Performance analysis of AODV and GPSR Routing Protocols in WSN

Sandeep Singh
M.Tech. Student Department of
Computer Science & Engineering
KNIT Sultanpur
singh.manhattan@gmail.com

Prof. B.P. Chaurasia
Associate Professor Department of
Computer Science & Engineering
KNIT Sultanpur
bpc1888@gmail.com

***Abstract*—** Wireless sensor networks(WSNs) are the contribution of many randomly distributed sensor nodes(source node or destination node), with features of high mobility, dynamic topology and frequent disconnection of nodes. These nodes are capable of measuring geographical and physical characteristics of the surrounding environment using radio waves as links between them. The physical characteristics they measure may be whether, humidity, earthquakes, surveillance, tracking etc. WSNs are different from wireless Local Area Networks (WLANs) and other computer networks in terms of limited resources like memory, power and life span. Energy usage is the greatest challenge for the WSNs. Today a tremendous amount of testing and researches are being done on the WSNs and its applications but still some issues need to be rectified.
Many routing protocols for various purpose are being used in this field. Some very important protocols are LEACH, AODV and GPSR, etc. It is observed that AODV and GPSR are found to be very compatible routing algorithms for WSN. Since AODV is routing protocol (infrastructure less) used in the MANETS hence provides a better algorithm for highly mobile nodes in WSN similarly GPSR is the well knows geographic routing protocol which uses the geographical positions of the randomly distributed nodes to make the routing path.

Keywords-WSN, WLAN, MANETS, AODV, GPSR

1. INTRODUCTION

The Wireless Sensor Network [1] is defined by random movement of mobile nodes in wireless scenario, in order to find the best possible path between sources to destination; routing protocols are used in wireless communication. As there is no dedicated path between the nodes, a routing strategy is helpful in exploring the shortest path. The wireless networks are mainly composed of two types of networks these are infrastructure based network and Ad-hoc network. In case of infrastructure based networks there is a central station called access point (AP) which provide a wireless link between AP and a mobile data terminal equipment having antenna (can be a laptop or notepad computer).The routing procedure is also controlled by these access points, in such environment. While in Ad-Hoc network there is no such an central point(or access point).Here nodes are self-configured and connect each other in ad-hoc manner. In WSNs the nodes are distributed in random manner and communicate to the base stations for data packet exchange.
The range of transmission is fixed. While in case of Ad-hoc networks the base station or access point is absent. Every node present in the network performs all the functions of base station and routing decisions are also taken by them. In a wireless network devices are distributed in random manner using sensor to mutually monitor physical or geographical conditions such as temperature, sound, vibrations, pressure, motion, pollutants and humidity at different locations of the earth. In a typical WSN there exist a lot of small sensor devices in the detection zones and all the sensor nodes uses the radio signals to communicate wirelessly to form a multi-hop and autonomous network system. All the sensor nodes communicates with each other to stay connect and with the data in the detected field and then send the result to the observer[2,3]. In addition nodes in WSN are prone to failure due to energy depletion, device failure, disconnection and low security due to malicious attack and so on[4].It results in low reliability of performance of sensor networks.

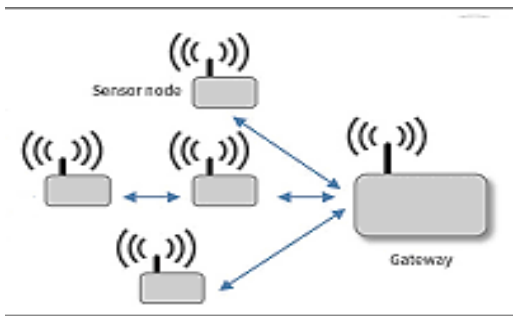


Fig 1.Wireless Sensor Nodes with Gateway Nodes

There are a lot of AODV routing protocols and their implementations which are suitable and have been designed for wireless sensor based environment viz AODVjr[5], AODVbis[6], Gossiping Based AODV,etc.In the Sections below we will discuss about some protocols and their categories.

