Comparative Analysis of Routing Protocol in Wireless Mesh Network using NS3

Sheenam[1], Prof Dr Divya Midhun[2], Prof. (Dr.) Sanjay Kumar Singh[3]

[1] Lincolon University, Malaysisa , Lincolon University, Malaysisa, Amity University UP Lucknow Campus,

Email ID : [1]pdf.sheenammiddha@lincoln.edu.my; [2] divya@lincoln.edu.my; [3] sksingh1@amity.edu

Abstract: To construct any wireless network, the two main methodologies are routing and protocol selection. The protocol that is used for a Mobile hoc network (MANET) should have the best data delivery and data integrity. Therefore, the most important step before choosing a protocol is to analyze its performance. Adhoc On-demand Distance Vector, Dynamic Source Routing, Optimized Link State Routing, and Destination Sequenced Distance Vector protocols are the subjects of performance investigation in this paper utilizing NS3 simulator. The functioning of the aforementioned protocols is typically compared on the basis of standard metrics: packet delivery ratio, delay, throughput of network.

Keywords: DSDV, DSR, OLSR, AODV

1 Introduction:

Routing protocols, which act as the intelligence that determines the route data packets take from their source to their destination, are essential components of wireless networks.These systems regularly evaluate network conditions to identify optimal paths while addressing the unique challenges of wireless environments, such as mobility and signal unpredictability's MANET protocols like AODV and DSR, routes are established as needed. Mesh networks preserve connectivity among far-off nodes by using hybrid approaches like HDMP. Directly affecting network performance metrics, including throughput, latency, and dependability, is the efficacy of wireless routing techniques. Notwithstanding their inherent instability, these techniques dynamically adapt to changing network design, manage intermittent connections, and balance traffic loads, therefore offering efficient data transport. Modern wireless routing systems use machine learning techniques more and more to predict network changes and modify routing decisions depending on past data, hence enhancing performance in complex wireless environments [1].

As the navigational framework of networks, routing protocols enable constant communication and data transfer between transmitters and receivers via linked systems. These protocols essentially define the rules and strategies controlling the information flow among routers and the selection of best paths for data packets crossing the network topography. Every router has a specialized routing table that first only contains data about directly connected networks, therefore limiting its immediate environment. By first exchanging topological information with nearby nodes and then throughout the whole network, routing protocols help to distribute topological knowledge and hence lead to a complete understanding of the general network structure. By means of this cooperative intelligence, routers can transfer packets along effective paths without prior knowledge of remote network components, hence enabling informed forwarding decisions. To determine the best path in real-time, the protocol's decision-making algorithms evaluate several criteria, including hop count, bandwidth availability, and network dependability. Routing protocols are fundamental in hybrid allocation systems for dynamically allocating traffic among several alternative channels, reacting to changing network conditions, and preserving effective resources [2].

1.1 Types of Routing Protocol

There are three main types of routing techniques utilized in wireless communication.

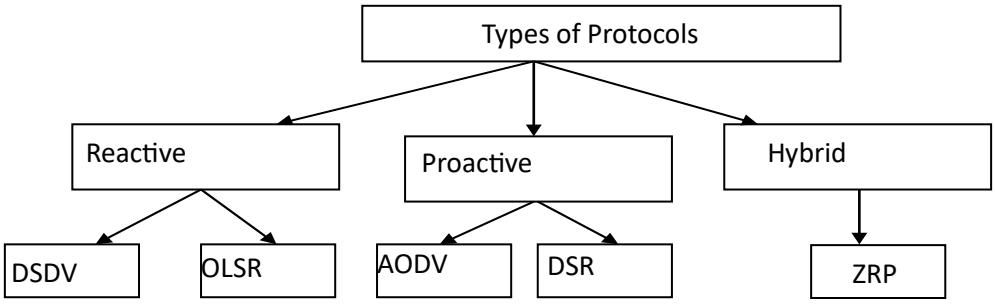

Figure 1: Types of Protocols

1.1.1 Reactive Routing

It is based on a table-driven technique, and each router keeps track of the paths leading to the destination clients present on the R-table. As a result, even if they are not required, routes are computed and cached to reduce overhead and bandwidth consumption by reducing the number of messages exchanged to preserve up-to-date routing information. For big and dynamic networks, this protocol is ineffective.

