Chapter 3

Research Methodology

3.1 Methodologies

In this section, some tools and methodologies, used at the time of development of the proposed RED based schemes, have been discussed.

3.1.1 MANET

A network facilitates the distribution of files and information between multiple computers. Computer networks can be interconnected through either Ethernet cables or using wireless cards that send and receive data or wireless medium like air. An ad hoc network establishes a link between various nodes without any base station. Mobile Ad Hoc Networks (MANETs) are quickly becoming a common mode in telecommunication because of easy deployment and fast configuration. They are used in disaster managements like earthquake, flooding, hurricane and military operations. These networks use broadcasting as a method for communication, for updating the topology, maintaining the network, giving warning messages. They comprise a group of network nodes thet link each of them using a wireless medium like air infrastructure. All the nodes are working as source, router or destination. The topology of the network can change dynamically because the nodes move in different directions, leave or join it. Such change creates problems in maintaining the routing process through energy loss, delay and instability in linking. So, the routing protocol must be designed to provide energy maintenance, avoid delay and make the link stable.

System grouping and routing strategies are being shown in Figure 3.1 and Figure 3.2. The wireless networks are categorized into two types. (i) Infrastructure network which needs a base station to function (ii) Infrastructure-free system that operates without a ground station for all nodes.

Latest developments in miniaturisation and the initiative for universal standards for wireless networking (Bluetooth, IEEE 802.11, RFID) have significantly encouraged the implementation of ad-hoc system and help for more sophisticated features. This enables a node to serve as a repeater as well as a wireless terminal and yet be small enough to be handheld. It is said that an ad hoc network is a self-organizing adaptive array of certain devices linked with wireless

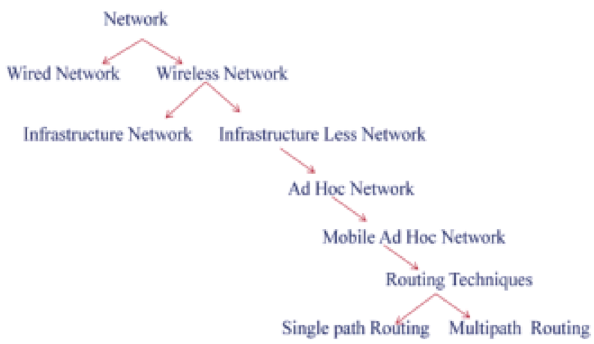

Figure 3.1: *Classification of Network and Routing mechanism*

Figure 3.2: *Example of sample Mobile Ad hoc communication system*

connexions. Normally, a cellular system is a decentralised network. The network is adhoc, since each node is able to forward data packet to other nodes, because it is dynamically defined which nodes will forward data.

In ad hoc networks, there are usually two types of frameworks: flat and hierarchical [3], [59]. A transceiver, an antenna and a power supply are fitted for each node in an ad hoc network. In terms of size, computing ability, communication range and battery capacity, the features of such nodes can differ widely. Depending on context, certain nodes may function as servers, others as clients, and few others may be versatile enough to operate as both. In some situations, in order to exchange knowledge from one node to another, each node can need to serve as a router [?].

The clustered design of ad hoc wireless networks gives them an advantage for a range of applications where it is difficult to focus on the central nodes. When opposed to wireless managed networks, it also increases the inter operability of wireless ad hoc networks. Ad hoc networks are also able to connect seamlessly with the current infrastructure-oriented network [59], [10]. Some of the utilizations are given below:

(i) If a catastrophe happens, it is likely that the current communication system will totally fail and it is important to regain connections immediately. An ad hoc wireless network with broad band capability can be used to get crisis response facilities in such a situation. A networking system may be built up in hours instead of weeks by using a hand-held ad-hoc network.

(ii) Wireless Adhoc networks have automotive infrastructure implementations and are referred to as Vehicular Adhoc Wireless Networks. Vehicles connect with each other within these networks and perhaps with wayside facilities. Users can be presented with a long range of utilizations ranging from transit protection to driver activity to internet connectivity through these.

(iii) There is no chance of providing infrastructure-oriented networks on battlefields. In such places, an adhoc network can be quickly deployed and assist in proper communication among the troops.

3.1.2 Routing in MANET

MANET is a self organised wireless multi hop network that is neither used attached infrastructure nor predetermined access point. It consists a set of nodes that employing radio communication. No base-station is present there to serve as the router on the MANET. Intermediate nodes serve as routers and these nodes are used by the source node to route their messages. Therefore the destination receives the packets from its sender node when each node transmits packet on the behalf of other nodes.Then it is required to forward data via several hops to the destination from starting node.In the same channel, between the nodes Ad-Hoc networks faithfully depend on multitop data transmission. Nodes interact via the intermediate nodes with one another. Therefore, in an ad-hoc network situation the effective performance and availability of each node is essential. An effective routing strategies is therefore needed to improve MANET communication. Designing messaging and creating protocols for such networks are a difficult task due to the complex existence in MANETs. The configuration of the routing protocols used to create and sustain multi-hop routes to facilitate data communication between nodes is one of the most critical facets of the communication process.