2. NETWORK ARCHITECTURE AND CHARACTERISTICS OF WSN AND APPLICATIONS

Specialists have made WSN applications for regions including social care and insurance, utilities, and remote observing. In human services, wireless gadgets make less intrusive patient checking and medicinal services conceivable. For utilities, for example, the power matrix, streetlights, and water municipals, wireless sensors offer a lower-cost strategy for gathering framework wellbeing information to lessen energy use and better oversee assets. Remote observing spreads an extensive variety of uses where wireless frameworks can supplement wired frameworks by diminishing wiring costs and permitting new sorts of estimation applications. Remote observing applications include:

1. Environmental observing of air, water, and soil
2. Structural observing for structures
3. Industrial machine checking
4. Process checking
5. Asset following

The WSN works on the following Architecture [7]:

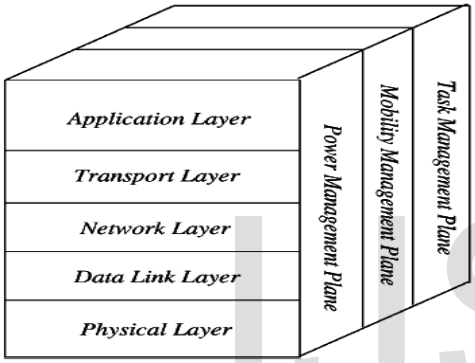


Fig 2.WSN layer Architecture

2.1 Application Layer

The application layer is responsible for network congestion management and provides software for a number of applications that convert the data in a clear form to find required information. Sensor networks arranged in a large number of applications in different fields such as agricultural, military, environment, medical, etc.

2.2 Transport Layer

The function of the transport layer is to deliver congestion control and trust where a lot of protocols employed to offer this function. These protocols use different algorithms for loss recognition loss recovery and prevention. The transport layer is exactly needed when a system is planned to contact other networks.

Providing a trustworthy loss recovery is more energy efficient and that is the reason behind that why TCP is not fit for WSN because it is connection less. In general, Transport layers can be divides into two categories that are Packet driven, Event driven.

2.3 Network layer

The main function of the network layer is routing of data control packet and data packet, it performs many of tasks based on the application, but in real, the main tasks are in the power conserving, partial memory, buffers, and sensor don't have a universal ID and have to be organized by their own.

The simple concept of the routing protocol is to explain a reliable path and redundant paths, according to a predefined benchmark scale called metric, which is different for different protocols. There are a lot of previously existing protocols for this network layer, they can be divided into two categories; flat routing and hierarchal routing or can be divided into three; time driven, query-driven and event driven protocols

2.4 Data Link Layer

The data link layer which is responsible for multiplexing data frame detection, data streaming, MAC, and error detection and control, confirms the reliability of point to point(unicast) (or) point to multipoint(multicast).

2.5 Physical Layer

The physical layer provides framework for sending (or) receiving a stream of bits over physical medium. This layer is used to select the frequency, production of a carrier frequencies, signal detection, Modulation & data encryption. IEEE 802.15.4 is set as a standard as typical for low rate particular areas & wireless sensor network with cheap cost, power consumption by terminals, density of terminals, the range of communication link to improve the battery life as well as life span of whole network. CSMA/CA is used to support star and peer to peer topology. There are several versions of IEEE 802.15.4.V

3. VARIOUS FEATURES OF WSN

Dynamic(Frequent Changing) Topology	Since nodes may have to move from one place to another
Frequent Disconnection in links of Network	The dynamic topology results in frequent disconnected network
Predictable Mobility	Nodes tend to have predictable mobility
Low Energy and short life span	Since nodes work on batteries and hence the life span is critical

Table 1

A. Design Factor

There are many factors to consider when designing a WSN. Will the network be node to node only or could base station used for communication? Which protocol will be employed

in such a mobile network? These and many others aspects will require analysis when determining the features and capabilities of a WSN.

