# Comprehensive Study and Overview of Vehicular Ad-HOC Networks (VANETs) in Current Scenario with Respect to Realistic Vehicular Environment

Debjyoti Saha
Department of Electronics & Telecommunication Engineering
(B.Tech 3rd Year)
SVKM's Narsee Monjee Institute of Management Studies
(Deemed-to-be-University),
Mukesh Patel School of Technology Management & Engineering, Shirpur, India

Pravin Wararkar
Department of Electronics & Telecommunication Engineering
(Assistant Professor)
SVKM's Narsee Monjee Institute of Management Studies
(Deemed-to-be-University),
Mukesh Patel School of Technology Management & Engineering, Shirpur, India

Shashikant Patil
Department of Electronics & Telecommunication Engineering
(Associate Professor)
SVKM's Narsee Monjee Institute of Management Studies
(Deemed-to-be-University),
Mukesh Patel School of Technology Management & Engineering, Shirpur, India

## ABSTRACT
Ad- Hoc networks are random networks which are user friendly to any nodes. Vehicular Ad-hoc network is a type of Ad-hoc network composing of vehicle associated with wireless communication. Wireless ad-hoc network consists of base transmission station, background server, and other processing software. Based on these things, this paper introduces about the VANETs, MANETs and newly FANETs. Firstly, this paper consist of Introduction to Ad-hoc networks, VANETs and its protocol, FANETs and MANETs and protocol. Apart from this the Network simulations are also includes ns-3. Evaluates about the routing protocols used in VANETs and network simulators such as ns-2 and ns-3. At last, it gives the information about the efficiency in the Quality of Service section.

## Keywords
VANETs, MANETs, Routing Protocols, Network Simulators and QoS.

## 1. INTRODUCTION
Ad-HOC network is a network which is created by individual devices for communicating between devices directly or temporarily. The mechanism of creating an ad-HOC network is not familiar to end-to-end users who are generally familiar to business networks, etc. In these business networks, the use of typical routers and wireless signals are used to transmit the data, but these routers has no relation to ad-HOC networking services.

There are several applications of ad-hoc networks as it is a key factor for evolution of wireless communication. Ad-Hoc networks of laptops are used in accident relief, wars and also in some conferences. Wireless Ad-HOC networks generally works on the principle of Mobile ad-hoc networks, it is a decentralized type of network. We call the network as ad-hoc because it does not rely on pre-existing structure that was formed by previous networks, it always forms new network for new communications. A perfect example of device that use pre-existing network is routers, to access the internet in public place these are used. Ad-hoc wireless networks are very much useful for transmission of data, files, etc. but this network does not have access to Wi-Fi network. It can also share one computer internet connection to another easily.

Well, there are also problems related to ad-hoc networks, such as bandwidth problems, control of power and data quality during transmission. To solve these problems multiple standardization efforts are being made. If in any case the main infrastructure of wireless communication is not present then to fix this problem the network itself becomes wireless hosts. These networks consists of several nodes that can communicate with the help of wireless links.

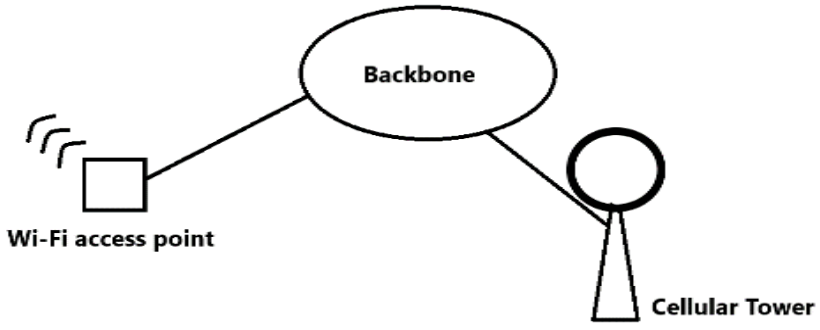


**Fig 1: Ad-HOC Network**

Vehicles on highway can operate their private ad-hoc network to solve the traffic problems between them. The vehicles can operate a pure ad-hoc network in which every single vehicle can face the traffic events. Similarly the access points situated near the roads can exchange information.

Wireless peer-to-peer networks is also known as ad-hoc mode of networks. In this P2P network two or more networks are can use valuable information's spontaneously without any central coordination. A simple definition of this network is, when two or more PC's are connected with some kind of wireless adapter they can build an independent network and whenever these connected PC's are in range they can share information easily.

## 2. MOBILE AD-HOC NETWORK

A mobile ad-hoc network is defined as network which is having many autonomous nodes often consisting of mobile devices. MANET can arrange themselves in various ways. The main principle of these ad-hoc networks are nothing but to correct the data and create an efficient route between the pair of nodes which are generally mobile devices, so that messages may be delivered in proper time. The MANET can be easily deployable and also it can self-configure if a problem occurs. For MANET to run properly there should be no extinction wireless links and nodes. Nodes must be able to detect traffic, because sometimes communicating nodes are out of range. A MANET is generally a standalone network or it can be connected to internet.

MANETs are used as an applications in military, sensor networks, rescue operations, free internet connection and sharing, conferences, etc. The main two characteristics are multi-hop and mobility. Multi-hop is a mechanism which is performed through MANET operation, this multi-hop requires a routing mechanism which is designed by mobile nodes. This operation is required to detect and act on, merging of two or more networks.

Dynamically establishing wireless networks and maintaining routes through forwarding packets for each of the users facilitate multi-hop communication.

MANET has following eight features:

### 2.1 Autonomous Terminal:

In MANET each mobile terminal is an autonomous node, whose purpose is to function as host and router. It can perform as a switching functions.

### 2.2 Disturbed Operation:

In disturbed networks, generally there are no background networks to control the network operations so the management of networks generally gets disturbed.

### 2.3 Multi-hop Routing:

Based on different links of protocols and attributes, the ad-hoc algorithms can be of two types' single-hop and multi-hop. MANET is simpler than multi-hop in terms of implementation.

### 2.4 Dynamic Network Topology:

The nodes in the network dynamically forms connectivity as they move about, forming their own network.

### 2.5 Fluctuating Link Capacity:

The channel from which the terminals communicate is familiar to noise, fading and interference and also it has less bandwidth.

### 2.6 Light Weight Terminals:

The MANET nodes are mobile devices which are less in CPU processing, has small memory size, and also low power storage.

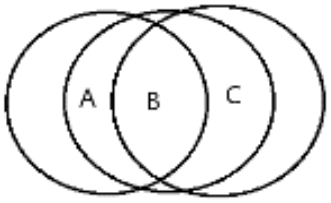


**Fig 2: A Mobile Ad-HOC Network and its 3 Nodes**

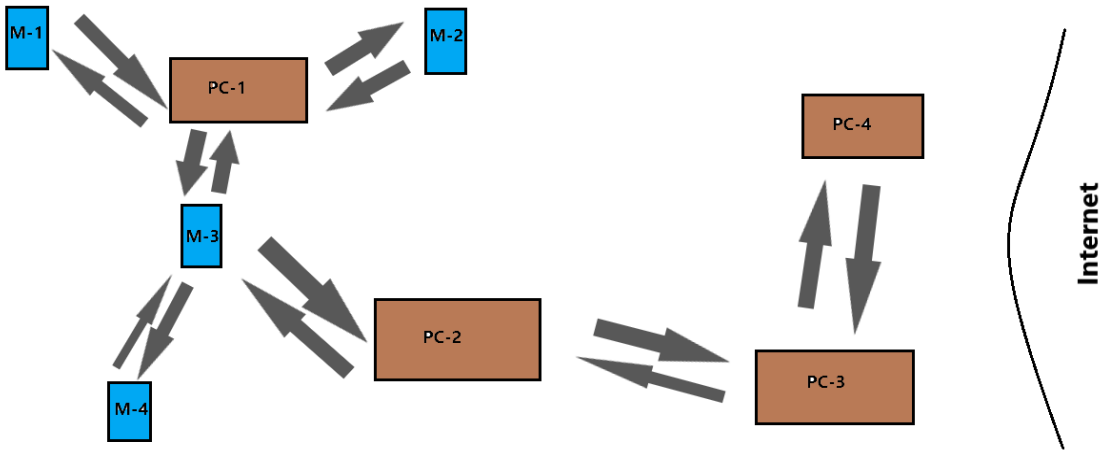


**Fig 3: Demonstration of MANET**

## 3. VEHICULAR AD-HOC NETWORK

Vehicular Ad-HOC networks are formed by applying the principles of mobile ad-HOC network. VANETs are the applications of MANETs. VANETs support vast range of applications from simple single hop information. VANETs can use any wireless network for their basis, the most used technology is short range radios. VANETs are generally responsible for the communication between two moving vehicles on the road to control the accident rates, traffics.

