Abstract—MANET is determined as a network that has many free autonomous nodes that can move locations and configure itself to various networks and operate without any centralized administration. Some MANETs are restricted to a local area of wireless devices (such as a group of laptop computers), while others may be connected to the Internet. For example, A VANET (Vehicular Ad Hoc Network), is a type of MANET that allows vehicles to communicate with roadside equipment. Because of the dynamic nature of MANETs, they are typically not very secure, so it is important to be cautious what data is sent over a MANET. There are various applications of MANET, In Commercial Sector: e.g. in fire, flood, or earth-quake. Local Level: e.g. conference or classroom. In MANET, congestion can take place between two intermediate nodes, occurs when bandwidth is insufficient and network data traffic exceeds capacity. This paper mainly studies and compares the performance of MANET routing protocols namely PSR, DSR, DSDV and AODV under various traffic loads with various maximum TCP congestion window size to improve congestion control in the routing. The metrics used to compare routing protocol performance are packet delivery ratio, average routing load, the average end-to-end time required with delay and average network throughput and mainly to overcome congestion situation and avoid packet loss in wireless networks.

Index Terms—Congestion control, Mobile Ad Hoc Networks (MANET), On-demand (reactive) routing protocol, Packet Delivery Ratio, Table-driven (proactive) routing protocol.

I. INTRODUCTION

Mobile ad-hoc network is dynamic in nature and due to the feasibility of having every node works on temporary bases there is no centralize control because and frequently changes their location and hence there is zero possibility to find the location of where the real destination node is and what changes in the location of the nodes can take. There might be a situation may occur when the whole data or some of data is not able to reach at destination on time because of congestion or because of any other reasons in the network, as data is dropped in the network.

Types of MANET:

Vehicular ad hoc networks (VANETs) are used for communication between vehicles and roadside equipment. Intelligent vehicular ad hoc networks (In-VANETs) are a kind of artificial intelligence that helps vehicles to behave in intelligent manners during vehicle-to-vehicle collisions, accidents. Smart phone ad hoc networks (SPANs) leverage the existing hardware (primarily Bluetooth and Wi-Fi) in commercially available smart phones to create peer-to-peer networks without relying on cellular carrier networks, wireless access points, or traditional network infrastructure. SPANs differ from traditional hub and spoke networks, such as Wi-Fi Direct, in that they support multi-hop relays and there is no notion of a group leader so peers can join and leave at will without destroying the network.

Internet based mobile ad hoc networks (iMANETs) are ad hoc networks that link mobile nodes and fixed Internet-gateway nodes. For example, multiple sub-MANETs may be connected in a classic Hub-Spoke VPN to create a geographically distributed MANET. In such type of networks normal ad hoc routing algorithms don’t apply directly. One implementation of this is Persistent System’s CloudRelay.

Military or tactical MANETs are used by military units with emphasis on security, range, and integration with existing systems. Common waveforms include the US Army’s SRW.

Table-driven (proactive) routing:

This kind of protocols maintains fresh lists of destinations and their routes by distributing routing tables at regular intervals of time throughout the network. The overhead with this is need of Respective amount of data for maintenance along with slow
reaction on restructuring and failures.[3]

Examples of proactive algorithms are:
- Destination Sequence Distance Vector :DSDV
- Optimized Link State Routing Protocol :OLSR
- DREAM

**On-demand (reactive) routing :**

This kind of protocol finds a route on demand by overloading the network with Route Request packets due to which there is high latency time in route finding. There are also chances of network clogging due to excessive flooding.

Examples of on-demand algorithms are:
- Power-Aware DSR-based[5]
- Ad hoc On-demand Distance Vector: AODV
- Dynamic Source Routing (RFC 4728)[2][3]

**Congestion control :**

Manages traffic involvement into a telecommunications network, to overcome congestive collapse by overcoming over subscription by decreasing the rate of packets. It completely different from flow control, which avoids the sender from overloading the receiver. The goal of congestion control is to manage the number of packets inside the network below the level at which performance leads to decrease.

