Traffic Visualisation of Performance Metrics between Routing Protocols for MANETS

T.Durgarao
PG Student, ECE Dept., QISIT

N.Srinivasulu
PG Student, ECE Dept., JNTUCEH

K.C.K.Naik
Asso.Prof & HOD, ECE Dept., QISIT

Dr.Ch.Balaswamy
Prof& HOD, ECE Dept., QISCET

Abstract

Mobile Ad hoc networks (MANETs) are combination of mobile nodes without existence of any centralized control or pre-existing infrastructure. Ad hoc networking allows portable devices to establish communication independent of a central Infrastructure. However, the fact that there is no central infrastructure and that devices can move randomly give rise to various kind of problems, such as routing and security. The primary goal of this research work study and investigate the performance metrics between DSDV, AODV and DSR routing protocols based on the CBR traffic. This paper presents traffic visualization based on CBR type analyzes the performance metrics are first node failure time, Network lifetime, and routing overhead, dropped rate of packets, Packet delivery ratio, and Average end to end delay by using discrete event simulator NS2.

Keywords: MANET, Packet delivery ratio, Network life time, Average end to end delay, Dropped packets.

1. Introduction

Wireless cellular systems have been in use since 1980s. We have seen their evolutions to first, second and third generation's wireless systems. Wireless systems operate with the aid of a centralized supporting structure such as an access point. These access points assist the wireless users to keep connected with the wireless system, when they roam from one place to the other. The presence of a fixed supporting structure limits the adaptability of wireless systems. In other words, the technology cannot work effectively in places where there is no fixed infrastructure. Future generation wireless systems will require easy and quick deployment of wireless networks. This quick network deployment is not possible with the existing structure of current wireless systems. Recent advancements such as Bluetooth introduced a new type of wireless systems known as mobile ad-hoc networks. Mobile ad-hoc networks or "short live" networks operate in the absence of fixed infrastructure. They offer quick and easy network deployment in situations where it is not possible otherwise. Ad-hoc is a Latin word, which means "for this or for this only." Mobile ad-hoc network is an autonomous system of mobile nodes connected by wireless links; each node operates as an end system and a router for all other nodes in the network. Nodes in mobile ad-hoc network are free to move and organize themselves in an arbitrary fashion. Each user is free to roam about while communication with others. The path between each pair of the users may have multiple links and the radio between them can be heterogeneous. This allows an association of various links to be a part of the same network. Recent advancements such as Bluetooth introduced a new type of wireless systems known as mobile ad-hoc networks. Mobile ad-hoc networks or "short live" networks operate in the absence of fixed

infrastructure. They offer quick and easy network deployment in situations where it is not possible otherwise. Ad-hoc is a Latin word, which means "for this or for this only." Mobile ad-hoc network is an autonomous system of mobile nodes connected by wireless links; each node operates as an end system and a router for all other nodes in the network. Nodes in mobile ad-hoc network are free to move and organize themselves in an arbitrary fashion. Each user is free to roam about while communication with others. The path between each pair of the users may have multiple links and the radio between them can be heterogeneous. This allows an association of various links to be a part of the same network.

Characteristics

Mobility Rapid deployment in areas without infrastructure often indicates that the users must explore an area and perhaps form teams that in turn coordinate among themselves to create a taskforce or a mission. We can have individual random mobility, group mobility, motion along preplanned routes, etc. So, the mobility model can have major impact on the selection of a routing mechanism and can thus affect the performance.

Multihopping A network where the path from source to destination traverses several other nodes is often called an ad-hoc network. Ad-hoc networks often exhibit multiple hops for spectrum reuse, and energy conservation. Battlefield secret operations also favour a sequence of short hops to reduce detection by the enemy.

Self-Organization The ad-hoc network must free to act individually to determine its own parameters which include addressing, routing, clustering, position identification, power control, etc. In some cases, special nodes (e.g., mobile backbone nodes) can coordinate their motion and dynamically distribute in the geographic area to provide coverage of disconnected islands.

Energy Conservation Nodes in the ad-hoc network (e.g., laptops, mobile phones and sensors, etc.) have limited CPU Capacity, storage capacity, limited power supply and they do not have capability to generate their own power (e.g., solar panels) this is referred as “thin client” this means the energy usage must be limited thus leading to the limited transmission range.

