CHAPTER-1

Introduction

1.1 Introduction

A computer network is an interconnected gathering of independent computers which helps communication in several ways. The growing need of reliable, efficient, and scalable computer networks have led to tremendous growth and development of computer technology in many diverse applications. Computer networks provide virtuous communication medium, sharing of resources, service reliability and cost-effectiveness. Sharing of resources include programs, applications, data, devices, memory space etc. are obtainable to any users on the network, nevertheless of the physical location of the computer systems that holds the resources and the user. A computer network comprises of two key components; networking infrastructure and distributed applications. The networking infrastructure facilitates transferring of data between interconnected or networked computer systems in which applications present. The distributed applications deliver services to the users and other applications, located on other computer systems of the network. Some examples of distributed applications are internet, electronic mail, ticket reservation system and banking authentication systems. Physical media that delivers connectivity to computers in a network does not have restrictions [Siva Ram Murthy *et al.* (2007)]. Some media used for network connectivity are optical fiber, copper cable and wireless radio waves. Computer networks are implemented in two forms wired or wireless, wired computer networks utilizes copper cables and optical fiber cables for connecting several computer systems in an network. Wireless networks utilize radio waves to connect the computer systems.

Different computer networks are able to connect each other by means of the devices called routers which use routing protocols for their IP address switching and route discovery. These routing protocols are developed based on routing algorithms. Routing algorithms can be defined as a mechanism that states the router how to

process. All these routing algorithms are different from one another regarding their design and efficiency and type. Routing algorithms can broadly be divided into following categories; static versus dynamic, single-path versus multipath, flat versus hierarchical, host-intelligent versus router-intelligent, intra-domain versus inter-domain, link-state versus distance vector. All these routing algorithms have different design, different working and different metrics to measure the best paths for routing. Wired networks and wireless networks use different routing algorithms for route discovery processes. Rapidly growing computer technologies have powered the computing devices with new kind of routing techniques. Routing protocols of wired networks fall short of meeting expectations when they put to use in wireless environments where there is a high degree of node mobility. A mobile ad-hoc network is a new generation wireless network which functions without having any centralized infrastructures. Due to absence of centrally controllable infrastructures, nodes in mobile ad-hoc networks acts as host and the routers and establish routes among other nodes of the network.

In mobile ad-hoc networks, route discovery between nodes takes place by the help of routing protocols. A mobile ad-hoc network usually symbolized as MANET contain small set or large set of nodes that communicate each other directly without depending upon access points or base stations and any centralized control setup. In mobile ad-hoc networks, nodes are mobile in nature, they move from one point to another randomly. This random movement of nodes makes MANETs to have dynamic network topologies [Bai *et al.* (2003)]. The dynamic and infrastructure less nature of mobile ad hoc networks postures a key challenge to efficient & accurate data packet routing. This leads to incredible expanse of research in routing protocols adjustable to the dynamic ad-hoc network states such as; size of the network, density of traffic scenarios and network splitting.

In mobile ad-hoc networks, routing protocols assumes communication between nodes (which also acts as routers) and facilitate them to select desired paths between source and the destination nodes. The routing algorithms perform route selection process between the nodes. Routing in ad-hoc networks becomes challenging as day by day portable device users are increasing. These portable

network supported devices are technically advanced and bandwidth consuming with the high defined video graphics applications etc. Many researchers have motivated on the algorithmic complexity of ad-hoc routers [Das *et al.* (1997), Guha *et al.* (1996), Parekh *et al.* (1994)]. Some other researchers have proposed new routing solutions [Perkins *et al.* (1994), Johnson *et al.* (1996)]. Protocols of mobile ad-hoc networks are optimized to reduce the number of hops from the source nodes to the destination nodes.

1.2 Computer Networks

Many computer systems connected together for sharing data from different geographical locations refers to computer networking. These can be wired, wireless or combination of both the wired and wireless. Mobile ad-hoc networks are new generation of the wireless networks. A computer network or data network is a communication network which permits different computer systems to exchange data. In computer networks, networked computer systems and computing devices interchange data by a data link. These networked systems and devices are refers to nodes or hosts of the network. The links between network nodes are established by cable media or wireless media. The well-known computer network is the Internet. Corporate offices, banks, industries, universities, schools and other business establishments have their own private network called intranet. Networked computer devices and systems that originate, route and terminate the data are known as nodes of the network [IR 1]. Hosts like personal computers, laptops, phones, servers and all other computing devices related to computer networking can be the nodes of the network.

Different computer systems said to be networked when a computer system capable to interchange data with another with or without having direct link to one another. Computer networks support vast numbers of services and applications such as VoIP (Voice over Internet Protocol), electronic mail, online transactions, engineering design and drafts, access to the world wide web, digital audio/video, shared use of application and SANs (Storage Area Networks) or memory storage servers, line printers, printers, scanners, fax machines and instant messaging applications and much more. Computer networks which switch such kind of

applications and services use application specific communication protocols along with TCP/IP (Transmission control protocol/ Internet protocol) suite and other protocol suits. Computer networks enable relational communications allowing users to communicate proficiently and easily by various means such as E-mail (Electronic mail), video phone calls, instant messaging, telephone, chat rooms and video conferencing. The key features of computer networks are providing access to shared files, storage systems, sharing of network and computing resources, computer hardware and associated computing devices and servers. Computer networks permits accessing, file sharing, data, and all other types of information subjected to authorized access. Network users may access resources provided by the network such as printing a document by using a shared network printer.

Cloud computing and distributed computing systems gets access to computing resources across the network to achieve tasks. Computer networks often attacked by the computer hackers and password crackers to disturb the networks and steal important files, data and information, network administrators are always alert by such activities and prevent them by the help of various software applications. Some hackers often try to deploy computer viruses or computer worms on networked devices and systems. Packet switched and circuit switched are some types of computer networks. In packet switched networks, data is formatted into several packets that are sent through the network to their destinations, all the packets received at the destination are assembled into their original message. In packet switched networks, the bandwidth of the transmission medium can be better shared between the users of the network as compare to circuit switched networks.

Data packets have two types of data; control information and user data or payload [IR 1]. The control information holds the data pertaining to the network requirements to deliver the user data. Network addresses of the source and destination, error detection codes and sequencing information are some examples of control information in a data packet. These control information is generally resides in the packet headers and trailers along with user data (pay load) in between them. Organizational establishments depend severely on the capability to share information

across the organization in an effective and productive manner. Computer networks have validated these technologies and now exist in almost every business. When it comes to set up a computer network, an organization may have two options; either a completely wired network or a wireless network. Wired networks use networking cable to connect computer systems whereas wireless networks use radio frequencies to connect the computer systems and devices. Organizations become more mobile owing to usage of wireless networks, hence they use miscellaneous setup of wired and wireless networks. Organizations use wired networks at their central network gateways and wireless networks at the end user setups [Joshua Muscatello *et al.* (2005)]. Computer networks are broadly classified as client-server networks and peer to peer networks.

