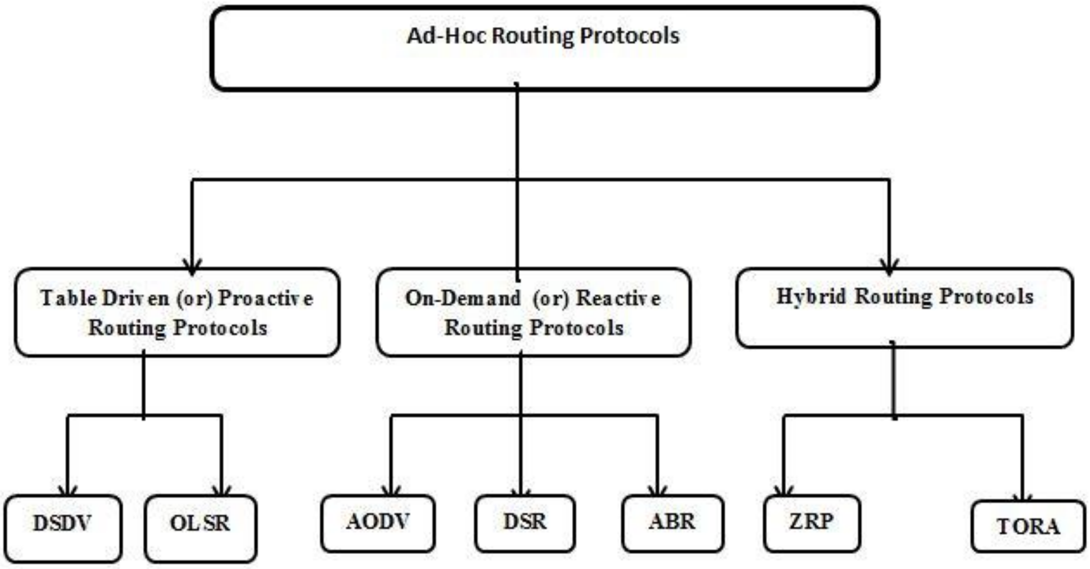

Ad-Hoc Routing Protocols
Table Driven (or) Proactive Routing Protocols
On-Demand (or) Reactive Routing Protocols
Hybrid Routing Protocols
DSDV
OLSR
AODV
DSR
ABR
ZRP
TORA

Figure 3.1 Classifications of Routing Protocols in Mobile Ad hoc Network

Few researchers are active in supporting the Quality of Service in Mobile Ad hoc Networks (MANETs), and they have introduced so many Quality of Service (QoS) routing protocols in this kind of environment. Some protocols provide Quality of Support for the availability of link for a given path. As the prediction of the availability of the link will optimize the routing protocols service [16]. Routing protocols for Mobile ad hoc networks (MANETs) can be classified as: pro-active protocols, re-active protocols and the hybrid protocols. The classification of these routing protocols based on various parameters is shown in table 3.1.

Parameters	**Reactive Protocol**	**Proactive Protocol**	**Hybrid Protocol**
Philosophy of Routing	Flat Routing	Flat/Hierarchical Routing	Hierarchical Routing
Scheme of Routing	On-Demand Routing	Table-Driven Routing	Combination of On-Demand and Table-riven Routing
Overhead of Routing	The value of Routing overhead is low	The value of Routing overhead is high	The value of Routing overhead is medium
Level of Scalability	It is not suitable for large sized networks	The scalability is low	The scalability is high and suitable for large sized networks
Routing information availability	Routing information is available whenever it is needed	Routing information is available all the time and stored in routing tables	It exhibits the combination of both Proactive Routing and Reactive Routing
Getting periodic updates	Getting periodic updates is not required as the routes are available on demand basis	Periodic updates are required whenever the topology of the network changes	Periodic updates are needed inside the zone
Capacity of Storage	Storage capacity is low and basically it depends on the number of routes	Storage capacity is high due to the presence of routing tables	Storage capacity basically depends on the size of the zone.
Support of Mobility	Maintenance of Routes	Getting periodical updates	Combination of both Pro-active and Reactive Routing

Table 3.1 Classification of routing protocols on various parameters

Flat Routing Protocols: Flat routing protocols are classified into two types; one is proactive routing protocol and other one is reactive routing protocol. The very common thing these protocols is that every node which participates in routing plays behaves in a similar way. Proactive routing is mostly based on LS (link-state) and Reactive routing is based on DV (distance-vector).

3.1 Pro-active protocols:

These are also called as Table-driven protocols and they work in a similar way to wired networks and they will maintain an up-to-date network map, and this routing protocol evaluates the routes in a continuous manner and tries to find new routes [17]. In this way, when a source needs a path to destination node, a packet has to be forwarded, if the route is known previously so there will no excess delay caused due to the process of route discovery. As the information needs updates in this way, it will need a lot of bandwidth and battery power which is limited in mobile ad hoc networks. Optimized Link State Routing (OLSR), Open Shortest Path First (OSPF) and some other Conventional Routing Schemes like Distance Vector Routing and Link State Routing will fall under the category of pro-active routing protocols.

3.1.1 Destination-Sequenced Distance Vector (DSDV):

One of the routing protocols of MANET is Destination Sequenced Distance Vector (DSDV), which is also called as Bellman Ford Distance Vector protocol. The Packets will be forwarded from one node to another node in the network by utilizing the routing tables of each node of the network. The routing table of each node lists all the available destinations, nodes of the next hop and the number of available hops to reach there. Every routing table entry of a node is contains sequence number which is created by the nodes of the destination. In Ad hoc On-Demand Distance Vector, the sequence number is used for avoiding the loops in the route and these sequence numbers determine the freshness of routes. In order to keep the routing tables consistency in a topology which is varying dynamically, every node transmits the updates periodically along with updates transmission when significant amount of new information is available in the network. Thus Destination Sequence Distance Vector acts as the pro-active protocol. The advertisements of route will be sent either by broadcast routing or multicast routing. An example of DSDV routing protocol is shown in the figure 3.2

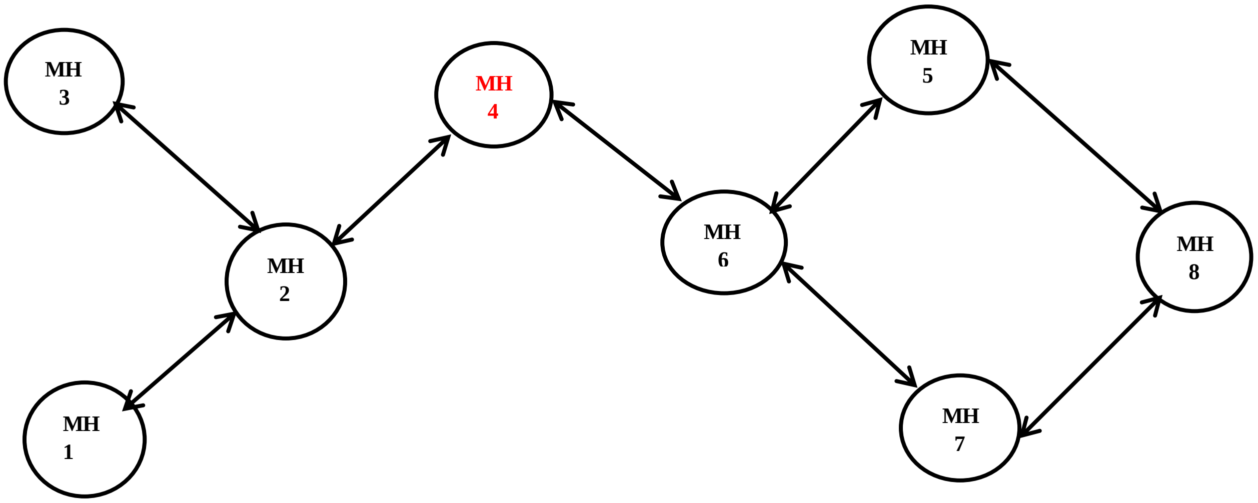


Figure 3.2 DSDV Routing protocol with 8 mobile hosts

Destination	Next Hop	Metric	Sequence Number
Mobile Host-1	Mobile Host-2	2	S406_MH4
Mobile Host-2	Mobile Host-2	1	S128_MH1
Mobile Host-3	Mobile Host-2	2	S564_MH2
Mobile Host-4	Mobile Host-6	0	S710_MH3
Mobile Host-5	Mobile Host-6	2	S392_MH5
Mobile Host-6	Mobile Host-6	1	S076_MH6
Mobile Host-7	Mobile Host-6	2	S128_MH7
Mobile Host-8	Mobile Host-6	3	S050_MH8

Table 3.2: The routing information and sequence numbers of DSDV routing protocol with destination mobile hosts

To decrease the amount of information which is carried by these advertisements, there are two types of packets defined. An example of DSDV routing protocol with sequence number information and mobile hosts is as shown in table 3.2. One packet carries the information of routing which is readily available which is also called as “full dump". Another packet carries the changed information since the last full dump. Full dumps will be transmitted less frequently when there is no mobility of hosts. If the movements of the nodes is very frequent and the size of incremental approximates the size of a network protocol data unit (NPDU), then full dump can be scheduled [18]. When a mobile host fetches updated information about routing, this information will be compared with the information which is readily available from the previous packets of routing information. A route which is having most updated sequence number will be used and the Routes with older sequence numbers will be removed. A route having the sequence number which is equal to an existing route will be chosen if it contains a better metric like having small number of hops. If the link to next hop of that route is broken, any route which is available through that next hop will be immediately assigned as an infinite metric and sequence number in updated form. These modifications will be broadcasted immediately in the packet having the routing information.

3.1.2 Wireless Routing Protocol (WRP):

Wireless Routing Protocol belongs to class of the algorithms for finding the best path; these algorithms can be defined as the shortest path algorithms in a distributed manner which evaluates the paths with the help of information like length and shortest path of second-to-last hop to each destination. Wireless Routing Protocol decreases the number of ways of occurrence of temporary routing loop. To achieve efficient routing, each node contain four requirements which are in the form of tables which gives information about distance, routing, cost of link and the list containing retransmission of message. Wireless Routing Protocol utilizes the update of periodic message transmissions to the nearest node neighbors. Acknowledgments should be sent by the nodes in the updated message response list. The nodes in the response list should send an idle Hello message to ensure connectivity, if no change is observed from the last update. A node will take decision to update its routing table or not after getting an update message from a neighboring node and always a node search for the best path utilizing the newly available information. Once, if a node gets a best path, it will send back that information to the original nodes in order to update their routing tables. After getting the acknowledgment, the original node will update its Message Re-transmission List. In this way, every time the routing information consistency will be checked by each node, which ensure removing the routing loops and always makes an efforts to achieve the optimized solution for network routing.

3.1.3 Cluster Gateway Switch Routing Protocol (CGSR):

Cluster Gateway Switch Routing protocol will consider a wireless mobile network in clustered form instead of network of flat type. In order to obtain the network structure into separate network structure but should be in groups which are interrelated to each other, the heads of the cluster will be elected by using the algorithm named cluster head selection algorithm [19]. By making different clusters, this CGSR protocol will get a processing mechanism in a distributed form in the network. One of the major draw-back of this CGSR protocol is that, the continuous change of selecting the cluster head will degrade the node resources and it will significantly degrade the performance of routing. An example of CGSR routing protocol is shown in figure 3.3.

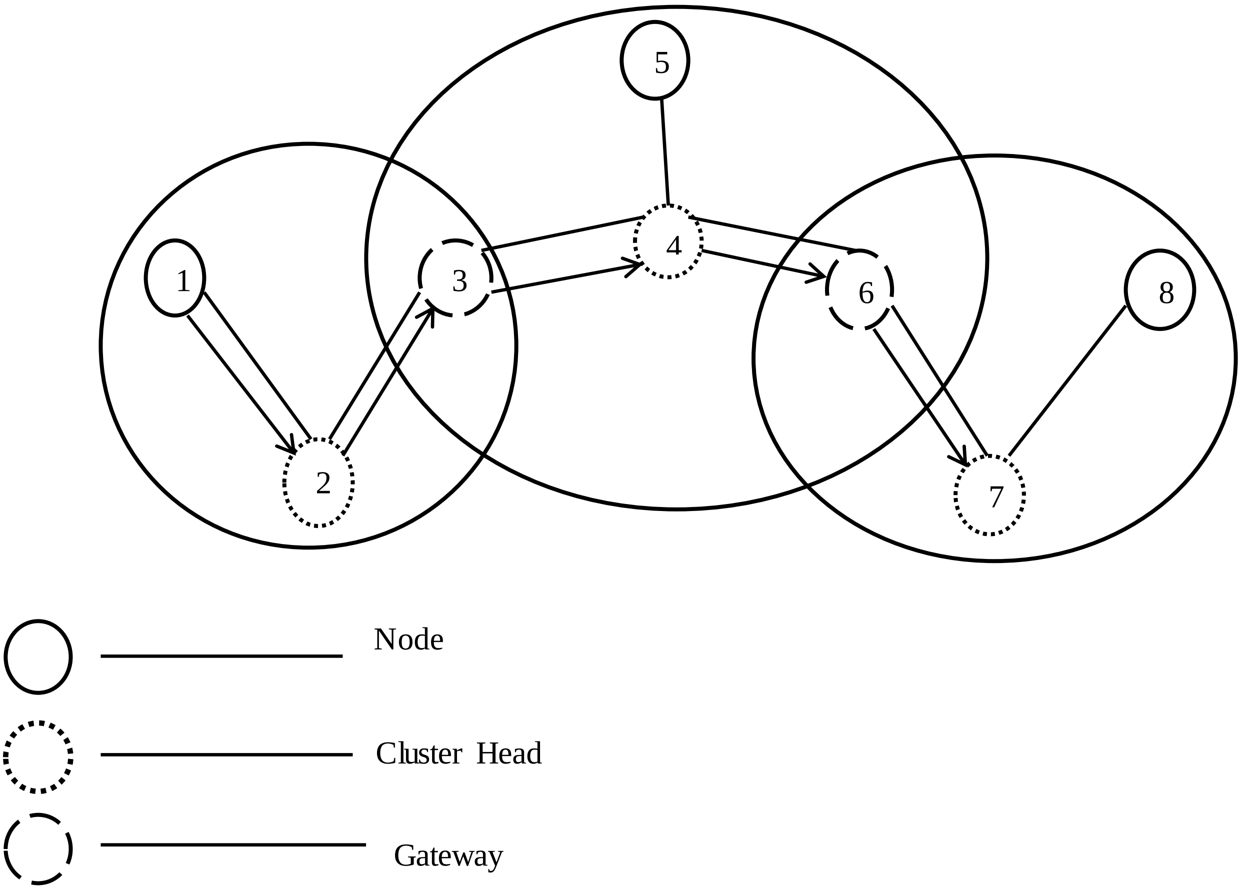


Figure 3.3 CGSR routing protocol with nodes, cluster heads and gateways which are connected in the network

CGSR uses protocol of DSDV as the basic scheme of routing. So, therefore it will be having the equal amount of overhead as that DSDV have. It modifies the DSDV by using the approach of hierarchical cluster head gateway routing to forward the traffic from source nodes to destination nodes [20]. The nodes which are within the communication range of two or more cluster heads are called Gateway nodes. If a node wants to transmit the packet, initially, the packet is first forwarded to its cluster head node, after that the packet will be sent from the cluster head node to gateway and then to another cluster head node, and this process will continue upon reaching the cluster head of the destination node. The packet is then transmitted from cluster head to the destination.

3.1.4 Source-Tree Adaptive Routing (STAR):

The STAR is mainly based on the algorithm of the link state. In STAR protocol, the links or the most selected paths which are connecting the destinations will be maintained by the router of the source tree. This protocol will considerably decrease the value of routing overhead in the network by using the approach of overhead routing of least value in order to the information regarding routing [21]. It supports the approach of optimum routing if required. This kind of approach will eliminate the procedure of updating the routes periodically which was existed in the algorithm of Link State. The updates of the Link state will be exchanged during the occurrence of certain events. The comparison of table-driven routing protocols on various parameters is as shown in table 3.3.

Paremeters	**Destination Sequence Distance Vector (DSDV)**	**Cluster Gateway Switch routing (CGSR)**	**WRP**
Complexity of Time (Addition of link or failure of link)	F(d)	F(d)	F(h)
Complexity of Communication	F(x=N)	F(x=N)	F(x=N)
Philosophy of Routing	Flat type of Routing	Hierarchical Routing	Flat type of Routing
Loop free routes	Loop free routes exist	Loop free routes exist	Loop free routes exist, but does not exist instantaneously
Multicast Capability	Does not exist	Does not exist	Does not exist
Required number of routing tables	Two routing tables are required	Two routing tables are required	Four routing tables are required
Frequency of transmitting the updates	Transmit the updates periodically and whenever needed	Transmit the updates periodically	Transmit the updates periodically and whenever needed
Sequence Numbers Utilization	Utilizes the sequence numbers	Utilizes the sequence numbers	Utilizes the sequence numbers
"Hello " Messages Utilization	Utilizes "Hello" Messages	Not utilizes "Hello" Messages	Utilizes "Hello" Messages
Existence of critical nodes	Critical nodes does not exist	Critical nodes exist (Cluster head)	Critical nodes does not exist
Metrics of Routing	Shortest Path	Shortest Path	Shortest Path

Table 3.3 Comparison of Table-Driven or Pro-Active Routing protocols based on various parameters

N=Number of nodes in the network

d=Diameter of the network

h=Routing tree height

x=Number of nodes which are affected due to the change in the network topology

So, the scalability of STAR is good in case of large networks as this protocol considerably decreased the consumption of the bandwidth for routing updates as well as it reduced the latency by utilizing the routes which are predetermined [22]. In case of large and heavy mobile ad hoc networks, this protocol will be having large overheads of memory and processing, as it is required for every node to keep a graph of partial topology of the network. The frequency of changing of this partial topology is high as the neighboring nodes are reporting the various source trees. The following table shows the classification of Table-Driven Routing protocols based on various parameters.

3.2 Re-active protocols:

These are also called as On-demand protocols which are dissimilar to pro-active protocols and they start the process of discovery of routing procedure whenever it is needed. If there is a requirement of route from source to destination is needed, a global search of route discovery procedure will be initiated. Just like Pro-active routing protocols it does not need the constant updates which are being forwarded in the network, but as the routes will not be available instantaneously it will create delays as the routes need to be found with some route discovery procedure. In few cases, the required route will be still available in the route cache which is maintained by the nodes. If this is the case, then there will be no additional delay as the routes need not to be discovered at that time. Protocols such as Ad hoc On-Demand Distance Vector (AODV), Temporally Ordered Routing Algorithm (TORA), and Dynamic Source Routing (DSR) are members of reactive routing protocol.