Scalability In some applications such as large environmental sensor fabrics, battlefield deployments, urban vehicle grids, etc. The ad-hoc network can increase in size to several thousand nodes. For wireless “infrastructure” networks scalability is simply handled by a hierarchical construction. The limited mobility of infrastructure networks can also be easily handled using Mobile IP or local handoff techniques. In contrast, because of the more extensive mobility and the lack of fixed references, pure ad-hoc networks do not tolerate mobile IP or a fixed hierarchy structure. Thus, mobility, jointly with large scale is one of the most critical challenges in ad-hoc design.

Security Ad-hoc networks are much more easily harmed to security attacks than conventional wired networks. An active attacker tends to interrupt the continuity of operations. Due to the complexity of the ad-hoc network protocols these active attacks are by far more difficult to detect in ad-hoc than infrastructure networks. Passive attacks are unique of ad-hoc networks, and can be even more harmful than the active ones. The active attacker may eventually discover and physically disabled/eliminated. The passive attacker is never discovered by the network. Like a “bug”, it is placed in a sensor field or at a street corner. It monitors data and control traffic patterns and thus infers the motion of rescue teams in an urban environment. This information is relayed back to the enemy headquarters via special communications channels with low energy and low probability of detection. To avoid the passive attacks require powerful new encryption techniques coupled with careful network protocol designs.

Applications

Military battlefield scenarios in which soldiers carry portable or wearable computers with radios for communication.

Rescue workers in post disaster areas where the fixed infrastructure is disabled.

Sensor networks in which many nodes scattered about the physical environment communicate information about the environment.

Temporary collaborations among colleagues

Vehicular networks are made of ad-hoc nodes placed in automobiles.

Cell phone call routing may benefit from ad-hoc networking technology.

2. Classification of Routing Protocols

The Ad hoc routing protocols are broadly classified into three categories those are

- Proactive routing protocols or Table driven routing protocols
  Example: DSDV
- Reactive Routing protocols or On-Demand routing protocols
  Example: DSR, AODV
- Hybrid routing protocols
  Example: ZRP

Proactive Routing Protocol (Table Driven)

In a network utilizing a proactive routing protocol, every node keeps one or more tables representing the complete topology of the network. These tables are updated constantly in order to keep up-to-date routing information from each node to every other node. To maintain the up to- date routing information, topology information needs to be alternate between the nodes on a regular basis, leading to comparatively high overhead on the network. On the other hand, routes will be available on request. Many proactive protocols arise from conventional link state routing, along with the Optimized Link State Routing protocol (OLSR).

Reactive Routing Protocol (On-Demand Driven)

Reactive routing protocols are on-demand protocols. These protocols do not try to keep correct routing information on all nodes at all times. Routing information is collected only when it is required, and route determination based on sending route queries throughout the network. The primary benefit of reactive routing is that the wireless channel is not subject to the routing overhead data for routes that may never be consumed. While reactive protocols do not have the fixed overhead needed by keeping continuous routing tables, they may have considerable route discovery delay. Reactive search procedures can also add a significant amount of control traffic to the network because of query flooding. Because of these weaknesses, reactive routing is less applicable for real-time traffic or in scenarios with a high volume of traffic between a large numbers of nodes.

Hybrid Routing Protocol

Wireless hybrid routing is depends on the idea of organizing nodes in groups and then allowing nodes different functionalities inside and outside a group. Both routing table size and update packet size are decreased by involving in them only part of the network (instead of the whole); thus, control overhead is decreased. The most popular way of building hierarchy is to group nodes geographically close to each other into definite clusters. Each cluster has a leading node (cluster head) to communicate to other nodes on behalf of the cluster hierarchy. In this way, each node has a local scope. Different routing strategies are used hierarchy. In this way, each node has a local scope. Different routing strategies are used inside and outside the scope. Communications pass across overlapping scopes. More efficient overall routing performance can be acquired through this flexibility. Since mobile nodes have only a single unidirectional radio for wireless communications, this type of hierarchical organization will be mentioned to as logical hierarchy to distinguish it from the physically hierarchical network structure.