There are various ways developed for congestion control:
- Adaptive Congestion Control
- Rate Control Protocol
- Explicit Congestion Control Protocol

**II. LITERATURE SURVEY**

This paper explains briefly problems with their respective solution that occurs due to congestion control in high speed network. Based on the study of different papers there are some important issues related to the proposed model. There are still some limitations with several protocols that were previously used for congestion control. TCP, a widely used protocol, works well in low speed data network but fails in high speed network, it gives poor performance. The old protocols were not able to satisfy main design requirements of congestion control protocols, such as high utilization, max min fairness, small queue sizes and no observable packet drops. To fix these issues new adaptive protocol introduced that has a learning capability [2].

![Fig. 1. Classification of Ad hoc Routing protocols](image_url)

The sub-service prediction detects a failure which may occur or disconnection of the network by establishing a list of critical object. Each controller can know the present status of all nodes of its group. To analyze the criticality, the sub-service can detect frequent failure or shutdown along with several types of items critical energy point. If there is fall in an energy level of a node [5]. When the routing protocols in MANET are not able to identify about the congestion, it results in the following issues. [6]

**Long delay:** This holds up the process of detecting the congestion. When the congestion is very complicated, it is better to select an alternate new path.

**High overhead:** Largely processing and repeated communication attempts are necessary for a new route discovery. If the multipath routing is utilized, it requires additional effort for upholding the multi-paths regardless of the presence of alternate route in network.

**Many packet losses:** The congestion control mechanism attempts to reduce the excess load in the network by either decreasing the sending rate at the sender side or by dropping the packets at the intermediate nodes else by executing both the process. This results in increased packet loss rate or minimum throughput.

Congestion is an important issue that can arise in packet switched network. Congestion is a situation in Communication Networks in which too many packets are present in a part of the subnet, performance
degrades. Congestion in a network may occur when the load on the network (i.e. the number of packets sent to the network) is greater than the capacity of the network (i.e. the number of packets a network can handle.) In other words when too much traffic is offered, congestion sets in and performance degrades sharply.

How to correct the Congestion Problem: Congestion Control refers to techniques and mechanisms that can either prevent congestion, before it happens, or remove congestion, after it has happened. Congestion control mechanisms are divided into two categories, one category prevents the congestion from happening and the other category removes congestion after it has taken place.

Congestion Types: Congestion can be differentiated into four different types [5]:

1. Instantaneous Congestion: It is caused by mild bursts, created naturally by business of IP traffic.

2. Baseline Congestion: It caused by systematic under-engineering of network or node capacity

3. Flash Congestion: It suggests periods of overload in a highly utilized network, where bursts from each single sources add up to create packet loss hills.

4. Spiky Delay: It a condition where no packets are forwarded for a long duration of time - the transit delay of packets increases up from few milliseconds to tens of seconds during this period.

Congestion Control Techniques: Several techniques can be employed for congestion control. These include

Warning Bit: A special bit in the packet header is set by the router to warn the source when congestion is detected. The bit is copied and piggy-backed on the ACK and sent to sender. The sender mentions the number of ACK (acknowledgment) packets, it receives with the warning bit set and adjusts its transmission rate accordingly.

Choke Packets: A choke packet is control packet generated at congested node and transmitted to restrict traffic flow. The source, one receiving the choke packet must reduce its transmission rate by a certain percentage.

Load Shedding: When buffers become full routers simply discard packets. Which packet is chosen to be the victim depends on the application and on the error strategy used in data link layer.

Random Early Discarded (RED): This is a proactive approach in which the router discards one or more packets before the buffer becomes completely full. Each time a packet arrives, the RED algorithm computes the average queue length.

Traffic Shaping: Another method to congestion control is to shape the traffic before it enters the network. It controls the rate at which packets are sent (not just how many). Used in ATM and integrated services networks. At connections setup time, the sender and carrier negotiate a traffic pattern (shape). Two traffic shaping algorithms are as follows Leaky Bucket Token Bucket.

As an outcome, a requirement of advanced congestion control protocol is observed. It is one of major challenge for MANETs. There are various ideas and solutions have been proposed to overcome this difficulty and try to fix the problem of interference during mobility and upgrade the cellular network design. In this way, ad-hoc networks are multi-hop networks in which data has to be transferred from sender to receiver through wireless links. The wireless links and pathetic protocol design not only degrade the performance but also restrict the ad-hoc network for limited applications. In this paper we are providing a proposal to deal with the congestion control problem in mobile ad-hoc networks.