- **Destination-Sequenced Distance Vector (DSDV)**

  This protocol is extended version of Routing Information Protocol (RIP). It has additional attribute, sequence number and retain a routing table for each entry with the help of these updated information of route it prevents from the network loop holes.

- **How Routing Occurs In DSDV??**

  In DSDV [13], each router maintains a routing table that consists of the number of neighbor nodes, the destination node, and the sequence number. This protocol uses the concept of dynamic topology, which every time maintains a new route to mitigate the data packets to the terminal node, deploying broadcasting and updating the information in the routing table.

  Those nodes that will receive the packets increment the metric every time, and an iterative process is followed until all nodes receive the updated packets with metric count. On receiving multiple packets from the same source node, the waiting time should be initiated [3].After the waiting period, the route selection is done considering the minimum value of the metric.

  .

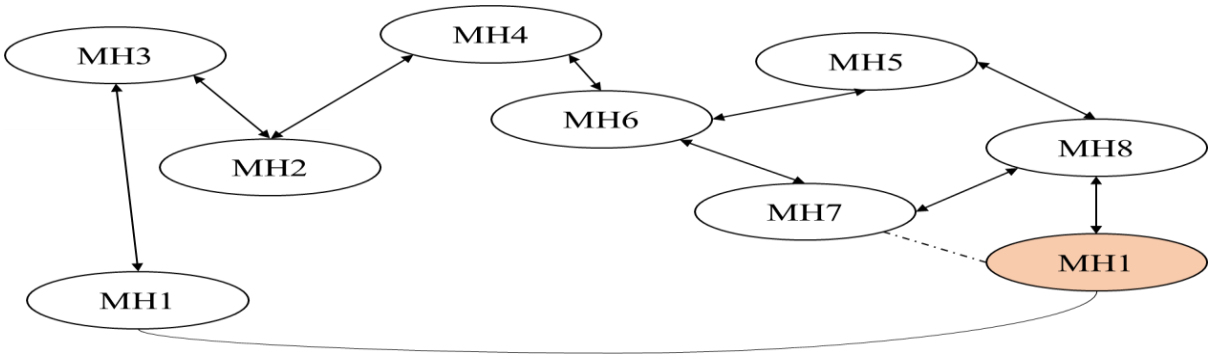

Figure 2: Example of DSDV

In Figure 2, all the nodes are connected to each other for sending data from one node to another node. Which maintains a routing table with four parameters, i.e., destination node, next hop, metric, and sequence number. The MH4 node, as depicted in the table below, traverses all the data from source to destination.

Table 1: R-Table of various Nodes

Destination	**Next Hop**	**Metric**	**Sequence Number**
DN1	NH2	3	S401_DN1
DN2	NH2	2	S123_DN2
DN3	NH2	2	S561_DN1
DN4	NH4	0	S321_DN3
DN5	NH6	2	S471_DN4
DN6	NH6	1	S4343_DN5
DN7	NH6	2	S1231_DN6

In this table after receiving a data from each node, destination node sends an advertisement message for confirmation of data with sequence no.

Table 2: Advertisement from NH4

Destination	Next Hop	Metric	Sequence Number
NH1	NH2	2	S401_DN1
NH2	NH2	1	S123_DN2
NH3	NH2	2	S561_DN1
NH4	NH4	0	S321_DN3
NH5	NH6	2	S471_DN4
NH6	NH6	1	S4343_DN5
NH7	NH6	2	S1231_DN6
NH8	NH6	3	S101_DN7

DSDV routing uses sequence numbers on route table entries to improve traditional RIP. These sequence numbers serve as timestamps, allowing mobile nodes to separate current from old routing data. After updates, nodes choose paths with better sequence numbers, therefore preventing routing loops in dynamic ad hoc networks defined by frequent topological changes. DSDV can keep exact routing paths with this simple improvement even in node mobility [4].