3.2.1 Ad hoc On-demand Distance-Vector Routing (AODV):

In mobile ad hoc networks and some wireless ad hoc networks, Ad hoc On-Demand Distance Vector routing is one of the routing protocols. It was developed in Nokia Research Centre. With this routing protocol the route is established by on demand basis. It is capable of both multicast and unicast routing. To ensure route freshness, AODV uses sequence numbers. It is self-starting, loop-free and generally adaptable for large number of nodes. To maintain routes

AODV defines control messages which are of three types. Node which requires route to another node generally transmits route request message. While flooding these messages, AODV uses expanding ring technique for optimization [23]. Time to live (TTL) was carried by RREQ which states the number of hops the message will be forwarded. At first transmission this value is set at predefined level and it will be increased at retransmissions. If no replies are received, then retransmissions will takes place. Each node maintains two counters which is Broadcast Id and Route sequence number.

Route Request Message (RREQ): The RREQ contains information like Broadcast Id, Source Address, Destination Address, Source sequence number, Hop count and destination sequence number. Whenever the source issues a new RREQ, the Broadcast id will be incremented.

Route Reply Message (RREP): A route reply message is unicasted back to the originator of a RREQ if the receiver is either the node using the requested address, or it has a valid route to the requested address. One of the main reasons for message unicasting towards back side is each and every route which forwards a Route Request packet caches the route to its originator. A basic AODV is shown in the figure 3.4

Nodes monitor the link status of next hops in active routes. When breakage of links in one of the route which is active was found, then message of Route Reply is used for notifying the other nodes in the network regarding link loss. To achieve this kind of mechanism for reporting, each and every node maintains a list which contains the IP address of its neighboring nodes which should be able to use that list towards every destination as a next hop.

Initially, when Node A desired to send information to node J, it does not have any route. Node A transmits a Route Request packet which is broadcasted to all other intermediate nodes available in the network. Upon forwarding route request from J from H, Node J creates a Route Reply packet. This Route Reply packet is unicasted back to node A by utilizing the cached entries which are stored in nodes H, D and G. Ad hoc On-Demand distance Vector develops different paths by utilizing the query cycle of route request and route reply. When a source node which does not have any route previously with itself needs route to destination node.

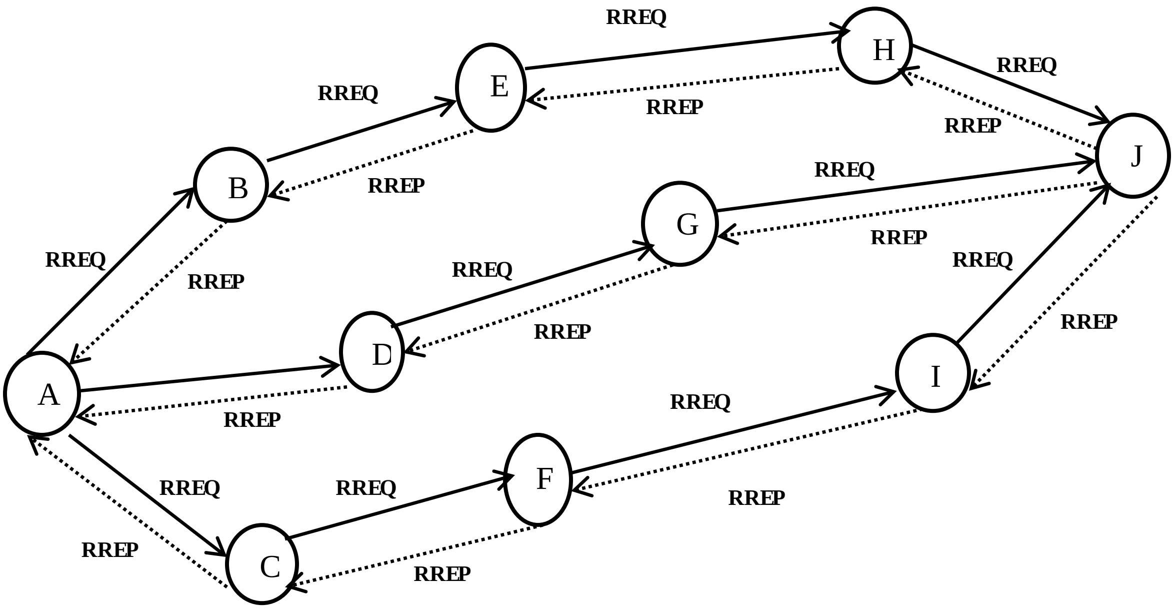


Figure 3.4 AODV routing protocol with nodes from A to J with node A as source and node J as destination

To achieve this, the source node broadcasts a Route Request Packet towards all other nodes in the network. After receiving these packets, the intermediate nodes update their routing information of the source node and make backward pointers towards source node in the tables of routing. Along with the IP address of source node, broadcast ID, present sequence number, the Route Request packet includes the latest sequence number of the destination node. After receiving the Route Request Packets by the nodes, the nodes will send a Route Reply Packet to the destination or if it has a route towards the destination with sequence numbers which is more than or equal to which already presented in the Route Request Packet. In this case, the nodes will unicast a Route Reply Packet to the source nodes. If it does not happen, it will re-broadcast the Route Request packet. Nodes will maintain tracking of the Route Request packets of IP address of source and broadcast IDs [24]. Upon receiving of Route Request Packets which they have processed previously, they will discard the Route Request Packets and they not forward them. Upon propagating of Route Reply Packets back to the nodes of source, nodes will make forward pointers towards the destination. After receiving the Route Reply Packet by the source node, the source node will start transmitting the packets of data to the destination nodes. After sometime, if the source gets a Route Reply Packet which contains a sequence number of greater value or the equal sequence number having a hop count of smallest value, the source node will update its information of routing for the destination node and it will start utilizing the best route. If the route is the state of active, it will be continued further. A route will be considered as the active route if the packets of data are transmitting continuously in that path from source to destination. If the source node regrets to send the packets of data, then the links will be in a state of time out and finally the routes will be deleted from the routing tables of intermediate node. If there is occurrence of any link breakage in the active route, the nodes which are upstream of the link break generates a message of route error to the source node to intimate it regarding destinations which are not reachable. Upon receiving of Route error packets, if the source node needs the route now, it can again begin the procedure for discovering routes. Multicast routes will be maintained in the same way. A node which desires to join a multicast group will broadcast a Route Request Packet with the set of IP address of destination to that multicast group with the 'J'(join) flag set to intimate that it want to join the group. Any node after receiving this Route Request packet which is a member of the multicast tree which is having a fresh sequence number for the multicast group will send a Route Reply Packet. As the Route Reply Packets will traverse back towards the source node, the nodes which are forwarding the messages will maintain pointers in their routing tables of multicasting. Upon receiving of the Route Reply Packets by the source nodes, they will monitor the route with the sequence number of fresh value, and after that the smallest hop count to the preceding member of multicast group. After the specific period of discovery, the source nodes will unicast a message of Multicast Activation to its desired next hop. The activation of route will be served by this message. A node which does not receive this kind of message that has maintained a multicast route pointer will be timed out and the pointer will be discarded. If the nodes upon receiving of the Multicast Activation were not a part of the multicast tree previously, it will maintain the best route from the received Route Reply Packets. Therefore the nodes must unicast a Multicast Activation to its next hop and this process will be continued until a node which was previously a member of multicast tree is reached. Ad hoc On-Demand Vector will maintain routes as long as the routes are active [25]. This contains having a multicast tree for multicast group life. Because, when the nodes in the network are moving, there may be chances of breakages of links along a route which occur during that route lifetime. The counting to infinity problem will be avoided by Ad hoc On Demand Distance Vector routing protocol from the distance vector algorithm by utilizing sequence numbers for each and every route. The counting to infinity problem is the situation where a node changes with other nodes in a loop. The following are the characteristics/features of the Ad hoc On-Demand distance Vector routing. AODV is having Unicast, Broadcast, and Multicast type of communication.

Route will be established On-demand with very less delay. The multicast trees which are connecting the members of group will be maintained for the lifetime of that group. Breakages of links in active routes will be repaired efficiently. All routes will be loop-free with the use of the sequence numbers. Usage of Sequence numbers will track the information accuracy. Ad hoc On-Demand distance vector will keep track for the next hop of the route instead of the complete route. Using HELLO messages periodically will track the neighbors.

Advantages and Disadvantages of Ad hoc On-Demand Distance Vector Routing: One of the major advantages of AODV protocol is the routes are obtained on demand and to find the latest route to destination, the destination sequence numbers are used. The delay is less in connection set up [26]. The HELLO messages which are range limited support route maintenance, which does not give unnecessary overhead in the network. One of the major disadvantages of this protocol is if the source sequence is very old, when intermediate nodes lead to inconsistent routes. One of the disadvantages of AODV is unnecessary bandwidth consumption due to periodic beaconing.

3.2.2 Dynamic Source Routing (DSR):

Dynamic Source Routing (DSR) is one of the reactive routing protocols which is similar to Ad hoc On-Demand Distance Vector Routing in operation. The primary difference between Ad hoc On Demand Distance Vector routing protocol and Dynamic Source Routing protocol is that Dynamic Source Routing achieve source routing, while Ad hoc On-Demand Distance Vector uses information of next-hop which is stored in the nodes of the route. Source routing is one of the routing techniques in which the packet sender predicts the entire node sequence, using that sequence the packets will be forwarded; the sender lists this route in the header of the packet and identifies the forwarding hop by the next node address to forward the packet to the destination node. The process of route discovery is same in both Dynamic Source Routing as well as Ad hoc On-Demand distance Vector routing. A node will check its route cache to obtain the route to destination. The node broadcasts the destination identity as a route request packet, if the desired route was not found in the route cache. Apart from the address of source and destination, each node request packet containing the record of the route, this record is nothing but accumulated record of the hop sequence taken by the route request packet as it propagating through the ad hoc network during process of discovery of route. If the packet reaches the node which does not includes the destination route, address will be appended to the route record in the request packet and it will re-broadcast the request further. If a packet reaches a host which is having route to destination, the host will append the route to the accumulated route record in the packet and reply with sending a route. For returning the route reply packet to the route request packet initiator, the node must be having a route to the initiator [26]. If it contains an entry of route for the initiator in its route cache, in such a case the packet of route reply will be unicast to the initiator. Otherwise, in the route records, the node will reverse the route of the packet containing route request, and utilize this route to send the packet of route reply. However, it needs the requirement of the wireless links to work equally in both the directions, as the links of wireless networks must be bi-directional. An example of DSR is as shown in the figure 3.5.

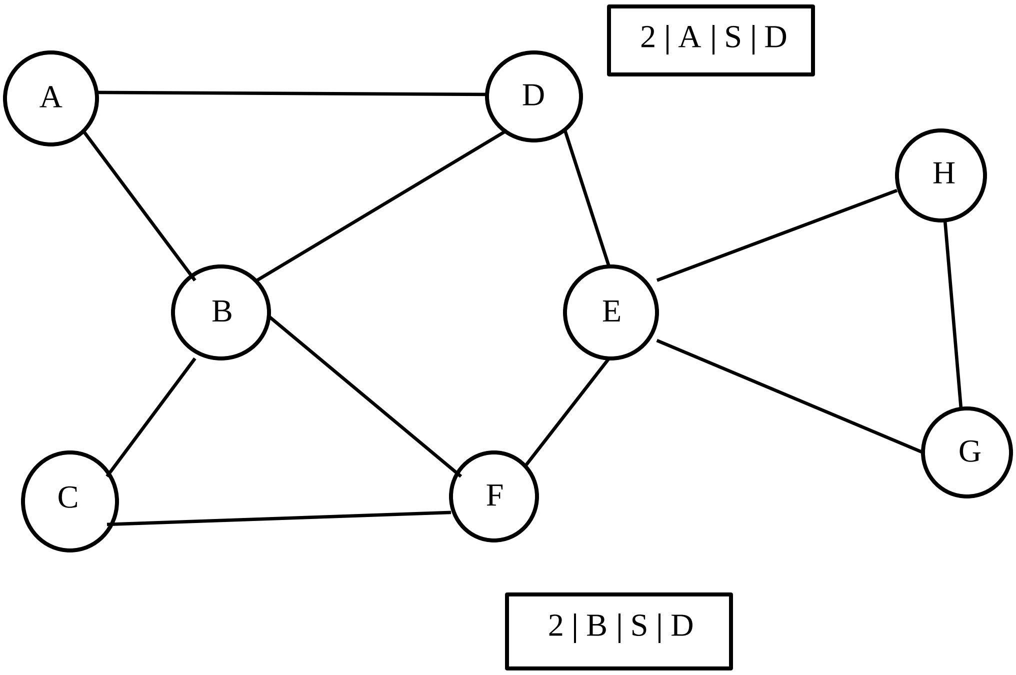


Figure 3.5 DSR routing protocol with nodes from A to H showing with the source and destination addresses

3.2.3 Temporally Ordered Routing Algorithm (TORA):

Temporally Ordered Routing Algorithm (TORA) is a distributed protocol which was designed in such a way so that it can be highly adaptive and can operate in a network which changes dynamically. For a given destination, Temporally Ordered Routing Algorithm (TORA) uses some arbitrary parameter called 'height' which is used to find the direction of a link between two nodes. As a result of this, multiple routes will be often presented for a specified destination, but it is not necessary that all of them will be having the shortest route.

In order to initiate a route for node, the node broadcasts a query to its neighboring nodes. This query will be re-broadcasted throughout the network until it reaches the destination, or a node that contains a route to destination. This node replies with an update that includes its height with respect to the destination which will be propagating back to the sender node. Every node which is receiving the update will set its own height to one which is greater than that of the neighbor which sent it. This forms directed link series from the sender node to the destination node in decreasing height order. If a node discovers failure of link, then it will set its own height which is higher than their neighbors, and issues an update to that effect which reverses the link direction between them [28]. If it discovers that it does not contain downstream neighbors, the destination will be lost, and it again issues a clear packet to discard the invalid links from the rest of the network. One of the main advantages to TORA is that it will support different/multiple routes between the pair of source and destination for packet transmission. The removal or failure of one node is resolved quickly without the intervention of source by changing to the available different route. An example of TORA Routing protocol is as shown in the figure 3.6.

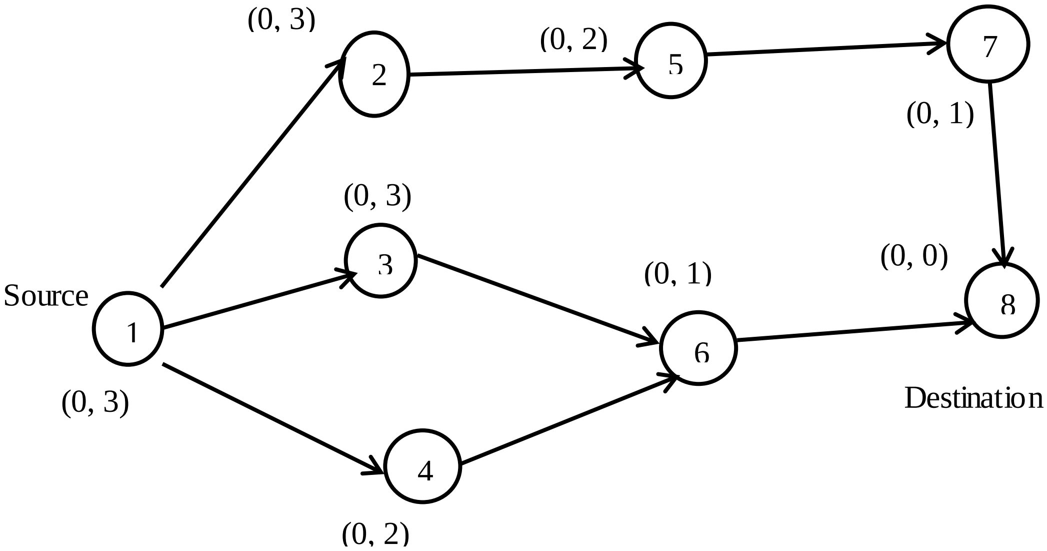


Figure 3.6 TORA Routing protocol with 8 nodes with 1st node as source and 8th node as destination with their positions

There are few drawbacks to TORA as well as the advantages. One of the drawbacks is that it relies on synchronized clocks. The presence of external time sources makes the supporting hardware to support it more expensively and initiates a single failure point if the source of the time is unavailable. TORA relies on lower intermediate layers for certain operations. It assumes the status of link sensing, discovery of neighbors, in order packet delivery, and resolution of addresses are readily available. The solution for this is to run the Encapsulation Protocol of Internet MANET which is also called IMEP at the layer which is placed immediately below TORA. This makes the overhead for this protocol which is very difficult to separate from that imposed by the required lower layer.

3.2.4 Associativity-Based Routing (ABR):

Associativity Based Routing protocol is defining a new metric of routing called "Degree of stability of association" for mobile ad hoc networks. In this routing protocol, the optimized route for mobile nodes will be chosen on the basis on the routing metric "degree of stability of association". Every node will generate the beacon periodically to disclose its presence. After receiving beacon message of beacon, the neighboring node will updates its own table of associativity [29]. After the reception of every beacon message, the associativity tick of the receiving node with the beaconing node will be increased. A highest associativity tick value of for any beaconing node gives the information that the node is comparatively static node. Associativity tick will be in reset position when any one of the neighboring node moves out of the other node's neighborhood.

3.2.5 Signal Stability–Based Adaptive Routing Protocol (SSA):

Signal Stability A-Based Adaptive Routing Protocol will focus on getting the best stable routes in mobile ad hoc network. This protocol will perform the procedure of discovery of new route on the basis on stability of location as well as the strength of the signal. On the basis of the strength of the signal, SSA will find the strong and weak channels in the network. SSA can be classified into two co-operative protocols which are the Static Routing Protocol (SRP) and the Dynamic Routing Protocol (DRP). The DRP uses two tables which are Routing Table (RT) and Signal Stability Table (SST). SST stores the strength of the signals of the neighboring nodes which was obtained by the periodic beacons from the neighboring node link layer. The strength of these signals will be recorded to classify as either weak signals or strong signals. The comparison of various On-Demand Routing protocols or Reactive protocols based on various Parameters is shown in table 3.4. DRP will receive all the signal transmissions and after processing the signals properly, it will send those signals to the SRP. SRP will send the packets to the stack of the upper layer of the nodes if that node is the desired destination node.