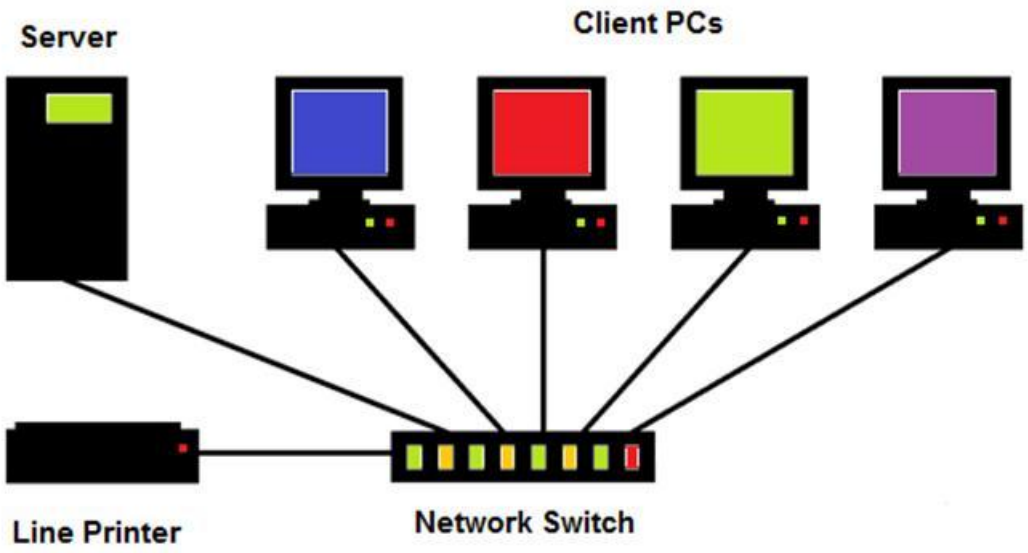

Fig.1.1. Client-Server Network Setup

Fig.1.1 illustrates the client-server model, a client-server network includes server processes, client processes and processes which generally reside on different computer machines. Fig.1.2 explores a peer to peer network with seven numbers of networked computer systems. Based on the transmission technology used, computer networks are classified under two categories, namely, broadcast networks and point to point networks.

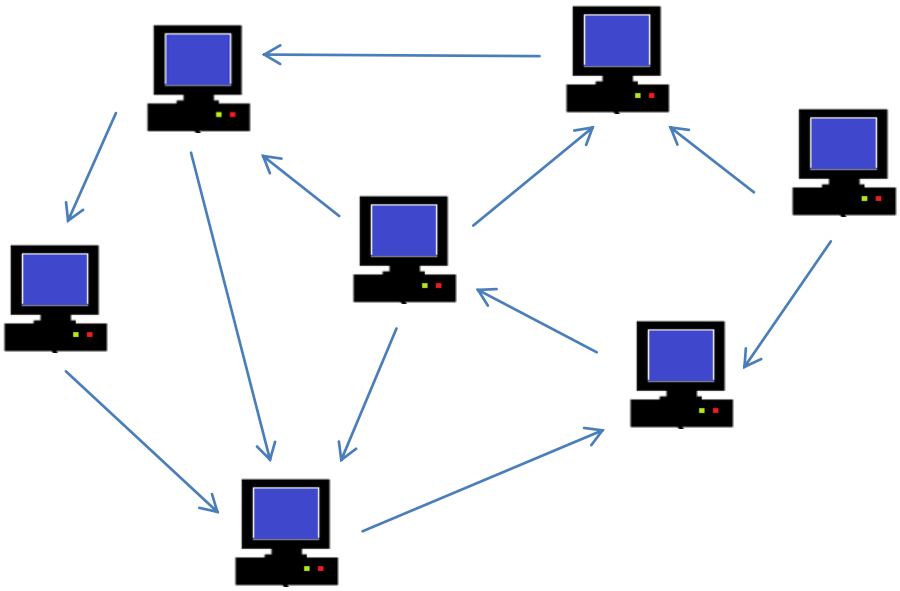

Fig.1.2. Peer to Peer Network Setup

1.3 Wired Networks

Different computer systems and computing devices collectively forms a computer networks, these networks are connected by means of either fibre optic cables or copper cables refers to wired networks. Generally, wired networks are very essential at the central network gateways of any organization because of their high speed connectivity as compare to the wireless network radio frequencies. For high performance computing establishments also wired networks are very much essential due to their high speed functionalities. Wired networks involve connecting of different computer systems and devices by means of cables, connectors and intermediate networking switches. Cables and connectors of different configurations are used for short and long distance connectivity. In case of optical fibre cables, MMF (Multi Mode Fibre) cables supports only short distances, whereas SMF (Single Mode Fibre) cables supports long distances.

In case of copper cables, CAT5-e (Category-e) cables supports short distances, whereas CAT-6e (Category-6e) cables supports slightly larger distances as compare to cat5-e cables. Based on geographic distance of the networks, networks can be classified as LANs (Local Area Networks), MANs (Metropolitan Area Networks) and WANs (Wide Area Networks). Local area networks are the most common networks

that can find today. Local area networks are used to connect computer systems and devices located within a small geographical area, such as within office buildings, schools, universities and homes. In local area networks, all the computer systems and devices are connected to a common broadcast medium. Ethernet is generally used as physical medium for connecting computers in a LAN. A metropolitan area network covers much larger area as compared to LAN. A MAN may be used to connect different business establishments or offices in the same city or town. LAN uses Ethernet technologies where as a MAN uses ATM (Asynchronous Transfer Mode) and FDDI (Fibre Distributed Data Interface) technologies.

IEEE (Institute of Electrical and Electronics Engineers) 802.3 is popularly called as Ethernet. Wide area networks generally cover large geographical area, which may span different cities or even countries. WANs may be connected through optical fibres, phone lines and satellite links. Point to point links is used as transmission medium in wide area networks. A network that connects two or more LANs such as WANs or MANs is called an internetwork. In order to operate, the computer networks require computer hardware and software. Devices such as network interface cards (NICs), switches, routers and gateways are some examples of computer network hardware. Network software includes operating systems of the computer systems such as Windows, Linux etc., operating systems that manages network switches has different layered network protocols that ensures the route discovery for communication between networked computer systems and devices [Siva Ram Murthy *et al.* (2007)].