Packet Delivery Ratio : The calculation of Packet Delivery Ratio (PDR) is based on the received and generated packets as recorded in the trace file. In general, PDR is defined as the ratio between the received packets by the destination and the generated packets by the source. Packet Delivery Ratio is calculated using awk script which processes the trace file and produces the result. Protocols are used to maintain data integrity, delivery, through put and packet drop ratio in mobile ad-hoc network. It is most important to study performance metrics factors like throughput and packet drop ratio of proactive and reactive protocols in mobile ad-hoc network. In this paper, a comparative performance analysis is based on protocols like the Dynamic Source Routing, the

---

Fig. 2. Concept Of Congestion

The sender mentions the number of ACK packets, it receives with the warning bit set and adjusts its transmission rate accordingly.
Ad-hoc On-demand Distance Vector, the Destination Sequenced Distance Vector and the Optimized Link State Routing protocols using NS2 simulator.

Due to mobility constraints and high dynamics, routing in Mobile Ad-Hoc Network is a very challenging task. In this work, we evaluate the performance of the routing protocols in mobile network environment. The objective of this work is to assess the applicability of these protocols in different mobile traffic scenarios. Here we considered Topology based routing protocols. In Topology-based routing protocols, both proactive (DSDV) and reactive protocols (AODV, DSR) have been considered for the study. Performance metrics such as packet delivery ratio, throughput, and end-to-end delay are evaluated using NS-2. Simulation results shows position based routing protocols gives better performance than topology based routing protocols.

III. SYSTEM ARCHITECTURE

This system architecture is shown in the below figure. The source node at the initial search path in its database, if it is not present it start creation of BFST, The BFST creation consist of 3 modules such as neighborhood trimming, route update, streamlined differential update. The route is select and source node send packet to destination. If the congestion occurs in the route, allowed-packet loss packet loss then Error Detection and Indication message (EDIM) is generated and send to source node.

![System Architecture](image)

Fig. 3. System Architecture

The multipath protocols are broadly classified into five categories based on their major goals. The goals are to improve delay, provide reliability, reduce overhead, maximize network life and support hybrid routing. Multipath routing protocols address issues such as multiple paths discovery and maintaining these paths. A mobile ad hoc routing network (MANET) is a network consisting of a set of mobile nodes with no centralized administration. MANET is self-configuring, self-organizing and self-maintaining. MANET may have dynamic topology. In addition, each mobile node has limited resources such as battery, processing power, and on-board memory (i.e., RAM). In MANETs, mobile nodes communicate with each other in a multi-hop fashion. That means a mobile node sends a packet to a destination through intermediate nodes. Hence, the availability of each node is equally important. Otherwise, the overall performance of the network may be affected. In order to meet these peculiar characteristics and design constraints, an efficient routing protocol is essential for MANET. Designing an efficient routing protocol for MANETs is a very challenging task and it has been an active area of research. Many routing protocols have been proposed and these protocols can be broadly classified as proactive and reactive. In proactive routing protocols like destination sequence distance vector (DSDV) mobile nodes update their routing tables by periodically exchanging routing information among themselves. A global search procedure issued by the route discovery mechanism in which a source node uses flooding mechanism to discover all the available paths to a destination. Once all paths have been discovered, a source node chooses a path, which is the shortest. When the shortest path algorithm is used, nodes located around the center of a network carry more traffic compared to other nodes that are located at the perimeter of the same network. Particularly, when multiple connections are setup in a network, the wireless links located at the center of the network carry more traffic and can, therefore, get congested. This type of congestion problem may affect the performance of a network in terms of delay and throughput. In mobility scenarios, the shortest path may break due to node movement. Moreover, communication through a wireless medium is inherently unreliable and is also subjected to link errors. Multi-path routing protocols proposed for MANET can be broadly classified as (a) delay aware multipath routing protocols, (b) reliable multipath routing protocols, (c) minimum overhead multipath routing protocols, (d) energy efficient multipath routing protocols and (e) hybrid multipath routing protocols.