B. Communication Paradigms

Like in other networks, different communication techniques are allowed in WSN like Unicast, Multicast and Broadcast. In unicast communications a node wants to communicate to another node only. In Multicast communication a node can communicate to multiple nodes. This requirement is raised in case of traffic overhead so that a node can sent the information to Base station via another node. Broadcast communication allow message to send to all nodes which lie in its range useful in providing information about weather conditions.

C. Environmental Constraints

The nodes in the WSN operate in a very different environment. The high mobility of nodes sometimes reduces the time available for message exchanges. Protocol required taking the advantage of nodes moving in various directions to maintain the communication link for long period of time.

D. Issues and Challenges

In a WSN the main threats to communication is connection loss, Battery life of nodes, Security of information, and interference of signals with other unofficial frequency band.

4. OVERVIEW OF ROUTING PROTOCOL IN WSN

Routing protocols is a set of rules and regulations that decide how node can select route, the incoming/outgoing packets between devices in a wireless environment and further differentiate in many types. Routing in WSN shows various different features from traditional infrastructure-less (ad hoc) networks. Initially, the mobility of nodes is resisted by the geographical layout of the environment, other nodes movement and distance between wireless nodes and base station nodes. It also affected by external factor like weather condition or the time period. Thus network become highly mobile, dynamic and an end to end path between the source and destination might not exit at the time of sending a message. Because of the great number of nodes which may participate in a WSN, routing protocol need to be localized to ensure its scalability, usually nodes make routing decisions alone based on information locally available in their close vicinity, therefore exchanging information with neighboring nodes via beacon message is a fundamental part of routing protocol, nodes can obtain position information from system like GPS and Galilo.

In this paper we mainly focus on unicast routing protocols, which broadly divided into two categories; Topological and geographical routing protocol. Topology based routing use link information that exists in the network to perform packet forwarding, and further classified into three categories proactive, reactive routing and hybrid routing protocols. Geographic routing protocols use the geographic position of the nodes to make the routing decisions. It is assumed that every node known its own geographical location using global positioning systems (GPS). We took the protocol from both these categories and perform the analysis. Our protocols are AODV and GPSR.

5. AD-HOC ON DEMAND DISTANCE VECTOR (AODV) ROUTING PROTOCOL

AODV [8] is an ad-hoc on demand distance vector routing protocol which is an on demand reactive protocol.

AODV establishes the connection for the communication with the help of control packets like RREQ and RREP and maintains the effective path using the control packets like HELLO and RERR. This routing protocol works in the two steps[9]:

1- Route Discovery,
2- Route Maintenance and deletion.

The working of AODV routing protocol can be interpreted with the help of following example:

1-Route Discovery:
Let node ‘S’ is the source node and it wants to send the data packet to the node ‘D’ which is destination node. Therefore the node S will broadcast the control packet RREQ (Route Request) which will be received here by the intermediate nodes. After that the intermediate node will create a reverse route to the source by sending a control packet RREP (Route Reply) and an effective path will be created towards ‘D’.

2-Route Maintenance and deletion:
The AODV maintains the path using the control packet HELLO. Using this packet AODV checks that the path is still maintained or not. If not then it sends a control packet RERR (Route Error).Also if a path is not used for long time the AODV deletes it from its routing table.

6. GREEDY PERIMETER STATELESS ROUTING (GPSR)

GPSR is a well-known geographic routing protocol which uses geographic positions of nodes to make the routing path. It assumed that each node known its own geographical location using global positioning system (GPS). GPSR makes greedy forwarding decision using only information about router’s immediate node in the network topology. When a packet reaches a region where greedy forwarding is impossible the algorithm uses the concept of routing around the perimeter of the region by keeping state only about the local topology. GPSR [10] uses the greedy approach to find out the immediate neighbors, which works on the principle that the node which is closest to the destination. An example of Greedy node explained in the figure 5 .Here ‘**S**’ want to send a packet to the destination ‘**D**’.