Performance Parameters	**(AODV)**	**(DSR)**	**(TORA)**	**(ABR)**	**(SSR)**
Complexity of Time (Initialization)	F(2d)	F(2d)	F(2d)	F(d+z)	F(d+z)
Complexity of Time (Post Failure)	F(2d)	F(2d) or 0 (Cache hit)	F(2d)	F(l+z)	F(l+z)
Complexity of Communication (Initialization)	F(2N)	F(2N)	F(2N)	F(N+y)	F(N+y)
Complexity of Communication (Post Failure)	F(2N)	F(2N)	F(2x)	F(x+y)	F(x+y)
Philosophy of Routing	Flat type of Routing	Flat type of Routing	Flat type of Routing	Flat type of Routing	Flat type of Routing
Loop free routes	Loop free routes exist	Loop free routes exist	Loop free routes exist	Loop free routes exist	Loop free routes exist
Multicast Capability	Multicast Capability exist	Multicast Capability does not exist	Multicast Capability does not exist	Multicast Capability does not exist	Multicast Capability does not exist
Requirement of Beaconing	No need of Beaconing	No need of Beaconing	No need of Beaconing	Beaconing is required	Beaconing is required
Possibilities of multiple routes	No multiple routes	Multiple routes exist	Multiple routes exist	No multiple routes	No multiple routes
Maintenance of Routes	Routes are maintained in Route table	Routes are maintained in Route Cache	Routes are maintained in Route table	Routes are maintained in Route table	Routes are maintained in Route table
Utilizing of Route cache or table expiration timers	Utilizing Route cache or table expiration timers	Not Utilizing Route cache or table expiration timers	Not Utilizing Route cache or table expiration timers	Not Utilizing Route cache or table expiration timers	Not Utilizing Route cache or table expiration timers
Methodology of Route Reconfiguration	Erases the routes and notifies the source	Erases the routes and notifies the source	Link will be reversed and the route was repaired	Sending query through localized broadcasting	Erases the routes and notifies the source
Metrics of Routing	Freshest and shortest path was the routing metric	Shortest path was the routing metric	Shortest path was the routing metric	Associativity and shortest path was the routing metric	Associativity and stability was the routing metric

Table 3.4 Comparison of various On-Demand Routing protocols or Reactive protocols based on various Parameters

l=Affected network segment diameter

y=Sum of all the nodes forming the directed path where the transition of REPLY packet occurs

Z=Diameter of the directed path where the transition of REPLY packet transits

If it is not the desired destination node, it will search for the actual destination in the routing table and route the packet towards destination. If it does not find any entry in the routing table for the desired destination, it will initiate the process of finding the actual route. Route-request packets will be forwarded to the neighbors utilizing the strong channels. After getting the request, the destination will select the first request packet and again it will send back the reply. The DRP will reverse the route which was selected and sends a message of route-reply to the route request initiator [30]. The node's DRPs along with the path will update their routing tables. If there is a failure of link, the intermediate nodes will send an error message to the source nodes informing about the failure of channel. The source will intimate all the nodes by sending an erase message about the link which was broken and will initiate the process of search new route to find optimized path to the destination.

3.2.6 Light-Weight Mobile Routing (LMR):

The LMR protocol is one of the On-Demand protocols of routing, it utilizes the technique of flooding to find its routes. The nodes in the LMR are having more than one route to every destination. This kind of feature will increase the protocol reliability by giving access to nodes to choose the available route to a desired destination without initializing the procedure of route discovery. One of the advantage of this protocol is every node will maintain information of routing to their neighbors. This leads to the avoidance of excess delays and overheads which are related with route maintenance. LMR will generate temporary routes which are not valid and it introduces excess delays in predicting a correct loop.

3.3 Hybrid protocols:

These protocols combine the advantages of Pro-Active and Reactive routing, by using the Pro-Active routing protocol locally and using the Reactive routing protocol inter-locally. This is partially based assuming that in mobile ad hoc networks most of the communication takes place among the nodes which are very close to each other and the changes in network topology is very significant if it happens in the node's transmission range. If there is a failure of the link or the disappearance of the nodes on the other side of the network, it will affect only local and neighboring nodes, but nodes on the other side of the network will not be affected.

3.3.1 Zone Routing Protocol (ZRP):

Zone Routing Protocol is compatible for different types of MANETs; this protocol is more suitable for those networks having large span and different patterns of mobility [31]. In ZR protocol, every node actively maintains routes in a local region, called as routing zone. The Zone routing protocol with nodes, cluster head and gateways is shown in figure 3.7.

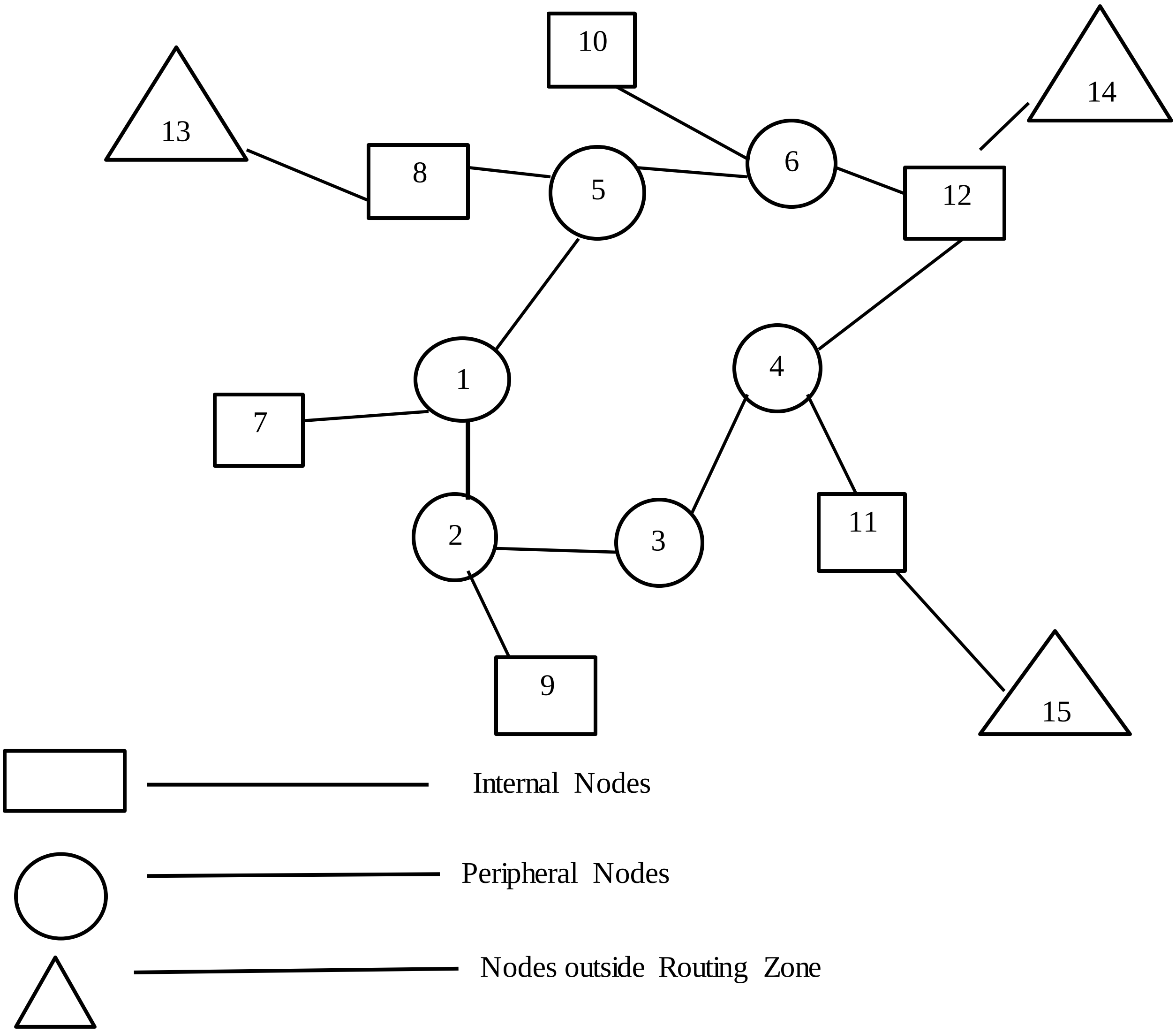


Figure 3.7 Zone routing protocol with nodes, cluster head and gateways

The creation of routing will be done using the mechanism of query-reply. For establishing distinguish network zones, initially a node have to be familiar with it's neighbors. A neighbor can be defined as a node having direct communication with that node, and the transmission range of one hop. The information of discovering the neighbor can be used as a basic factor for Intra-zone Routing Protocol (IARP) [32]. Instead of broadcasting blindly, ZRP utilizes a mechanism of query control to decrease the traffic of route query by routing the query messages from the query source from zones of routing. A covered node can be defined as a node belongs to the node routing zone that has received a route query. While forwarding the query packet, a node which determine if it came from its neighbor node or not. If it is coming from the neighboring node, then it will mark the neighboring nodes which are known in its same zone as covered. The query will be forwarded until it reached the destination. The destination will send the reply message back through the reverse path as well as creating the route.

3.3.2 Sharp Hybrid Adaptive Routing Protocol (SHARP):

SHARP adapts both the reactive and proactive type of routing by the proactively shared dynamically varying information about routing. This protocol will describe the zones of proactive nature in the nodes vicinity. The radius of the node-specific zone will describe the total number of nodes in a zone having proactive nature. The nodes which are within the radius of the zone of a particular node will become the node members of that proactive zone. If a node does not existed within a proactive zone for the required destination, the mechanism of reactive routing (query-reply) will be used to make the route to that node. The mechanism of proactive routing will be used within the proactive zone. With respect to the central node, nodes in the proactive zone will maintain the routes proactively. The proactive zones will be created automatically in this protocol, if few destinations are addressed frequently. If the packets have been reached any of the nodes in the vicinity of the zone, the proactive zones will act as packet collectors, which will route the packets to the destination efficiently.

3.4 Hierarchical Routing Protocols:

When wireless network size increases, the flat routing protocols will produce too much of routing overhead for the Mobile Ad hoc Network (MANET). In this case a hierarchical solution may be preferable. Hierarchical state routing (HSR) is primarily depends on the algorithm of Link State routing. Dissimilar to other routing protocols, Hierarchical state routing (HSR) maintains addressing in a hierarchical way and contains map of topology. One of the algorithms which forms clusters like Cluster Gateway Switch Routing (CGSR) can be utilized to keep the nodes in the form of clusters [33]. Every cluster is having three kinds of nodes which are as follows: The first one is a cluster node and it works for each node as a coordinator locally, the other two nodes are the nodes of Gateway and these nodes stay in two different types of cluster.

3.5 Geographical Routing Protocols

There are two approaches to geographic mobile ad hoc networks:

1).Actual geographic coordinates (as obtained through GPS – the Global Positioning System).

2). Reference points in some fixed coordinate system.

One of the major advantages of the geographic routing protocols is that they will stop the searches for various destinations along the network. If the most recent coordinates of particular geographical position are well known then data as well as the control packets will be sent in the direction of the destination. This reduces the control overhead in the network [14]. One of the major disadvantages is that each and every node must access to their coordinates of geographical position most of the time to make the protocols of geographical routing to be more useful. The updates of the routing must be done quickly when compared to the rate of network mobility to ensure the most effective location-based routing. Protocols which come under geographical routing protocols are:

1).Geo-Cast (Geographic Addressing and Routing)

2).DREAM (Distance Routing Effect Algorithm for Mobility)

3).GPSR (Greedy Perimeter Stateless Routing)

CHAPTER 4 Transmission Control Protocol (TCP)

4.1 Transmission Control Protocol (TCP)

The research of The Transmission Control Protocol (TCP)/Internet Protocol (IP) was developed before the development of Open System Interconnection (OSI) model. So, the layers in the Transmission Control Protocol (TCP)/Internet Protocol (IP) will not match the layers in the Open System Interconnection (OSI) model. The TCP/IP protocol which was developed contains four types of layers which are the layer of host-to-network, internet layer, transport layer, and application layer. While comparing TCP/IP model to that of OSI model, the functionality of the layer of host-to-network is equal to the physical and data link layers combination [34]. The functionality of internet layer and network layer are same, and the functionality of the application layer is equal to the functionality of the presentation, session and application layers. And the transport layer of Transmission Control Protocol (TCP)/Internet Protocol (IP) will perform some functionalities of the session layer. So, the Transmission Control Protocol (TCP)/Internet Protocol (IP) protocol contains five layers which are Physical Layer, Data Link Layer, Network Layer, Transport Layer, and Application Layer. The top four layers of the Transmission Control Protocol (TCP) will give physical standards, interfacing of the network, inter-networking, and transport functionalities which is similar to the top four layers of the Open System Interconnection model. The first three layers in the model of OSI are indicated in Transmission Control Protocol (TCP)/Internet Protocol (IP) with a single application layer.

TCP/IP is a hierarchical type of protocol which contains modules of interactive type and gives a particular type of functionality. However, it is not necessary for the modules to be dependent on each other. In case of model of OSI, it specifies the implementations of functionalities which belong to different layers, the TCP/IP protocol layers of different protocols which are independent and they can be matched and assembled which depends on the system requirements. If the protocol of the upper-level is supported by the protocols of one or more lower-level is called hierarchical protocol. At the level of transport layer, three protocols are defined by TCP/IP which is called User Datagram Protocol (UDP), Transmission Control Protocol (TCP) and Stream Control Transmission Protocol (SCTP). At the level of the network layer, the Internetworking Protocol (IP) defines the TCP/IP. The basic TCP/IP model with the functioning of the each layer is as shown in figure 4.1. Apart from this, there are few different protocols which support movement of data in this layer.

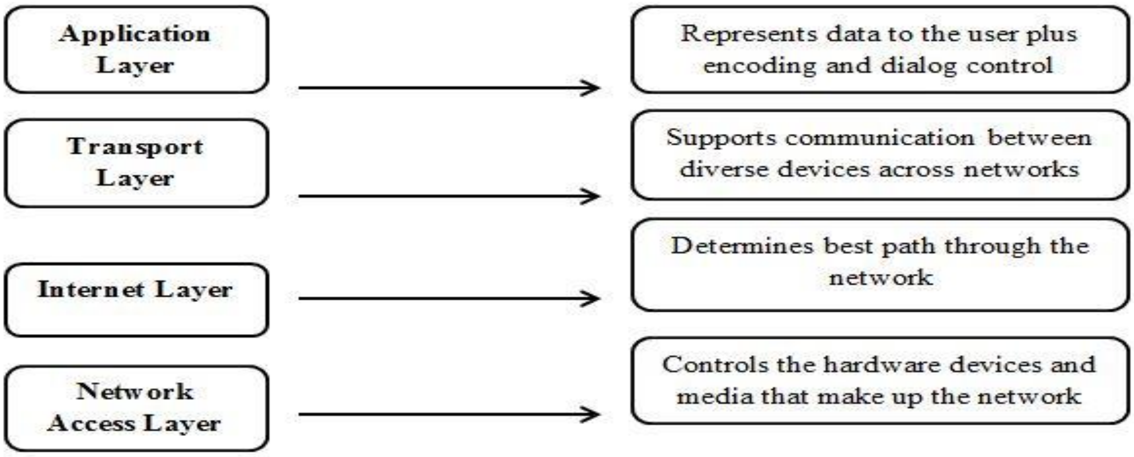

Application Layer
Transport Layer
Internet Layer
Network Access Layer
Represents data to the user plus encoding and dialog control
Supports communication between diverse devices across networks
Determines best path through the network
Controls the hardware devices and media that make up the network

Figure 4.1 Basic TCP/IP Model

4.1.1 Physical and Data Link Layers

Transmission Control Protocol (TCP) /Internet Protocol (IP) will not define any specific protocol at the data link and physical link layers. TCP will support the protocols of standard as well as the proprietary. A network in Transmission Control Protocol (TCP)/Internet Protocol (IP) inter-network will be either a network of local area or a network of wide-area. The physical performs the functionality which is necessary to transmit the bit stream over the existing physical medium [35]. It also coordinates the specifications of the electrical as well as the mechanical functions of the medium of transmission and interface. It also describes the functionalities that how interfaces and physical devices have to work for the efficient transmission of data. The rate of the transmission will be defined by the physical layer. It defines the bit duration as well. The synchronization between the sender and receiver in terms of data transmission will be achieved through Physical layer. The physical layer also deals with Line Configuration like connecting the devices through point-point configuration in which two devices will be connected as well as configuration of multi-point where several devices will be connected. It defines the type of network topology through which various devices are connected like Ring Topology, Star Topology, Mesh Topology, Bus Topology and Hybrid Topology. The physical layer describes the transmission direction among various devices like Full-Duplex, Half-Duplex and Simplex.

The data link layer performs the function of making the data free from the errors obtained from the physical layer to the network layer. The data link layer converts the bits of data obtained from network layer into frames. The data link layer establishes the physical address to the frame by attaching the header to the frame, so that the frame will be routed to the desired destination device [36]. It performs the operation of the mechanism of the flow control through which the receiver should not be overburdened as sometimes the data transmission of the transmitter will be more than data reception rate of the receiver. The data link layer re-transmits the lost or damaged frames as well as identifying the duplicate frames in order to avoid the errors by performing the error control mechanism. It performs the access control mechanism when multiple devices try to access the available single link.

4.1.2 Network Layer

At the level of network layer, TCP/IP supports four supporting protocols which are Address Resolution Protocol (ARP), Reverse Address Resolution Protocol (RARP), Internet Control Message Protocol (ICMP) and Internet Group Message Protocol (IGMP). The kind of mechanism used by the TCP/IP protocols for transmission is Internetworking Protocol (IP). IP is connectionless and un-reliable protocol and its best efforts for service delivery which indicates that IP will not provide checking of errors as well as tracking. IP will assume the underlying layers un-reliability and it will do its best to get a transmission through to its destination, without any guarantees. IP sends the data in the form of packets called datagrams and each of these datagrams will be sent separately. These Datagrams will be sending along various routes and they will arrive out of the sequence and sometimes it can be duplicated. Internet Protocol does not any control of route tracking as well as it does not have any option for reordering the datagrams which are already reached at the destination. Internet Protocol gives effective functionality of transmission which allows free the user to attach only these facilities which are necessary for a specific application and the maximum efficiency.

a) Address Resolution Protocol: For associating the logical address with physical address, the Address Resolution Protocol (ARP) was useful. In a complicated physical network, like Local Area Network (LAN), every device which was connected with that particular link will be recognized with either station address or physical address. When the Internet address of the node is found, Address Resolution Protocol is utilized to determine the node’s physical address.

b) Reverse Address Resolution Protocol: The Reverse Address Resolution Protocol (RARP) allows the host to determine the Internet address when the physical address is well-known. The internet address is utilized by the computer/work station when it is connected to the network for the first time.

c) Internet Control Message Protocol: The mechanism of Internet Control Message Protocol (ICMP) was utilized by gateways as well as the hosts in order to send the notification of the problems of the datagram to the sender. ICMP sends the messages like error reporting and query.

d) Internet Group Message Protocol: The Internet Group Message Protocol (IGMP) was utilized to allocate the simultaneous message transmission to a large group of receivers.