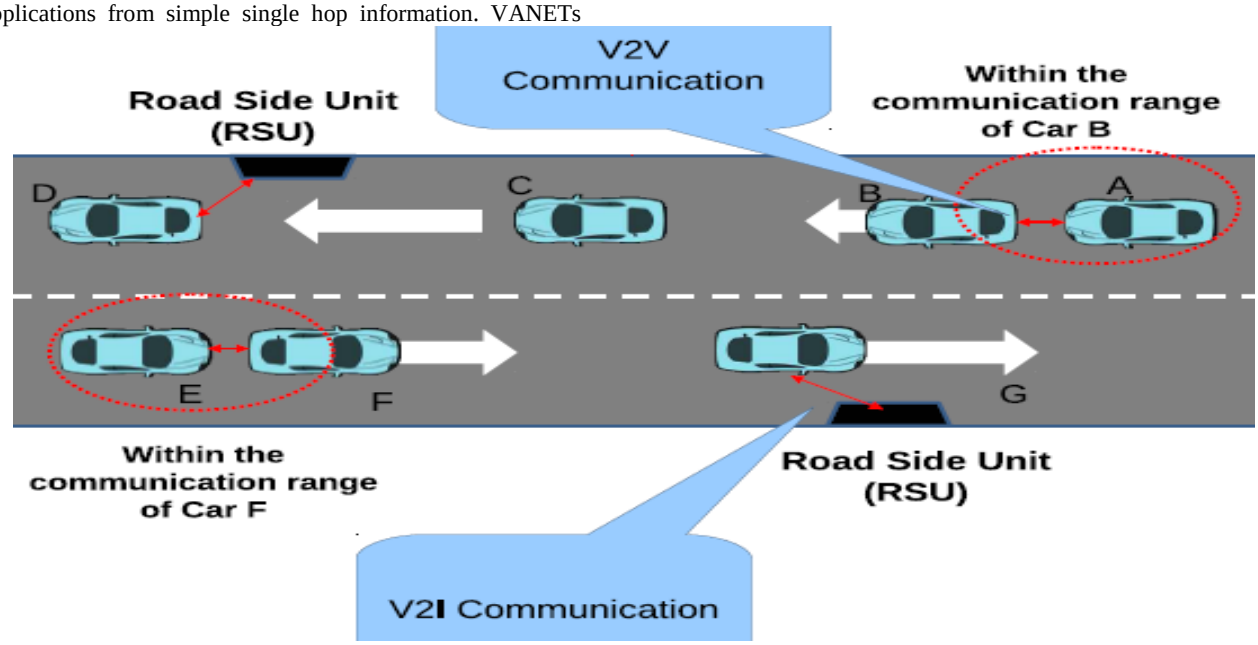


**Fig 4: Creating an Ad-HOC Network (VANET)**

Vehicular networks can communicate with vehicle to infrastructure (V2I) and also vehicle to vehicle (V2V). As we know vehicles move randomly as compare to the nodes for MANETs, that's why VANET is slightly different from

MANET. VANET routing protocol is known as Ad-HOC on Demand Vector (AODV). There are several possibilities form communication in VANETs, the first one is communicating with the help of WLAN. The second possibility is the region were the vehicles communicate directly without any help of RSU.

VANET has many key characteristics of vehicular activity like acceleration, deceleration, changing lanes and human driving pattern. Routing in VANET is slightly different from MANET because of its capability of highly dynamic and changing topologies. These routing protocol can be classified into five major categories namely:

Ad-HOC, Location based, Cluster Based, Broadcast and Geocast.

To prevent VANET from hacking, Network on Wheels (NOW) and other secure vehicular communication are running for addressing such security issues.

Best security to these VANETs programs to build an authentication mechanism in each node. The hierarchy of VANET can be classified as:

- Position based routing protocol.
- Topology based routing protocol.
- Broadcast based.
- Cluster based.
- Geocast based.

### 3.1 DSDV Routing Protocol:

It refers to Destination Sequence Distance Vector. It is a proactive protocol in which every node maintains a table of information.

### 3.2 AODV Routing Protocol:

It refers Ad-hoc on Demand Distance Vector. It is a reactive routing protocol which establishes a route to destination when there is a demand occurs for transmission of the data.

### 3.3 DSR Routing Protocol:

It refers to Dynamic Source Routing. It helps to maintain the source routing in which every neighbor in DSR maintains the entire network.

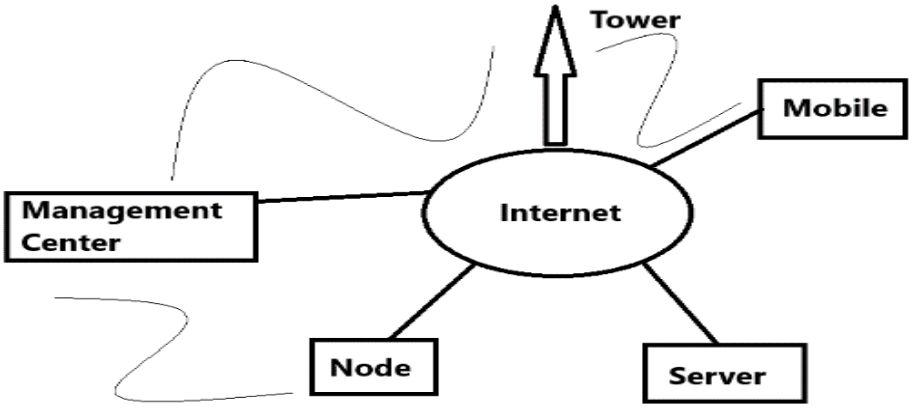


**Fig 5: VANET Domain**

## 4. FLYING AD-HOC NETWORKS

Flying ad-hoc network is a group Unmanned Air Vehicles (UAVs) communicating with each other without any need of access points. The necessary part is that at least one of the UAV must be connected to base stations or satellite. UAVs work without pilot/autopilot, this is the reason it is cheaper and the devices required for connectivity are small. Nowadays FANETs are used in military and civil applications, managing wildfire and disaster.

Two factors affect this FANET protocol. The first one is mobility model and second one is traffic pattern by the human beings while driving. FANETs is also known as the special case of mobile ad-hoc networks, it consists of two parts- ad-hoc network and receivers point like base stations or satellite. UAVs have many disadvantages, using multi-UAVs may solve this:

- Minimize the completion time of the request.
- Minimize the cost and maintenance.
- Increase scalability.
- Increase sustainability.

The FANET characteristics are the following:

### 4.1 Node Mobility

The UAVs has the speed of around 30-460 km/h, and this speed causes communication problems.

### 4.2 Mobility Models

In mobility models, the flight plan is predetermined at each step there is a change.

### 4.3 Node Density

The average number of UAVs is called Node Density.

### 4.4 Network Topology

In order to higher mobility, degree, topology changes frequently.

### 4.5 Radio Propagation Model

The UAVs uses line of sight between them and ground base.

## 5. POSITION BASED ROUTING PROTOCOL

Position based routing protocol is used for position information to identify the accurate location of the nodes as well as the corresponding nodes too. By focusing on this location technique, the performance is better than topology based routing protocol. One advantage of this type of routing protocol is that it runs on local information to forward the data rather than keeping it to wide spread area information. Position routing of every node is located by using location services and forwarding techniques.

There are several position based protocol as mentioned:

- DREAM(Distance Routing Effect Algorithm Mobility)
- LAR(Location Aided Routing)
- GLS(Grid Location Services)
- GPSR(Greedy Perimeter Stateless Routing)

The performance of position protocols is based on their designed parameters such as Loop free, Distributed operation, Path strategy, Packet forwarding, Overhead, Adaptive to mobility, etc.