In this area of investigation, a significant amount of work has been done and several protocols for multi-hop routing have been bloomed. Many of these protocols, such as DSDV [**?**], DSR [26], AODV [**?**], TORA [40], and others, build and retain best-effort routes.

3.1.2.1 Routing Protocol Schemes

There are three simple Ad-Hoc routing techniques which are existed. One is considered a table-driven or constructive routing strategy, while the next one is source-initiated and is referred to as a demand-driven or reactive approach. In comparison to these two fundamental approaches, the third is a blended approach that incorporates some of the elements of both constructive and reactive methods. This classification is represented in Figure 3.3.

3.1.2.2 Proactive strategy

Each node continuously preserves the full network routing information in a constructive scheme. The path would be readily accessible anytime a node has to forward a packet, so there is no hesitation in looking for a path. Nevertheless, diligent schemes can expend a large amount of limited wireless energy on keeping the modified routing information accurately for a extremely complex topology. The examples of these protocols which are built on these technique are (i) Destination Distance vector(DSDV)Routing[3](ii) Streamlined connection state Routing .

3.1.2.3 Reactive strategy

Nodes retain only routes having active destinations in reactive schemes. For any new destination, a route search is required. Therefore, due to path quest, the contact overhead is lowered at the cost of path setup delay. For the ad hoc world, these devices are chosen because battery life is maintained both by not sending and receiving the data packets.

3.1.2.4 Hybrid strategy

This protocol splits the system into regions for mixed strategies, and runs a pragmatic rules among the regions and apply a specific methodology to route the packet between zones. For big systems where clustering and separation of the network is very usual, this strategy is best suited.

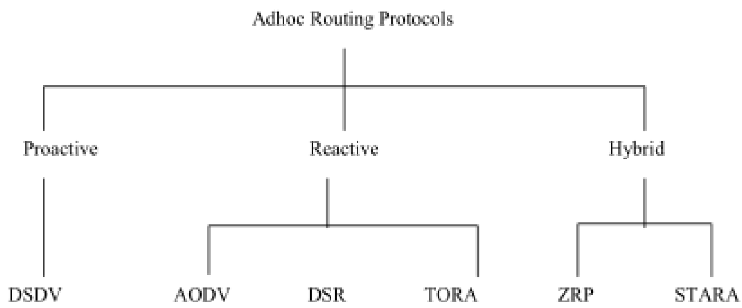

Figure 3.3: *Categorization of Ad hoc routing protocols*

3.1.3 Congestion in MANET

Congestion is a state where too much data is carried by a node or connection. Network congestion degrades the performance of the network; it not only increases packet losses and depletion of bandwidth, but also wastes energy and other congestion recovery resources. This can lead to a congestion collapse if no suitable congestion management is carried out. The congestion collapse is a condition that can be experienced by a network if no helpful contact happens due to congestion. Therefore, congestion management is important to prevent network congestion and to enhance post-congestion efficiency. Regulation of congestion can be carried out by the technique for detecting congestion. It is possible to assess congestion within the networks by using various measures, such as the length of the queue, incoming rate, and outgoing rate. In MANET, congestion is caused by limited availability of resources. Increased number of users can cause congestion. The queue is used to hold packets to be transmitted, overflow within a particular node causes congestion. Link reliability also is the cause of congestion. When the ink is broken, congestion is increase by the packet retransmission. When more number of nodes try to grab the channel at the same time, congestion will occur.

3.1.4 Active Queue Management

Active queue management (AQM) systems typically have three queue management components: (1) the measure of congestion, (2) congestion control function and (3) the process of feedback [8], [31], [56] and [54]. The indicator for congestion is used to assess whether there is congestion. The queue management for the role of congestion control dictates what should be done when it senses congestion. The process for input the congestion signal which used to warn the source to adjust its rates of transmission. The role of congestion control is to drop all receiving packets when the queue becomes full, with a probability of one (1), and packets are dropped by the congestion signal.

The goal of the AQM based routing protocol is to maintain the rate of packet reaching at the waiting line, that is some proportion of the capability of the link. It regulates queue length circuitously [6]. A queue-based AQM adjusts on the (fast or average) dimension of the waiting line [29] and its activity is to maintain the size of the queue at a level of objective measure [55], [23], [34].