3. Description of Routing Protocols

3.1 DSDV (Destination Sequenced Distance Vector Routing Protocol)

The Destination-Sequenced Distance Vector Routing Protocol is a Table-driven routing protocol. Since each node maintains one or two tables which consists of routing information from that node to every node in the network, packets are transmitted between the stations of the network by using these routing tables. The routing table, at each of the stations consists of all available destinations, and the number of hops to each. Each route table entry is tagged with a sequence number, which is originated by the destination station. To maintain the consistency of routing tables in a dynamically varying topology, each station periodically transmits updates, and transmits updates immediately when significant new information is available. Routing information is advertised by broadcasting or multicasting the packets which are transmitted periodically and incrementally as topological changes are detected.

DSDV solve the problem of routing loops and count to infinity by associating each route entry with a sequence number indicating its freshness. In DSDV, a sequence number is linked to a destination node, and usually is originated by that node (the owner). The only case that a non-owner node updates a sequence number of a route is when it detects a link break on that route. An owner node always uses even-numbers as sequence numbers, and a non-owner node always uses odd-numbers. With the addition of sequence numbers, routes for the same destination are selected based on the following rules:

- a route with a newer sequence number is preferred
- In the case that two routes have a same sequence number, the one with a better cost metric is preferred.

The list which is maintained is called routing table. The routing table contains the following:

- All available destinations' IP address
- Next hop IP address
- Number of hops to reach the destination
- Sequence number assigned by the destination node
- Install time

The sequence number is used to distinguish stale routes from new ones and thus avoid the formation of loops.

3.2 AODV (Ad hoc on Demand Vector Routing Protocol):

Ad-hoc On-demand Distance Vector Routing (AODV) is an improvement on the Destination Sequenced Distance Vector routing (DSDV). AODV minimizes the number of broadcasts by creating routes on-demand as opposed to DSDV that maintains the list of all the routes. To find a path to the destination, the source broadcasts a route request packet. The neighbours in turn broadcast the packet to their neighbours till it reaches an intermediate node that has recent route information about the destination or till it reaches the destination. A node discards a route request packet that it has already seen. The route request packet uses sequence numbers to ensure that the routes are loop free and to make sure that if the intermediate nodes reply to route requests, they reply with the latest information only. When a node forwards a route request packet to its neighbours, it also records in its tables the node from which the first copy of the request came. This information is used to construct the reverse path for the route reply packet.

3.3 DSR (Dynamic Source Routing Protocol):

The Dynamic Source Routing protocol (DSR) is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. DSR allows the network to be completely self-organizing and self-configuring, without the need for any existing network infrastructure or administration. Dynamic Source Routing, DSR, is a reactive routing protocol that uses source routing to send packets. It uses source routing which means that the source must know the complete hop sequence to the destination. Each node maintains a route cache, where all routes it knows are stored. The route discovery process is initiated only if the desired route cannot be found in the route cache. To limit the number of route requests propagated, a node processes the route request message only if it has not already received the message and its address is not present in the route record of the message.

DSR uses source routing, i.e. the source determines the complete sequence of hops that each packet should traverse. This requires that the sequence of hops is included in each packet's header. A negative consequence of this is the routing overhead every packet has to carry. However, one big advantage is that intermediate nodes can learn routes from the source routes in the packets they receive. Since finding a route is generally a costly operation in terms of time, bandwidth and energy, this is a strong argument for using source routing. Another advantage of source routing is that it avoids the need for up-to-date routing information in the intermediate nodes through which the packets are forwarded since all necessary routing information is included in the packets. Finally, it avoids routing loops easily because the complete route is determined by a single node instead of making the decision hop-by-hop. The protocol is composed of the two main mechanisms of "Route Discovery" and "Route Maintenance", which work together to allow nodes to discover and maintain routes to arbitrary destinations in the ad hoc network. All aspects of the protocol operate entirely on demand, allowing the routing packet overhead of DSR to scale automatically to only what is needed to react to changes in the routes currently in use. The protocol allows multiple routes to any destination and allows each sender to select and control the routes used in routing its packets.