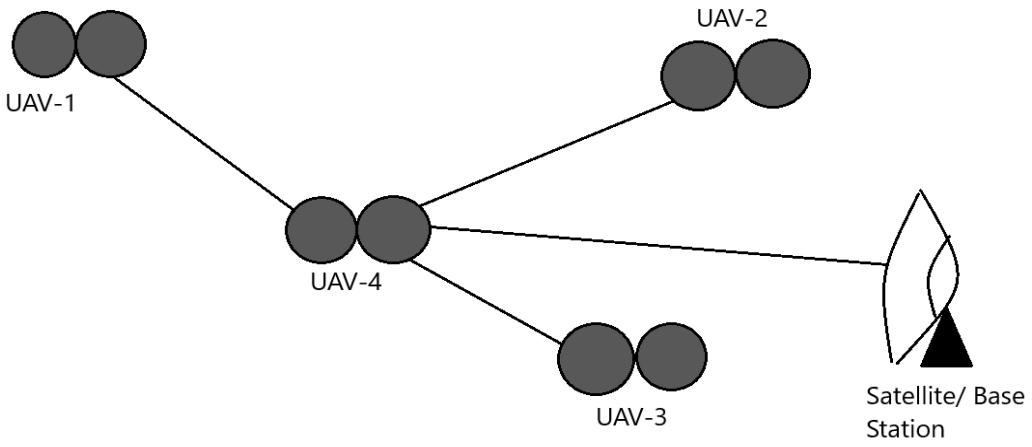


**Fig 6: Demonstration of FANET**

## 5.1 Location Aided Routing Protocol:

This protocol uses location information provided by the mobile nodes by using services related to location that are GPS and many more just to reduce the traffic of discovery overhead. Mainly two regions are defined to reduce overhead problem, they are Request zone and Expected zone.

Request zone is defined as the area in the present node forwards the requests of route. This operation is performed only when the receiving node is already inside the zone, if the node is not available in the request zone then it discards the message of that node and proceeds to next. Whereas, in expected zone there is maximum probability of determining the destination node which is generally a mobile. We can calculate the possible position by taking assumption of its average velocity multiplied by the time difference.

## 5.2 Distance Routing Effect Algorithm Mobility:

DREAM works on the information gathered on location, and is determined by GPS system for communications. The combination of proactive and reactive protocol were the source node sends the data to the destination. DREAM algorithm is a proactive protocol which promotes limited flooding of location. DREAM uses directional flooding which increases the probability of optimal route, also it decreases its capacity of taking maximum networks with vast number of data's.

## 5.3 Grid Location Services Routing:

It uses location services for geographic locations. The working of GLS is that it breaks up the network area into some hierarchical structure around the system. This method of forming a structure makes the full use of information and it can be unique or permanent.

## 5.4 Greedy Perimeter Stateless Routing:

The location of the nodes are forwarded to the packets which are situated in some distance. The node which present nearer to the destination point is termed as a greedy point or approach. This routing protocol uses two different methods: greedy forwarding and perimeter forwarding.

**Table 1: Strategies of Position Based Routing Protocol**

| Protocol | Path Strategy | Path Selection | Scalability |
|---|---|---|---|
| LAR | Multipath | Hop count | Medium |
| ALARM | Multipath | Link duration | High |
| DREAM | Multipath | Hop count | Medium |
| GLS | Single Path | Hop count | Medium |
| GPSR | Single Path | Hop count | Medium |

# 6. CLUSTER BASED ROUTING PROTOCOL

Cluster based routing protocol is a routing protocol which is designed for mobile ad-hoc network. This protocol divides the ad-hoc nodes into number of overlapping and disjoint cluster in a distributed manner. The division of nodes leads to cluster and each cluster has a cluster head which maintains the cluster information about the membership. The cluster membership is valuable when there is requirement of inter-cluster nodes.

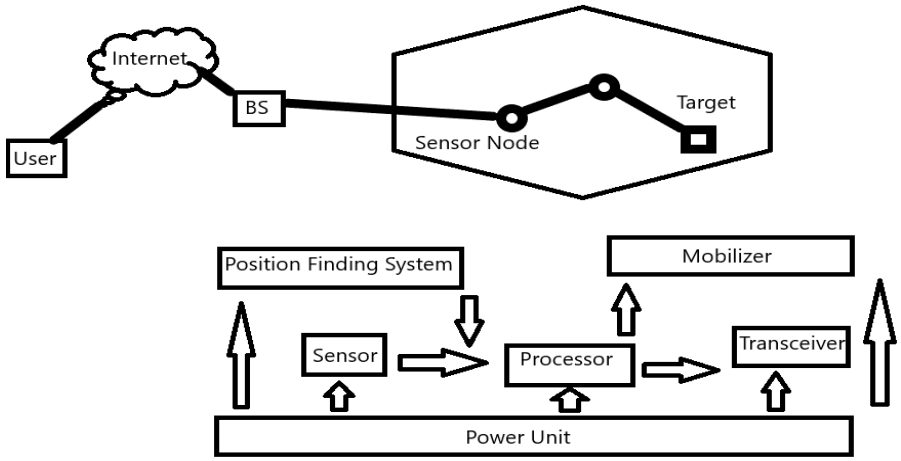


**Fig 7: Sensor Node Architecture**

By the method of clustering the nodes into group the CBRP minimize the traffic and also makes it time efficient. CBRP has following features:

- Fully distributed operation.
- Less flooding traffic during the dynamic route discovery process.
- Explicit exploitation of unidirectional links.

There are several challenges which are essential for designing routing protocols.

## 6.1 Node Deployment

The very application dependent and which affects the performance of routing protocols. Firstly, the nodes are placed manually and the informative data is passed through those nodes. To pass the data frequently the coverage of the area should be satisfied first. The node deployment is a good choice when the nodes are costly for the operation, but has a drawback that it is not good for harsh or bad weather/environment.

## 6.2 Energy Consumption

The first and major perspective of the routing protocols is to transfer data through the sensors and destined it in secure manner. The sensor node is a energy consuming device which often consumes in sensing, processing, receiving and transmitting information. Due to these factors they have limited energy resources. Best choice is to design such routing protocol which less in energy consumption and also accurate in giving results.

## 6.3 Coverage

In wireless network, every node represents a view of the environment. A given image of environment from the node is limited in both range and accuracy.

## 6.4 Scalability

The nodes deployed in the environment may not be constant. It may be of 100's or 1000's. The routing protocol's main principle is that it should be able to work with large number of nodes.

## 6.5 Quality of Service

The QoS parameters can be bandwidth, delay, throughput and jitter. For a moment target examine and tracking requires less transmission delay for sensitive data.

# 7. TOPOLOGY BASED ROUTING PROTOCOL

Topology protocols are the protocols which depends on the information about current links and is used to perform packet forwarding. The topology based routing protocols are classified into proactive, reactive and hybrid protocols.

## 7.1 Proactive Routing Protocol

These are also known as table-driven protocols. Proactive routing protocols are similar to connectionless tasks of data networks. These routing protocols is further consists of DSDV and OLSR, and if any changes occur in these protocols it gets updated throughout the network. Proactive protocols maintain the information of available paths even if the path is not in used.

The main disadvantage of proactive routing is the maintenance of the unused paths. However the proactive protocols may not always be a best choice for highly mobile network in MANETs.

## 7.2 Reactive Routing Protocol

Reactive protocols employs a slow approach towards the nodes only to discover routes. This protocols only maintain those routes which are in use at any time. The requirement of bandwidth is lesser as compare to proactive protocols, but when it comes determination of the routes it delays for large amount of time. As it only maintains the routes which are in use, therefore it requires to perform discovery process before the exchanging of packets. The next disadvantage of reactive protocols is that, though it is maintaining the routes which are in use still it may generate a network when the topology changes.

## 7.3 Hybrid Routing Protocol

Hybrid routing protocols adds up both proactive and reactive protocols to obtain higher efficiency and capacity. Though it is a combination of two, then also it requires maintenance in every mode of protocols. MANETs is different from other networks by its dynamic topology. Because of poor convergence and low communication, topology based routing

protocol suffers a lot of loss in vehicular nodes. Position based routing protocols has been the best choice to overcome the disadvantages of topological changes.