- **Optimized Link State Routing Protocol (OLSR)**

  The OLSR protocol system is a prominent Internet routing protocol that enhances the performance of mobility-based networks. This protocol is categorized as a proactive network routing protocol, sometimes referred to as a table-driven routing protocol. This protocol employs the control message below to identify nodes and disseminate connection state information among them. This enables the alteration of paths utilizing the shortest routes that an ad hoc network might potentially traverse.

  (a) A control message called HELLO that is used to find the node that is one or two hops distant from the response. Depending on which hop node has the shortest path to the subsequent hop nodes, the sender selects multipoint relay (MPR).

  (b) In an ad hoc network, multipoint relay (MR) and TOPOLOGY CONTROL (TC), an OLSR control message, are transmitted to disseminate information about surrounding nodes.

1.1.2 Proactive Routing

It works with on-demand routing protocol with the help of that route is discovered by flooding the route request to all other nodes and cache is maintained with all the source and destination routes [5].

- **AODV PROTOCOL**

  This protocol establishes routing information based on demand or requirement rather than maintaining it in advance. It is known as the "on-demand routing protocol" because of its nature. It is based on the distance vector routing technique, in which every node keeps a routing table populated with the next hops' routing information that is shared by its neighbors. On the target path, the next hop additionally contains information about its neighboring router. Based on requirements, the minimal distance between two nodes is computed and modified on matching routing tables. If a route record is not utilized or revived after a set amount of time, it will be removed. Additionally, it employs a technique based on sequence numbers to guarantee the constant availability of a network devoid of loops. AODV integrates four control messages for route discovery and maintenance, which are as follows:

- **1.14.1 How AODV Route Discovery works??**

  1**. Route Request (RREQ)**: When a node does not have a path to the target node, it uses the RREQ message to request one. Usually, the message is disseminated throughout the network. A route is chosen based on the RREQ's reachability to the target or mediator node. Several parameters are included in the RREQ message, including the broadcast ID, source and destination addresses, the sequence number of the source node, and the target node's last observed sequence number. (Sender Address, Sender Sequence Number, Broadcast Identifier, Receiver Address, Receiver Sequence Number, Number of Hops) (1) We use the pair source_address and broadcast_id to uniquely identify RREQ. The source increments the broadcast_id by one with each new request. The network's neighbors can broadcast Route Requirement (RREQ) to other neighbors or send Route Reply (RREP) signals back to the source [6].

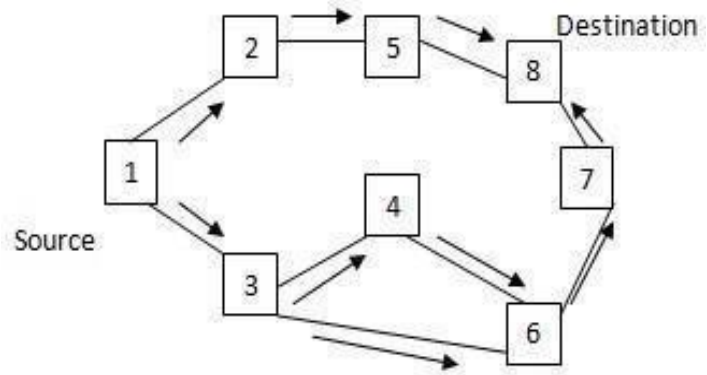

Figure 3: Data Transmission from source to destination

2. **Route Reply (RREP):** Any node that detects a fresh path to the destination or acts as the destination itself sends a unicast route answer message to the originator in response to the route inquiry message. These response messages use symmetric links and track the opposite direction of the related route inquiry. Upon query reception, every intermediate node in the transmission network changes its routing database with destination information. Should the query be processable and the destination or any intermediary node lack a suitable path back to the source, a route response message is sent nevertheless. As seen in (2), the composition of this response message consists of origin_address, target_address, target_sequence_number, number_of_hops, and validity_duration. (2) Every node in the communication channel generates a forward pointer to help the route answer to be returned to the origin. Should a node not be part of the approved path from the source to the destination, the response message is denied after a 3000-millisecond timeout.