In AQM based research, different authors use different performances parameters to prove the efficacy of their proposed AQM schemes. These include fairness, jitter delay, packet loss, throughput and goodput of the application of links use, queue stability, responsiveness, sophistication and robustness. It could be useful for AQM studies to define standardised definitions in conjunction with uniform implementation, for all these metrics based thresholds where applicable. A prevalent calculation and set of statistics may also be able to applicable. It could be helpful to have a common, online and open AQM performance repository of results for the researchers to upload those results with their algorithm. This makes an ongoing comparison possible. Often, this will have more definite way of judging success in terms of progression of the performance of the whole research arena of AQM. However there are some findings on the AQM schemes based on the performance metric, the evolutionary procedure of AQM is a problem because the web environment is more complicated.

3.1.5 Random Early Detection (RED)

Floyds et al. proposed Random Early Detection (RED) [16] in 1993. Random Early Detection (RED) gateways in packet-switched networks for congestion avoidance. The gateway senses incipient congestion by calculating the average queue size. The gateway could monitor congestion connections in two ways:(i) falling packets at the gateway and (ii) setting a bit in the headers of packets. The gateway significantly reduces or identifies each arriving packet with a certain likelihood when the average queue size reaches a predetermined threshold. The specific probability indicates the feature a queue having average size. RED gateways make the overall queue size smaller and allow packets to burst regularly in the queue. During congestion, the likelihood that a given link is told by the gateway to minimise its window is approximately proportional of the share of bandwidth link across the gateway. RED gateways are designed to complement a protocol such as TCP for transport-layer congestion control. The RED gateway has no prejudice toward bursty traffic and prohibits certain links from being internationally coordinated, reducing their windows at the same time. To demonstrate the quality of RED gateways, simulations of a TCP / IP network are used. since, the developed tiny sensor nodes have low cost, low power consumption and they are multi operational and limited in size, so they contribute to increase usage of sensor networks in most real-time monitoring application [1] [13] [20]

RED's benefits are recognised by few researchers over drop tail routers. But there are some issues that decrease its efficiency. We propose to make some adjustments to the classic RED design unlike current RED improvement strategies. The majority of the original RED remains constant. The limitations of RED algorithm are as follows:

(i) If congestion is too high, it is impossible for the gateway to controlling the average queue size by numbering a fraction at most packet max_p so the average size of the queue will surpass. The max_{th} and the gateway mark each packet before each packet is picked.

(ii) The coming data packet is discarded with P_a probability even when the current queue size is empty. It will happen if the average queue size lies between minimum and maximum values.

(iii) As communications minimize their sending percentage then window instantly decreases but the average queue size would decline slowly. If the average queue length is higher then entering data will be fall with greater probability in no congestion condition.

(iv) If congestion becomes instantly high, instant queue size will be increase and the limits of queue will be raised and exceeded but no packets will be randomly dropped because the average size of the queue is less than min_{th}.

(v) RED efficiency is dependent on the number of competitors participating in flows / sources. When the load is high, the RED output is degraded.

(vi) Wild queue fluctuation is detected with RED when the traffic load is change.

(vii) RED achievement is conscious to the size of the packet.

(viii) RED output is incredibly susceptible to the configurations of its variables.

3.2 Performance Metrics

Under different conditions in Network Simulator 2 (NS2), various performance metrics are used to evaluate our proposed scheme. Simulation scenarios are defined as varying the network size by node variable number, node mobility variation, and connection variable number.

Output alone should not be regarded as a performance measure in MANET. In order to verify the network efficiency, Reid and Seide [49] insisted on calculating packet failure, end-to - end delay and jitter. Durkin [50] has shown that the most relevant measures for CBR traffic are packet loss and delay.

In the current research, for both standard DSR and updated DSR, efficiency metrics such as throughput, average end-to - end latency, packet transmission fraction (PDF) and percentage packet loss have been measured and evaluated. The output indicators listed above were determined as follows:

3.2.1 Throughput

The instant throughput can be computed if the time been considered as instant time. Similarly, the average throughput can be computed using the same relationship by considering the time as total simulation time.

$Throughput = \frac{No.\ of\ bytes\ received \times 8}{Time \times 1000} kbps$

3.2.2 Average Goodput

Goodput is a communication's throughput which is defined as the amount of useful data transmitted in bits per unit time by the MANET to a certain endpoint. It is a ratio between both the amount of information delivered with the total delivery time.

3.2.3 Average End-to-End Delay

The average end-to - end delay is a calculation of the average time needed for each data packet to be transmitted from the origin to the final point. Higher end-to - end delays suggest network congestion.

3.2.4 Packet Delivery Fraction (PDF)

Packet Delivery Fraction (PDF) is the ratio of packets received effectively to the number of packets sent. A higher PDF value reveals that the network does better with smaller packet losses.

3.2.5 Percentage Packet Loss

Packet loss is calculated with respect to packets received as a proportion of packets destroyed.

$\%Packet\ Loss = \frac{No.ofpacketssent - No.ofpacketsreceived}{No.ofpacketssent} \times 100$