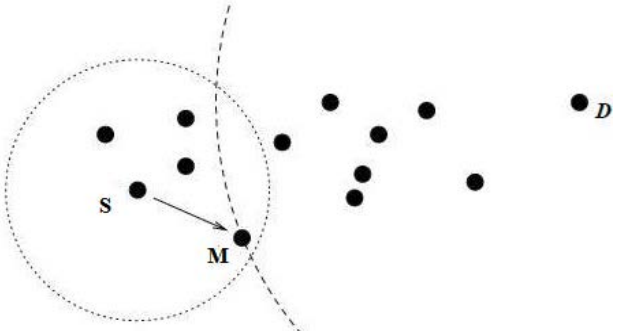


Fig 5. GPSR Routing Protocol working

S's radio range is denoted by the dotted circle and it forward the packet to '**M**', which is closest to the destination '**D**', the process continues until the packet reaches to the destination. In case of greedy failure or not receiving a packet from a neighbor for longer time than time out interval't', GPSR router deletes the neighbor from its table. Greedy forwarding is based only on knowledge of only forwarding node immediate neighbors. This helps WSN due to high Mobility of nodes. GPSR proposed the perimeter forwarding algorithm, but it's not an efficient, especially in urban area.

7. GPSR FUNCTIONALITY

GPSR protocol normally devised in to two groups:
1. Greedy forwarding: This is used to send data information to the closest nodes to sink.
2. Perimeter forwarding: This is used to such regions where there is no closer node to sink.
The proposed routing (GPSR) scheme is based on the energy consumption model to send a message to a base station. Source node is greater than the energy needed for a short range transmission. GPSR protocol is extended using aggregation node. Aggregation node is responsible for transmitting messages to the base station and routing is decided using the next hop member.
GPSR makes greedy approach for forwarding the packet using only information about immediate neighbors of router in the network topology.

- GPSR consists of two methods for forwarding packets:

1. Greedy Forwarding
2. Perimeter Forwarding

Greedy Forwarding is used to send data to the closest nodes to destination. Perimeter Forwarding is used where Greedy Forwarding fails

1. Greedy Forwarding

Find neighbors who are the closer to the destination forward the packet to the neighbor closest to the destination

2. Perimeter Forwarding

Apply the right-hand rule to traverse the nodes.
Pick the next opposite direction node.

7.1 Optimal Route Selection:

Procedure 1: route discovery

Input: ID of source node S and Destination node D
Outputs: optimal route from source to destination
Begin
if (ID D = ID N)
Forward packet to D;
Else
Determine the rectangle restricted searching area;
searching_area = [Xmin , Xmax , Xmin, Xmax];
broadcast RREQ to D in the searching_area;
Activate (BROADCAST_TIMER);
Calculate route probability of connectivity and packet delay;
if (p max – p other > E)
return route with the probability of connectivity pmax;
else
delete routes with the probability of connctivity p other < p max – p threshold;

return route with packet delay d min;
end if
end if
End of Route Discovery

7.2 Next-Hop Selection

Procedure 2: Next-Hop selection
Inputs: positions and speed of the neighbours
Outputs: The optimal next-hop forwarding node
begin
do
if (D forwarding_road_segment = D current_road_segment)
else
forward to the N intersection_node;
else
forward the packet directly to its farthest N neighboring_node;
while (forwarding node is not destination node);
forward packet to destination node;
end if
end if
end while
End of Next-hop Selection

8. SIMULATION AND METHEDOLOGY

8.1 Simulation Assumptions

The following assumptions are considered when build the TCL
1) For simplicity, all flows in the system are assumed to have the same type number of source node. Each sender has constant bit rate (CBR) traffic with the rate of data rate/number of stations packet per second.
2) The source node is 20,40,60,80, to 100 nodes with maximum connection is 20 nodes and if the nodes are varied for the calculation it is mentioned in area.
3) The implementation of GPSR routing protocols.