4.1.3 Transport Layer

The transport layer in TCP/IP was represented by two protocols which are TCP and UDP. Generally, IP works as host-to-host protocol as it can send packets from one physical device to another physical device [37]. UDP and TCP serves as protocols in transport level as they are responsible for message delivery from one process to another process. A new type of transport layer protocol called SCTP has been obtained to achieve the requirements of advanced applications.

a) User Datagram Protocol: The User Datagram Protocol (UDP) is the simplest protocol of the transport protocol of Transmission Control Protocol (TCP)/Internet Protocol (IP). UDP is a protocol of process-to-process type which adds addresses of the ports, error control techniques like checksum and information containing length of the data from the upper layer.

b) Transmission Control Protocol: The Transmission Control Protocol (TCP) will support the complete services of the transport layer to applications. As TCP is a reliable and stream oriented transport-layer protocol. As the term stream indicates the orientation of connection. A connection should be provided between the transmitting end and receiving end to achieve the data transmission. Every time, when sending the data, TCP break the data stream into smaller segments. Every segment contains the sequence number for along with an acknowledgment number for the received segments. Segments will be transmitted across the network inside the datagrams of IP. At the receiving end, TCP gather the datagram as it is and again orders the transmission based on the sequence numbers.

c) Stream Control Transmission Protocol: The Stream Control Transmission Protocol (SCTP) gives the support for various newer applications like voice over Internet. It is a protocol of transport layer which assembles the characteristics of UDP and TCP.

The following diagrams shows the different functionalities/Services provided by the different layers of the Transmission Control Protocol (TCP). The services offered by Application layer are FTP, SMTP, HTTP, BOOTP DHCP, TFTP, DNS and PING. The services offered by the Transport layer id TCP, UDP and ICMP [38]. The services offered by the Network Layer are ARP, IP. The Ethernet service is provided with the help of Physical Layer. The different services provided by the different layers of the TCP are as shown in the figure 4.2.

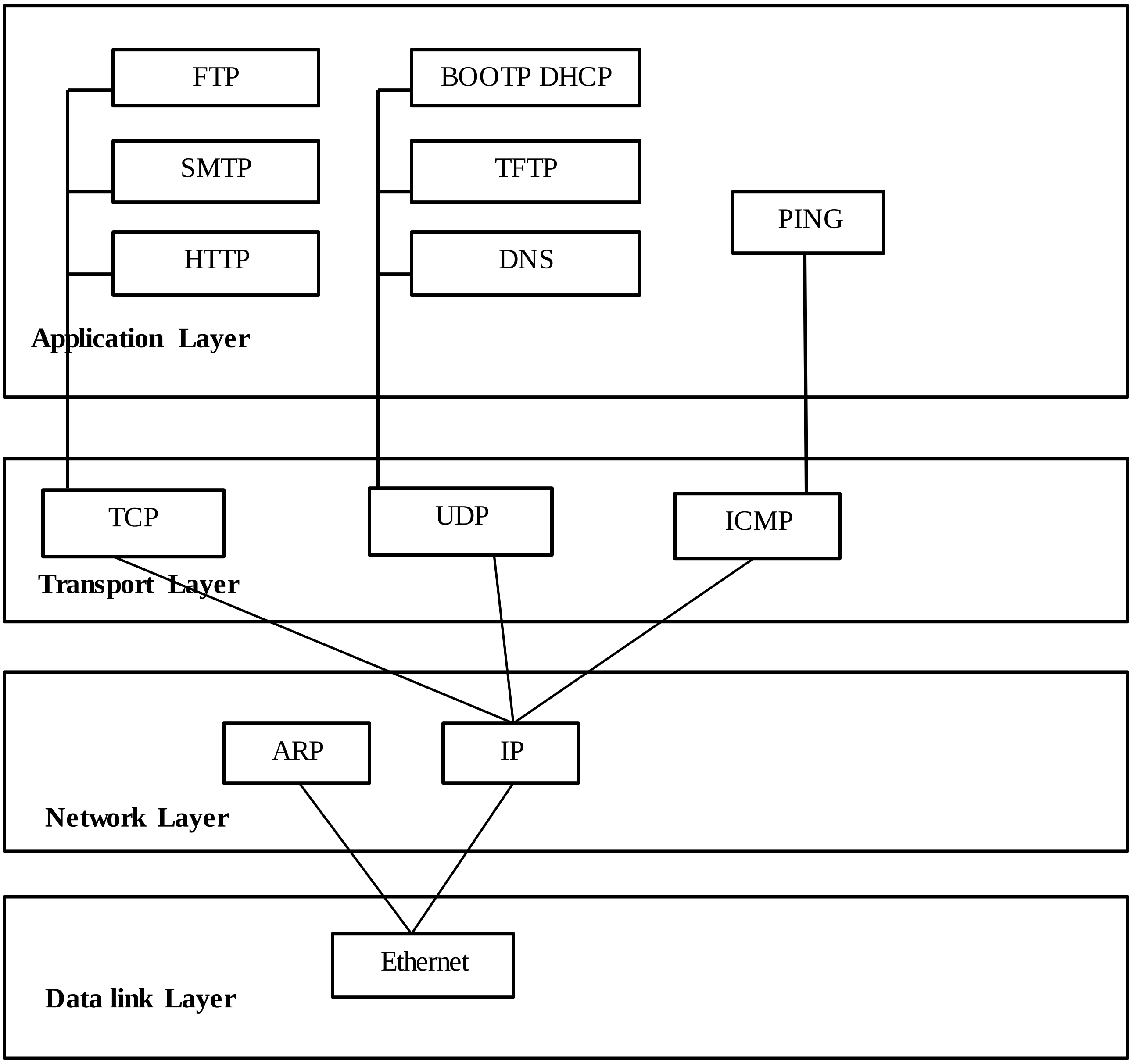


Figure 4.2 Services offered by the different layers of TCP

4.1.4 Application Layer

The application layer allows the user; either it is human based or software based for getting access the over network. Application Layer generally provides user interfaces and supporting various services like remote file access, electronic mail, shared database management, transfer and some different types of information services in distributed manner. The application layer gives the database sources in a distributed manner and tries to access the information globally regarding various services [39]. This is the layer which provides the service of forwarding the email as well as the storage of the emails. This layer permits the users to get access to various documents presented in remote locations as well as fetching the files from remote work stations to the personal computer.

4.2 Variants of the Transmission Control Protocol (TCP)

Based on the establishment of the communication between the sender/source nodes, intermediate nodes, receiver/destination nodes and the handling the route creation as well as the failure of the routes, various researchers have introduced different modifications to the traditional/standard TCP to improve the performance of the TCP as well as handling the route failures effectively which are also called as TCP variants. The different variants of standard/basic TCP are Feedback based TCP, TCP Explicit link failure notification (TCP-ELFN), Ad hoc TCP (ATCP), Split TCP (STCP) and TCP-Bus. These different variants use different techniques in order to handle the route failure and achieve the optimized performance which can be described as below.

4.2.1 Feedback based TCP (TCP-F):

Feedback based TCP is one of the approaches in order to tackle the failure of routes in Mobile ad hoc Networks (MANETs). This kind of approach will permit the sender of TCP to differentiate the losses between failure of routes and congestion in the network. This can be implemented in the following manner. When the node routing agent will find the failure of the route, the node will send a notification of the Failure of the route in the form of packet to the sender node. After the reception of the notification of the failure of the route, the sender node will go into a state called snooze state. The sender of the TCP will be in the state of snooze and the sender will not send the packets for some amount of time and remain in the state of freeze which are timers as well as the size of the congestion window. The sender of the TCP will stay in the state of snooze till it is informed with the re-establishment of the route with the help of notification of Route Re-establishment. Upon the reception of the notification of the route re-establishment, the sender of the TCP will leave the state of snooze and resume the transmitting the packets on the basis of the past sender window and values of the timeout. In order to avoid the scenario of blocking in the state of snooze, the sender of the TCP, upon the reception of the notification of failure of the route will initiate the timer of the failure of the route. After the expiration of this timer, the algorithm for controlling the congestion will be initiated as usually.

4.2.2 TCP-Explicit Link Failure Notification (ELFN)

It is a technique which is quite alike to Feedback based TCP (TCP-F). This technique is mainly based on the interaction between routing protocol and TCP. The main aim of this interaction is to intimate the agent of TCP about the occurrence of failure of routes. The message of ELFN is used regarding the failure of route to the sender by the protocol for routing [40]. The message of Explicit Link Failure Notification is Internet Control Message Protocol (ICMP) which includes the addresses and ports of sender as well as the receiver and packet sequence number of TCP. After the reception of the Explicit Link Failure Notification message, the source will keep the retransmission timers in snooze state and will stay in sleep mode. During this time, the sender of TCP will check the availabilities of routes which are restored for transmitting the data. If the sender receives the packet of acknowledgment, then the sender of the TCP will resumes the retransmission timers.

4.2.3 Ad hoc TCP (A-TCP)

This technique uses the feedback of network layer. Apart from the failure of routes, Ad hoc TCP consider the Bit Error Rate (BER) of high values for analyzing the overall performance. The sender of the TCP will be in the state of congestion control or in the state of data retransmission. The Ad hoc TCP layer is placed between the IP layers and TCP Layer of the source nodes of TCP. Ad hoc TCP will monitor the information of the present state of the network with the help of Explicit Congestion Notification (ECN) messages and Internet Control Message Protocol (ICMP) message and after that Ad hoc TCP will keep the agent of TCP in the required state. After receiving the message of “Destination Unreachable”, the agent of TCP will into a state called persist state. The agent of TCP in this state will be in the stat of frozen and no packets will be sent till a new route is established. The Explicit Congestion Notification (ECN) will be used as a mechanism to inform the sender explicitly about the congestion in the network. After receiving the Explicit Congestion Notification (ECN), Congestion control algorithm of TCP will be initiated. For detecting the loss of packets because of errors in the channels, the Ad hoc TCP will monitor the received Acknowledgements [41]. Upon the reception of three duplicate Acknowledgements by Ad hoc TCP, the TCP will not forward the third duplicate acknowledgement but it keeps the TCP in the state of persistent and retransmits the lost packet as early as possible from the buffer of the TCP. Upon reception of the next acknowledgement, the Ad hoc TCP will make TCP back to the normal state. Ad hoc TCP will evaluate under different parameters such as lossy links, congestion, packet reordering and partition. With all of these parameters, the transfer time of a given file using Ad hoc TCP has given enhanced performance when compared to standard TCP.

4.2.4 TCP-BuS

The capability of Buffering and Sequence information utilize the feedback of the network to detect the failure of the routes. The basic scheme in this proposal is the capability of buffering in mobile nodes. The source-initiated On-demand Associativity Based Routing protocol has been selected for this scheme. The following enhancements are proposed which are Explicit notification, Extending timeout values, Selective Retransmission request, Avoiding unnecessary requests for fast retransmission, Reliable retransmission of control message

Explicit Notification: In Explicit Notification, two control messages will be utilized to inform the source regarding the failure of the route and re-establishment of the route. These type of messages are called Explicit Route Disconnection Notification (ERDN) and Explicit Route Successful Notification (ERSN). Upon reception of the ERDN from the node which detected the failure of the route, the source will stop sending. After the re-establishing the route by the Pivoting Node (PN) by utilizing a Query generated locally, the PN will transmit the Explicit Route Disconnection Notification (ERSN) to the source. Upon reception of the Explicit Route Disconnection Notification ERSN, the source will resume the transmission of data.

Extending timeout values: While reconstructing the route, the packets will be buffered in the path from source to Pivoting Node. For avoiding the events of timeout during the Route Re-Construction phase, the value of the retransmission timer for the buffered packets will be doubled.

Selective retransmission request: As the value of retransmission timer value is doubled, the packets which are lost in the path from the source to Pivoting Node will not be retransmitted till the expiration of the adjusted retransmission. In order to avoid this problem, source will be given an indication which retransmits the lost packet in a selective manner.

Avoiding unnecessary requests for fast retransmission: When a route is constructed back, the destination will notify the source regarding the lost packets in the path from the Pivoting Node to destination [42]. Upon reception of this notification, the source will retransmit these lost packets. The packets which are buffered in the path from the source to the Pivoting Node will arrive at the destination much earlier than the packets which are retransmitted. In this case, the destination will reply with duplicate acknowledgements. These request packets which are not necessary will be avoided for fast retransmission.

Reliability of retransmitted control message: For getting the reliable operation of TCP-BuS, the routing control messages like Explicit Route Disconnection Notification (ERDN) and Explicit Route Successful Notification (ERSN). The reliability of the transmission is achieved by overhearing the channel upon transmission of the control messages. If a node sent a control message but did not overhear this message which was relayed during the timeout, it will conclude that the control message will be lost and it will retransmit this message.

4.2.5 Split-TCP

The connections of TCP which are having the large number of hops will experience the route failures frequently because of mobility. For improving the throughput of these connections and to rectify the non-equity problems, a scheme of Split-TCP was introduced to remove the large TCP connections. The interface node which is located between two segments is called the proxy. The agent used for routing will determine if the node which acts as a proxy will be utilizing the inter-proxy distance. The comparison of various TCP variants based on different parameters is shown in table 4.1.

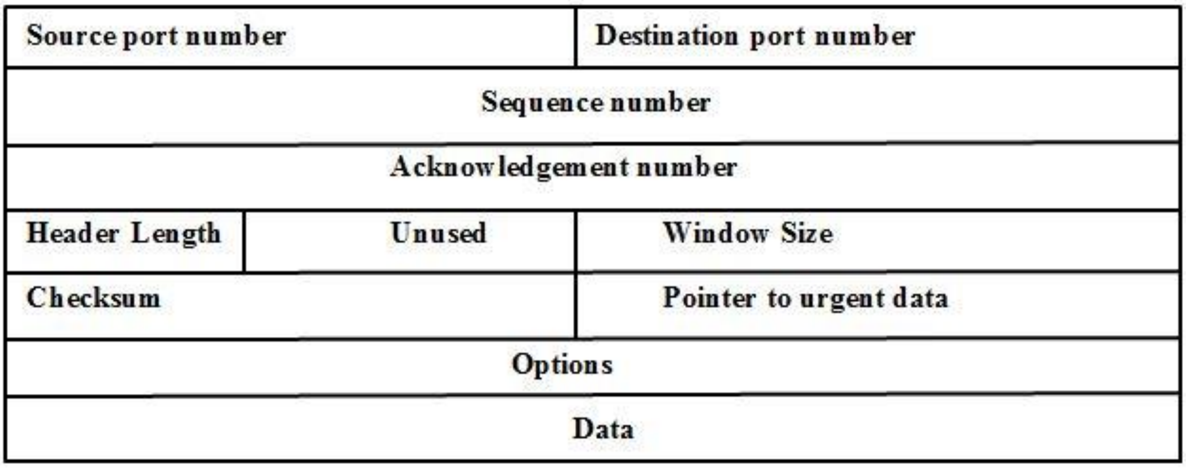
Parameter	Feedback based TCP (TCP-F)	TCP-ELFN (Explicit Link Failure Notification)	Ad hoc TCP (ATCP)	TCP-Bus
Detection of Route failure	The packet of Route Failure Notification (RFN) will freeze the timers of TCP sender	The packet of Explicit Link Failure Notification (ELFN) will freeze the timers of TCP sender	Internet Control Message Protocol (ICMP) "destination unreachable" message will freeze the timers of TCP sender	The Explicit Route Disconnection Notification (ERDN) packet freezes the timers of TCP sender
Bit Error Rate (BER)	Can be handled up to some extent	Cannot be handled	Can be handled	Cannot be handled
Detection of Route Reconstruction	The packet of Route Re-establishment Notification (RRN) will unfreeze the timers and resumes the TCP to its original state	Route Re-establishment can be detected with the help of probing mechanism	Route Re-establishment can be detected with the help of probing mechanism	The packet of Explicit Routing Successful Notification (ERSN) will unfreeze the timers and resume the TCP to its original state
Reordering of the Packets	Can be handled up to some extent	Cannot be handled	Can be handled	Cannot be handled
Congestion Window and Retransmission timeout (RTO) after Route Reconstruction	Old Congestion Window and Re-Transmission timeout	Old Congestion Window and Re-Transmission timeout	Reset for each new Route	Old Congestion Window and Re-Transmission timeout
Reliability of transmitting control messages	Cannot be handled	Cannot be handled	Cannot be handled	Cannot be handled

Table 4.1 Variants of TCP on the basis of various parameters

The proxy will receive the TCP packets and store them and send the acknowledgement to the source nodes by sending the acknowledgment locally. The proxy is the main reason for transferring the packets with required rate to the next segment which is located locally. After the reception of Local Acknowledgement, the proxy will serve the buffer of the packet. To maintain source to the destination reliability, an Acknowledgement will be sent from destination to the source just like basic TCP. This will be obtained by utilizing the two windows which are end-to-end window and congestion window. The end to end window contains congestion window as well.

4.3 Segment structure of Transmission Control Protocol (TCP)

The Transmission Control Protocol will get data from a stream of data and divide the data into chunks and attach a TCP header which creates the segment of TCP. The segment of the TCP will be encapsulated into an Internet Protocol (IP) datagram which is then exchanged with the peers. The TCP packet is different from the segment of TCP; the segment of TCP refers to the TCP protocol data unit (PDU), datagram to the IP PDU, and frame to the data link layer PDU. The Processes will transmit the data by calling the TCP and pass the buffers of data in the form of arguments. The TCP will pack the data which is obtained from these buffers into the segments and calls the IP module in order to transmit every segment to the TCP destination [43]. The segment structure of the TCP is as shown in the figure 4.3. A segment of TCP comprises of data section and segment header. The header of TCP includes 10 mandatory fields and an extension field which is optional. The header is followed by the data section. The contents of data section are payload data which is carried for application. The data section length is not specified in the segment of TCP header. It is obtained by subtracting the combined length of the header of the TCP and the IP header in encapsulated form from total length of the Internet Protocol datagram.



Source port number		Destination port number
Sequence number		
Acknowledgement number		
Header Length	Unused	Window Size
Checksum		Pointer to urgent data
Options		
Data		

Figure 4.3 Segment structure of TCP

CHAPTER 5 PROBLEM BACKGROUND

5.1 Comparison of MANETs with Wired Networks

MANETs are different from wired networks with regards to hardware infrastructure, addressing, naming and routing. There is a clearer view of the limitations and strengths of the ad hoc networks. These differences are explained in the following subsections.

5.1.1 Infrastructure

A conventional network most often consists of a fixed infrastructure that is built up of computer nodes, routers, switches, bridges, base stations, gateways and other network devices that are all connected with wires. One of the main characteristics of these networks is that their topology is fixed. When there is a need to reconfigure the network or add more network devices there has to be physical manual intervention. During the reconfiguration of the network, there is most often loss of services in either nodes or the entire network while the changes are carried out. Moreover, traditional wired networks usually have centralized administration, since many of the nodes rely on central servers for storage, access and processing of data.

Wireless networks and more specifically ad hoc networks follow a different paradigm that resolves some of these issues. Due to the use of wireless signals as a transmission medium that is utilized in wireless networks, problems of cabling reconfiguration and possible service unavailability caused by topology changes are avoided. Ad hoc networks add to this ability and allow the formation of networks on-the-fly without the need of any existing infrastructure [44]. The results is an on-demand network that has all the advantages of the wireless network combined with a virtually easy to setup system, in contrast with the conventional wired networks where their establishment requires tedious administrative tasks. Furthermore, since ad hoc networks are formed without any external aid but from the participating nodes themselves, and the topology of the network may change arbitrarily, centralized solutions in administration and in data sharing are not as frequently used as in conventional wired networks.