IV. SOFTWARE REQUIREMENT AND SPECIFICATION

User Interfaces:
The proposed system gives the user friendly GUI, the system provides the following GUI:
1. Source node sending packet Window
2. Packet sending Window.
3. Destination window
4. Simulator Window
Hardware Interfaces:
1. Hard Disk: 80 GB
2. RAM: 512 MB
3. Processor: Intel Pentium 4 and above

Software Interfaces
1. Technology Used: Core Java, Jung
2. Tools: JDK 1.5 or above, Netbeans
3. Operating System: Windows XP or above

Assumptions and Dependencies
1. User must have basic knowledge of MANET
2. Network should be generated initially
3. At the intermediate node user must perform the aggregate function

System Features
System Features-I (Functional Requirements)
1. It is user friendly
2. It provides an easy interface to user. It performs the aggregation function

System Features-II (Non-Functional Requirements)
1. The time required for processing the application or for detecting the congestion is less
2. The time required for sending the packet is very less
3. The application must be scalable and reliable

V. MATHEMATICAL MODEL

Modeling Routing Operations:
Assumptions
Nodes of network are placed in grid.
Nodes have different Life Times.
Certain sections of grid are prone to power or any other failure.

After network initializes, there can be different variations in network parameters.

Proactive Route Discovery Overhead
Route discovery overhead bears two parts i.e. Overhead due to RREQ Propagation Overhead due to RREP generation and propagation. Either way, control overhead of route discovery process is highly dependent upon number of hops a packet has to cross for reaching desired destination.

VI. IMPLEMENTATION STATUS

A. Preprocessing Module

PSR provides every node with a breadth-first spanning tree (BFST) of the entire network rooted at itself. To do that, nodes periodically broadcast the tree structure to their best knowledge in each iteration.

- The Problem of Congestion Minimized Multipath

Program CMM (G(E, V), (t, s), (F), (Cue), (C), (R))

Minimize

\[ \alpha = \max_{e \in E} \left( \frac{(X_e + C_u e)}{C_e} \right) \] (1)

Known:

\[ \sum_{e \in E} X_e = \sum_{e \in T} F_e = \theta \]
\[ \sum_{e \in E} F_e = \sum_{e \in T} F_e \quad \forall t \neq (s, t) \]
\[ \theta < \frac{C_e}{e} \quad \forall e \in E \]

Subject To:

\[ \sum_{e \in E} X_e = \sum_{e \in T} X_e = \theta \] (2)
\[ \sum_{e \in E} F_e = \sum_{e \in T} F_e \quad \forall t \neq (s, t) \] (3)
\[ \theta \leq F_e \quad \forall e \in E \] (4)

Based on the information collected from neighbors during the most recent iteration, a node can expand and refresh its knowledge about the network topology by constructing a deeper and more recent graph. This knowledge will be distributed to its neighbors in the next round of operation. On the other hand, when a neighbor is deemed lost, a procedure is triggered to remove its relevant information from the topology repository maintained by the detecting node. Intuitively, PSR has about the same communication overhead as DV-based protocols. We go an extra mile to reduce the communication overhead incurred by PSR as routing agents. Due to its proactive nature, the update operation of PSR is iterative and distributed amongst all nodes in the network. At the beginning, node v(source node) is only aware of the existence of itself therefore, there is only a single node in its BFST, which is root node v. By exchanging the BFSTs with the neighbors, it is able to construct a BFST. In each iteration, nodes exchange their spanning trees with their neighbors. When a neighbor is seemed to be lost, its contribution to the network connectivity should be removed this process is called neighbor trimming. The neighbor trimming procedure is triggered at v about neighbor u either by the following cases: No routing update or data packet has been received from the neighbor for a given period of time. A data transmission to node u has
Distance-Vector Algorithms:

Distance-vector algorithms are often referred to as Bellman-Ford algorithms because they are based on the shortest-path computation algorithm by Bellman. Distance-vector algorithms have been used in several packet-switched networks such as Arpanet. Distance-vector algorithms perform their route computation on a per-destination basis. If a link fails, only routes for those destinations which were routed over the failed link need to be recomputed. Moreover, the computation is localized to one part of the network only the routers upstream of the failed link. Therefore, distance-vector algorithms are simpler. The primary disadvantages of DBF are re-routing loops and counting-to-infinity problem. A routing-table loop is a path special in the routers routing tables at a particular point in time, such that the path visits the same router more than once before reaching the intended destination. A router is said to be counting-to-infinity when it increments its distance to a destination until it reaches a predefined maximum distance value. Some solutions such as split horizon and poisson reverse have been proposed to overcome.