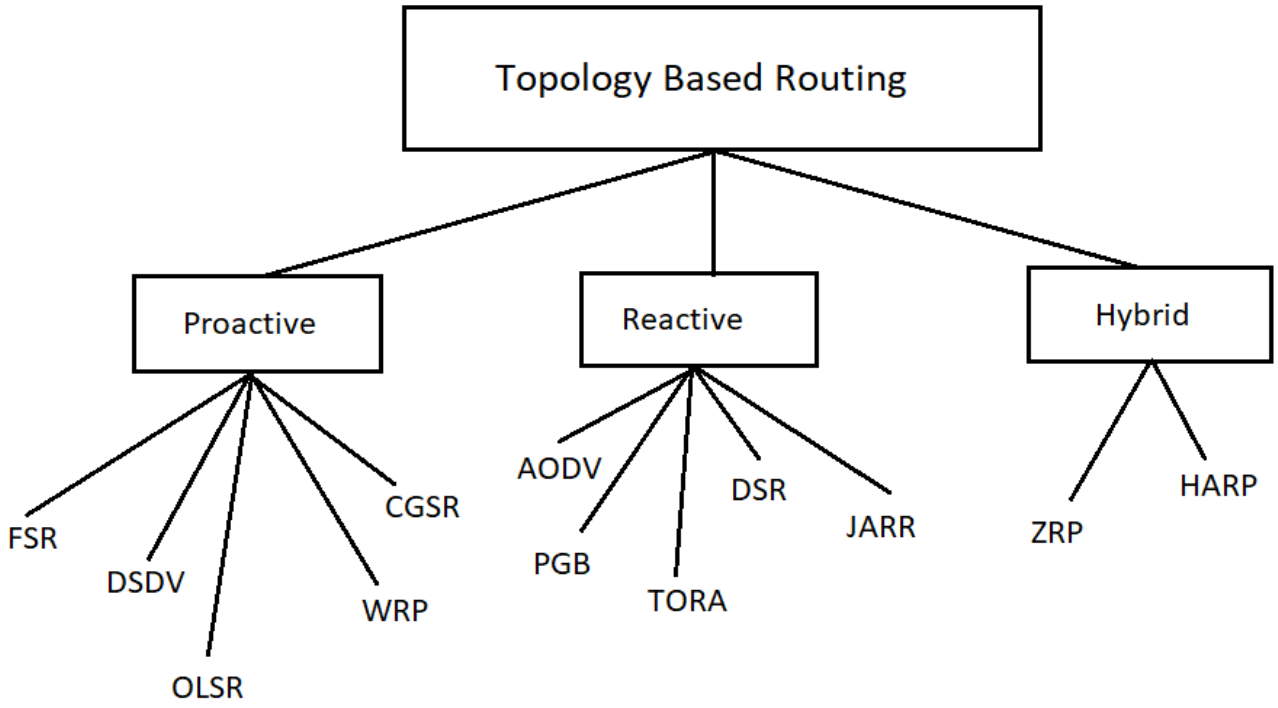


**Fig 8: Types of Topology Based Routing Protocol**

## 7.4 Dynamic Source Routing (DSR)

DSR allows the network to be self-organizing without any need of any administration. The DSR protocol has two main mechanisms, "Route Discovery" and "Route Maintenance". These two mechanisms discover and maintains the route of ad-hoc networks. A basic advantage of DSR is that it has ability to store multiple route in their route cache. DSR helps to maintain the source route protocol where every sub-route maintains the whole network.

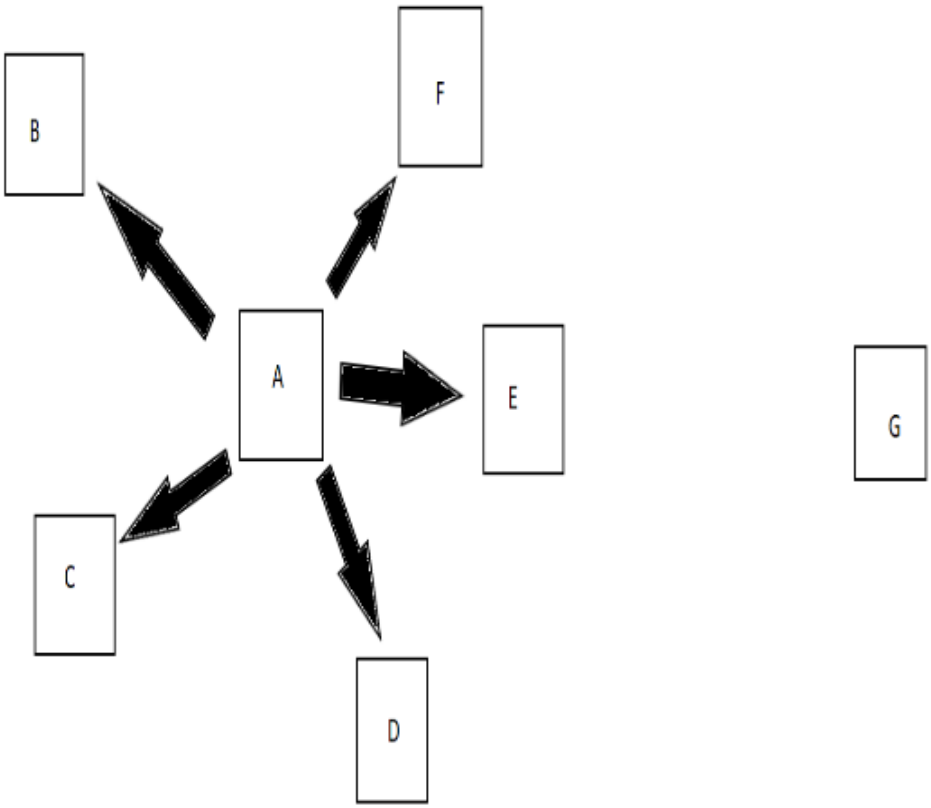


**Fig 9: Dynamic Source Protocol**

Basically a dynamic source routing is reactive routing protocol, which identifies the communication path only when it needs to communicate. For example when a source node (S) wants to send a packet to some node D, but it does not know the path of node D, then node source node S discover the route to transfer the information. For this route request (RREQ) is used to find the route discovery. Now source node S appends an identifier and forwards the RREQ which later on finds node D.