8.2 Configuration Table:-

PARAMETERS	VALUES
Operating System	Linux (Ubuntu 12.04)
NS-2 version	NS-2.35 (IEEE 802.11)
No. of Nodes	20,40,60,80,100
Radio propagation model	Propagation/TwoRayGround
Network interface type	Phy/WirelessPhy
Packet Size	1000
Traffic Type	TCP-CBR
Execution Time	10sec
Antenna Type	Omni-Antenna
Transmission Range	800*800 m
Frequency	914e+6
Receive Threshold	3.652e-10
Carrier Sense Threshold	1.559e-11
Node movement Threshold(v_i)	5/10/15/25/30 m/s
Initial Energy	100 joules
Performance parameters	Delay, Energy, Throughput, PDR, PLR, Overhead
Routing Protocol (Proposed)	AODV,GPSR , Greedy Forwarding Algorithm in ns-2.35

Table 2

9.RESULT AND ANALYSIS

The proposed work is simulated with the help of NS-2.35. The simulation parameters are given in table-2. The simulation table defines various parameters and regarding that values are defined. Simulation can be done using 20,40,60,80,100 nodes. The simulation area is 800*800 meter square. The AODV and GPSR routing protocols are used to route the hops using wireless network interface. The packet size of network is 1000.

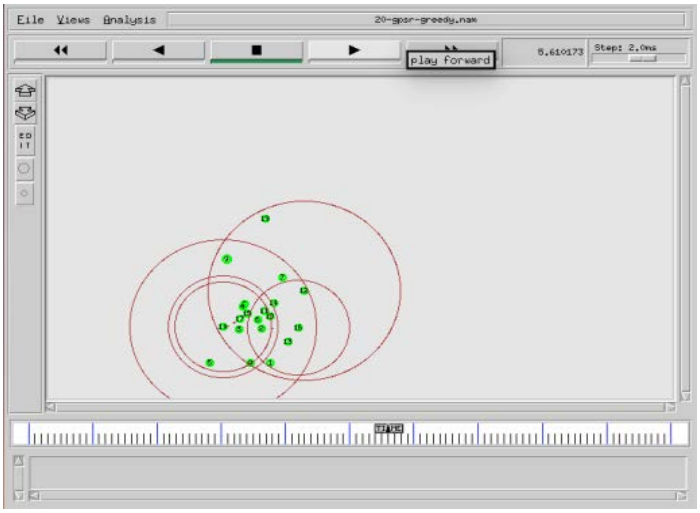


Fig 6. Network animator for Routing of 20 nodes in WSN

10. Performance parameters for comparison

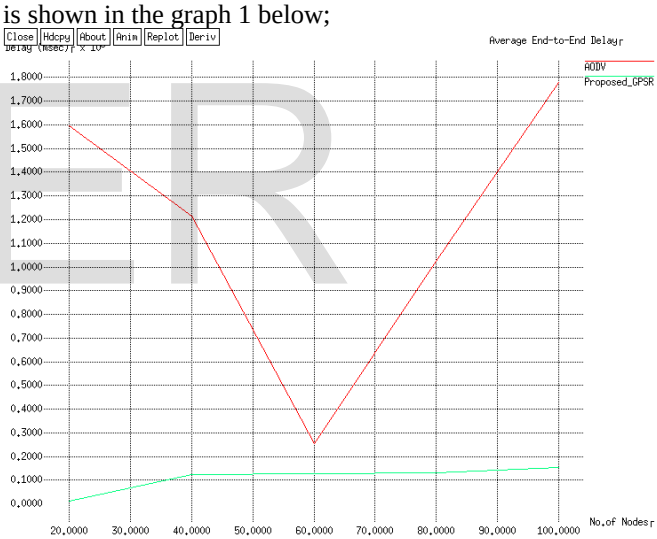
We will take six performance metrics for study on AODV and GPSR routing protocol that are End-to End delay, Energy Consumption, Routing Overhead, Packet delivery ratio, Packet loss ratio and Throughput for various number of nodes with high mobility.