Route Discovery:

Route Discovery is used whenever a source node desires a route to a destination node. First, the source node looks up its route cache to determine if it already contains a route to the destination. If the source finds a valid route to the destination, it uses this route to send its data packets. If the node does not have a valid route to the destination, it initiates the route discovery process by broadcasting a route request message. The route request message contains the address of the source and the destination, and a unique identification number. An intermediate node that receives a route request message searches its route cache for a route to the destination. If no route is found, it appends its

address to the route record of the message and forwards the message to its neighbours. The message propagates through the network until it reaches either the destination or an intermediate node with a route to the destination. Then a route reply message, containing the proper hop sequence for reaching the destination, is generated and unicast back to the source node.

Route Maintenance:
Route Maintenance is used to handle route breaks. When a node encounters a fatal transmission problem at its data link layer, it removes the route from its route cache and generates a route error message. The route error message is sent to each node that has sent a packet routed over the broken link. When a node receives a route error message, it removes the hop in error from its route cache. Acknowledgment messages are used to verify the correct operation of the route links. In wireless networks acknowledgments are often provided as e.g. an existing standard part of the MAC protocol in use, such as the link-layer acknowledgment frame defined by IEEE 802.11. If a built-in acknowledgment mechanism is not available, the node transmitting the message can explicitly request a DSR-specific software acknowledgment to be returned by the next node along the route.

4. Simulation Environment

The Proposed protocol is implemented with the object oriented discrete event simulator. In our simulation, 16 mobile nodes move in a 1000 meter x 1000 meter square region for 200 Seconds simulation time. The Simulator Environment is created by using TCL Script with the help of following parameters included in the table.

Propagation	Two Ray Ground Propagation
No. of Nodes	16
Area Size	1000x1000 m^2
MAC	802.11
Simulation Time	200 Sec
Traffic Source	CBR
Packet Size	512 bytes
Antenna type	Omni directional
Packet Transmission Power	0.4 mw
Packet Receiving Power	0.1mw
Routing Protocols	DSDV, AODV, DSR
Initial Energy of nodes	X joules (Different Energies are used)

Table 4.1. Simulation Environment

The simulation environment observes by using the Network Animator (NAM). The below figures are the snapshots of simulation environment