1.3.1 Local Area Networks

Local Area Networks, commonly referred as LANs are owned by private entities. Deployment of these networks is generally carried out within a building or any organizational or institutional campus up to some kilometres in size. LANs are broadly used to connect computers and work stations in Universities, Institutes, company offices, government departments and factories to share resources (hardware resources) and for exchange of information. LANs are classified into three categories based on their characteristics; which are according to their size, type of transmission technology they use and the type of topology they use. Local Area Networks are

limited in size; in other words, worst-case broadcast time is restricted and recognized in advance. Knowing this restriction helps to use some other kinds of network designs. Limited size of local area networks simplifies the network management.

LANs uses the transmission technology of the cable (Optical/Copper/Wireless radio frequency) and/or wireless medium. Traditional LANs run at speeds 10 Mbps to 100 Mbps (Megabits per second), but advancement in technology made it possible to run LANs even at 1000 Mbps. Traditional LANs have less delay and make less errors. Newer LANs can operate up to 10 Gbps (Gigabits per second) to 40 Gbps speed. Numerous topologies are possible for broadcast local area networks. LANs use certain types of network topologies; bus, star, ring, mesh, partial mesh and hybrid (combination of either) topologies. Any corporate or campus wide LANs generally involves WAN (Wide Area Networks) links at their back-end in order to connect themselves to the external world. These WAN links are terminated at the gateways of such organizations. This gateway setup consists of network routers, bandwidth aggregation devices, enterprise firewalls, DNS (Domain Name Server) servers and central core switches of the local area networks. LANs consist of various network distribution switches and access switches all around the organisational campus for ensuring point to point network connection. These entire LAN setup make sure the bandwidth distribution and network resource distribution all over the network. Local area networks support various network topologies discussed above (bus, ring, star, mesh and hybrid topologies). Hybrid topologies are involved with combination of different conventional topologies namely; bus topology, ring topology, star topology and mesh topology. Mesh topology also involved with partial mesh topologies. Wired networks can be connected in these topological fashions in order to provide proper redundancy to all the networked systems, when their main links fails (excluding bus and single ring topologies, where redundancy is challenging, however redundancy in these topologies achieved by connecting dual cables). These topological designs of the networks are common and in practice since years, which helps networked systems and devices to have connections from other links during failure of main link occur. Fig.1.3 explores an organizational wired computer network, where services and applications of wide area network from different geographical location have been incorporated into the local area network of an organization. Wide area network

services may include internet services from ISPs (Internet Service Providers) or services from private central networks of an organization, these private and huge networks comprise of wide area networks and local area networks which are also called as intranets.

The illustrated organizational network (Fig.1.3) has WAN links from other distinct networks, these WAN links gets terminated at the LAN side routers. The Router provides facilitation such as conversion of single IP (Internet Protocol) address into many IP addresses. In other words, router provides different paths to the local area network for transmission through the wide area network links. Router acts as a intermediate network device between WAN and the LAN links. Some organizations use bandwidth aggregators for switching multiple internet leased lines in order to maintain redundancy and to uplift the internet services with zero down time. Some organizations use enterprise firewalls for high end network ports security and prevention of external attacks to the LAN. Bandwidth aggregators are directly connected to the routers at LAN side and the output of the bandwidth aggregator terminates at input of the firewalls. Firewalls are connected to the core or central switches of the LAN. These central switches then distribute the services to the entire organizational network setup.

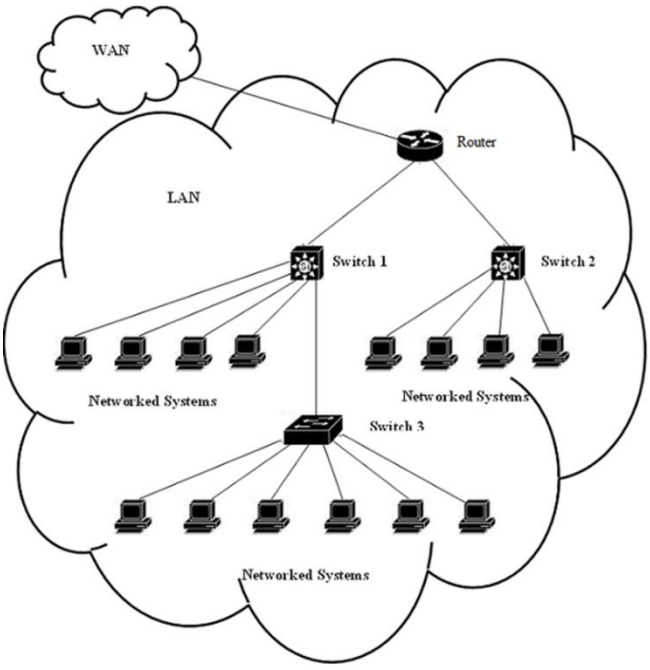

Fig.1.3. Wired Network Setup

1.3.2 Metropolitan Networks

A metropolitan network (MAN) generally referred with the network expansion in a city. The well-known example of metropolitan network is cable television network existing in every city. The cable television system has grown rapidly from their conventional community antenna systems with deprived over the air television reception. Earlier the cable television system was locally designed ad-hoc systems. As demand for these networks grown up, reputed companies involved for systematic and structural cabling across the city. After the structural cabling in the cities, these companies were heavily involved with the television programming to design cable television channels. Nowadays highly specialized television channels are commonly available and every cable television operators are providing these channels.

Specialized cable television channels includes all news, all sports, all entertainment, all kids related shows, all cooking and business so on. Earlier these channels were projected for television reception only, when internet is attached with bulk users, the cable television operators realized the up gradation of their systems with new technologies to provide two-way internet service through the unused parts of the spectrum. The cable television system adapted a way to distribute television through the metropolitan area network [Andrew S. Tanenbaum (2004)].

1.3.3 Wide Area Networks

Wide area networks generally referred by term WAN connects large geographical areas, often a country or continent. Wide area networks contain collection of computer systems and devices which runs user applications and programs. Often these networked systems called as hosts, these hosts are connected by the subnets (sub networks). The hosts are end user personal computers (PCs) or other computing devices and systems which are owned by the users. Communication subnets are classically owned by the ISPs (Internet Service Providers), subnets carry messages or internet traffic from host to host. Design of wide area networks are greatly streamlined by separation of communication aspects (subnet) of the network

from the application aspects (hosts or end user systems). Subnets of most wide area networks comprised of two distinct components namely, transmission lines and switching components. Transmission lines are the media by which movement of bits from host to host takes place, these can either be copper wires, optical fiber cables or radio links in case of wireless transmission. Switching components are dedicated computers that connect different transmission lines. Upon arrival of a data stream on an incoming transmission line, the switching component needs to choose an outgoing transmission line on which to forward it. [Andrew S. Tanenbaum (2004)].

1.4 Wireless Networks

During 1901, an Italian physicist Guglielmo Marconi proved a ship to shore wireless telegraph by the help of Morse code. Modern wireless technologies use the basic principles of wireless communication. Wireless networks are divided into three major categories; system interconnection, wireless local area networks (WLANs) and wireless wide area networks (WWANs).