10.1 End -to-End Delay

The average end-to-end delay of data packets is the time interval between the two that is data packet generation time and the time when the last bit arrives at the destination node during data packet transfer. A little amount of end-to-end delay is acceptable in any network whether wired or wireless.
This also can be defined as the average time interval required for transmitting a data packet from IP layer of source node to the IP layer of destination node, including transmission delay, propagation delay and queuing delay.

The Average End-to-End Delay of data transmission = Σ (Time when the data Packets enter in the Queue) - Σ (Time when the data Packet is received by destination)

The average end to end delay of AODV and GPSR in WSN is shown in the graph 1 below;



Graph 1

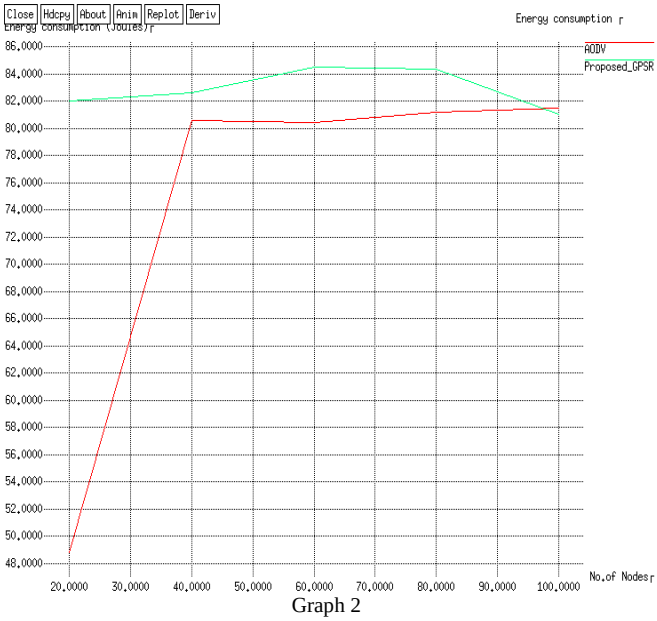
10.2 Energy Consumption

Energy Consumption of nodes can be defines as the average of the sum of the total energy consumed by each node during transmission.
This can be used to defines the life span of wireless sensor network and also can be used to define the reliability of that network
We calculate energy of nodes by the formula-

Energy Consumption = Sum of x and y coordinates/Total number of nodes participating network

Here in the Graph 2 the average energy consumption by nodes is shown; here in the graph red line represents the energy consumption while using AODV protocol and the

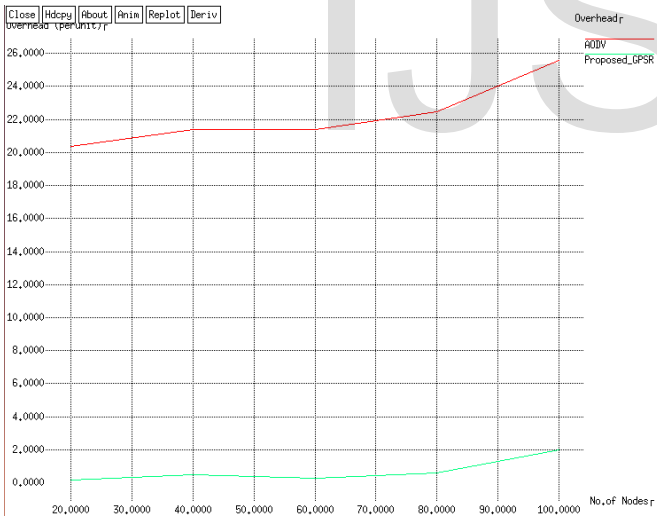
green line represents the energy consumption while using GPSR routing protocol.