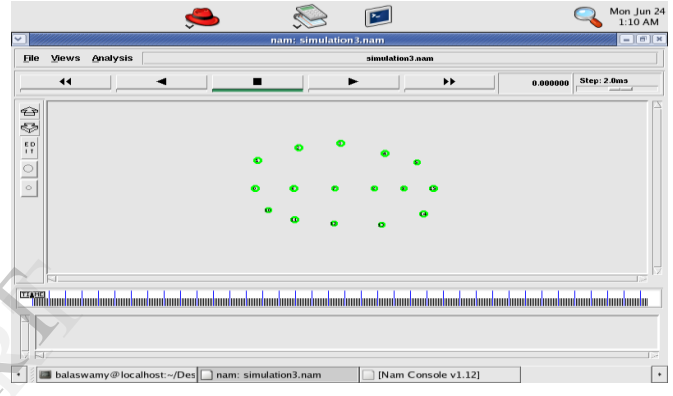

Fig. 4.1.Network Scenario

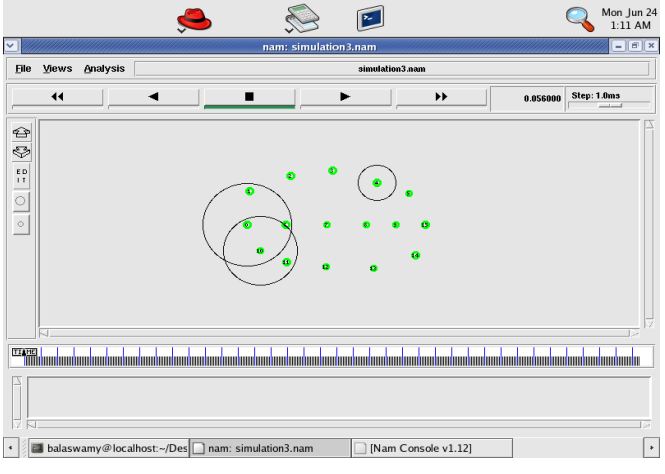

Fig.4.2. Route Discovery

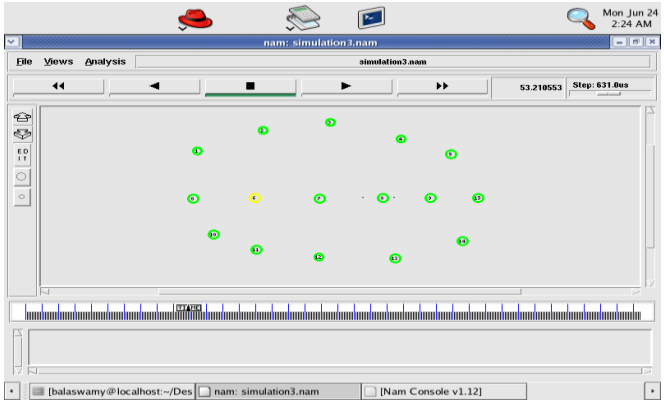

Fig.4.3. Packet Transmission

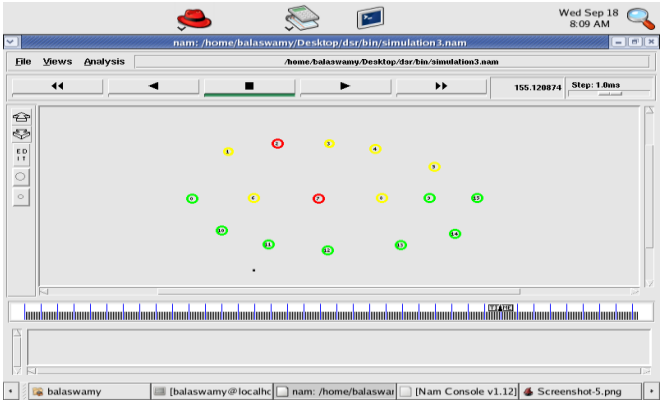

Fig.4.6 Dropped Packet

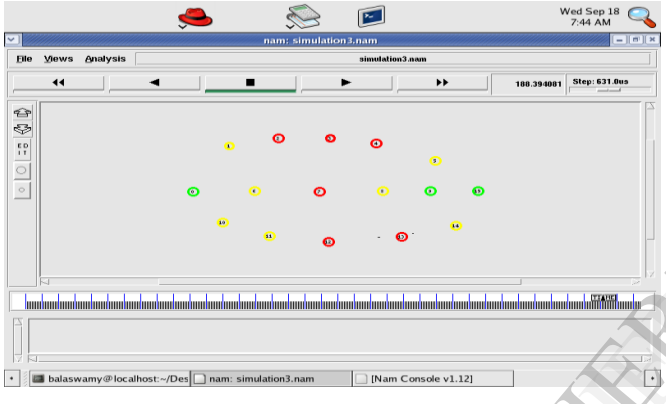

Fig.4.4. Network Life Time Calculation

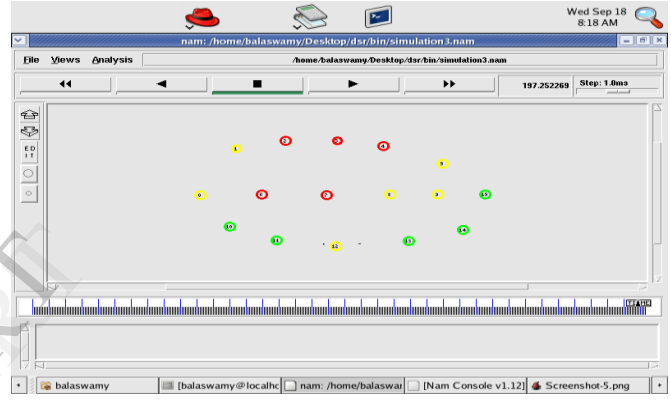

Fig.4.7. DSDV Life time calculation

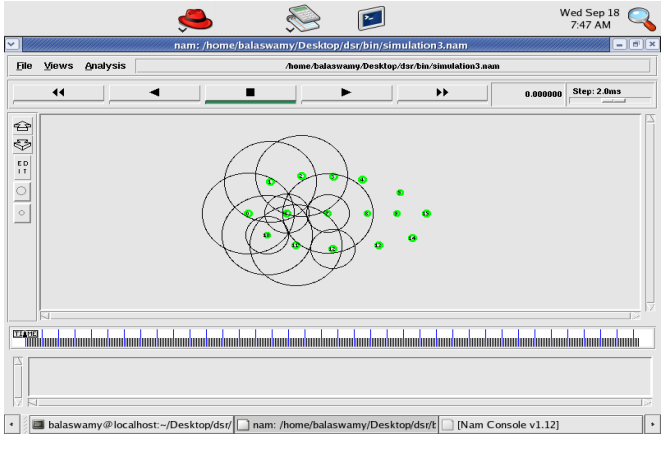

Fig.4.5. Broadcasting in DSDV

5. Performance Metrics

Packet delivery ratio: The ratio of the data packets delivered to the destinations to those generated by the CBR sources. Received packets and sent packets number could be easily obtained from the first element of each line of the trace file.

Packet delivery ratio (%) = (received packets/sent packets)*100

Average end-to-end delay: This includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC, and propagation and transfer times.

For each packet with id (Ii) of trace level (AGT) and type (cbr), we can calculate the send (s) time (t) and receive (r) time (t) and average it.

Routing overhead: It is the ratio of the routing packets sent and the total packets sent. Each hop-wise transmission of a routing packet is counted as one transmission.

Calculation of the routing overhead:

Routing overhead = routing packets sent / total packets sent

Network Lifetime: It represents the lifetime of network when the all routes are fail.