5.1.2 Addressing

In traditional networks, the address distribution is performed either manually and the network administrator handles the assignment of the addresses or this process is carried out by using special protocols. The servers that implement these special protocols as well as other address allocation entities use the hardware address of the network interface to assign addresses and guarantee their uniqueness. However, in ad hoc networks there is no central authority responsible for assigning IP addresses. Therefore, this issue becomes more complicated. Therefore there is no guarantee that the address that was taken or somehow assigned to the node reflects either the node's geographical location due to mobility, or that it is unique in the present network of which the node is a part.

5.1.3 Routing

The operation of routing in wired networks is performed by special dedicated equipment that can either be hardware-based devices designed for this task or computer nodes equipped with several network interfaces and adequate software to perform the actual routing [45]. In ad hoc networks a node does not need to be equipped with several network interfaces, since all communication is usually done through a single wireless channel which is broadcast in nature. In distinction with that of wired networks, in case of ad hoc networks all the nodes in the network have to participate in routing process. Each and every node in the ad hoc network must forward network traffic in favor of other nodes. All the nodes that are participating in the process of routing set up the network traffic to flow over multiple hops of the ad hoc network.

An important property of ad hoc routing is that a flat addressing scheme is used, thus the routing tables of the participating nodes may end up consisting of separate IP addresses with no correlation to each other. On the other hand, in wired networks, routing tables most often contain network prefixes along with the appropriate network interface identifiers and not specific addresses.

5.2 Problem Definition in TCP

TCP is very reliable and successful protocol ever since its deployment in fixed networks both wired and wireless networks. Internet and World Wide Web networks are very good examples that show the excellent performance of TCP. Efficiency and security are its key features. Transmission Control Protocol (TCP) is the predominant Internet protocol and it carries approximately 90% of Internet traffic in today‘s heterogeneous wireless and wired networks. Transmission Control Protocol (TCP) is end to end reliable protocol as it tries to provide data transmission between two nodes with higher reliability. TCP is widely used as a connection oriented transport layer protocol that provides reliable data packet delivery over unreliable links. The primary purpose of Transmission Control Protocol (TCP) is to provide reliable and connection oriented data transfer service among different applications and should be able to give these kinds of services even on the top of a communication system which are having unreliability [46]. It is necessary for Transmission Control Protocol (TCP) to consider data transfer, reliability flow control, multiplexing, TCP segment, and congestion control and connection management. TCP does not depend on the underlying network layers and, hence, design of various TCP variants is based on the properties of wired networks. A basic TCP/IP model is shown in the figure 3.1. But it is not possible for congestion control algorithms of Transmission control protocol (TCP) to perform well in different networks up to the mark. The Transmission Control Protocol (TCP) has been extensively tuned to give good performance at the transport layer in the traditional wired 27 network environment. Transmission Control Protocol (TCP) in its standard form is not suitable for mobile ad hoc networks (MANETs) because loss of packets due to link failures will leads to invocating of Transmission Control Protocol (TCP) congestion control mechanisms.

A serious issue arises when such a successful protocol fails in case of MANETs. The question arises why does TCP’s performance degrades in MANETs. After studying the structure and nature of MANETs, it is found that mobility of the nodes is the main reason of the failure.

The mobility of the nodes causes frequent changes in the topology of MANET network. This intern causes frequent route failures.

In this thesis, it has been tried to trace out the problems of TCP in MANETs, their reason and find suggest an approach to improve the performance of protocol.

Following problems are being faced in a mobile network:-

1) Congestion

2) Bandwidth utilization

3) Delay

There are various protocols used in order to overcome congestion, bandwidth utilization, delay.

A topology will be created and then a comparison is made with its output and overall performance with respect to the other topologies. The following parameters will be considered for the comparison of performance:

1) Delay

2) Bandwidth

3) Throughput

4) Good put

5) Energy efficiency

6) Round Trip Delay time

So, frequent link failures and re-establishment cause a very unpredictable connectivity among nodes in network. In such a scenario it is very obvious for TCP to fail, it being a connection-oriented protocol. The following figure shows TCP

5.2.1 Behavior of TCP in Ad-hoc Networks

TCP is a reliable, stream-oriented transport layer protocol which has been designed for use over fixed networks like the Internet. It has been established that packet error/loss rates over the Internet due to transmission errors are of the order of 1%. In other words, packets are rarely lost [47]. Route failures and disruptions are very infrequent as the network is fixed. Therefore, packet loss, which is detected by TCP as a timeout, is interpreted to be a symptom of congestion in the network. In response, TCP invokes congestion control mechanisms. In other words, TCP cannot distinguish between congestion on the one hand and packet loss due to transmission errors or route failures on the other. This inability of TCP to differentiate between congestion and packet loss leads to degradation of performance in ad-hoc networks. In an ad-hoc network, packet losses are frequent in the error-prone wireless medium. However, the effect of these losses can be reduced using reliable link layer protocols. Route failures, which can occur frequently and unpredictably during the lifetime of a transport session, depending on the relative motion of MHs in the network, are more difficult to handle. The mobility of node causes route disruption, when the routing protocol reestablishes the route, it will take so much time to construct the route back again. During this period of time, no packet can reach the destination through the existing route. This will result in the queuing and possible loss of packets/acknowledgements, which will be interpreted by the transport protocol at the source as congestion.

Consequently the source will:

1. Retransmit unacknowledged packets upon timing out.

2. Invoke congestion control mechanisms that include exponential back-off of the retransmission timers and immediate shrinking of the window size, thus resulting in reduction of the transmission rate

3. Enter a slow start recovery phase to ensure that the congestion has reduced before resuming packet transmission at the normal rate.

This is undesirable for the following reasons:

1. When there is no route available, there is no need to retransmit packets that will not reach the destination.

2 .Packet retransmission wastes precious MH battery power and scarce bandwidth.

3. In the period immediately following the re-establishment of the route, the throughput will be unnecessarily low as a result of the slow start recovery mechanism even though there is actually no congestion in the network.

From study of above sections, it is concluded that mobility of nodes causes a degraded performance of TCP protocol, since there are losses in transmitted packets and also high delays [48]. Problem further worsens when TCP invokes congestion control which is not the required solution. Higher mobility rate and high network density combined with high traffic rate would cause worst possible problem in MANETs. Hence a solution approach is needed that can improve the performance of protocol.

CHAPTER 6 PROPOSED RESEARCH OBJECTIVE

The Proposed Research Objective includes:

1) To improve the Performance of TCP using Feedback Scheme and adaptive back-off response and classify the type of TCP on the basis of the effective utilization of the congestion window size. By this way, the source can be able to differentiate the failure of routes and congestion in the network to handle the failure of routes in an efficient manner in the ad hoc networks.

2) Reducing the Round Trip Delay Time (RTT) by introducing the notifications of the failure of the routes as well as the re-establishments of the routes and saving the power of the source as well as the destination nodes.

3) To reduce the packet-loss or packet-drop in TCP as well as increasing the packet delivery ratio by searching the alternate routes and avoiding the transmission network transmission errors.

4) Implementing the requirements of Quality of Service like reserving the bandwidth by evaluating the performance of network in terms of throughput and routing overheads for different number of nodes.

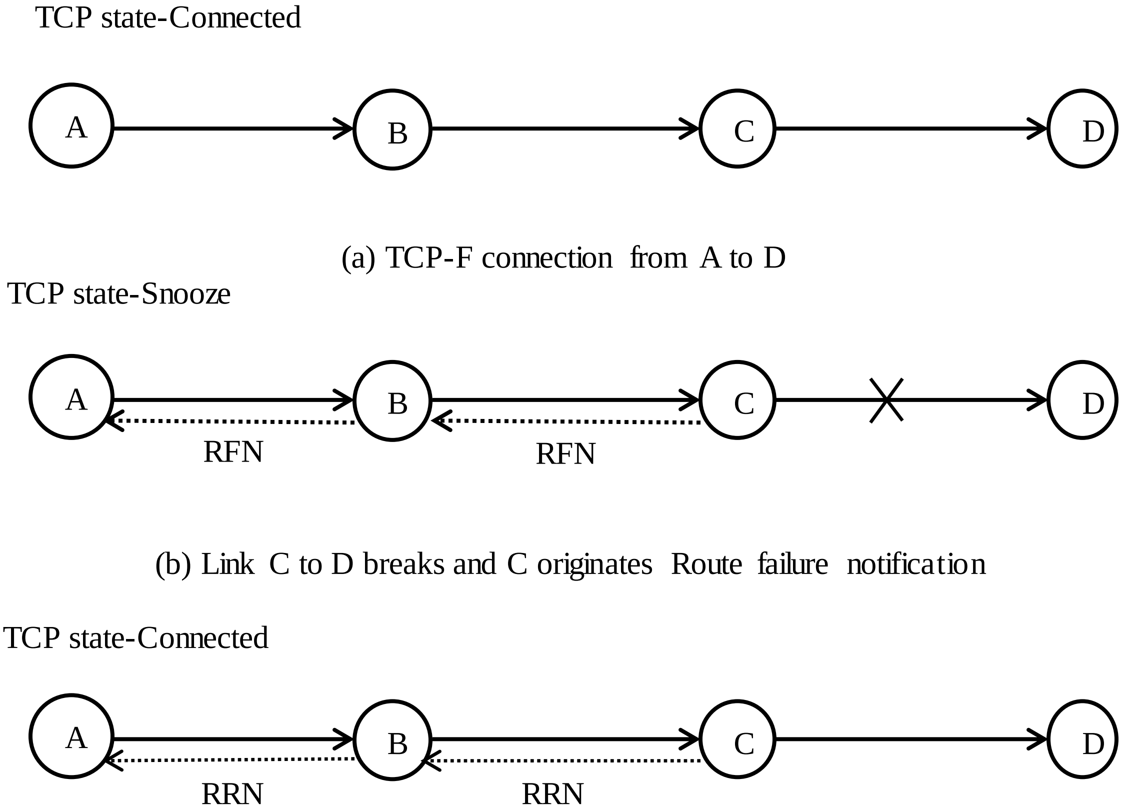
CHAPTER 7 PROPOSED RESEARCH METHODOLOGY

The proposed research methodology introduces feedback based and adaptive back-off response approach for improving the performance of the TCP. This methodology can be implemented using NS-2 Simulator and various performance parameters like Throughput, Good-put, Round trip delay time (RTT) can be measured. It proposes modifications to the traditional TCP for improving performance in ad hoc wireless networks. TCP feedback requires the support of a reliable link layer and a routing protocol that can provide feedback to the TCP sender about the path breaks. The protocol for routing has to restore the broken link as early as possible. TCP feedback aims to minimize the throughput degradation resulting from the frequent path breaks that occur in ad hoc wireless networks. During the session of Transmission control protocol (TCP), there will be several breakages of paths which results in significant loss of packets and delay occurred due to re-establishing of path. Upon detection of packet loss, the sender in a TCP session invokes the congestion control algorithm leading to the exponential back-off of retransmission timers and a decrease in congestion window size.

7.1 Feedback based TCP (TCP-F) with adaptive back-off response

In TCP Feedback, an intermediate node, upon detection of a path break, originates a route failure notification (RFN) Packet. This RFN Packet is routed toward the sender of the TCP session. The TCP sender's information is expected to be obtained from the TCP packets being-forwarded by the node. The intermediate node that originates the RFN packet is called the failure point (FP). The failure point maintains information about all the RFNs it has originated so far. Every intermediate node that forwards the RFN packet understands the route failure, updates its routing table accordingly and avoids forwarding any more packets on that route. If any of the intermediate nodes that receive RFN has an alternate route to the same destination, then it discards the RFN Packet and used the alternative route to the same destination, then it discards the RFN packet and uses the alternate path for forwarding further data packets, thus reducing the control overhead involved in the route reconfiguration process. Otherwise, it forwards the RFN toward the source node. When the sender of TCP receives a notification packet of route failure, it will go into snooze state. In the snooze state a sender stops sending any more packets to the destination, cancels all the timers, freezes its congestion window, freezes the retransmission timer, sets up a route failure timer. This failure timer is dependent on the routing protocol, network size and the network dynamics and is to be taken as the worst case route reconfiguration time. When the route failure timer expires, the TCP sender changes from the snooze state to the connected state.

When the node receives the notification packet of route re-establishment, it will transmit all the packets which are stored in its buffer, assume that the network reached its previous state. A Feedback based TCP model is shown in the figure 7.1. This can also take care of all the packets that were not acknowledged or lost during transit due to the path break. In fact such a step avoids going through the slow-start process that would otherwise have occurred immediately after a period of congestion. The route failure timer set after receiving the RFN packet ensures that the sender does not remain in the snooze state indefinitely.



(a) TCP-F connection from A to D

(b) Link C to D breaks and C originates Route failure notification

(c) Link C-D rejoins and C originates Route Re-establishment Notification

Figure 7.1 Implementation of Feedback based TCP with nodes A, B, C, D

Once the route failure timer expires, the sender goes back to the connected state in which it reactivates the frozen timers and start sending the buffered and unacknowledged packets. This can also take care of the loss of the RRN packet due to any possible subsequent congestion. TCP Feedback permits the TCP congestion control algorithm to be in effect when the sender is not in the snooze state, thus making is sensitive to congestion in the network. Based on the effective utilization of the congestion window size, the implemented feedback based TCP protocol is classified into two types used for different applications which are Full Congestion window TCP termed as Fcwnd-TCP and Partial Congestion window TCP termed as Pcwnd-TCP which are briefly described as below.

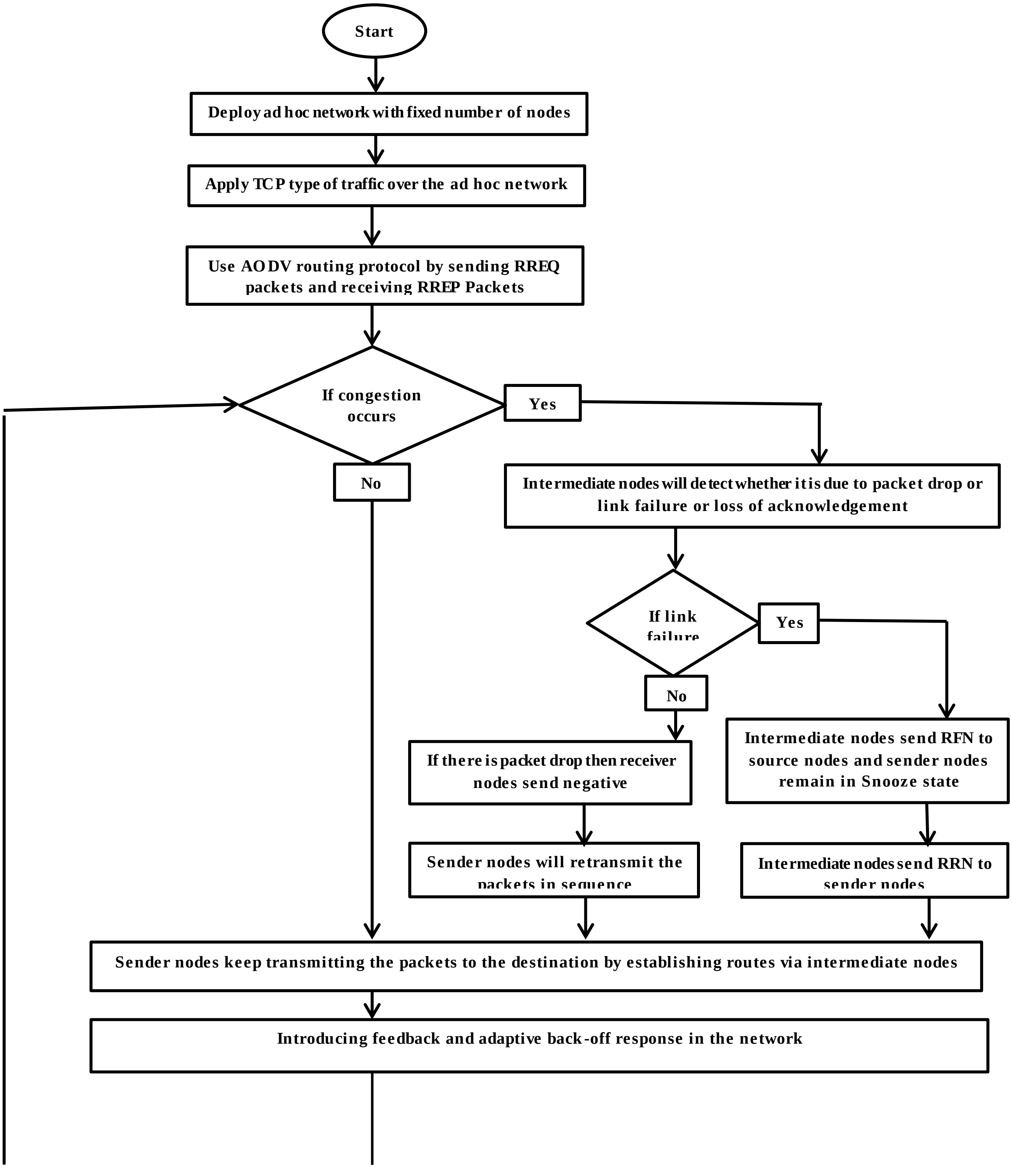
7.1.1 Full Congestion window TCP (Fcwnd-TCP)

The advantage of Full Congestion window TCP (Fcwnd-TCP) is the utilization of the high bandwidth of the network. When compared to standard TCP Full congestion window TCP (Fcwnd-TCP) have the supportively of big-sized congestion window. Full congestion window TCP (Fcwnd-TCP) modifies the size of the window which was released and locked due to the occurrence of the congestion which is the motive of the total size of the window. If the size of the window is small, then Full Congestion window TCP (Fcwnd-TCP) will works as similar to the standard TCP. If the window size is large then Full Congestion window TCP (Fcwnd-TCP) increases the size of the window by choosing the value based on the exact window value in the operation. These changes eliminate the slow working of ordinary TCP. Full Congestion window TCP (Fcwnd-TCP) works well and it permits the full consumption of multiple gigabit links and high delay. On the basis of the magnitude of window size, the increase in larger size and decrease in smaller size of the window makes the Full Congestion window TCP (Fcwnd-TCP) to give better performance than the ordinary TCP. This approach makes high-speed ad hoc links to full utilization and it does not degrade the advantages of the ordinary TCP. Even when Full Congestion window TCP (Fcwnd-TCP) share bandwidth with the ordinary TCP connections, the performance is still good. Multiple connections of the ordinary TCP is having almost the same performance of the single connection of the Full Congestion window TCP in terms of controlling the congestion. Some protocols which are non-TCP can delay the connections of the ordinary TCP which are not TCP-friendly. When the source node receives the acknowledgement from the destination node then the source node will evaluate the Round trip delay time (RTT) and this value is stored in the RTT Table. Using RTT table, the average and maximum values are found and it is used to calculate the bandwidth availability. From the minimum RTT value and the RTT value, arrival and the expected rate of the connection is calculated. From the RTT differences, the variation will be estimated and if the arrival rate is high or the variation is high, then the size of the window will be adjusted. With the consecutive value of the window, the state of the window will be identified whether it is open, variant, close. If the window is in the state of open, then average variation of the window will be computed from the last point at which it is opened. If the window is in the state of invariant, then the average variation of the window will be computed from the last open point to the point it is in the closing state. The value of the variation will be computed in the form of large, undecided and small. If it is small variation type, then default operation of TCP is executed to enhance the transmission. If it is large type of variation, then the size of the window is adapted to the maximum size of the window and the execution of the transmission is done with respect to the size of the window.