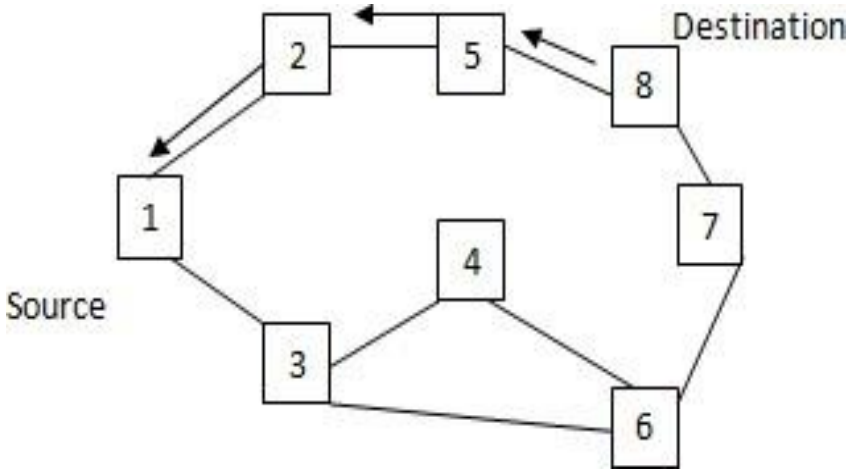

Figure 4: Reply Transmission from source to destination

3. Route Error (REER): A route failure signal is sent to notify the network of the disrupted links when one or more destination nodes become inaccessible from the source. When a node detects a disconnection, it signals its nearby neighbors with a route error alert. After that, the nearby nodes distribute the alarm around the network, mostly concentrating on those nodes whose active data paths might have been disturbed by the severed link.

4. HELLO: A hello message is being sent out to nearby nodes in order to verify network connectivity. Because it returns a path or link along with a variety of node-related information, this message is sometimes referred to as a link status message.

- **Routing Table:**

Table 3: Route Discovery and Response Details

Node ID	Broadcasted RREQ To	Hop Distance	Target Node	Returned RREP Path
1	Node 2	1	Node 8	1 → 2 → 5 → 8
2	Nodes 1, 2, 5	2	Node 8	2 → 5 → 8
5	Nodes 1, 2, 5	1	Node 8	5 → 8
8	1 → 2 → 5 → 8	3	Node 8	-

AODV protocol maintains a routing entry in the form of table and it notified all the neighbors regarding the route breakage and route failure. It maintains all the information on the basis of route discovery and route reply and store the information in routing table.

- **DSR:**

DSR is a straightforward and effective routing technology created especially for use in mobile node multihop wireless ad adhoc networks. It lets nodes dynamically build a source route over many intermediary hops to any destination inside the ad hoc network. Afterwards, the header of every transmitted data packet includes the entire ordered list of nodes it must pass through. This approach makes packet routing almost loop-free and eliminates the necessity for the intermediate nodes that the packet is routed through to have up-to-date routing information. Other nodes that forward or overhear any of the packets can simply cache this routing information for later use because it is included in the header of each data packet. DSR combines route maintenance and discovery, performing them only when necessary [7-8].

1. To find the best way from the source to the destination, the network uses route discovery. Every node has a cache with past obtained routing data. The source first checks this cache for a legal path when it plans to broadcast data. Should such a path exist, it is followed to deliver the message. The node starts the pathfinding process in the lack of a found path.