Throughput Throughput refers to the performance of tasks by a computing service or device over a specific period. It measures the amount of completed work against time consumed and may be used to measure the performance of a processor, memory and network communications. It can be represents Bits per Second.

Packet A packet is the unit of data that is routed between an origin and a destination on the Internet or any other packet switch network. A packet consists of two kinds of data: control information and user data (also known as payload). The control information provides data the network needs to deliver the user data,

Jitter: Jitter is the variation in the time between packets arriving, caused by network congestion, timing drift, or route changes. A jitter buffer can be used to handle jitter.

Transmission time: The transmission time, is the amount of time from the beginning until the end of a message transmission. In the case of a digital message, it is the time from the first bit until the last bit of a message has left the transmitting node. The packet transmission time in seconds can be obtained from the packet size in bit and the bit rate in bit/s as

Packet transmission time = Packet size / Bit rate

6. Experimental Results

The results obtain based on the trace files

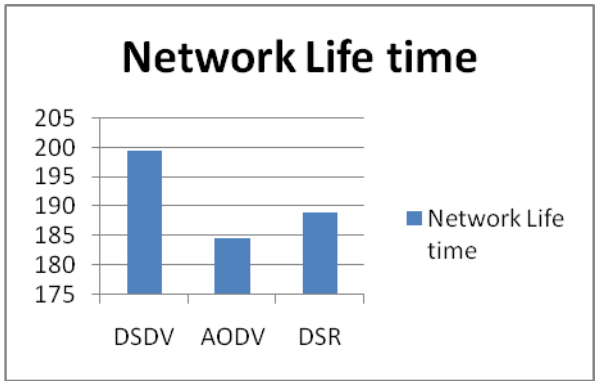

Fig.6.1. Network Lifetime

The diagram 6.1 shows Network Lifetime consider routing protocols like DSDV, AODV and DSR.

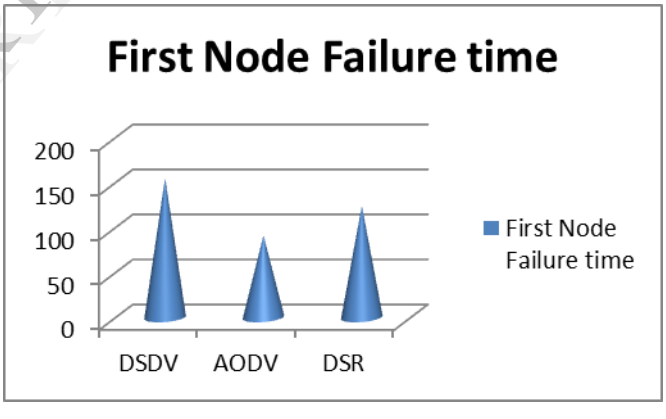

Fig.6.2. First node failure time

The diagram 6.2 shows First node failure time consider routing protocols like DSDV, AODV and DSR.