Graph 2

10.3 Routing Overhead

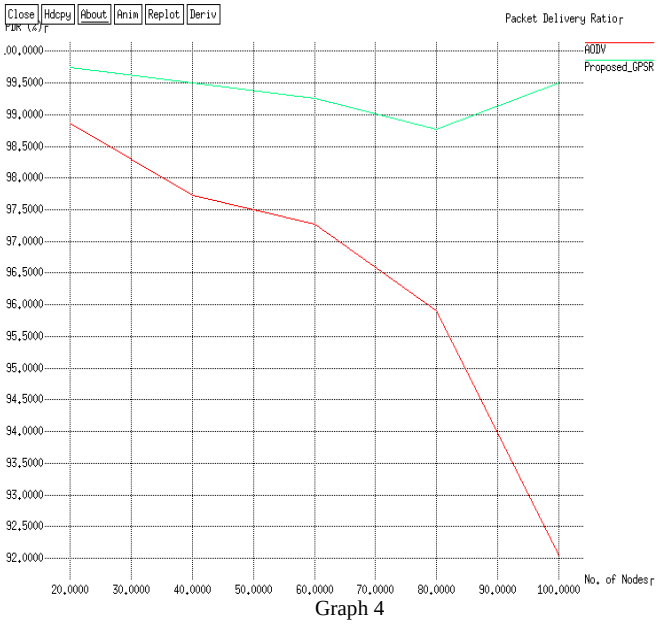
The routing overhead in the network is defined as the network congestion (traffic load) while the transmission is taking place. The overhead may be for control packets or may be for data packets. Here the overhead in both Protocols is shown below in graph 3.



Graph 3

10.4 Packet Delivery Ratio

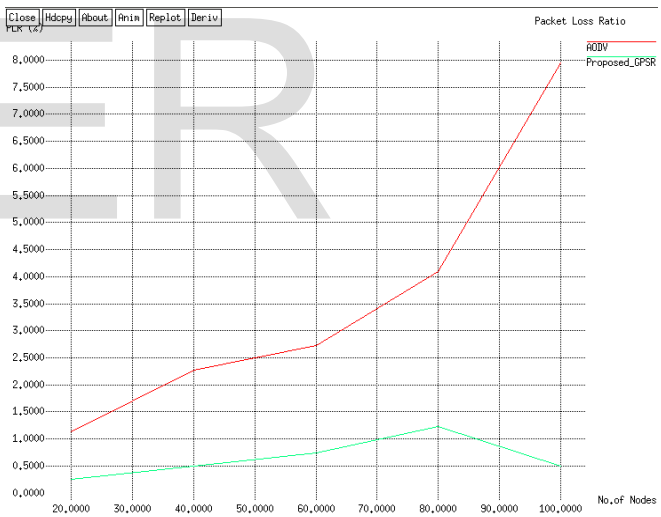
Packet Delivery Ratio (PDR) is the ratio of the number of packets transmitted by the traffic source (Sender nodes) and the number of packets received by traffic sink (Receiver nodes).It measures the loss rate as seen by transport layer protocol .It characterizes both the correctness and efficiency of ad-hoc routing protocols and the geographical routing protocol. A high packet delivery ratio is required in any network. Here the packet delivery ratio of both the protocols is shown below that is of AODV and GPSR in graph 4.