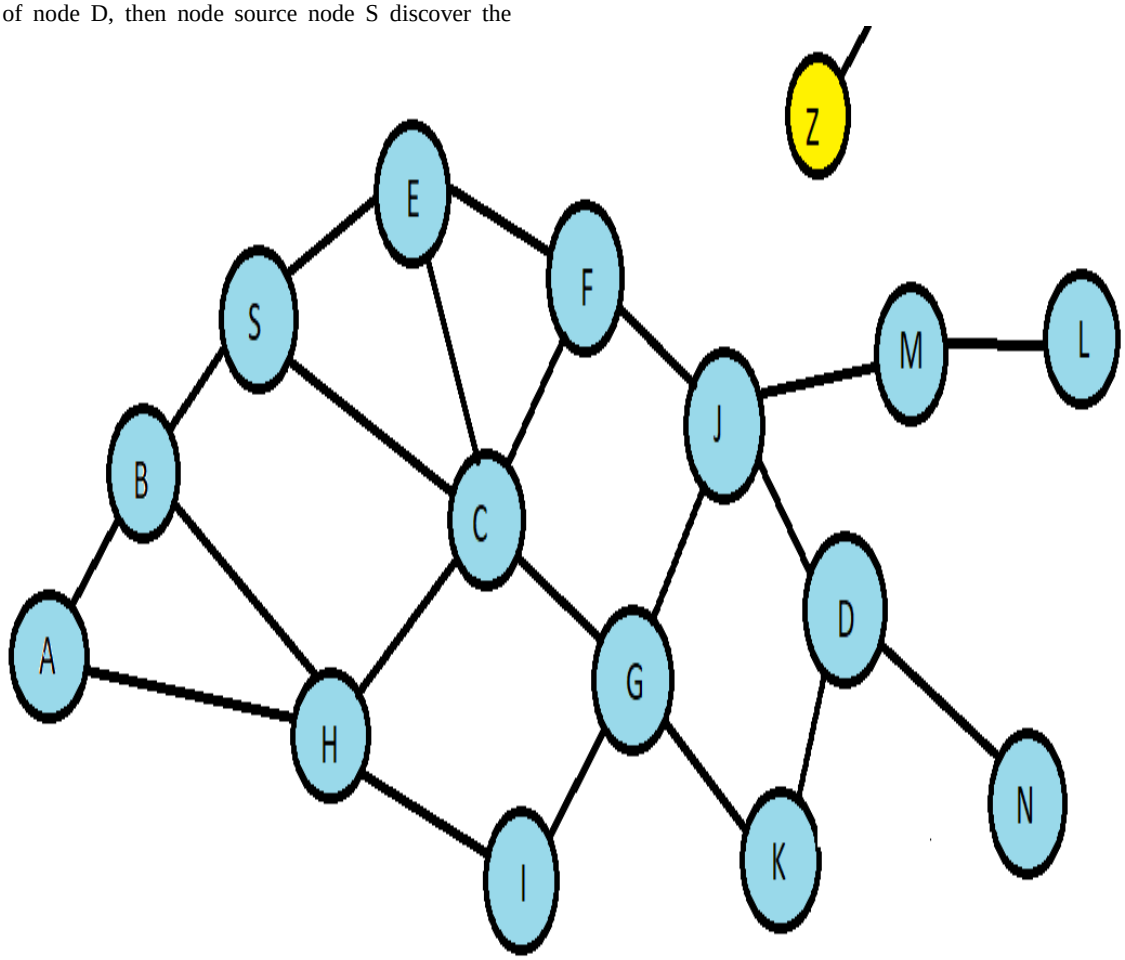


**Fig 10: Packet Transmission**

In the above diagram we can see the S node which sends the message to further nodes B, C, E. While transmission of data from node B & C to node H, the collision rate increases as it is receiving the data from nodes. It becomes a disadvantage for DSR. Now as node C has already received RREQ packet it will not transmit further even if it receives from other nodes. Here node H & node G are transmitting the information to node C.

Nodes [S, E, F, J] denotes a sequence which says the process of RREQ packet being received. In the diagram node J and node K both will broadcast the RREQ to node D which is the destination node. As node J and K are hidden from each other, their transmission of data may collide while reaching node D.

Node D knows that it is a destination node and will not transmit the data to any other node and similarly like RREQ which was generated by node S, node D generates RREP packet and transmit it to node S. The process of sending the RREP is obtained by reversing the route appended by received

RREQ. When the node S receives the RREP from node D, it stores the reply into the cache memory of node S. The storage of RREP in the cache helps the node S to remember the path if in any case node S wants to send data packet to node D then it stores to packet header. This mechanism of data packet transmission from source node to destination node and vice-versa is known as source routing.

## 7.5 Destination Sequence Distance Vector (DSDV)

It is also known as hop-hop routing protocol. The nodes present in this protocol stores one hop and these hops are responsible for reaching the destination node. DSDV deals with loop-free routing which is the only advantage which is above the traditional routing protocol. DSDV consist of two packets for sending a protocol, they are Incremental and Full Dump. In full dump type the packets are send with the information of routing, whereas in incremental the updates of that particular packets are send. DSDV protocol is not a best choice for long networks as it is utilizing more bandwidth and updates of hops.

It is an extension of Distance vector routing protocol, as it has drawbacks of not knowing about other nodes DSDV is initiated. DSDV updates the table of each node in reaching the routing, the node only updates the table if and only if the sequence number is higher than the previous one. The DSDV routing table entry is as follows: <destination, next hop, distance, sequence number>.

It is proactive routing protocol, which refers of maintaining information of all the known destinations. Those routing information are periodically updated.

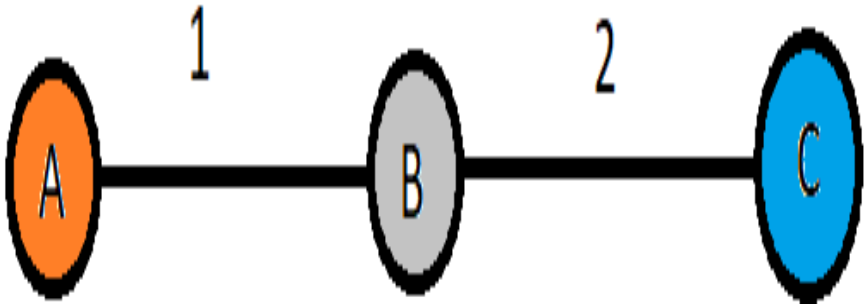


**Fig 11: Node Transmission Display (1)**

**Table 2: Routing Table 1**

| Dest. | Next | Metric | Seq. |
|---|---|---|---|
| A | A | 1 | A550 |
| B | B | 0 | B100 |
| C | C | 2 | C588 |

In the route table we have 3 nodes namely A, B, C, the metric from A-B is 1 and the metric of B-C is 2. Every node when broadcasts their table they change their sequence number and every node has their own route table which denotes the receiving time of that node. In the diagram we can see the table of 3 nodes and sequence update.

By comparing with the route table we conclude that selection of better metric is necessary when the sequence numbers are equal and the selection of destination sequence number should be higher, this ensures the use of newest information from destination.

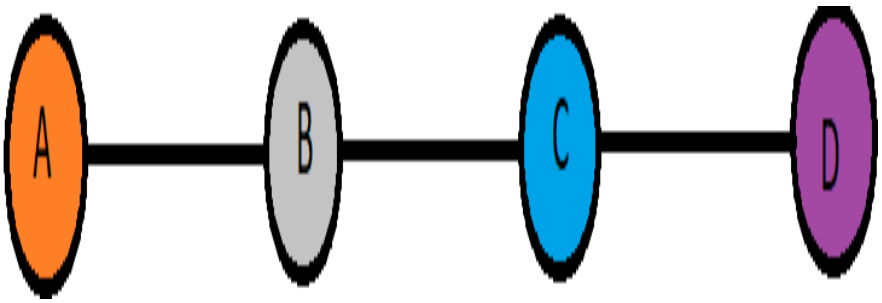


**Fig 12: Node Transmission Display (2)**

Now by inserting a new node D whose sequence number is D-000, which means it has no idea of any other node. As node C precedes the new node D, the route table of node C will insert the values of node D. Here the sequence number of node C is C-590 which becomes C-592 and forwards it to node D and node B. The node B broadcasts the information but it has no effect on node C as it has higher sequence number, while node C detects the broken link and increases the number by 1.

**Table 3: Routing Table 2**

| Dest. | Next | Metric | Seq. |
|---|---|---|---|
| **A** | **B** | **1** | **A550** |
| **B** | **B** | **2** | **B100** |
| **C** | **C** | **0** | **C588** |

**Table 4: Routing Table 3**

| Dest. | Next | Metric | Seq. |
|---|---|---|---|
| **A** | **A** | **1** | **A550** |
| **B** | **B** | **0** | **B102** |
| **C** | **C** | **1** | **C592** |
| **D** | **C** | **2** | **D000** |

In the figure we have four nodes A, C, D, E and A wants to send data to E. So in this mechanism A will start discover packet which maintains sequence number and broadcast id. A will send RREQ packet to all the neighboring nodes, suppose it broadcast a packet <A, 1, 1, E, 0>. As we know that the information transmitted by A was for E but it will reach node C first as it is neighbor node. Now node C has no information for node E, so it will broadcast the packet sent by node A.

Before broadcasting the packet sent by node A, it will change the hop count. Hop count is the distance between the current node and the sender node. The updated packet by C would be <A, A, 1, 1>, node C stores the entry for the reverse path source. The next node D also broadcast the packet sent by previous node C, by updating the details of the packet it further sends to node E.

**Table 4: Routing Table 3**

| Dest. | Next | Metric | Seq. |
|---|---|---|---|
| A | A | 0 | A550 |
| B | B | 1 | B100 |
| C | B | 3 | C558 |
| **Dest.** | **Next** | **Metric** | **Seq.** |
| A | A | 0 | A550 |
| B | B | 1 | B104 |
| C | B | 2 | C590 |
| D | | | |

hen the RREQ packet reaches the destination node it generates RREP packet and as the neighboring nodes keeps track of the reversing path in their route table, it becomes easier for RREP to complete the path.