7.1.2 Partial Congestion window TCP

Partial Congestion window TCP (Pcwnd-TCP) protocol is a high type of acceleration which allows devices to achieve the highest throughput for critical situations with high congestion. This protocol optimizes the high link loss. In case of normal TCP, it typically results in underutilization. This protocol removes the congestion control algorithm of TCP from the inner connections. Therefor it permits the link to high saturation and removes the probability of link underutilization. Partial Congestion window TCP (Pcwnd-TCP) protocol is suited for the situations which encompasses the ad-hoc connections which have high packet loss. Partial Congestion window TCP (Pcwnd-TCP) protocol is the standard TCP which does not have congestion control challenges. Partial Congestion window TCP (Pcwnd-TCP) supports the traffic of the network as fast as it can. Once the data of the TCP is sent then the acknowledgement of the packet is received from the destination. When the source node receives the acknowledgement then it calculates the Round trip delay time, upon it stores those values in RTT table. Using that table, the maximum and average values both are found. The product of those values with the bandwidth of the link is used to evaluate the bandwidth availability. Based on the available bandwidth values and class for which bandwidth is calculated with respect to the maximum value of the bandwidth. From the present size of the window and the value of the bandwidth, the frame setting value will be computed. If the present window size is larger than the average window size along with an half utilized value of bandwidth, then no adjustment will be needed for the frame.

If the present window size is larger than the average window size along with unutilized value of bandwidth, then the frame is adjusted to dynamic window size. The Feedback based adaptive Transmission Control Protocol step wise implementation is as shown in the figure 7.2 in the form of flow chart previously.


Start
Deploy ad hoc network with fixed number of nodes
Apply TCP type of traffic over the ad hoc network
Use AODV routing protocol by sending RREQ packets and receiving RREP Packets
If congestion occurs
Yes
No
Intermediate nodes will detect whether it is due to packet drop or link failure or loss of acknowledgement
If link failure
Yes
No
If there is packet drop then receiver nodes send negative
Intermediate nodes send RFN to source nodes and sender nodes remain in Snooze state
Sender nodes will retransmit the packets in sequence
Intermediate nodes send RRN to sender nodes
Sender nodes keep transmitting the packets to the destination by establishing routes via intermediate nodes
Introducing feedback and adaptive back-off response in the network

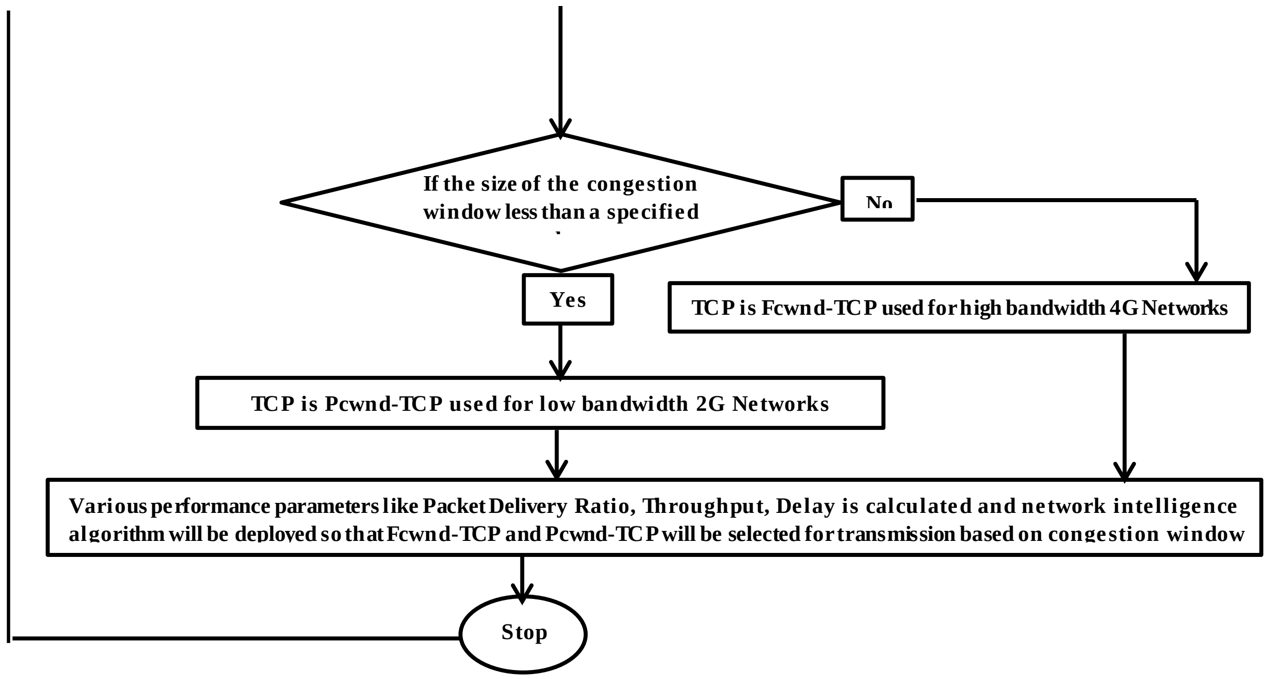

If the size of the congestion window less than a specified
No
Yes
TCP is Fcwnd-TCP used for high bandwidth 4G Networks
TCP is Pcwnd-TCP used for low bandwidth 2G Networks
Various performance parameters like Packet Delivery Ratio, Throughput, Delay is calculated and network intelligence algorithm will be deployed so that Fcwnd-TCP and Pcwnd-TCP will be selected for transmission based on congestion window
Stop

Figure 7.2 Flow chart of implementation of Feedback based TCP with adaptive back-off and it's components Fcwnd-TCP and Pcwnd-TCP

7.2 Comparison of Full Congestion Window TCP and Partial Congestion Window TCP

Full Congestion Window Transmission Control Protocol (TCP) will get the complete usage of expenditure in bandwidth of the network without under-utilizing all the features and advantages provided by TCP. This contains controlling the congestion in a safe manner, even in the situations where the connections of Full Congestion window TCP is sharing the links of Wide Area Network with the normal connections of TCP. It is not necessary to evaluate the Wide Area Network bandwidth availability. Full Congestion Window TCP automatically regulates the throughput required for transmission as per the requirements. In case of Partial Congestion window TCP, it permits the users to utilize the complete available bandwidth between two different geographical locations. Partial Congestion Window TCP usage will leads to considerable loss of packets as well as congestion and is modeled to utilize at specific bandwidth irrespective of loss of packets or congestion. Users can adjust the limit of the bandwidth for Partial Congestion Window TCP which makes them to utilize the complete bandwidth which is available on the allocated connection.

7.3 Algorithm

1) Deploy an ad hoc network with fixed number of mobile nodes in three dimensional space.

2) Apply TCP type of traffic over the ad hoc network.

3) Use Ad hoc On-Demand Distance Vector routing protocol by sending the Route Request Packets (RREQ) from the source nodes towards the destination which are traversing through various intermediate nodes and receive the Route Reply Packets (RREP) from the destination.

4) Feedback scheme will be introduced in the network.

5) Occurrence of congestion in the network:-

(If it is due to congestion)

{

Then, the intermediate nodes will detect whether it is due to packet drop or link failure or due to loss in Acknowledgement

a) Occurrence of link failure

(If it is due to link failure)

{

Then, the intermediate nodes will send the Route Failure Notification (RFN) to source nodes and the sender nodes will remain in snooze state.

After that, the Intermediate nodes will send the Route Re-Establishment Notification to sender nodes upon the detection of routes.

}

(If it is not due to link failure)

{

If there is packet drop, then the receiver nodes will send the negative acknowledgement to the source nodes.

Source nodes will retransmit the packets according to their sequence numbers assigned to each packet.

```
}

}

(If Congestion does not occur)

Sender nodes keep transmitting the packets to the destination by establishing routes via intermediate nodes

5) Feedback Adaptive back-off response will be introduced in the network to improve the performance of TCP

6) Based on the utilization of the size of the congestion window.

(If window size is less than specified value or utilizing partially)

{

        This kind of TCP is Partial congestion window TCP (Pcwnd-TCP) which is used for low bandwidth 2G networks.

}

(If window size is more than specified value of utilizing completely)

{

        This kind of TCP is Full congestion window TCP (Fcwnd-TCP) and used for high bandwidth 4G networks

}

7) Various performance parameters like Packet Delivery ratio, Throughput, Delay is calculated and network intelligence algorithm will be deployed and based on that Fcwnd-TCP and Pcwnd-TCP will be selected for data transmission based on congestion window size.

8) The process will continue as usual until the occurrence of Congestion.
```

CHAPTER 8 RESEARCH OUTCOME

8.1 Performance improvement of TCP using feedback based adaptive nature

The effect of route failures, being the characteristics of ad hoc mobile networks, on basic TCP performance has been studied. In Transmission Control Protocol (TCP), if the source does not know information about the failure of route, the source still transmits packets even the network is in down position. This leads to packet loss and performance degradation. As the TCP considers congestion is the reason for the packet loss, TCP will initiate the algorithm of congestion recovery when the route is reestablished which leads to throttling of transmission.

A scheme called feedback-based Transmission control protocol with adaptive back-off response is proposed such that the failure point will inform the source about the failure of routes and reestablishment of routes thus differentiates the failure of routes from congestion. As the route reestablishment delay grows, feedback based Transmission Protocol with adaptive nature will perform significantly better than basic/standard TCP. This is attributed to the fact that unnecessary timer back-offs was prevented during the route failure interval.

This methodology improved the performance of TCP by reducing the Packet loss so that the source can distinguish between route failure and network congestion and to handle Route failure in ad hoc networks. The methodology increased the throughput, Good-put and reduced the Round trip delay time. This approach reduced the degradation of the performance. As the overall delay was reduced so TCP-F performed better than the basic/standard TCP.

8.2 Performance parameters of TCP

The following are the various performance metrics which gives the improved performance with Feedback based TCP with adaptive nature over the basic/standard TCP.

Good-put (%): The number of useful information bits delivered by the network to a certain destination per unit of time. It does not include protocol overhead bits and retransmitted packets.

End-to-End delay (Seconds): The ratio between the time for receipt of data minus the data transmission time and number of data packets received.

Routing traffic (Normalized routing overhead): The ratio between the number of routed packets and the number of packets received.

Throughput (%): It is given by the received data ratio taking into account all data sent.

Round trip delay time: It is defined as the sum of the time taken for the packet/data to reach the destination from source and the time taken for the acknowledgement packet to reach the source.

Packet delivery ratio: It is the ratio of actual packet delivered to total packets sent.

Bandwidth: Range of frequencies within a given band, in particular that used for transmitting a signal

Packet loss: Packet loss is measured as a percentage of packets lost with respect to packets sent.

8.3 Simulation model in Network Simulator (NS2)

For analyzing the TCP behavior and comparing the performance of basic TCP with the mechanism of the proposed adaptive feedback based TCP, a simulation model was designed in network simulator (NS2) which includes source, destination, intermediate routers, and congestors. The simulation model is shown in the figure 8.1. Congestor will induce the packets of dummy type into the routers with a specific rate of arrival, by this way the traffic load can be controlled in the network. The link controller controls these routers separately and the connection between these routers was established with the help of links which are bidirectional in nature. The link controller will periodically break the links periodically by keeping the state of the link to the “down” and again back to “up” after a specified amount of delay. The link will be randomly chosen and the chances of the failure of each link are equal. While routing the packet from one node to another node or one hop to another hop, if a router observes a link failure, then the packet will be dropped at that instant. If feedback is using at this instant, then the router will forward the messages as notifications to the sender. High amount of priority will be given to these kinds of messages; so, they will not be maintained in queue with normal packets.

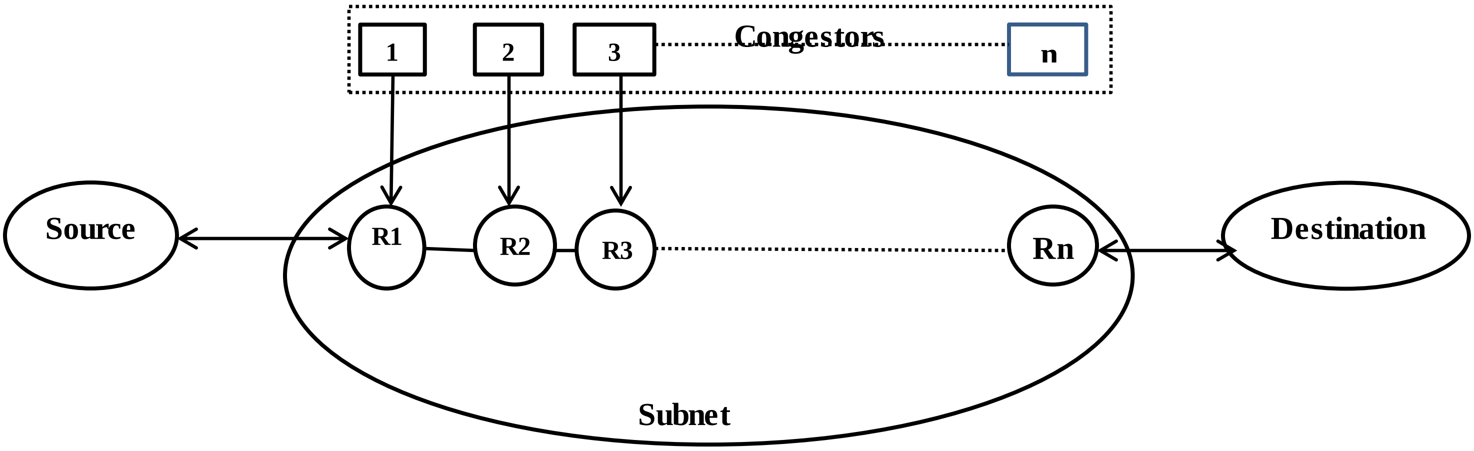


Figure 8.1: Figure showing simulation model of feedback based TCP protocol with adaptive back-off response with nodes and routers

Feedback based TCP mechanism is used at the destination as well as the source. The implementation of the TCP and it's simulation model implemented in network simulator (NS2) is shown in figure 8.2.

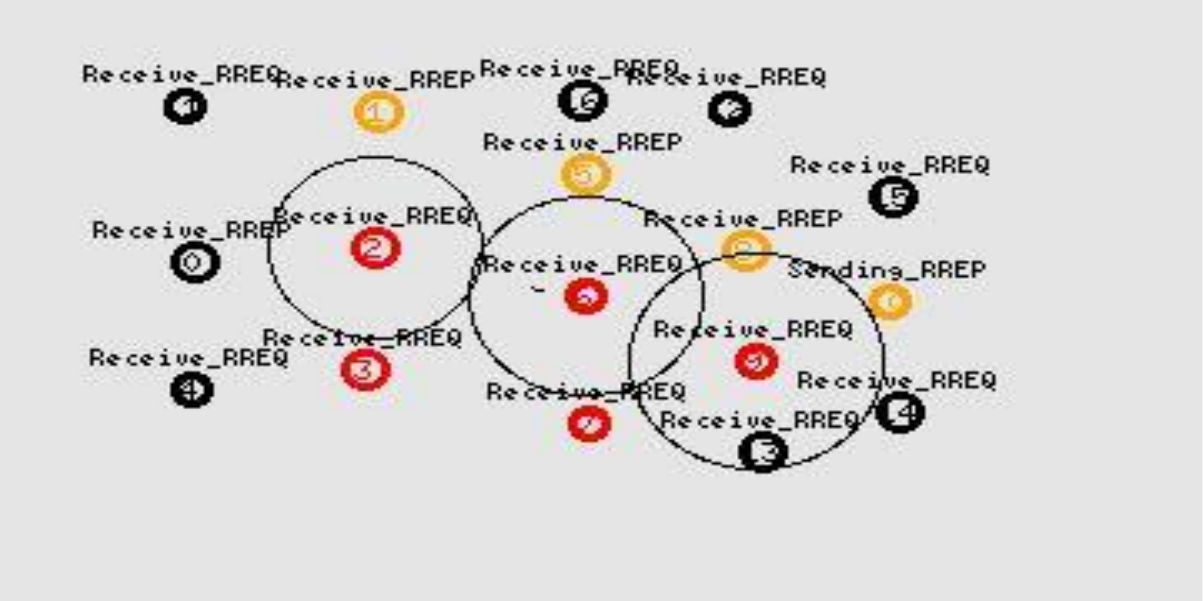


Figure 8.2: Implementation of simulation model in NS2 with source and destination nodes

This model will analyze the effect of change in network topology. The router's load will be controlled by changing the rate of the generation of the packets. The delay for reestablishing the routes will show the network capability how it is responding for the changes in the topology. By changing the delay of re-establishment of routes and rate of arrival of congestion, the performance of transport protocols was compared with the network layer function performance by changing the values of network traffic load. In this simulation model, a fixed size packet of 200 bytes and rate of data transmission of 10 kb/s were used. Between the source and destination, around 12 hops are created and the size of the window is adjusted to 10 kilo bytes which accommodate approximately 50 packets. The routing protocol used in this simulation is the Ad hoc On-Demand Distance Vector routing (AODV) as it is the most efficient and best routing among all the available routing protocols in the MANET. TCP agents are attached to different nodes. Sink nodes as well as the source nodes are defined with their positions in flat grid topography of xy plane in Network simulator. The theoretical procedure for calculating the size of the congestion window is follows.

1) The congestion window size of the TCP will be increased after the reception of the packet of acknowledgement. In this case, the size of the congestion window is:

$$CWS = CWS + A(CWS) / (CWS)$$

2) The congestion window size of the TCP will be decreased when the packet was loss in the process of transmission. In this case, thes size of the congestion window is:

$$CWS = (1-B(CWS)) * CWS$$

Where A(CWS) is the increased congestion window size during Round trip delay time

B(CWS) is the decreased congestion window size during Round trip delay time

CWS stand for "Congestion Window Size"

CHAPTER 9 RESULT

The comparative analysis of the basic TCP with the feedback based TCP is obtained. From the results it is found that the feedback based TCP has achieved the optimized performance with the standard TCP. So, by using the feedback based TCP adaptive back-off response is introduced in the network which is used to classify the TCP into Full congestion window TCP and Partial congestion window TCP. The various performance parameters like Throughput, packet loss and delay are plotted against the number of nodes.