1.4.1 System Interconnection

System interconnection refers to interconnection of components of a computer system or device by means of short range radio frequency. Every computer system has essential components like monitor, keyboard, mouse and printer which are generally connected to the CPU (Central Processing Unit) by the help of cables. Some newer computer systems comes with wireless components such as wireless mouse, wireless keyboard etc. Interconnection of these components is possible by the help of Bluetooth technology. Bluetooth is a short range wireless network technology which connects the components of a computer system without cables. Bluetooth technology also allows connecting scanners, digital cameras, headsets, micro phones and other devices. System interconnection networks use master-slave model, the system CPU unit is master which communicates to its peripheral devices; mouse, keyboard etc., are slaves. The master manages the slaves controlling their broadcasts, transmissions, setting up of transmission frequencies etc. [Andrew S. Tanenbaum (2004)].

1.4.2 Wireless Local Area Networks (WLANs)

As discussed in earlier section of this chapter, local area networks require extensive wiring and cabling for interconnecting different computer systems and devices. In order to overcome from the wiring and cabling, researchers have discovered the possible usage of radio waves and infrared light for interconnecting different computer systems in a network [Gfeller (1981)]. This has given rise to development of wireless LANs and wireless WANs, where wireless transmission is applied at the physical layer of the network. In wireless LANs, both portable terminals and mobile terminals can move from one place to another, portable terminals can only be accessed during their stationery position, whereas mobile terminals are more powerful, and can be accessed even when they are in motion. Wireless local area networks strictly upkeep the mobile work stations.

In wireless local area networks, computer systems use a radio modem and an antenna to communicate with other systems. Communicating systems generally have antennas either on their ceilings or wireless WNICs (Wireless Network Interface Cards) with the CPU units. However, computer systems communicate directly with each other in peer to peer mode. Wireless local area networks are commonly increasing in small offices, schools, homes, cafeterias, conference rooms, hostels, airports etc. WLANs are generally deployed at those locations, where Ethernet is troublesome or not possible. IEEE 802.11 is declared as wireless LANs standard, many systems implemented it and it has become extensive [Andrew S. Tanenbaum (2004)]. Wireless LANs can operate in either of two configurations; with base station present and without base station, the 802.11 WLAN standards take care of these operations and create facility for both the measures.

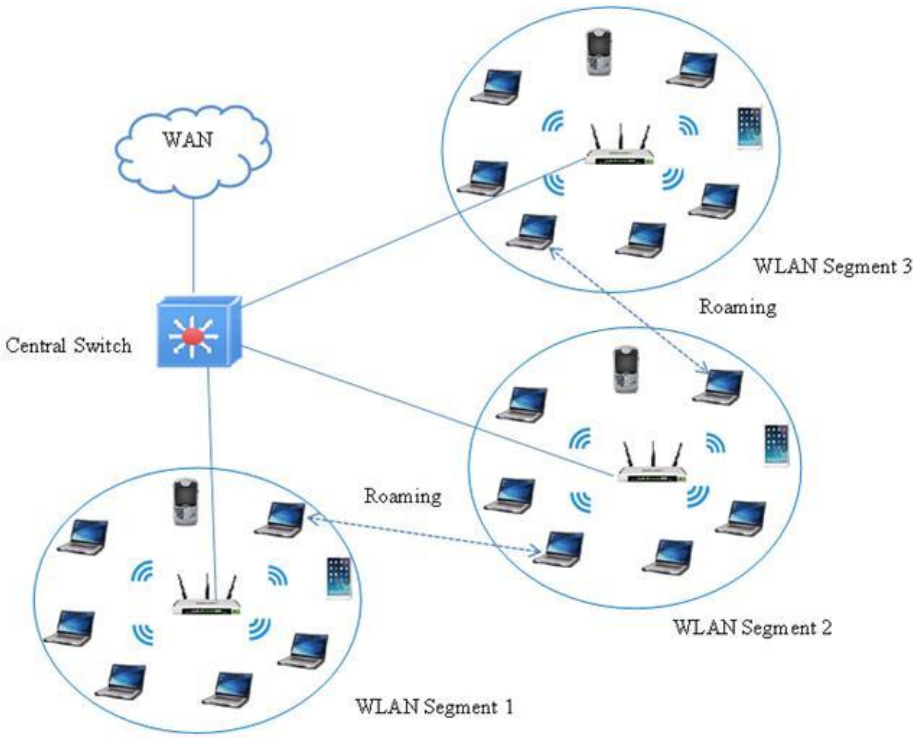

Fig.1.4. Wireless LAN Setup

Fig.1.4 demonstrates the wireless local area network setup [IR 2]; WAN (Wide Area Network) links are connected to the central core switch of the WLAN setup and subsequent segmental wireless switches are connected to the central switch by optical fibre cables. User end systems such as laptops and I-phones (Internet Phone) are connected to the wireless switches by radio links.

1.4.3 Wireless Wide Area Networks (WWANs)

Wireless wide area networks also called as cellular wireless networks. Wireless connections in local loops are referred to WLL (Wireless Local Loop). WLL provides wireless access to homes and offices. The cellular concept is a method to confirm utilization of the available radio spectrum. In general, the geographical area required to cover by the cellular network is divided into many cells, which are usually deliberated to be hexagonal. The reason behind this deliberation is; shapes which fully cover a two-dimensional geographical region without any overlaps. These shapes can be square, triangle, and hexagon. The hexagon shape is similar to the circular coverage area of a transmitter. An ideal model of the cellular radio system comprised of an array of hexagonal cells. These hexagonal cells have BS (Base

Station) situated at the centre of every cell. Available spectrum of a cell is utilized for uplink and download link channels.

Mobile terminals (MTs) communicate with the base stations by the uplink channels and base stations (BSs) communicate with the mobile terminals (MTs) by downlink channels [Siva Ram Murthy *et al.* (2007)]. The basic concept of the cells depends upon frequency re-use. Frequency re-use refers to usage of same frequency by different users, divided by some distance and without interfering one another. Signal strength of the electromagnetic waves gets attenuated with the distance and frequency re-use is totally depends on it. The group of cells which utilizes the entire radio spectrum is called a cluster. For instance, a cluster of size 'N' means; it has 'N' number of cells with in that cluster. Any two cells within a cluster cannot use channels of same frequency.

Clustering safeguards distances between those cells which uses same frequency. Wireless wide area networks use radio spectrum for distribution of bandwidth among different clusters and clusters have many cells within themselves. Every cell in a cluster has base station and mobile terminals of the cluster or cells get connected to the base stations for communication. Base stations receive signals from the high towered antennas which supports long distance wireless communications. Different high towered antennas get connect each other by line of sight. High towered antennas are collectively responsible for wireless coverage for entire clusters which falls within their transmission range.Fig.1.5 explores the cells of a WWAN cluster.