Graph 4

10.5 Packet Loss Ratio

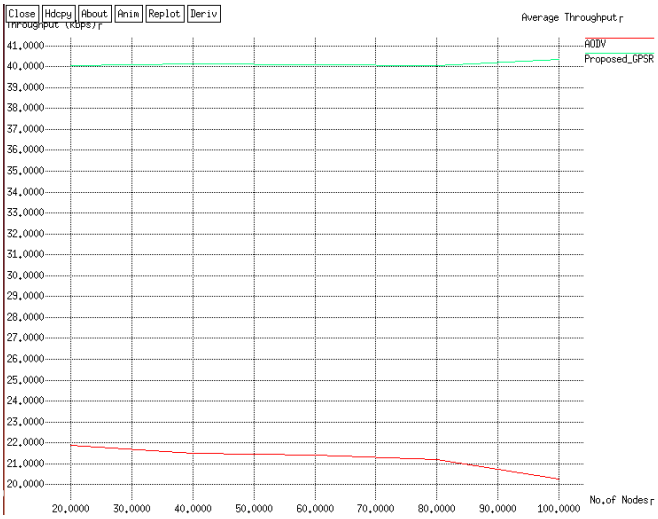
The packet loss ratio is defined as the ratio of packet lost with the total number of packets sent. Packet loss may occur when one or more packets (may be controlling packet or may be data packet) travelling across computer network fail to receive by their destination.



Graph 5

10.6 Throughput

Throughput is the number of packets that are passing through the communication medium in a particular time interval. This performance metric determines the total number of packets that have been completely delivered from sender node to receiver node and it is directly proportional to the density of node that is it can be improved with increasing density of node



Graph 6

11. CONCLUSION AND FUTURE WORK

In this paper we have studied about the WSN protocol and the various routing protocols like AODV, Secondary path AODV, GPSR and optimal path GPSR and various performances metric like end to end delay, Energy Consumption, Overhead, packet delivery ratio, packet loss ratio and throughput and in various Environments.

In future we can simulate the above mentioned routing protocols with the same performance metrics with varying the mobility model and conclude their performance that how they behave with mobility model and packet sizes.

12. REFERENCES

[1] T. Haenselmann, "An FDL'ed Textbook on Sensor Networks", April 2006, http://pi4.informatik.uni-mannheim.de/~haensel/sn_book/. Retrieved in November 2009.

[2] Akyildiz, I.F.; Su, W.; Sankarasubramaniam, Y.; and E. Cayirci., "A survey on sensor network", IEEE Communications Magazine 40(8), 102–114, 2002.

[3] Callaway, E.H., "Wireless Sensor NetWork: Architechture and Protocal", CRC Press LLC, Boca Raton, pp. 41–62, 2004.

[4]Liu, H.; Nayak, A.; and Stojmenović, I., "Fault Tolerant Algorithms/Protocols in Wireless Sensor Networks", in Guide to Wireless Sensor Networks , Misra, S.; Woungang, I.; Misra, S. C., Eds. Springer, New York, pp. 261-291, 2009.

[5] I. Chakeres, and L. Klein-Berndt, "AODVjr, AODV Simplified", Mobile Computing and Communications Review, Vol. 6, No. 3, pp. 100-101, July 2002.

[6] C. E. Perkins, E. Belding-Royer, and I. Chakeres, "Ad hoc On-Demand Distance Vector (AODV) Routing", draftperkins-manet-aodvbis-01, IETF Internet Draft (Work in progress), February 2004.

[7] Tarun Agarwal "Wireless Sensor Network Architecture and its Application" https://www.elprocus.com/architecture-of-wireless-sensor-network-and-applications/(Accessed 2018)

[8]Akshai Aggarwal,Savita Gandhi; "PERFORMANCE ANALYSIS OF AODV, DSDV AND DSR IN MANETS" International Journal of Distributed and Parallel Systems (IJDPS), November 2011, pp: 167-177.

[9]Prashant Kumar Maurya ,"An Overview of AODV Routing Protocol", International Journal of Modern Engineering Research (IJMER) www.ijmer.com Vol.2, Issue.3, May-June 2012 pp-728 732 ISSN: 2249-6645

[10] B.Karp, and H.T. Kung. GPSR: greedy perimeter stateless routing for wireless networks. In MOBICOM'00, pages 243–254, Boston, Massachusetts, United States, 2000.