B. Congestion Detection EDIM Packet

The route discovery procedure is done by using RREQs. Once the route has been discovered the source node start sending packets along the discovered path. At the receiver side the congestion is identified by calculating the T_w path. After waiting for T_w seconds, the receiver node checks the total number of packets received during that period and calculates the packets loss count. If the packet loss count is more than ALLOWED_PACKET-LOSS, then the receiver initiates EDIM packet to the receiver as a broadcast message. The receiver node was made to measure the number of packets received. If the number of packets received is found to be less than allowed loss, it initiated an EDIM (Packet Error Announcement Message) error message towards the source. Upon receiving the EDIM error message the source node increases the packet sent interval. EDIM packet is a data packet only having the source node information with cause of nodes/link failure.

C. Algorithm of generation of EDIM packet

```cpp
void CMP::check congestion()
{
    define CONGESTIONINTR
    int pkt loss count = pkt to be recv - recv data pkt;
    double ALLOWED_PKT LOSS = pkts to be recv * 0.1;
    if(pkt loss count > ALLOWED_PKT LOSS)
        cout Network is congested;
        send EDIM packet(src id);
        EDIM pkt sent = 1;
        recv data pkt=0;
}
```

VII. COMPARISON WITH SIMILAR SYSTEMS

A global search procedure issued by the route discovery mechanism in which a source node uses flooding mechanism to investigate all the available paths to a destination. Once all paths have been discovered, a source node chooses a path, which is the very short. When the shortest path algorithm is used, nodes located around the center of a network carry more traffic related to other nodes that are located at the perimeter of the same network. Particularly, when multiple connections...
are arranged in a network, the wireless links located at the center of the network carry more traffic and get congested. This kind of congestion problem may disturb the performance of a network in terms of delay and throughput.

The ad-hoc network does not have any fixed network infrastructure which leads to frequent changes in topology. In mobility scenarios, the shortest path may get spited due to node movement. Moreover, communication through a wireless medium is inherently unreliable and is also leads to link errors. In today’s condition, many congestion control techniques have been implemented with TCP that introduce the congestion problem to the source node. The TCP congestion control mechanisms [7] are Tahoe TCP, Reno TCP, New Reno TCP and SACK TCP.

When congestion takes place, packets transferring from the source to the destination, it leads to many problems such as packet loss and long delay. This problem becomes more visible when there is large scale transmission network. There are many congestion control techniques such as EDAPR (Early congestion detection and adaptive routing in MANET) [9], where in EDAPR the node detects the congestion early and send a warning message to non congested nodes (NHN). The non-congested nodes finds then alternative path by using adaptive path mechanism.

Another approach for the congestion control is DCDR (Dynamic congestion detection and control routing in ad hoc networks) [8]. In DCDR, the congestion is detected by the average queue length of the node. When the congestion is detected the node sends the warning message to its neighboring nodes. The nodes then detect the alternative path to send the packets to its destination.

The following are the advantages of MANETs:
1. They provide access to information and services 2. Regardless of geographic position. 3. These networks can be set up at any place and time. 4. Some of the applications of MANETs are 5. Military or police exercises. 6. Disaster relief operations. 7. Mine cite operations. 8. Urgent Business meeting

VIII. PERFORMANCE MEASURES AND EFFICIENCY CALCULATION:

Testing is an investigation conducted to provide stakeholders with information about the quality of the product or service under test. Software testing also provides an objective, independent view of the software to allow the business to appreciate and understand the risks of software implementation. Test techniques include, but are not limited to, the process of executing a program or application with the intent of finding software bugs. Software testing can also be stated as the process of validating and verifying that a software program or application or product:

1) Meets the business and technical requirements that guided its design and development;
2) Works as expected; and
3) Can be implemented with the same characteristics

Software testing, depending on the testing method employed, can be implemented at any time in the development process. However, most of the test effort occurs after the requirements have been defined and the coding process has been completed. As such, the methodology of the test is governed by the software development methodology adopted. Different software development models will focus the test effort at different points in the development process. Newer development models, such as Agile, often employ test driven development and place an increased portion of the testing in the hands of the developer, before it reaches a formal team of testers. In a more traditional model, most of the test execution occurs after the requirements have been defined and the coding process has been completed.

IX. RESULT ANALYSIS:

A. Black Box Testing

Black box testing methods focus on the functional requirements in the software. That is, black box testing enables us to derive sets of input conditions that will fully exercise. All functional requirements of the program Black box testing attempts to find errors in the following categories:

- Incorrect or missing function
- Interface errors
- Errors in data structure or external job access
- Performance errors
- Initialization and termination errors.

In the proposed application with the help of this technique, we do not use the code to determine a test suite; rather, knowing the problem that were trying to solve, we come up with four types of test data:

- Easy-to-compute data
- Typical data
- Boundary / extreme data
- Bogus data

But in our application we does not provide any external data, the role of user is only to give number of nodes for formation of clusters anf for the formation of sink node.

B. White Box Testing

White box testing is a set case design method that uses the control structure of the procedural design to derive test cases. Using white box testing methods, we can derive test cases that:

- Guarantee that all independent paths within a module have been exercised at least once
- Exercise all logical decisions on their true and false sides
- Execute all loops at their boundaries and within their operational bounds
- Exercise internal data structures to ensure their validity

In the proposed application the white box testing is done by the developer implemented the code, the implemented code is studied by the coder, determines all legal (valid and invalid) NAND illegal inputs and verifies the outputs against the expected outcomes, which is also determined by studying the implementation code.

Testing types:

C. Unit Testing

Unit testing enables a programmer to detect error in coding. A unit test focuses verification of the smallest unit of software design. This testing was carried out during the coding itself. In this testing step, each module going to be work satisfactorily as the expected output from the module. **Project Aspect** The front end design consists of various forms. They were tested for data acceptance. Similarly, the back-end also tested for successful acceptance and retrieval of data. The unit testing is done on the developed code. Mainly the unit testing is done on modules.

D. Integration Testing

Through each program work individually, they should work after linking together. This is referred to as interfacing. Data may be lost across the interface; one module can have adverse effect on the other subroutines after linking may not do the desired function expected by the main routine. Integration testing is the systematic technique for constructing the program structure while at the same time conducting test to uncover errors associated with the interface. Using integrated test plan prepared in the design phase of the system development as a guide, the integration test was carried out. All the errors found in the system were corrected for the next testing step. **Project Aspect** After click key distribution in the back end the key are distributed to each node.

E. System Testing

After performing the integration testing, the next step is output testing of the proposed system. No system could be useful if it doesn’t produce the required output in a specified format. The outputs generated are displayed by the user. Here the output format is considered in to two ways. One in on screen and other in printed format. **Project aspect** The entire project was tested and found successful.

Test Plan

Test Plan Identifier: Attack Detection It is use to identify test plan uniquely.

1) Purpose of the Test Plan Document The main purpose of this document is to fit a particular project as needs. It documents and tracks the necessary information required to effectively define the approach to be used in the testing of the project as product. The Test Plan document is created during the Planning Phase of the project. Its intended audience is the project manager, project team, and testing team.

2) Objective of Test Panning To find as many defects as possible and get them fix.

3) Items to be Tested OR Not to be Testes Describe the items/features/functions to be tested that are within the scope of this test plan. Include a description of how they will be tested, when, by whom, and to what quality standards. Also include a description of those items agreed not to be tested.