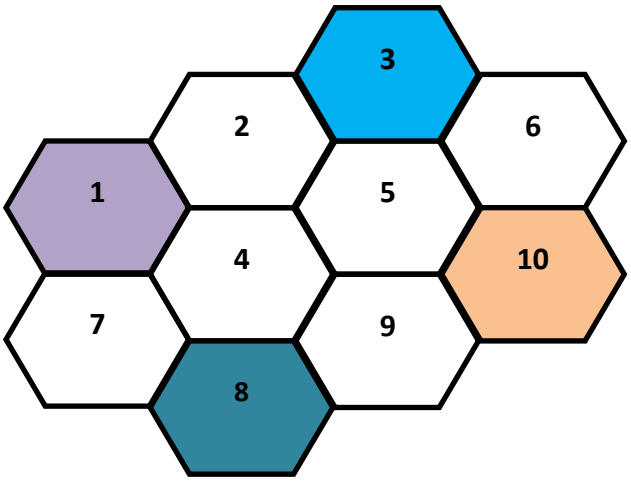

Fig.1.5. Wireless WAN cluster of ten cells

1.5 Network Hardware and Software

Computer network hardware includes different kind of network switches, ports, modules and the network interface cards installed in a computer system. In case of optical fibre cables; for SMF (Single Mode Fibre) and MMF (Multi Mode Fibre) cables, different kinds of connectors are used for short and long distance communication. Multi-mode fibre cables are used for short distance communication whereas single mode fibre cables are used for long distance communication with appropriate ports and modules. In wireless communication, different kind of MODEM (Modulator-Demodulator) antennas are used for radio propagation that includes base stations and wireless access points. Computer networks use different software at different network layers in order to reduce complexity, network software is organised as a set of different layers. These software layers perform specific functions and propose their services to next higher layer.

In order to access services of the lower layers, every layer is provided with a SAP (Service Access Point). The SAP is a kind of interface by which higher layers can access services obtainable from their immediate lower layers. Information passed through the SAP is called IDU (Interface Data Unit) which consists of SDU (Service Data Unit) and control information associated with the SDU. Service data unit holds the authentic data, SDU splits into several units at the layers and each such unit is called PDU (Protocol Data Unit). Different network layers have specific protocols; these network layers are architecture by the OSI (Open System Interconnection) and TCP/IP (Transmission Control Protocol/Internet Protocol) reference models. The OSI reference model includes the following layers; physical, data link, network, transport, session, presentation, and application layers. The TCP/IP reference model includes; host-to-network, internet, transport and application layers [Andrew S. Tanenbaum (2004)].

1.6 Mobile Ad-Hoc Networks (MANETs)

Ad-hoc networks are new generation wireless networks, the principle behind ad-hoc networks is multi-hop relaying. The use of ad-hoc voice communication was in practice during ancient days by the tribal societies with a thread of repeaters of

drums, trumpets and horns, sometimes line of shouting men positioned on different heights. In 1970, ALOHA net was invented by Norman Abramson and his fellow researchers at the University of Hawaii. Features such as single-hop wireless packet switching and multiple access resolution for sharing single channel were incorporated in the invented ALOHA net. The achievement of ALOHA net had prompted extensive interest in various directions of computer network communication including PRNET (Packet Radio Network) project sponsored by DARPA (Defence Advanced Research Projects Agency) [IR 3]. DARPA extended more projects on multi-hop wireless networks through the SURAN (Survivable Radio Networks) project which intended to provide ad-hoc networking with small, low-cost, low-power devices comprising of efficient protocols. These ad-hoc networks proposed by the DARPA were proved improved scalability and survivability. Recognizing the necessity of open standards in this evolving area of computer network communication, a work group of IETF (Internet Engineering Task Force) designated the mobile ad-hoc networks (MANETs) working group [IR 4] was constituted to standardize the protocols and functional specifications of mobile ad-hoc wireless networks. This working group of MANET focussed its efforts towards providing improved and standardized routing functionalities to upkeep self-organizing mobile networking infrastructure. MANET (Mobile Ad hoc Network) is an infrastructure less decentralized wireless network, which do not depend on centralized organization or switching points unlike in wired and other wireless networks.

MANET is a self-organizing and self-configuring network. In mobile ad-hoc networks, routing protocols postulate communication between routers and prompt them to select routes between a source and a destination. Mobile ad-hoc networks have been the emphasis of research interest since last three decades. In ad-hoc network, nodes connect each other dynamically in a random manner. The dynamic topographies of mobile ad-hoc networks require improved version of routing protocols. MANET is a wireless ad hoc network, which has a routable networking scenario with self-forming and self-healing capabilities without a centralized infrastructure. In MANET, route choices are performed by the routing algorithms. Ad-hoc wireless networks falls in that category of wireless networks which use multi-hop radio relaying, these networks have capabilities of functioning even without the

support of any fixed infrastructure, hence these are also called infrastructure less networks. Operating without the support of central infrastructure or access points makes the routing complex. Fig.1.6 demonstrates a mobile ad-hoc network comprising of nodes 'N1' to 'N10'.