9.1 Simulated Results for Standard TCP (S-TCP) and Feedback based TCP (TCP-F)

The results are generated by plotting the X-Graphs in the Network Simulator (NS2) and the values obtained in the X-Graphs are again plotted in the Microsoft Office Excel.

The following figure 9.1 in the form of graph shows the throughput which is taken on the y-axis versus number of nodes which is taken on x-axis for S-TCP and TCP-F.

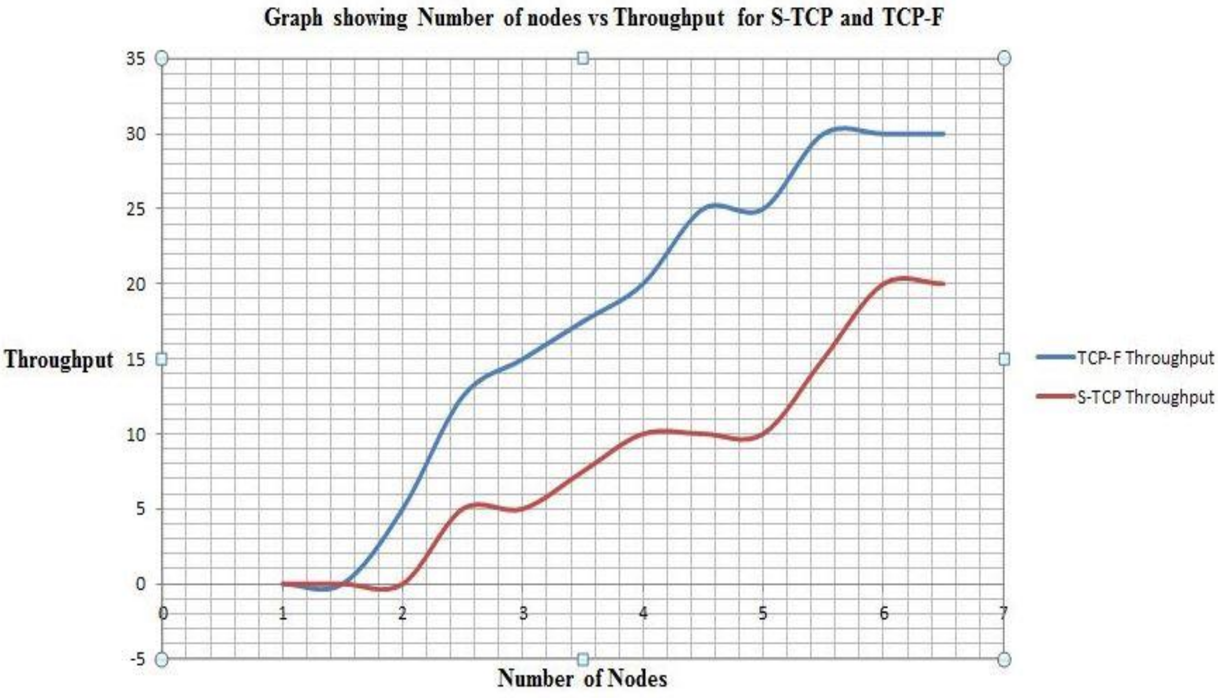


Figure 9.1: Graph for Throughput vs Number of nodes for S-TCP and TCP-F

Since, throughput is directly proportional to the number of mobile nodes deployed in the network. From the graph it can be observed that basically the throughput increases with increases with increase in the number of nodes and it decreases with decrease in number of nodes for both Standard-TCP or S-TCP as well as Feedback based TCP or TCP-F. But, the increase in throughput is more for Feedback based TCP (TCP-F) when compared to the Standard TCP (S-TCP), this is due to the fact that feedback gives the enhanced performance.

The following figure 9.2 in the form of graph shows the Packet Loss which is taken on y-axis versus number of nodes which is taken on x-axis for Standard TCP (S-TCP) and Feedback based (TCP-F). Here, it is observed that the packet loss is directly proportional to number of nodes. With the increase in the number of nodes, the packet loss increases for both Standard TCP (S-TCP) and Feedback based TCP (TCP-F). And the packet loss decreases with decrease in the number of nodes for both the Standard TCP (S-TCP) and Feedback based TCP (TCP-F).

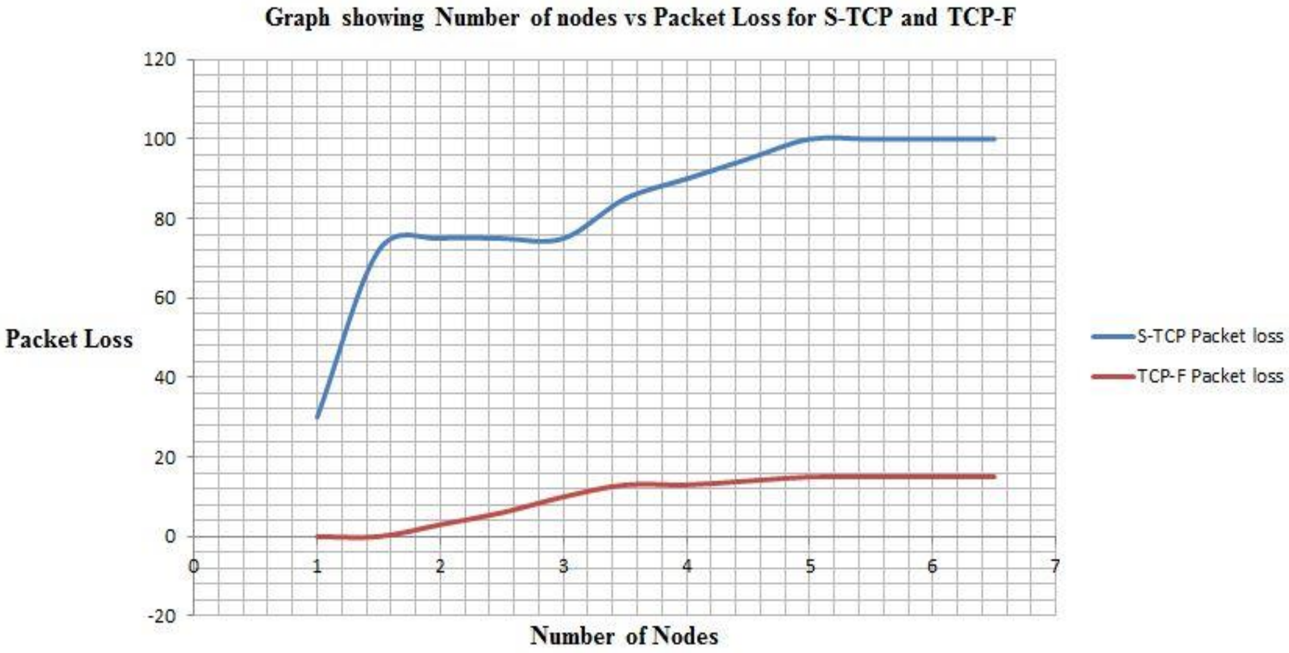


Figure 8.2: Graph for Packet Loss vs Number of nodes for S-TCP and TCP-F

For the same number of nodes, the packet loss is more for Standard TCP (S-TCP) when compared to Feedback based TCP (TCP-F), the reason behind this is that in case of normal TCP, the route failure will be treated as the congestion and there may be the chances for the packet drop at the intermediate nodes as link from intermediate nodes to destination does not exist which was overcome by the Feedback based TCP by sending the Notification of Route Re-Establishment. After that, once the route from intermediate nodes to destination is found, the source will be intimated with Route Re-Establishment Notification.

The following figure 9.3 in the form of graph shows the Delay which is taken on y-axis versus number of nodes which is taken on x-axis for Standard TCP and Feedback based. Here, it is observed that the Delay or Round trip Delay time (RTT) is directly proportional to number of nodes.

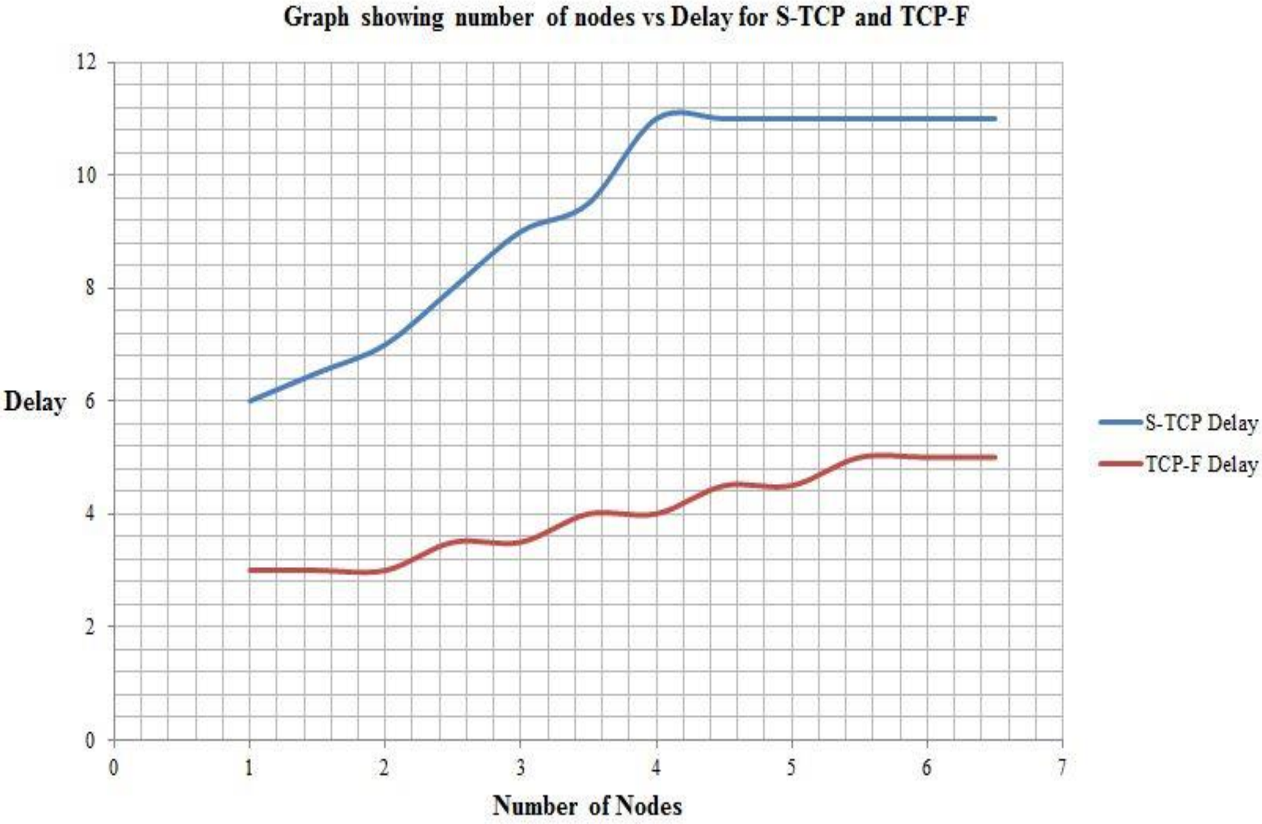


Figure 8.3: Graph for Delay vs Number of nodes for S-TCP and TCP-F

With the increase in the number of nodes, the delay increases for both Standard TCP and Feedback based TCP. And the Delay decreases with decrease in the number of nodes for both the Standard TCP and Feedback based TCP. For the same number of nodes, the Delay is more for Standard TCP when compared to Feedback based TCP because when a feedback which is sent from the intermediate nodes to the source will make the source nodes to transmit data in the path where there are no link breakages, this makes using Feedback based TCP having less delay. In case of Standard TCP, the source nodes will the data directly without knowing the link breakages. So, the feedback based TCP gives the enhanced performance due to less delay.

The following table 9.1 shows the comparison of the Standard TCP and Feedback based TCP in terms of various parameters like Throughput, Utilization of Bandwidth, Route Re-Establishment Delay, Good put, Energy efficiency, Round Trip Delay Time (RTT), Packet Loss, and Packet Delivery Ratio.

Performance Metric	**Standard TCP**	**Feedback based TCP**
1. Throughput	Low	High compared to basic TCP
2. Bandwidth Utilization	High	Low
3. Route Re-Establishment Delay	High (Typically 4 to 6 sec)	Low (Typically 1 to 3 Sec)
4. Good put	Very Low	High
5. Energy efficiency	Low	Relatively high
6. Round trip delay time (RTT)	High (2 Sec for 6 Packets)	Low compared to basic TCP
7. Packet Loss	High compared to TCP-F	Low
8. Packet Delivery ratio	Low	High

Table 9.1: Table showing comparison of Basic/Standard TCP (S-TCP) and Feedback based TCP (TCP-F) in various performance metrics

9.2 Simulated Results for Full Congestion Window-TCP (Fcwnd-TCP) and Partial Congestion Window TCP (Pcwnd-TCP)

The Full Congestion Window-TCP (Fcwnd-TCP) and Partial Congestion Window TCP (Pcwnd-TCP) are the sub-classification of Feedback implemented with the adaptive back-off response and the classification is done on the effective utilization of the available congestion window size. And the size of the congestion will be adjusted according the available bandwidth.

The following figure 9.4 in the form of graph shows the Throughput which is taken on y-axis versus number of nodes which is taken on x-axis for Full size congestion window TCP and Partial size congestion window TCP. Here, it is observed that the Throughput is directly proportional to number of nodes. With the increase in the number of nodes, the Throughput increases for both Full size congestion window TCP and Partial size congestion window TCP. And the Throughput decreases with decrease in the number of nodes for both the Full size congestion window TCP and Partial size congestion window TCP. For the same number of nodes, the Throughput is more for Fcwnd-TCP when compared to Pcwnd-TCP.

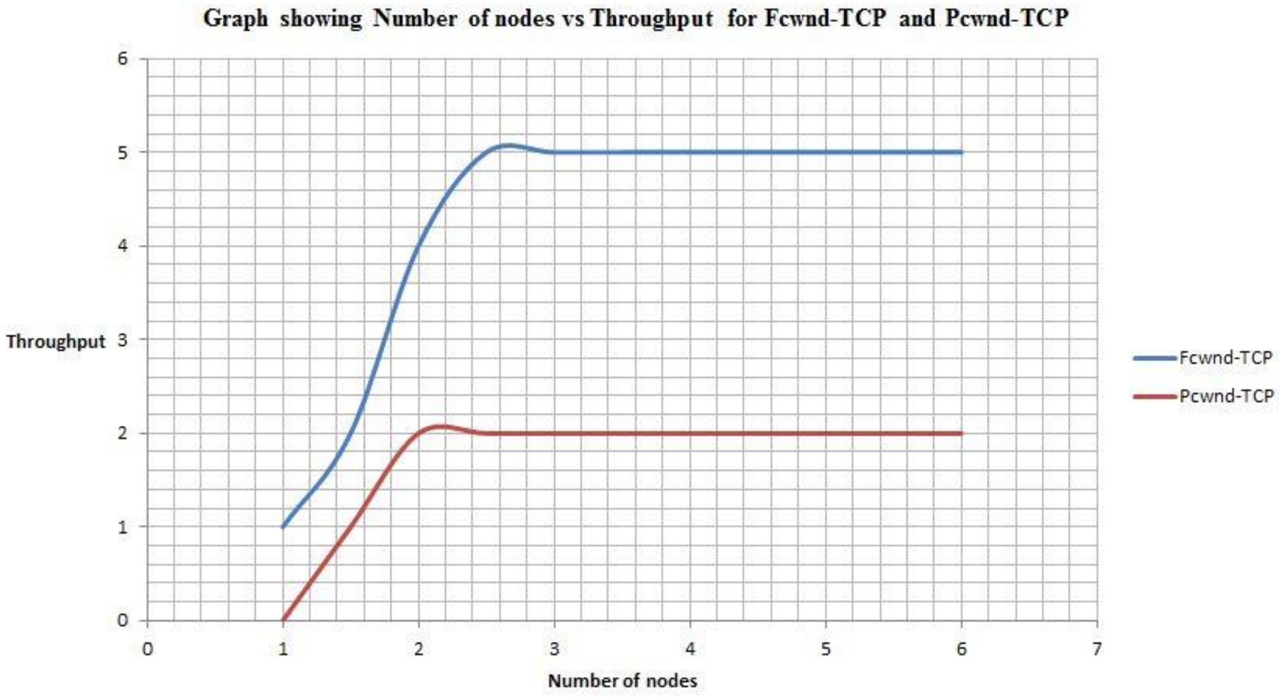


Figure 9.4: Graph for Throughput vs number of nodes for Fcwnd-TCP and Pcwnd-TCP

The following figure 9.5 in the form of graph shows the Delay which is taken on y-axis versus number of nodes which is taken on x-axis for Full size congestion window TCP and Partial size congestion window TCP. Here, it is observed that the Delay is directly proportional to number of nodes. With the increase in the number of nodes, the Delay increases for both Full size congestion window TCP and Partial size congestion window TCP. And the Delay decreases with decrease in the number of nodes for both the Full size congestion window TCP and Partial size congestion window TCP. For the same number of nodes, the Throughput is more for Fcwnd-TCP when compared to Pcwnd-TCP.