4) Items to be tested
   - Overall functionality of the application
   - User Interface of the application

5) Not to be Testes
   - Performance of the application

6) Test Approach
   - Describe the overall testing approach to be used to test the project as product.
   - Provide an outline of any planned tests.
   - There are many approaches like:
     - Black Box Testing
     - White Box Testing
   - Here we used Black Box Testing approach. In Black Box Testing we just give input to the system and check its output without checking how system processes it.

7) Test Pass OR Test Fail Criteria
   - When actual and expected results are same then test will be passed. When actual and expected results are different then test will be failed.

8) Test Entry OR Exit Criteria
   - Describe the entry and exit criteria used to start testing and determine when to stop testing.
   - Exit criteria: When bug rate fall below certain level we can stop testing.
   - Exit criteria: When bug rate fall below certain level we can stop testing.

9) Test Suspension OR Resumption Criteria
   - Describe the suspension criteria that may be used to suspend all or portions of testing. Also describe the resumption criteria that may be used to resume testing.
   - Suspension criteria: if there is large change in application like change in requirements we can suspend work for some time.
   - Resumption criteria: after resolving the respective problem we can resume work.

End-to-End Delay in TCP with Density.

In order to reduce the packet losses, a congestion identification scheme is proposed at the receiver.
PSR the receiver node is made to measure the number of packets received. If the number of packets received is found to be less than allowed loss, it initiated an error message towards the source. Upon receiving the error message the source node increases the packet sent interval. The performances of PSR for different scenario have been analyzed. The average end to end delays have been studied for different scenario.

**PDR in UDP with velocity.**

From the plot of PDR, we observe that PSR has higher packet delivery ratio than other three protocols. Specifically, the PDR of PSR, OLSR and DSDV, which are proactive routing protocols is always 32 percent delivery when Vmax = 24m/s. The reliability of DSR is relatively lower, which can go below 6 percent at high speed (Vmax = 24m/s).

**Routing overhead with velocity.**

The routing overhead of all protocols with varying rates of node velocity is plotted. We observe in the plot here that as Vmax decreases, the overhead of all protocols comes down.

**X. Outcome with Success Definition**

The main goal of congestion control is to decrease the delay and buffer overflow caused by network congestion and hence enable the network to perform better. The aim of this paper, is to determine the performance measures like throughput packet delivery ratio, Average end-to-end delay, and Routing overhead of MANETs Routing-PSR, AODV, DSDV, OLSR and ZRP with varying scalability and offered load under different mobility models. The multipath routing protocols proposed for MANET is widely used depending upon the environment. The OLSR protocol is basically made for large and dense network but having drawback of high loss rate of packets due to higher routing overhead relatively compared to other proactive routing protocol such as DSDV and PSR. When the nodes are neither too sparse so that the network connectivity is good nor too dense so that the channel can be spatially reused, these protocols have a fairly high Packet Delivery Ratio (PDR).

So as per above study it can be concluded that there is PDR (Packet Delivery Ratio) for PSR is about 70 percentage. As if comparison of PSR, Packet Delivery Ratio with other protocols likes OLSR, DSR and DSDV. Packet Delivery Ratio it is relatively better because after all its having improvement over 0-10. So this scenario to get works on Packet Delivery Ratio of PSR and increases the PDR from 70 to near about 901%

**ACKNOWLEDGMENT**

This is a great pleasure immense satisfaction to express my deepest sense of gratitude thanks to everyone who has directly or indirectly helped me in completing my dissertation work successfully. I express my gratitude towards Seminar guide Prof. Varsha R. Dange and P. G. Coordinator Prof. Varsha R. Dange and Arati Dandavate, Head of Department of Computer Engineering, Dhole Patil College of Engineering, Pune who guided encouraged me in completing the dissertation work in scheduled time. I would like to thanks our Principal, for allowing us to pursue my dissertation in this institute.

**REFERENCES**


[8] Context aware routing management architecture for airborne networks Addison Betances, Kenneth Mark Hopkinson , Mark Silvius Department of Electrical and Computer Engineering, Air Force Institute of Technology, Wright-Patterson AFB, OH 45433, USA.


[10] International Journal of Application or Innovation in Engineering Management (IAIEM)Web Site: www.iaiem.org Email: editor@iaiem.org, editoriaiem@gmail.com Volume 2, Issue 9, September 2013.