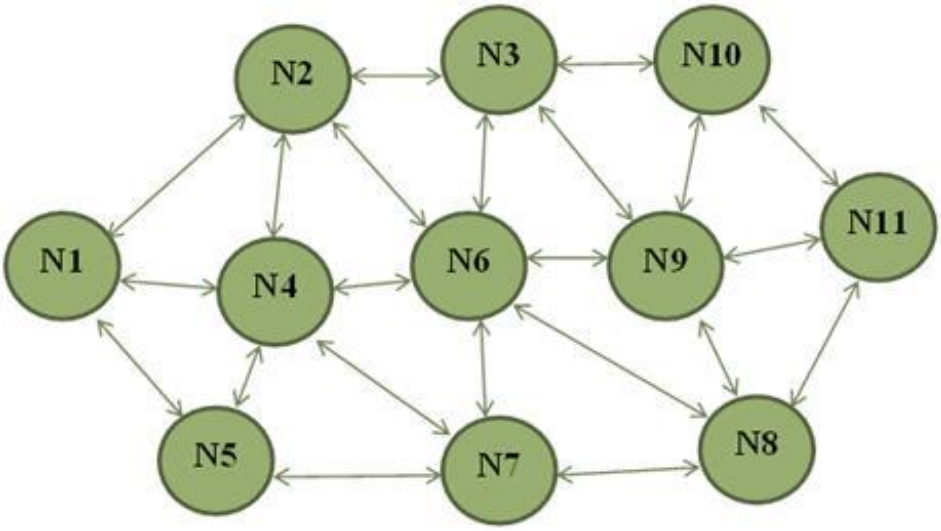

Fig.1.6. Mobile ad-hoc network with 'N' set of nodes

Mobile ad-hoc networks are packet-switched networks; they have multi-hop wireless links with shared radio channels. They encounters frequent path breaks due to mobility of nodes, however these networks support quick and cost-effective deployments. Based on carrier sense mechanism, mobile ad-hoc network supports dynamic frequency reuse but at the same time synchronization is difficult causing bandwidth consumption. In cellular networks, bandwidth reservation is easier but in mobile ad-hoc networks, bandwidth reservation requires complex medium access control protocols [Siva Ram Murthy *et al.* (2007)]. Application domains of mobile ad-hoc networks include military operations, battle fields, emergency search and rescue operations, and collaborative computing. In mobile ad-hoc networks, self-organization and maintenance properties are built into the network and mobile hosts require more intelligence. Important objective of MANET routing protocols is to discover paths with minimum link overheads and quick reconfiguration when path break occurs. Many issues are yet to be addressed in order to achieve successful

deployment of mobile ad-hoc networks in commercial establishments, though their extensive existence at defence.

1.6.1 Routing Protocols in Mobile Ad-Hoc Networks

As discussed in earlier sections of this chapter, mobile ad-hoc wireless network consists of small or large set of mobile nodes which also called as mobile hosts are connected by wireless links. Due to mobile nature of nodes, the topologies of MANETs keep changing randomly. Routing protocols that discovers routes for data packets to follow from a source node to the destination node applied in conventional wired networks cannot be applied in mobile ad-hoc networks. This is because of their highly dynamic topologies, absence of centralized infrastructures such as access points and base stations, bandwidth-constrained wireless links and energy or resource constrained nodes. Earlier, there are many routing protocols that have been proposed for mobile ad-hoc networks. Routing protocols in mobile ad-hoc networks are classified into four main categories, each category has sub categories. The four main categories are; based on routing information update mechanism, based on the use of temporal information of routing, based on topology information organization and miscellaneous classifications based on utilization of specific resources.

Based on routing information update mechanism, routing protocols of MANET are classified as table-driven or proactive, on-demand or reactive and hybrid. Examples of table-driven or proactive routing protocols are; DSDV (Destination Sequenced Distance Vector), WRP (Wireless Routing Protocol), CGSR (Cluster-head Gateway Switch Routing), STAR (Source Tree Adaptive Routing), OLSR (Optimized Link State Routing), FSR (Fisheye State Routing), HSR (Hierarchical State Routing) and GSR (Global State Routing). Examples of on-demand or reactive routing protocols are; DSR (Dynamic Source Routing), AODV (Ad-hoc On Demand Distance-Vector), ABR (Associativity Based Routing), SSA (Signal Stability-based Adaptive Routing), FORP (Flow Oriented Routing Protocol) and PLBR (Preferred Link Based Routing). Based on the use of temporal information for routing, mobile ad-hoc network routing protocols are classified into two categories namely path

selection using past history and path selection using prediction. Examples of path selection using past history are; DSDV, WRP, STAR, DSR, AODV, FSR, HSR and GSR. Examples of path selection using prediction are; FORP, RABR (Route-lifetime Assessment Based Routing) and LBR (Life Based Routing).

Based on topology information organization, routing protocols of MANETs are classified into two categories namely flat routing and hierarchical routing. Examples of flat routing are; DSR, AODV, ABR, SSA, FORP and PLBR. Based on utilization of specific resources routing protocols are classified into three categories namely power-aware routing, routing using geographical information and routing with efficient flooding. Example of power-aware routing is PAR (Power Aware Routing). Example of routing using geographical information is LAR (Location-Aided Routing). Examples of routing with efficient flooding are; OLSR and PLBR. The classification of routing protocols in mobile ad-hoc networks is not reciprocally exclusive and some routing protocols fall in more than one class [Siva Ram Murthy *et al.* (2007)].Routing is a process by which route discovery takes place between a source nodes to the destination nodes. In mobile ad-hoc networks, each mobile node acts as a router. The most important aim of routing algorithms in ad hoc network is to create an accurate and proficient route among all the member nodes and to make sure correct and timely discharge of packets [Rutvij *et al.* (2012)].

1.6.2 Core Issues in Routing

Routing algorithms perform two main functions, one is the selection of routes for various source-destination pairs and the other is delivery of messages to their exact destinations once the route discovery is achieved. The second function is theoretically upfront using a range of protocols and data structures. There are two key performance measures which are significantly affected by the routing algorithms namely the throughput and average packet delay. Throughput can also be called as quantity of service and average packet delay can be termed as quality of service [Dimitri Bertsekas*et al.* (2004)].

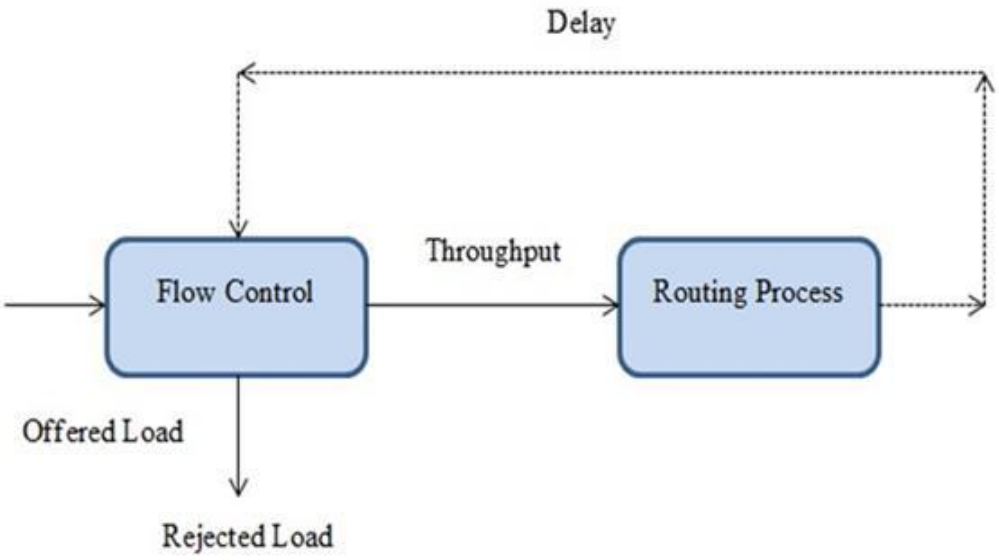

Fig.1.7. Routing and Flow control

Packet flow control permits more traffic into the network; however a better routing retains low delays. Process of routing interacts with the packet flow control to determine the throughput and average packet delay (performance measures) by the support of feedback mechanism as shown in Fig.1.7. During less traffic loads that are offered by the external locations to the subnets, the traffic loads will be completely accepted by the network, that is,

$$\text{Throughput} = \text{Offered Traffic Load} \tag{1.1}$$

During excess offered traffic loads, a portion of the offered traffic load will be rejected by the flow control, that is,

$$\text{Throughput} = \text{Offered Traffic Load} - \text{Rejected Load} \tag{1.2}$$

The offered traffic load allowed into the network will encounter an average delay per packet, and it is determined by the routes selected by the routing algorithms. Though the throughput will also get affected by the routing algorithms since usual flow control schemes function on the basis of prominent balance between throughput and average packet delay. In other words, rejection of offered traffic load begins with respect to increase in amount of average packet delay. When routing algorithms successfully keeps lesser delays, then the flow control algorithms permits more traffic loads in to the network [Siva Ram Murthy *et al.* (2007)].