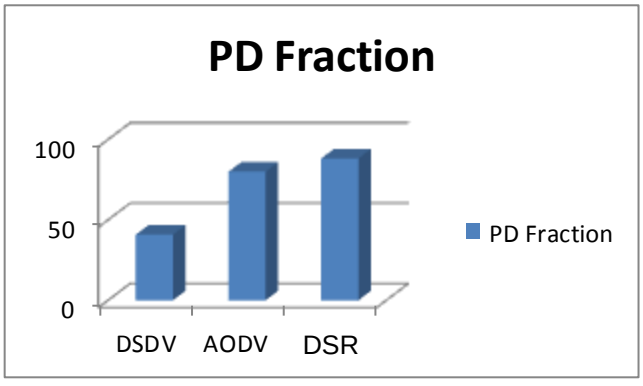

Fig.6.3. Packet Delivery Ratio Fraction

The diagram 6.3 shows Packet Delivery Ratio Fraction Consider routing protocols like DSDV, AODV and DSR.

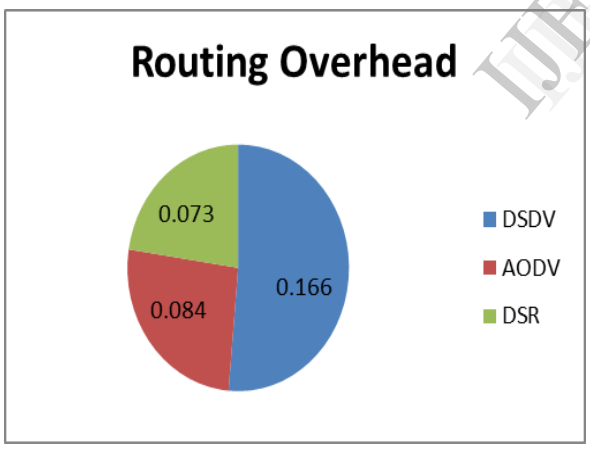

Fig.6.4.Routing Overhead

The diagram 6.4 shows Routing Overhead consider routing protocols like DSDV, AODV and DSR.

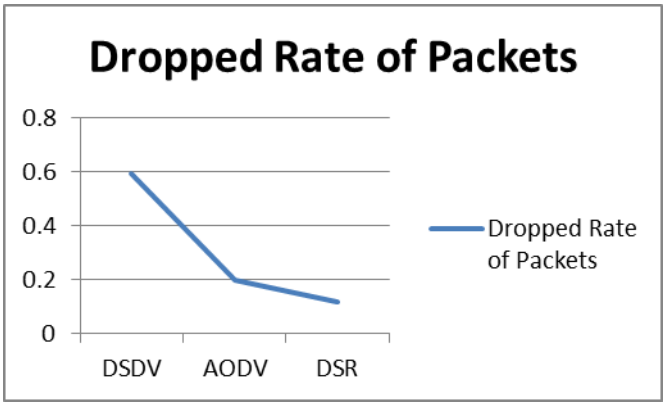

Fig.6.5.Dropped Rate of Packets

The diagram 6.5 shows Dropped Rate of Packets consider routing protocols like DSDV, AODV and DSR.

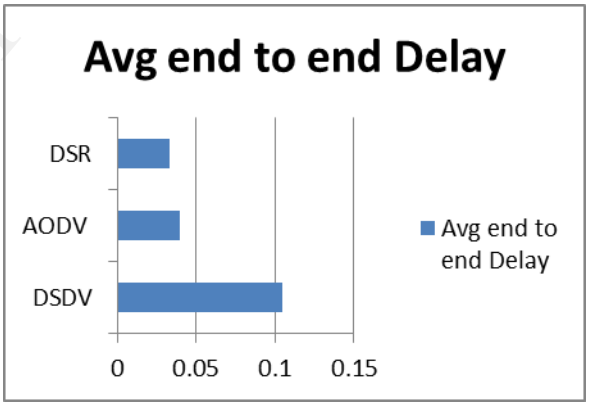

Fig.6.6. Average end to end delay

The diagram 6.6 shows Average end to end delay consider routing protocols like DSDV, AODV and DSR.