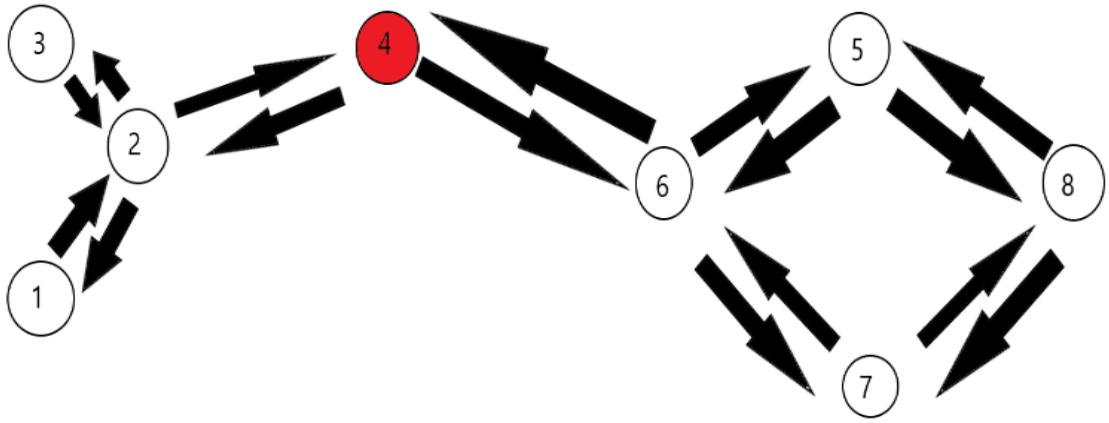


**Fig 13: DSDV**

## 7.6 Ad-hoc On Demand Distance Vector (AODV)

AODV is based on distance vector routing algorithm. It works when it requests for the route as it is an application of reactive routing protocol. There are two main features of AODV protocol, loop-free routing and immediate notification. The immediate notification alerts the route that link breakage is present and the node is affected. The AODV algorithm has various messages for discover links, they are Route Request (RREQ), Route Reply (RREP) and the last one is Route Error (RERR). To establish a communication connection it discovers path. After that the source node telecasts RREQ packet with its broadcast ID to the destination. In the receiving node, a backward pointer source generates a RREP packet if the location is the destination.

In the figure we have four nodes A, C, D, E and A wants to send data to E. So in this mechanism A will start discover packet which maintains sequence number and broadcast id. A will send RREQ packet to all the neighboring nodes, suppose it broadcast a packet <A, 1, 1, E, 0>. As we know that the information transmitted by A was for E but it will reach node C first as it is neighbor node. Now node C has no information for node E, so it will broadcast the packet sent by node A.

Before broadcasting the packet sent by node A, it will change the hop count. Hop count is the distance between the current node and the sender node. The updated packet by C would be <A, A, 1, 1>, node C stores the entry for the reverse path

source. The next node D also broadcast the packet sent by previous node C, by updating the details of the packet it further sends to node E.

When the RREQ packet reaches the destination node it generates RREP packet and as the neighboring nodes keeps track of the reversing path in their route table, it becomes easier for RREP to complete the path.

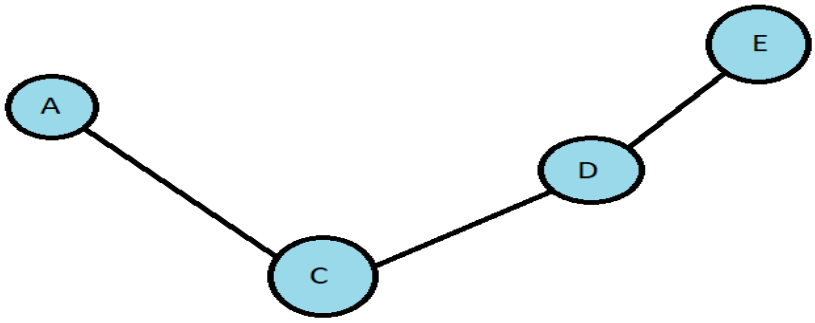


**Fig 14: AODV**

## 7.7 Ad-hoc On Multipath Distance Vector (AOMDV)

AOMDV is multipath extension of AODV protocol. In this protocol multiple routes are found between source and destination, if one route fails to communicate it uses alternate route to make connection. AOMDV promotes multipath routing which is the next version of single-path routing and has capability of handling loads and also it avoids the possibility of overlapping or mixing of networks.

Whenever a node wants to send data to another node it starts searching for route discovery and this phase is initiated by broadcasting route request (RREQ). In AOMDV routing protocol, it allows the node to receive multiple route request packet and also allows them to set reverse path. So there may be possibility of one node having multiple route request path for another node.

In the figure node D is receiving two route request path, so node D is having at least two options two send its data to node S, either it will take the path [D, A, S] or [D, B, S]. When a node is maintaining multiple paths for destination it may be possible that the paths might be having two different hop-count, because of this which hop count is being shared with which node is not predicted.

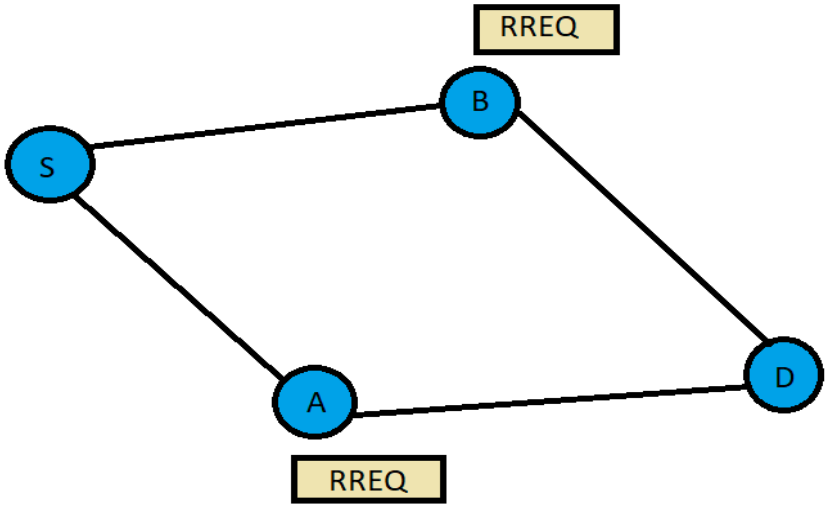


**Fig 15: AOMDV**

Now if the node D wants to transmit the data to node S, it will have possibility of multiple hop count path. In AOMDV the path having maximum hop count is always occupied for transmission of data. So here node D is having two paths [D, B, S] and [D, C, A, S], the information is transferred by the path [D, C, A, S].

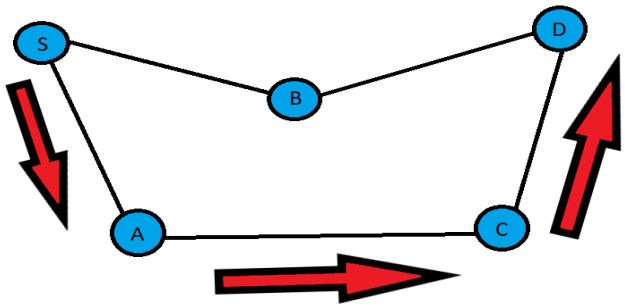


**Fig 16: Node D Transmission**

## 7.8 Zone Routing Protocol (ZRP)

This protocol has defined the routing of zones in which the definition of range in hops in each node is required. The routes of nodes which are in the routing zone is available immediately and which lie outside the zone is determined by on-demand routing protocol for the required destination. This protocol can reduce the communication overhead as compared to proactive protocols. The only disadvantage of this protocol is for large values of routing protocols, instead of behaving like proactive it behaves like reactive protocol.

## 7.9 Optimize Link State Routing Protocol

This protocol is proactive routing where runs are available whenever needed. It is possible to reduce the overhead in the existing network for which MPR is used. This routing protocol uses two control messages: hello and topological control. The hello messages are used to determine the information about the status. Topological control messages are used to broadcast the information of its own.

## 7.10 Location- aided Routing Protocol

This protocol is based on the using of location information by use of location services like GPS. To reduce the route discovery process two regions are defined: Request Zone and Expected Zone. Request zone is the area in which the node forwards the request only when it is inside the zone. The expected zone is the area in which there is maximum chances of finding the destination node.

## 7.11 Adaptive Location- aided Mobile ad-hoc Network Routing Protocol

It is hybrid, adaptive to protocol which uses LAR. It uses link for duration of feedback at each node so that it can determine appropriate forwarding method. It also adapts the operation of current network mobility which increases packet overhead.

# 8. NETWORK SIMULATOR

Traffic simulator is a process used in telecommunication engineering to measure the efficiency of communication network. Telecommunication components are complex with real world system with contains very different components which interact. The analyses of such system can be extremely difficult, modelling technique tends to analyses each components rather than relationships between the components. Simulation is approach which could be used to model large, complex system or for the performance of the measurement purposes.

The selection of simulation as a modelling tool is usually because it is less restrictive, other modelling techniques imposed mathematical restriction on the process and also requires multiple intrinsic assumptions to be made. Network traffic simulation usually follows following 4 steps:

- Modelling the system as dynamic stochastic.
- Generation of realization of stochastic process.
- Measurement of simulation in data.
- Analyses of output data.