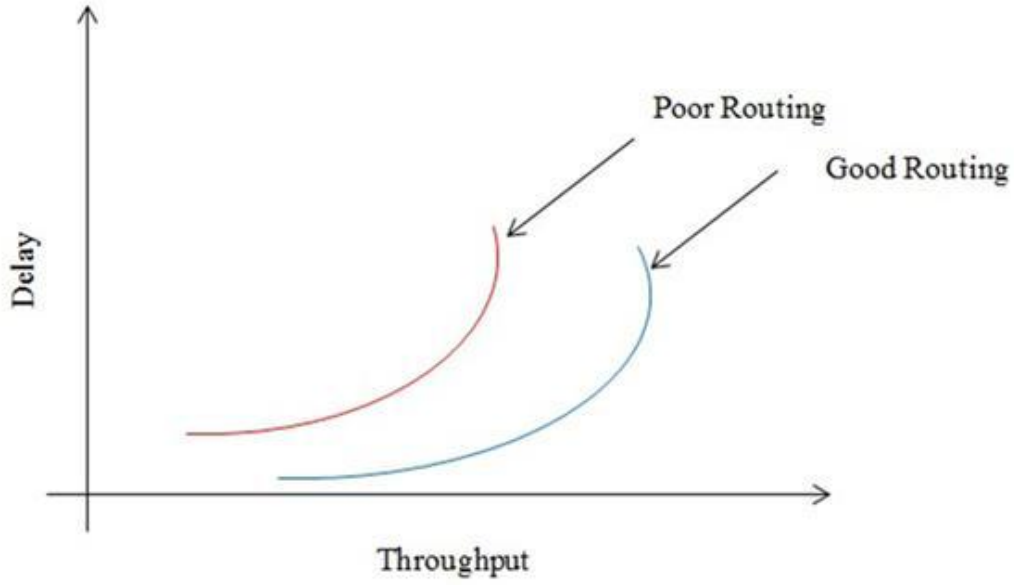

Fig.1.8. Performance measures curves for good and bad routing

Flow control determines the accurate balance between the throughput and average packet delay, under higher offered traffic load conditions, the effect of good routing can realize much favourable delay-throughput curve through which flow control functions as shown in Fig.1.8.

1.6.3 Ideal MANET Routing Protocol Characteristics

Owing to issues and challenges in MANETs and wireless networks, routing protocols of wired networks are not suitable and cannot be used in wireless ad-hoc networks [Siva Ram Murthy *et al.* (2007)]. Thus, in order to overcome from the issues and challenges, the wireless ad-hoc networks need dedicated routing protocols. An ideal MANET routing protocol should have the following characteristics [Siva Ram Murthy *et al.* (2007)]:

- The ideal routing protocol must have fully distributing characteristics as centralized routing carry large amount of overheads due to which scalability is not possible. As compare to centralize routing, distributed routing is more fault-tolerant but it has a drawback of single point of failure.

- The ideal routing protocol must be adaptive to frequent changes in network topology occur due to node mobility.

- Number of network nodes that involve in route maintenance and computation must be lesser. Each and every node of the network must have quick and easy access to available routes, in other words; time required for setting the connection must be minimum.

- The ideal routing protocol must be free from decayed routes and free from loops.

- Number of broadcast made by each and every node in the network must be limited in order to avoid number of packet collisions. The transmissions in the network should be reliable so that message loss can be reduced and occurrence of decayed routes can be prevented.

- When network topology becomes stable, the ideal routing protocol must converge to optimal routes. This convergence must carry out quickly.

- The ideal routing protocol must use scarce resources such as computing power, bandwidth, memory, and battery power optimally.

- Each and every node in the network must only try to store information pertaining to the stable local topology. Topology information maintained by the network nodes must not be updated when changes occur in remote part of the network.

- An ideal routing protocol must be able to provide some level of QoS (Quality of Service) as per demands made by the applications, and it must support time-sensitive traffic.

1.7 Media Access Control Protocols in Mobile Ad-hoc Networks

Mobile nodes in mobile ad-hoc networks share a common broadcast radio channel. Due to inadequate radio spectrum, the bandwidth accessible for communication in MANETs is also limited. Therefore, access of shared medium must be managed in such a way that every node gets a better share of the available bandwidth and this bandwidth must be utilized resourcefully. Characteristics of the wireless medium are entirely different from that of wired medium, mobile ad-hoc

networks required to address exclusive concerns like limited bandwidth availability, node mobility, error-prone broadcast channel, hidden and visible terminal problems and energy or power constraints, and these concerns of MANETs are not applicable to the wired networks. Hence, mobile ad-hoc networks require different set of MAC (Media Access Control) protocols for managing and controlling access to the shared medium. MAC protocols for mobile ad-hoc networks can be classified into numerous categories and these categories are based on initiation approach, time synchronization and reservation approaches. MAC protocols for MANET are classified into three elementary types; contention-based protocols, contention-based protocols with scheduling mechanisms, contention-based protocols with reservation mechanisms.

Contention based protocols follow contention-based access policy, nodes of the network does not make any sort of resource reservations on priority basis. When a node receives a data packet for transmission, it contends with neighbour nodes for access to the shared channel [Siva Ram Murthy *et al.* (2007)]. Contention-based protocols cannot deliver QoS (Quality of Service) guarantees to the transmission sessions because nodes do not access the channel regularly. Contention-based protocols with scheduling mechanisms concentrate on packet scheduling at nodes and scheduling up of nodes for channel access. During node scheduling, every nodes treated equally in order to avoid bandwidth starves among nodes. Scheduling based schemes are used to achieve priorities among flows whose packets are queued at the network nodes. Contention-based protocols with reservation mechanisms provide QoS guarantees when mobile ad-hoc networks required supporting real-time traffic. In order to support such real-time traffic, priority based bandwidth reservation is required, these protocols can offer QoS provision to time-sensitive traffic sessions. Media access control protocols in mobile ad-hoc networks involved certain issues that are required to be addressed; bandwidth efficiency, quality of service support, synchronization, hidden and exposed terminal problems, error-prone shared broadcast channels, distributed nature or lack of central coordination and mobility of nodes.