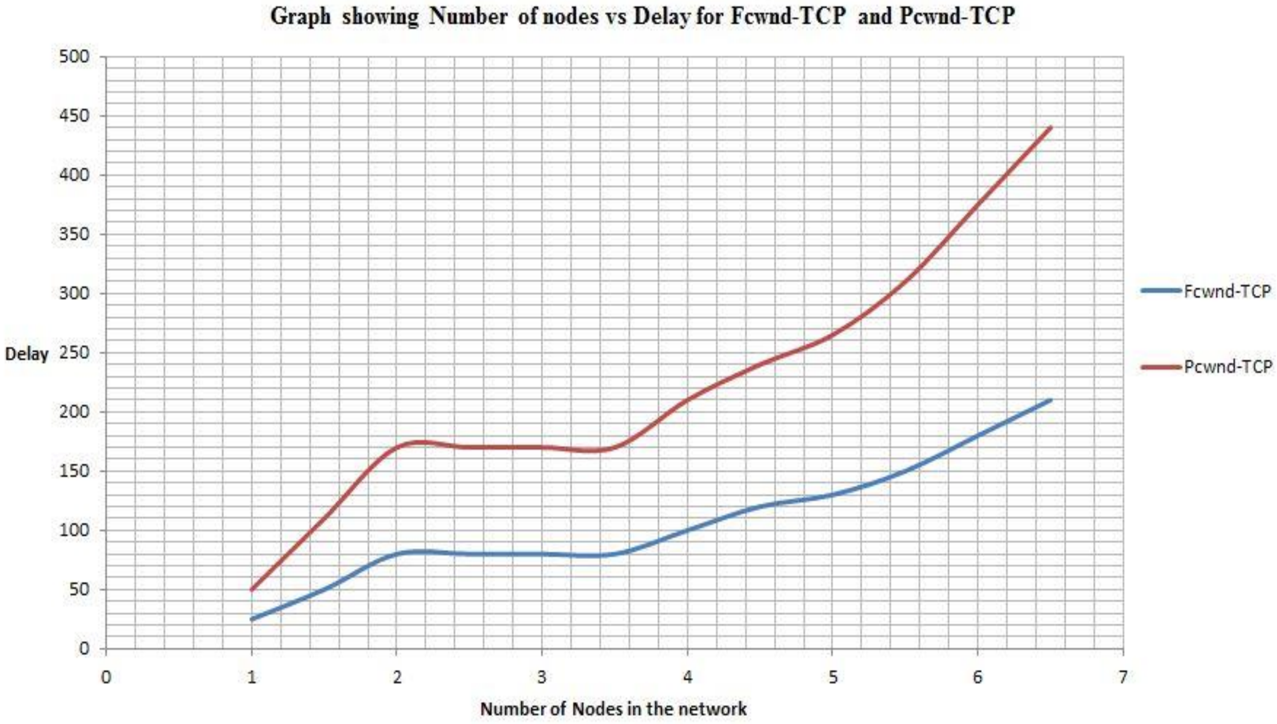


Figure 9.5: Graph for Delay vs number of nodes for Fcwnd-TCP and Pcwnd-TCP

The following figure 9.6 in the form of graph shows the Packet loss which is taken on y-axis versus number of nodes which is taken on x-axis for Full size congestion window TCP and Partial size congestion window TCP. Here, it is observed that the Packet loss is directly proportional to number of nodes. With the increase in the number of nodes, the Packet loss increases for both Full size congestion window TCP and Partial size congestion window TCP. And the Packet loss decreases with decrease in the number of nodes for both the Full size congestion window TCP and Partial size congestion window TCP. For the same number of nodes, the Packet loss is more for Fcwnd-TCP when compared to Pcwnd-TCP.

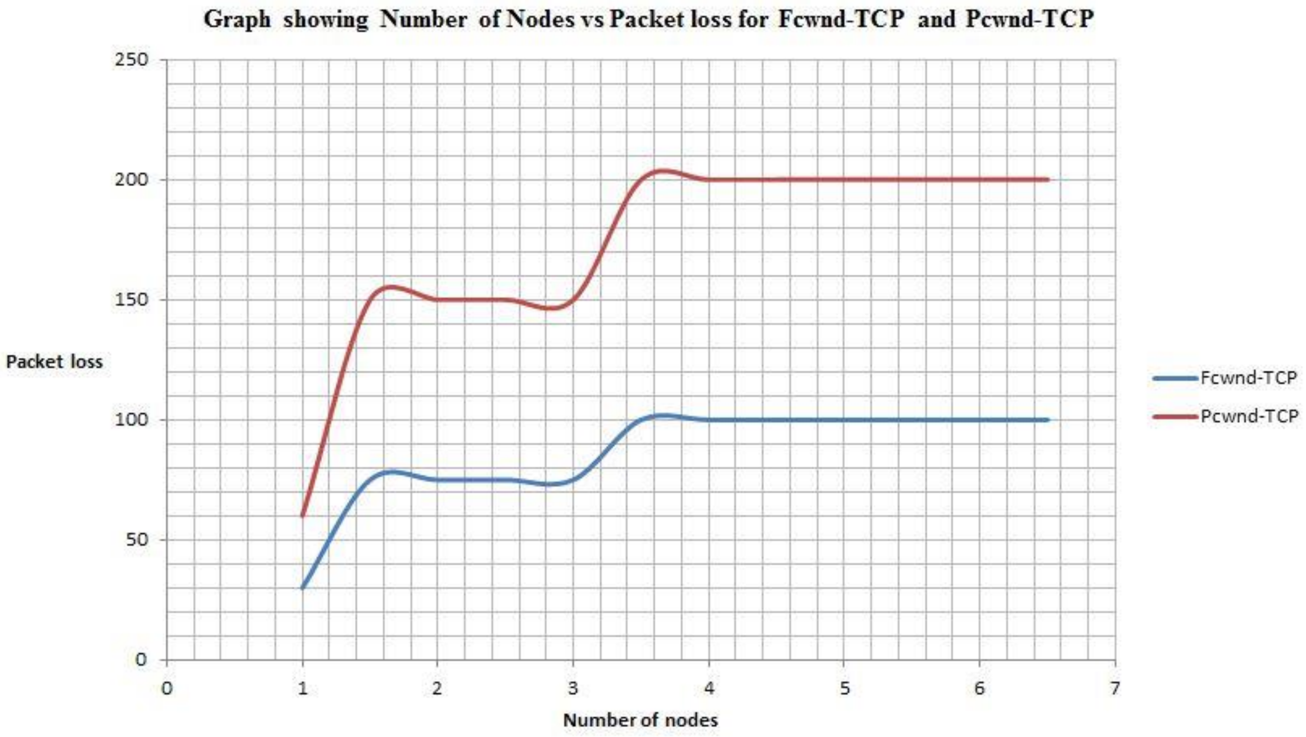


Figure 9.6: Graph for Packet loss vs number of nodes for Fcwnd-TCP and Pcwnd-TCP

CHAPTER 10 CONCLUSION AND FUTURE SCOPE

It is concluded that the effect of route failures, which are characteristic of ad hoc mobile networks, on basic TCP performance are analyzed. In Transmission Control Protocol (TCP), if the source does not know about the failure of routes, the source will transmit the packets continuously even when intermediate nodes in the network is unable to route those transmitted packets to the destination. This leads to packet loss and demission of performance. As the TCP considers the packet loss as the congestion and it will start the algorithm of congestion control when the route is reestablished, leading to throttling of transmission. In the proposed feedback-based adaptive back-off response, the failure point located at the intermediate nodes will notify the source about the failure of route and route reestablishments, thus makes the source to distinguish failure of routes from the congestion. The relative performance of basic TCP and TCP-F was studied and simulated in NS2 in terms of various parameters like Throughput, packet loss and delay and it is found that the feedback based TCP has shown improvement in performance. With the increase in the delay of route reestablishment, TCP-F performs significantly better than standard TCP. After that, based on the congestion window size, the TCP classified into Full congestion window TCP and Partial congestion window TCP. The future extension of this work is during the occurrence of route failure, large amount of acknowledgements and packets will be lost and the after coming packets will reach the destination once the route has been re-established. This will create some gaps in the window of the receiver; this will affect the cumulative acknowledgement of TCP. So, it is worthy to explore the alternative end-to-end acknowledgement schemes like Selective Acknowledgement (SACK) and compare the performance of this technique with the performance of the existing technique utilizing the scheme of cumulative acknowledgement in ad-hoc networks.

CHAPTER 10 REFERENCES

[1] Ahmad. Hanbali, E.Altman, P.Nain. A Survey of TCP over Ad hoc networks. *INRIA B.P. 93, 06902 Sophia Antipolis Cedex, France June, 2005*

[2] GUO Jianli, LIU Hongwei, DONG Jian and YANG Xiaozong. HEAD: A Hybrid Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks. *TSINGHUA SCIENCE AND TECHNOLOGY ISSN 1007-0214 36/49 pp202-207 Volume 12, Number S1, July 2007 H*

[3] Shivashankar, Hosahalli Narayanagowda Suresh, Golla Varaprasad and Guruswamy Jayanthi. Designing Energy Routing Protocol With Power Consumption Optimization in MANET. *IEEE Transactions on Emerging Topics in Computing Digital Object Identifier 10.1109/TETC.2013.2287177*

[4] Eman S. Alwadiyeh and Ala F A Aburumman. Interference-Aware Multipath routing protocols for Mobile Ad hoc Networks. *13th Annual IEEE Workshop on Wireless Local Networks 2013 978-1-4799-0540-9/13/$31.00 ©2013 IEEE*

[5] Songtao Guo, Member, IEEE, Changyin Dang, Senior Member, IEEE, and Yuanyuan Yang, Fellow, IEEE. Joint Optimal Data Rate and Power Allocation in Lossy Mobile Ad Hoc Networks with Delay-Constrained Traffics. *IEEE TRANSACTIONS ON COMPUTERS, VOL. 64, NO. 3, MARCH 2015*

[6] Kartik Chandran, Sudarshan Raghunathan, S. Venkatesan and Ravi Prakash. A Feedback Based Scheme For Improving TCP Performance In Ad-Hoc Wireless Networks. *Computer Science Program University of Texas at Dallas Richardson, TX 75083-0688*

[7] Gavin Holland, Nitin Vaidya, “Analysis of TCP Performance over Mobile Ad Hoc Networks”, *Wireless Networks, vol. 8, pp. 275–288, 2002.*

[8] D. Pacifico, M. Pacifico, C. Fischione, H. Hjalrmasson and K. H. Johansson. Improving TCP Performance During the Intra LTE Handover. *IEEE "GLOBECOM" 2009 2009978-1-4244-4148-8/09*

[9] Shengming Jiang, Dajiang He and Jianqiang Rao "A Prediction-Based Link Availability Estimation for Routing Metrics in MANETs", *IEEE Transactions on Networking, Vol. 13, No. 6, December 2005.*

[10] Liang Qin and Thomas Kunz, "Increasing Packet Delivery Ratio in DSR by Link Prediction", *Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS'03), pp. 300−309, 2003. 121*

[11] Adrian J. Cahill, Phillipn L. De Leon and Cormac J. Sreenan, "Link Cache Extensions for Predictive Routing and Repair in Adhoc Wireless Networks*", 4th International Conferences on Mobile and Wireless Communication Network, September 02.*

[12] Sofiane Boukli Hacane et al., "Predictive Preemptive Ad hoc On-demand Distance Vector Routing", *Malaysian Journal of Computer Science, Vol. 19, No. 2, pp. 189−195, 2006.*

[13] S. Crisostomo, S. Sargento, P. Brandao and R. Prior, "Improving AODV with preemptive local route repair", *International Workshop on Wireless Ad-hoc Network, 2004.*

[14] P. Mani and D. W. Petr, "Development and performance characterization of enhanced AODV routing for CBR and TCP traffic", *Wireless Telecommunications Symposium, 2004.*

[15] G. S. Sreedhar and D. A. Dr., "MALMR: Medium Access Level Multicast Routing for Congestion Avoidance in Multicast Mobile Ad Hoc Routing Protocol MALMR Medium Access Level Multicast Routing for Congestion Avoidance in Multicast Mobile Ad Hoc Routing Protocol," *Glob. J. Comput. Sci. Technol. Network, Web Securre., vol. 12, no. 13, pp. 22–30, 2012.*

[16] Amit Aggarwal, Stefan Savage, Thomas Anderson, "Understanding the Performance of TCP Pacing", *14th Annual IEEE Workshop on Wireless Local Networks 2013 978-1-4799-0540-9/13/$31.00 ©2013 IEEE*

[17] Chandra Kanta Samal, "TCP Performance through Simulation and Testbed in Multi-Hop Mobile Ad hoc Network", *International Journal of Computer Networks & Communications (IJCNC),Vol.2, No.4, July 2010.*

[18] Thomas, Brian, Noble, "The End-to-End Performance Effects of Parallel TCP Sockets on a Lossy Wide-Area Network", *International Workshop on Wireless Ad-hoc Network, 2004.*

[19] K. Sundaresan, V. Anantharaman, H.-Y. Hung-Yun Hsieh, and A. R. Sivakumar, "ATP: a reliable transport protocol for ad hoc networks," *IEEE Trans. Mob. Comput., vol. 4, no. 6, pp. 588–603, Nov. 2005.*

[20] J. Karlsson, A. Batlle, A. J. Kassler, and B.-S. Lee, "TCP Performance in Mobile Ad Hoc Networks Connected to the Internet," *Rev. Cient. Period., vol. 10, no. 1, pp. 1–3, 2007.*

[21] N. Shukla, N. Gupta, N. Parveen, and M. Scholor, "Survey Of Cross Layer Based TCP Congestion Control Techniques in MANET," *Int. J. Emerg. Technol. Adv. Eng. Website www.ijetae.com ISO Certif. J., vol. 4, no. 3, pp. 446–452, 2014.*

[22] Xiang Chen, Hongqiang Zhai, Jianfeng Wang and Yuguang Fang, "A Survey on Improving TCP Performance over Wireless Networks", *4th International Conferences on Mobile and Wireless Communication Network, February 2002.*

[23] Feng Wang, Yongguang Zhang, "A Survey on TCP over Mobile Ad hoc networks", *International Journal of Computer Networks & Communications (IJCNC),Vol.2, No.4, August 2012.*

[24] Hari Balakrishnan, Venkata Padmanabhan, "How Network Asymmetry Affects TCP", *Wireless Networks, vol. 8, pp. 275–288, 2002.*

[25] Fabius Klemm, Zhenqiang Ye, Srikanth, V. Krishnamurthy, Satish, K. Tripathi, "Improving TCP Performance in Ad Hoc Networks using Signal Strength based Link Management", *IEEE Trans. Mob. Comput., vol. 4, no. 6, pp. 588–603, Nov. 2005.*

[26] Renaud Sallantin, Cédric Baudoin, Emmanuel Chaput, Fabrice Arnal, Emmanuel Dubois, André-Luc Beylot, "Initial Spreading: a Fast Start–Up TCP Mechanism", *38th Annual IEEE Conference on Local Computer Networks.*

[27] Aditya Kartnik, Anurang Kumar, "Performance of TCP congestion control with explicit rate feedback", *IEEE Journal on selected areas in communications, vol. 13, no. 8, 1995.*

[28] Youssef Bassil, "TCP Congestion Control Scheme for Wireless Networks based on TCP Reserved Field and SNR Ratio", *International Journal of Research and Reviews in Information Sciences (IJRRIS), ISSN: 2046-6439, Vol. 2, No. 2, June 2012.*

[29] Bakre, Badrinath, "I-TCP: Indirect TCP for Mobile Hosts", *In Proceedings of ICDCS 95, 1995.*

[30] Hari Balakrishnan, Srinivasan Seshan, Elan Amir, and Randy H. Katz, "Improving TCP/IP Performance over Wireless Networks", *Proceedings of the 1st ACM Conference on Mobile Computing and Networking, Berkeley, CA, November 1995.*

[31] K. Brown and S. Singh, "M-TCP: TCP for Mobile Cellular Networks", *ACM Computer Communications Review, vol. 27, no. 5, pp. 19 43, 1997.*

[32] Ramakrishnan and Floyd, "A Proposal to add Explicit Congestion Notification (ECN) to IP", *Internet Draft, January 1999.*

[33] P. Sinha, N. Venkitaraman, R. Sivakumar, V. Bharghavan, "WTCP: A Reliable Transport Protocol for Wireless Wide-Area Networks", *ACM Mobicom, Seattle, WA, 1999.*

[34] Saverio Mascolo, Claudio Casetti, Mario Gerla, M. Y. Sanadidi, and Ren Wang, "TCP Westwood: Bandwidth Extimation for Enhanced Transport over Wireless Links", *ACM Mobicom, 2001.*

[35] Lawrence S. Brakmo, and Larry L. Peterson., "TCP Vegas: End to End Congestion Avoidance on a Global Internet", *IEEE Journal on selected areas in communications, vol. 13, no. 8, 1995.*

[36] Wu E.H.-K., and Mei-Zhen Chen, "JTCP: Jitter-based TCP for Heterogeneous Wireless Networks", Selected Areas in Communications, *IEEE Journal, vol. 22, no. 4, pp. 757-766, 2004.*

[37] Wie-Qiang Xu, Tie-Jun Wu, "TCP Issues in Mobile ad hoc networks: Challenges and Solutions", *Proceedings of the 23rd IEEE International Conference on Distributed Computing Systems Workshops.*

[38] Sofiane Hamrioui, Jaime Lloret, Pascal Lorenz, Mustapha Lalam, "TCP Performance in Mobile Ad hoc Networks", *Network Protocols and Algorithms ISSN 1943-3581 2013, Vol. 5, No. 4.*

[39] Qingyang Xiao, Ke Xu, Dan Wang, Li Li, Yifeng Zhong, "TCP Performance over Mobile Networks in High-speed Mobility Scenarios", *International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 2, February 2013.*

[40] Haejung Lim, Kaixin Xu, Mario Gerla, "TCP Performance over Multipath Routing in Mobile Ad Hoc Networks", *International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 2, February 2013.*

[41] Pavel V.Nikitin, Onur Celebioglu, "TCP performance in mobile wireless environment: channel modelling and network simulation", *Proceedings of the 25th IEEE International Conference on Distributed Computing Systems Workshops.*

[42] Aniket Deshpande, Ashok Kaushal, "Feedback-based Adaptive Speedy Transmission (FAST) Control Protocol to Improve the Performance of TCP over Ad-Hoc Networks", *2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Sept. 21-24, 2016, Jaipur, India.*

[43] Gururaj H L, Ramesh, "Congestion Control for Optimizing Data Transfer rate in Mobile Ad-hoc Networks using HSTCP", *International Conference on Emerging Research in Electronics, Computer Science and Technology – 2015.*

[44] Dhenakaran, Parvathavarthini, "An Overview of Routing Protocols in Mobile Ad-Hoc Network", *International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 2, February 2013.*

[45] Fumiaki Hirose, Masahiko Fukuhara, Tomoya Hatano, Hiroshi Shigeno, Ken-ichi Okada, "A Two-Level ECN Marking for Fair Bandwidth Allocation between HSTCP and TCP Reno", *Proceedings of the 25th IEEE International Conference on Distributed Computing Systems Workshops.*

[46] Raghav Bhardwaj , Parminder singh, "Routing Protocols In Mobile Adhoc Network : Review", *International Journal of Advances in Computer Science and Communication Engineering (IJACSCE) Vol 2 Issue2 (June 2014).*

[47] Aniket Deshpande, Ashok Kaushal, "MX-TCP and HS-TCP as Possible Options to Overcome TCP Limitations in Multi-Hop Ad-Hoc Networks*", International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 12, December 2015.*

[48] J. V. Maisuria and R. M. Patel, "Overview of Techniques for Improving QoS of TCP over Wireless Links," *2012 International Conference on Communication Systems and Network Technologies, 2012, pp. 366–370.*

[49] A. Singh, M. Mei Xiang, A. Konsgen, C. Goerg, and Y. Zaki, "Enhancing fairness and congestion control in multipath TCP," *6th Joint IFIP Wireless and Mobile Networking Conference (WMNC), 2013, pp. 1–8.*

[50] Z. Fu, P. Zerfos, H. Luo, S. Lu, L. Zhang, and M. Gerla, "The impact of multihop wireless channel on TCP throughput and loss," *IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No.03CH37428), 2003, vol. 3, pp. 1744–1753.*