There are generally two kinds of simulation communication networks, they are discrete and continuous simulation. Discrete simulation are also known as discrete event simulation and are web based stochastic system. In simple words we can say that system contain number of states and is modelled using set of variables. If the value of variable changes it's called an event and is reflected in the change in the system state.

As the system is dynamic it is constantly changing and also as it is stochastic the element of randomness in the system. Representation of discrete simulations is performed using states equations that contain all the variables influencing the system. Continuous simulation also contains state variables, these however changes continuously with time. Continuous simulation are usually modelled using differential equations to attract the state of the system with reference to time.

## 8.1 Advantages of Simulation

- Normal analytical technique make use of extensive mathematical modelling which requires assumptions and restrictions to be placed on the model, this can result in avoidable in accuracy in the output data.
- Analyst can study the relationship between components in details and can simulate the projecting of multiple design options.
- It is possible to easily compare alternative design, so as to select the optimum system.

## 8.2 Disadvantages of Simulation

### Disadvantage of simulation:

- Accurate simulation model development requires extensive resources.
- The simulation results the only as good as model.
- Optimization can only be performed involving few alternate as the model usually developed using limited number of variables.

# 9. SIMULATION OF URBAN MOBILITY (SUMO)

SUMO is source open traffic simulation packet which includes net import and demand modelling.

SUMO is used to investigate research topics such as route choice and traffic light. As SUMO is open source, there are two reasons that makes it open source. Firstly, the support of traffic simulation community with some free tool which can be implemented. Secondly, there are some open source traffic simulators are available.

SUMO is not only a traffic simulator, but also it is a suite of applications which helps in simulation of traffics. SUMO requires the description of road networks and traffic to simulate, both have to generate by using different sources.

SUMO is completely microscopic simulator. The vehicles are defined by identifier or by any name, the departure time and route by vehicle. The definition of vehicles can be generated by different sources. Origin/destination matrices describes the movement of traffic in vehicle number per time.

# 10. VANETMOBISIM

VanetMobisim is extension of CANUMOBISIM. CANUMOBISIM reduces the levels of details in some particular scenarios. VanetMobisim consists of all features of CanuMobisim furthermore it also has its own set of possibilities in vehicular mobility. Therefore, VanetMobisim provides higher degree of realism.

VanetMobisim provides both macro-mobility and micro-mobility for the representation of definition of mobility modelling. Macro-mobility concerns about the road topology, structure in unidirectional and bi-directional, also some road characteristics like speed limits, stop signs, traffic, lights, etc. VanetMobisim introduces maps from TIGER database that usually supports for multiple lane roads, directional flows, and speed constraints.

Micro-mobility modelling is often related to all principles of individual vehicles such as speed changing, acceleration and deceleration. This helps to communicate between the vehicles known as vehicle-to-vehicle and also with the infrastructure known as vehicle-to-infrastructure.

## 10.1 Characteristics of VanetMobisim

- Open source mobility model generator.
- Most importantly used for VANETS.

Platform independent software.

- Introduce both the mobility modelling techniques.
- It can be validated.

# 11. NETWORK SIMULATOR-3

Ns-3 is discrete network simulator for systems, targeted for educational purposes and research. Ns-3 is a free software under the GNU GPLv2license. It is an open source version, if the user want to re-design some protocol, implement them or test them can be work out on ns-3. Before working on ns-3, the user should be aware of Linux basics, basics of programming, networking basics.

There are some tools of war which the user should have to run ns-3. If you are window user or MAC user you should not download the software directly in the system as it may damage the important data's already present in it. Further it may corrupt out the windows or MAC. The tools of war are Vmware, Virtual box and for MAC user Fusion.

After the completion of vmware download, create a virtual machine. Name a new ID and password to proceed the installation process of Ubuntu. Specify the disk size which is recommended as 20 GB, but its maximum limit is up to 2 GB. Store the software in multiple files.

The virtual machine which is created is entirely a different computer, it is having different IP and identity. If you want to copy something from C drive and paste it in virtual machine it will not work. Once all the updates are done restart the virtual machine and type the command, "*/sudo apt-get update".* The next thing is just a copy paste command, after getting the full update execute the code,"*sudo apt-get install gcc g++ python python-dev mercurial bzr gbd* valgrind *gsl-bin libgsl0-dev libgsl0ldbl flex bison tcpdump sqlite sqlite3 libsqlite3-dev libxml2 libxml2-dev libgtk-2.0 libgtk2.0-dev uncrustify doxygen graphviz imagemagick texlive texlive-latex-extra texlive-generic-extra texlive-generic-recommended texinfo dia texlive texlive-latex- extra texlive-extra-utils texlive-generic-recommended texi2html python-pygraphviz python-kiwi python-pygoocanvas libgoocanvas-dev python-pygccxml".*

While downloading these above files it will take approx. of around 800-900 MB. Extract the allinone bz2 file in the Ubuntu and download the synaptic, synaptic contains all the packages or dependencies which the user can install by going to properties. Run the first file known as "build.py" file. The execution will go through the compiler phase and will extract files from around 2308 in built files.

# 12. QUALITY OF SERVICE

## 12.1 End-to-End Delay

This QoS is a guaranteed delay service in ad-hoc networks, which works from one end of the work to another. End-to-End delay says about the function of packetisation, that is the fixed length of the packet divided by its rate added with the propagation delay given by its length of the link divided by the speed of light. The queuing delay refers to the que at which the delay is occurring. The basic meaning of End-to-End delay is that, if we know the upper bound of the queuing delays namely $Q_1$ (t),

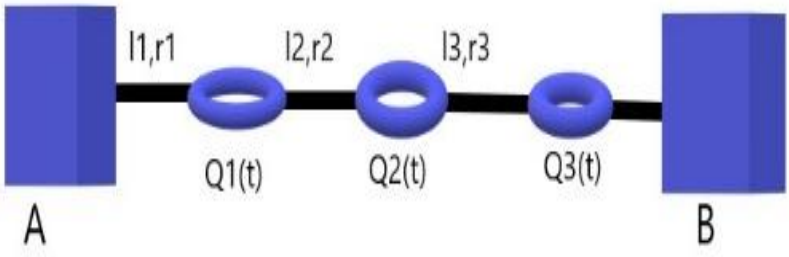


**Fig 17: End-to-End Delay**

$Q_2(t)$ and $Q_3(t)$ then we will know the upper bound of End-to-End delay.

$$\textbf{End-to-End delay, } \tau = \Sigma\left(\left(\frac{p}{r}\right) + \left(\frac{l}{c}\right) + Q(t)\right)$$

This can understand by the following example as, if we that which que the packet passes through and what is the size of the buffer also the rate which is going to serve the packet then we can calculate the maximum delay the packet can encounter through the router.

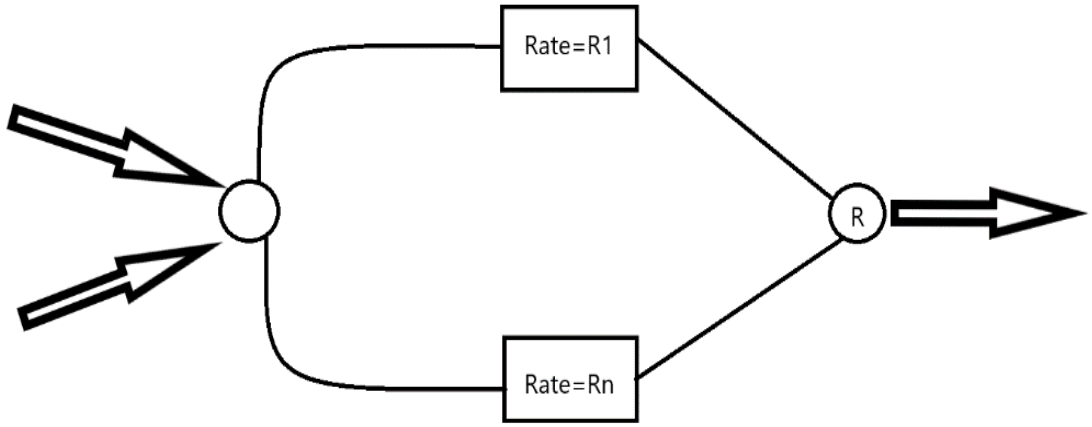


**Fig 18: Calculation of Maximum Delay**

Putting it all together we get firstly the "sigma-rho constraint traffic" in the leaky bucket regulator. Each router in the path will wait for "Waited for Queuing(WFQ)" in order to get the service rate, R1 for that particular flow and buffer size, B and the same will work for the router 2 followed by router 1. And to check that the packets are following the correct path, packet classification is used for it so that it can reach its perfect destination.