MACAW (Multiple Access Collision Avoidance Protocol) is a contention-based media access control protocol which is based on the multiple access collision avoidance protocol proposed by the researcher Karn [Karn (1990)]. The FAMA

(Floor Acquisition Multiple Access) is another contention-based media access protocol which is based on a channel access persuasion, which comprised of carrier-sensing function with a collision-avoidance negotiation between the sending source and the receiving destination nodes [Fullmer *et al.* (1995]. Some other MAC protocols available for MANETs are; BTMA (Busy Tone Multiple Access) [Tobagi *et al.* (1975)], MARCH (Media Access Reduced Handshake Protocol) [Wu *et al.* (1987)] and RI-BTMA (Receiver Initiated- Busy Tone Multiple Access) [Talucci *et al.* (1997)].

1.8 Scope of the Thesis

The present thesis deals with study and performance analysis on some well-known routing protocols in mobile ad hoc networks. Study and performance analysis on the AODV, DSDV, OLSR and DSR routing protocols were executed in this thesis. The thesis consists of seven chapters including the current one entitled "Introduction". The remaining chapters are organized as follows.

Chapter-2 includes some of the major works in the related area of mobile ad-hoc network routing protocols. Various state-of-the-art technologies as available in the literature are discussed in brief in this chapter. The latest trends in the field of development of various techniques of performance improvements in MANET routing protocols and their applications in various fields have been reviewed in detail. Security issues associated with the routing in mobile ad hoc networks were also discussed in this chapter. Various performance measuring metrics have been debated in detail along with the details of the simulation tools used also discussed in this chapter. Based on the literature survey carried out in this chapter, the motivation behind the present study is outlined at the end of this chapter.

Chapter-3 is devoted to studying and comparative performance analysis of different node density and node pause time effects on standard AODV, DSDV and OLSR routing protocols. Node density refers to the network models comprising of a different set of nodes and node pause time refers to the halt position of a mobile node. Networks of different sets of nodes were created to test the behavior and performances of the routing protocols. Similarly, different node pause time intervals

were considered for examining the performances and deeds of the routing protocols. There were two scenarios fixed for each effect; simulation scenario - I and simulation scenario - II. For these scenarios, many network parameters were taken into consideration. For simulation scenario - I, different set of nodes used were 30,40,50,60,70,80,90 and100. Simulation time was fixed to 150 seconds with no pause time. Wi-Fi mode was set to the ad-hoc mode with a rate of 2Mbps (802.11b). Transmit power was set to 7.5dBm with 10 number of fixed source/sink connections. Random waypoint mobility model was used for a rectangular region of 300 × 1500 m to ensure node mobility at a speed of 20 m/s. Transmission data rate was fixed to 2.048 Kilobits per second along with the data packet size of 64 Bytes using friss loss model. For simulation scenario - II, different node pause times considered were 5,10,15,20,25,30 seconds with 50 numbers of network nodes and rest network parameters were set as in simulation scenario - I. In this chapter, various performance measuring metrics were analyzed and the obtained results were discussed with suitable comments along with tables and graphs.

Chapter-4 is involved with the study and analysis of diverse node velocity and transmit power effects on standard AODV, DSDV, and OLSR routing protocols. Node velocity refers to the speed at which mobile nodes travels. Transmit power refers to the transmission power by which a source node transmits the data packets to the destination node. Random waypoint mobility model was used for the simulation-based node mobility with different speeds. Study and analysis of different node velocity and transmit power effects were conducted in two cases. In the first case, analysis of varied node velocity effects was taken into account and in the second case, analysis of diverse transmit power were considered. Different values of node velocities were; 10 m/s, 20 m/s and 30 m/s and 3.5dBm, 4.5dBm, 5.5dBm, 6.5dBm, 7.5dBm, 8.5dBm and 9.5dBm were considered as different transmit power values. Other network parameters were kept similarly as in chapter-3 in order to maintain the same test platform for testing performance and behavior of the standard AODV, DSDV and OLSR Routing protocols for different varying parameters.Different network parameters were set for simulation-based experiments in a 300 x 1500 m rectangular simulation region. Separate experiments were conducted for each value of node velocity and the transmit power. Obtained packet data was used for analyzing

different performance evaluating metrics. At the end of the chapter, results were tabled and plotted with appropriate comments.

Chapter-5 includes investigations on performances of the standard and attributes revised routing models of AODV, DSDV, and OLSR routing protocols in different node density scenarios. Performance analysis accomplished in chapter-3 and chapter-4 reveals weak performances of AODV and DSDV routing protocols as compare to OLSR. Hence, routing parameters of AODV and DSDV protocols were primarily investigated for possible performance improvements considering one of the effect studied earlier that is, different node population scenarios. These analyses were carried out in three different sections; section 'A' deals with the AODV routing protocol, section 'B' deals with DSDV routing protocol and section 'C' deals with the OLSR routing protocol. In every section, the performance of the revised routing model was compared with the performance of the standard routing model in order to check performance improvements. Routing attributes of the standard routing protocols were altered to test possible performance improvements. Attributes of the parameters associated with each routing protocol were tested for different values according to their functions and to achieve performance enhancements in the routing protocols. In chapter-5, comparative performances of the attribute revised routing models were also discussed in section 'D'. Obtained packet data was utilized for analyzing various performance calculating metrics such as; the throughput, packet delivery ratio, end-to-end delay, packet loss and normalized routing load. At the end of this chapter, results were discussed in detail with graphs.

Chapter-6 includes investigations on performances of the standard and attribute revised routing models of DSR routing protocol in different node population scenarios. Routing attributes of the standard dynamic source routing (DSR) protocol were altered in order to obtain a new DSR protocol design namely, the REV.DSR (Revised DSR). Performances of the REV.DSR was tested and compared with the performances of the STD.DSR (Standard DSR) to check possible performance improvements in different node densities. Suitable network parameters and attributes revised dynamic source routing parameters were set for this analysis. Like in previous chapters, obtained packet data was employed for analyzing various performance

evaluating parameters namely, the throughput, packet delivery ratio, end-to-end delay, packet loss and normalized routing load. In this chapter, various performance measuring metrics were analyzed and the obtained results were discussed with suitable comments along with tables and graphs.

Chapter-7 concludes some major outcomes and findings of the thesis. This chapter presents the overall conclusions drawn from the results presented in chapters 3 to 6 of the thesis. Finally, based on the constraints and limitation of the present study, an outline regarding the future scope of the works in the related area of research has been presented at the end of this chapter.