Working Environment:

VM player
Red hat Linux 4 Operating System
Network Simulator 2
Java Trace Analyser
Trace Graph analyser 202

7. Conclusion

Generally in MANET the design of Routing protocols are very important criteria because the performance of network depends on the design of routing protocols. In this paper, we are using ad-hoc routing protocols like Destination Sequence Distance Vector Routing protocol (DSDV), Ad hoc on Demand Vector Routing Protocol (AODV) and Dynamic source routing protocol (DSR).Considering the performance metrics Network Lifetime, Packet Delivery Ratio, First node failure time, Avg End to End Delay, Transmission time and Dropped Packet Information analysed the performance of the Mobile Ad-hoc Network with the help of CBR traffic using the Network Simulator Software.

8. References

[1]. Parul sarma, Aravind Kalia, Jawahar Thakur "Performance Analysis of AODV, DSR and DSDV routing protocols in MANET " Journal of Information System and Communications. ISSN: 0976-8742&E-ISSN: 0976-8750, Volume 3, Issue 1, 2012, pp-322-326.

[2]. D.Gokula Krishna, Sharma, Narasimha murthy "Design and Implementation of a routing protocol for MANET" sasTech volume 10, Issue2, Sep 2011.

[3].Amith Khandakar, "Step by Step Procedural Comparison of DSR,AODV and DSDV Routing Protocols" IPCSIT Volume 40(2012).

[4]. S.Rajeswari, Dr.Y.Venkataramani " Traffic Performance Analysis of MANET Routing Protocols" IJDPS Vol.2, No.3, May 2011.

[5]."Comparative Performance AODV,DSDV and DSR routing protocols in MANET using NS2" ICACE 2010 IEEE Communication Society.

[6]. "Extensive Simulation performance Analysis for DSDV,DSR and AODV MANET Routing Protocols " 27th International Conference on Advanced Information Networking and its Applications Workshop: IEEE Communication Society.

[7]. S.Kulakarni "Performance Analysis of Energy Efficient routing in MANET" IJSSST, Vol.10.No.1. ISSN:1473-804X online, 1473-8031 Print.

[8].P.Manickar, Guru Bhaskar, M.Girija, Dr.D.Manimegalai "Performance Comparison of Routing Protocols in MANET" IJWMN Vol.3.No.1 Feb 2011.

Author Profile

T.Durgarao received the B.Tech in Electronics and Communication Engineering from GITAM University in the year 2010. Now he is pursuing M.Tech in VLSI&ESD from JNTU Kakinada. His research interest in wireless networks.

N.Srinivasulu presently pursuing his MS degree from JNTU Hyderabad. He received the B.Tech Degree in ECE from JNTU Kakinada. He has published Four Research papers in International Conferences and One International Journal. His area of Interest is Mobile Ad-hoc Networks, Wireless Communication Networks and VLSI. He is EDAS Identifier and Active Member of IAENG, IAEST and IACSIT Professional Societies.

K.C.KULLAYAPPA NAIK received the B.Tech and M.Tech. Degrees in Electronics and Communication Engineering from MITS, Madanapalle in 2004 and 2007 respectively .Since 2007 he has been working as assistant professor in various organizations. Now he is working as Associate Professor& HOD in the department of ECE at QISIT, Ongole. His research interest in wireless networks.

Dr.Ch.Balaswamy received the B.E degree in ECE from S.R.K.R. Engineering College, Bhimavaram in 1998. He received the M.Tech degree in ECE from Inad College of Engineering , Hassan, India in 2001. He received his Ph.D. from JNTU Ananthapur in 2010. He has 13 years' experience in teaching for U.G and P.G students. He guided many B.Tech and M.Tech projects. He has published Seven International Journals and Seven Research papers in National and International Conferences. His area of Interest is Mobile Ad hoc Networks, Micro Processors & Controllers and Embedded System. He is active member of ISTE, IAENG and IAEST Professional Societies.