To set this process initially a protocol is used which is known as "Reservation Protocol (RSVP)" and IETF RFC 2205 which demonstrates that what to do in this protocol.

## 12.2 Throughput

To measure the efficiency of a packet or to measure the rate at which the packet delivery is efficient is known as Throughput. Generally, the efficiency of any substance should be as high as possible just to get good feedback, same the value of throughput should be also high for good network. It is measured in bits/seconds or bps.

The throughput is defined as the average rate of the packet which has been delivered between transmitter and receiver through any mode of communication channel.

$$\textit{Throughput} = \frac{\textit{Total packets recieved} * \textit{Size of packet} * 8}{\textit{Time}}$$

## 12.3 Jitter

As the throughput is responsible for the transmission of packets with general information, the jitter at the receiver end is responsible for the deviation improvement which may occur during the transmission from the transmitter. Jitter can also be used as a transmitter, it has much higher rate of transmission than throughput. It is measured in seconds.

If there are two packets I and j where j>I then the jitter obtained is given by,

$$\textit{jitter} = ((\textit{recievtime}(j) - \textit{sendtime}(j)) - (\textit{receivtime}(i) - \textit{sendtime}(i)))/(j - i)$$

## 12.4 Packet Delivery Ratio

Packet delivery ratio, as the name suggests the delivery of packet at the receiver end successfully without any error has been occurred. Though this term measure the percentage of the packets received at the receiver end. The improvement of PDR is possible as to get better efficiency and faster delivery. To improve PDR, the system from which it is transmitted has to be less computational, and also for secondary purpose, to avoid any delay in the delivery it should have an alternative route. Alternate route is not used as much the primary route though this route is maintained. The secondary route is used for the transmission of packets when the primary route is broken. For better PDR the ratio should be maximum.

$$\textit{PDR} = \left(\left(\frac{\textit{Total packet recieved}}{\textit{Total packet sent}}\right) * 100\right)$$

## 12.5 Packet Loss Ratio

The ratio of total packet lost while transmission and the total packet sent gives the packet loss ratio. With many consequences of error free transmission, there are some sources which causes an error in the delivery. PLR gives the accurate information that how much is lost w.r.t how much data was sent. For better feedback PLR should be as low as possible.

$$\textit{PLR} = \left(\left(\frac{\textit{Total packet sent} - \textit{Total packet recieved}}{\textit{Total packet sent}}\right) * 100\right)$$

# 13. CONCLUSIONS

In conclusion, we have studied about various types of Ad-hoc Networks and its consequences with some QoS. We studied that how can VANETs help in traffic solutions in roads, communication of vehicle-to-vehicle and avoiding accident

which can be really helpful. The continuation of research in VANET and other Ad-hoc Network will help the evolution of vehicles and also the innovation of new technology.

## 14. REFERENCES

[1] Sabih ur Rehman, M. Arif Khan, Tanveer A. Zia and Lihong Zheng, "Vehicular Ad-Hoc Networks (VANETs) - An Overview and Challenges", Journal of Wireless Networking and Communications vol.3, pp. 29-38, 2013.

[2] Manjot Kaur, Sukhman Kaur and Gurpreet Singh, "Vehicular Ad Hoc Networks", Journal of Global Research in Computer Science, vol.3, pp.1-3, ISSN-2229-371X, 2012.

[3] Wenshuang Liang, Zhuorong Li, Hongyang Zhang, Shenling Wang and Rongfang Bie,"Vehicular Ad hoc Networks: Architectures, Research Issues, Methodlogies, Challenges and Trends", International Journal of Distributed Sensor Networks, vol.2015, pp.3-4, 2014.

[4] Sudha Dwivedi and Rajni Dubey,"Review Trust in Vehicle Scenario in VANET", International Journal of Future Generation Communication and Networking, vol.9 No.5, pp.305-314, 2016.

[5] Namita Chandel, Vishal Gupta,"Comparative Analysis of AODV, DSR and DSDV Routing Protocols for VANET City Scenario, International Journal on Recent and Innovation Trends in Computing and Communication, vol.2, pp.1380-1384, ISSN-2321-8169, 2014.

[6] Alex Hinds, Michael Ngulube, Shaoying Zhu and Hussain Al-Aqrabi,"A Review of Routing Protocol for MANET", International Journal of Information and Education Technology, vol.3, No.1, pp.2-4, 2013.

[7] Shameer Mohamad, Imran Khan,"A Survey Secure Routing Protocols Mobile Adhoc Networks", International Journal of Computer Science Engineering Techniques, vol.1, Issue 1, pp.1-3, 2015.

[8] Aravindan B, Dhivakar A, Shreehari V. V,"Dynamic High Secure Protocol for Mobile Adhoc Network", International Journal of Engineering and Techniques, vol. 2, Issue 2, pp.4-7, 2016.

[9] Parma Nand, S. C. Sharma,"Routing Load Analysis of Broadcast based Reactive Routing Protocols AODV, DSR and DYMO for MANET", International Journal of Grid and Distributed Computing, vol. 4, No. 1, pp.2-4, 2011

[10] Wenjia Li and Anupam Joshi,"Security Issues in Mobile Ad Hoc Networks- A Survey", University of Maryland, Baltimore County, pp.8-15, 2003.

[11] Ali Dorri, Seyed Reza and Esmail Kheyrkhah,"Security Challenges in Mobile Ad-hoc Networks", International Journal of Computer Science & Engineering Survey, vol. 6, No. 1, pp.2-8, 2015.

[12] Atta ur Rehman Khan, Sardar M. Bilal and Mazliza Othman,"A Performance Comparision of Network Simulators for Wireless Communication", pp.2-4, 2011.

[13] John Heidemann, Nirupama Bulusu, Jeremy Elson, Chalermek Intanagonwiwat, Kun-chan Lan, Ya Xu, Wei Yu, Deborah Estrin, Ramesh Govindan,"Effects of Details in Wireless Network Simulation", USC/Information Sciences Institute, USC/ISI TR-2000-523b, pp.3-7, 2001.

[14] Muneer Bani Yassien and Nour Alhuda Damer,"Flying Ad-hoc Networks: Routing Protocols, Mobility Models, Issues", International Journal of Advanced Computer Science and Applications, vol.7, No.6, pp.4-7, 2016.

[15] Laiq Khan, Nohman Ayub and Amir Saeed,"Anycast Based Routing in Vehicular Adhoc Network using Vanetmobisim", World Applied Sciences Journal, vol.7, ISSN-1818-4952, pp.1341-1352, 2009.

[16] Ramesh C. Poonia, Vikram Singh,"Performance Evaluation of Radio Propagation Model for VANET using Vanetmobisim and NS-2", International Journal of Distributed and Parallel System, vol.3, No. 4, pp.3-7, 2012.

[17] Michael Behrisch, Laura Bieker, Jakob Erdmann, Daniel Krajzewicz,"SUMO- Simulation of Urban Mobility", IARIA Conferences, pp.2-5, 2011

[18] A B M Moniruzzaman, Sadekur Rahmann,"Analysis of Topology Based Routing Protocols for VANET", International Journal of Computer Application, vol.*, No.*, pp. 2-7, 2014.

[19] Pankaj Rohal, Ruchika Dahiya, Prashant Dahiya,"Study and analysis of Throughput, Delay and Packet Delivery Ratio in MANET for Topology Based Routing Protocols, International Journal for Advance Research in Engineering and Technology, vol.1, Issue 2, ISSN-2320-6802, pp. 4-5, 2013.

[20] Preeti Aggarwal, Pranab Garg,"AOMDV Protocols- A Review", International Journal of Advanced research in Computer Science & Technology, vol.4, Issue 2, ISSN-2347-8446, pp. 32(1-3), 2016.

[21] Behra Rajesh Umashankar, rakhi Kumari Purnima,"A Comparative Study of Topology and Position Based Routing Protocols in MANET", International Journal of Advance research in Computer Science & Technology, vol.2, Issue 2, ISSN-2347-8446, pp. 72(3-4), 2014.