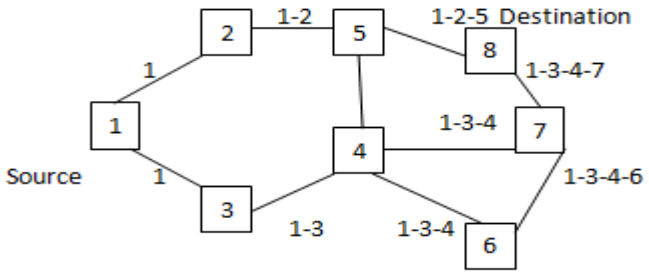

Figure 5: Optimal route selection from source to destination

2. On the other hand, route maintenance works to keep a path free of loops such that optimality is guaranteed regardless of route changes. Additionally, it guarantees that paths from the source to the destination are always being monitored and available. The route cannot be used for packet transmission if any hops are shifted or cease to function; in such an event, the route discovery process must be repeated in order to preserve the route. The DSR does not broadcast frequent messages, just like any other protocol. Because of this, DSR produces the fewest number of overhead packets.

2. Simulation and Results Analysis

This section of the study assesses the performance of an ad hoc network utilizing several routing metrics and investigates the influence of routing protocols inside a working ad hoc environment via a controlled series of simulations. The simulations were performed utilizing Network Simulator (NS) version 3. The findings derive from an evaluation of critical parameters designed to elucidate the impact of the Blackhole attack on the functionality of routing algorithms in ad hoc networks. The subsequent criteria are regarded as metrics for performance evaluation [9-10].

2.1 Network Simulation Environment:

The Network Simulator version 3 (ns-3) is a robust discrete-event network simulator utilized for research and educational purposes in networking. Authentic channel and propagation models are employed to simulate wireless communication among sensor nodes. The Two-Ray Ground model is employed to determine the strength of the received signal. An omnidirectional antenna is configured to transmit signals in all directions. The Wireless Mesh Network employs the Ad-hoc On Demand Distance Vector (AODV) routing protocol to manage route discovery and maintenance in response to dynamic changes.

Table 4: Simulation Environment Parameters

Simulator	NS-2.35
Channel Type	Wireless Channel
Mobility Model	Two-Ray ground Radio Propagation Model
Network Interface Type	Wireless Phy/IEEE 802.11
Antenna Model	Omni-directional
Number of mobile-nodes	15
Routing Protocol	AODV, DSDV, DSR, OLSR
Simulation Time	50 sec
Network Size(m*m)	1000 *1000
Network	Wireless Mesh Network

2.2 Performance Metrics:

Performance metrics are quantitative indicators that demonstrate the operational efficiency, reliability, and effectiveness of a network or system during simulations.

a. **Delay**: It is the time required for informational packets to transit from the network's source node's application layer to the valid destination node's application layer. It is also known as average end-to-end latency when used as a parameter.

$$\text{Total Delay}=T_D + P_D + TP_D + Q_D \quad \text{.....(1)}$$

In equation 1 T_D represents Transmission Delay, P_D is Propagation Delay,TP_D Processing Delay , Q_D queue delay.

b. **Packet Delivery Ratio**: It is the percentage of data packets delivered to a legal destination node to the total number of data packets transmitted by the originating source node. It is the rate of data packets arriving from the source node compared to the rate of actual data packets arriving.

$$\text{Packet Delivery Ratio}= \frac{P_1+P_2+P_3.....P_n}{T} \quad \text{.....(2)}$$

In equation 2 $P_1 \ldots . P_n$ represent number of packets successfully delivered and T represent the total packet sentThis ratio is usually expressed as a percentage.

c. **Throughput**: It is a series of effective data packet relays from a mobile network's source node to a destination node via a communication channel.

$$\text{Throughput}=\frac{\sum_{k=0}^{n} P}{T} \quad \text{.....(3)}$$

In equation 3 p represents the total packets from o to n and T represents the total time taken. In networking, this could be calculated over a specific period, considering the number of bits or packets successfully transmitted over the network during that time.

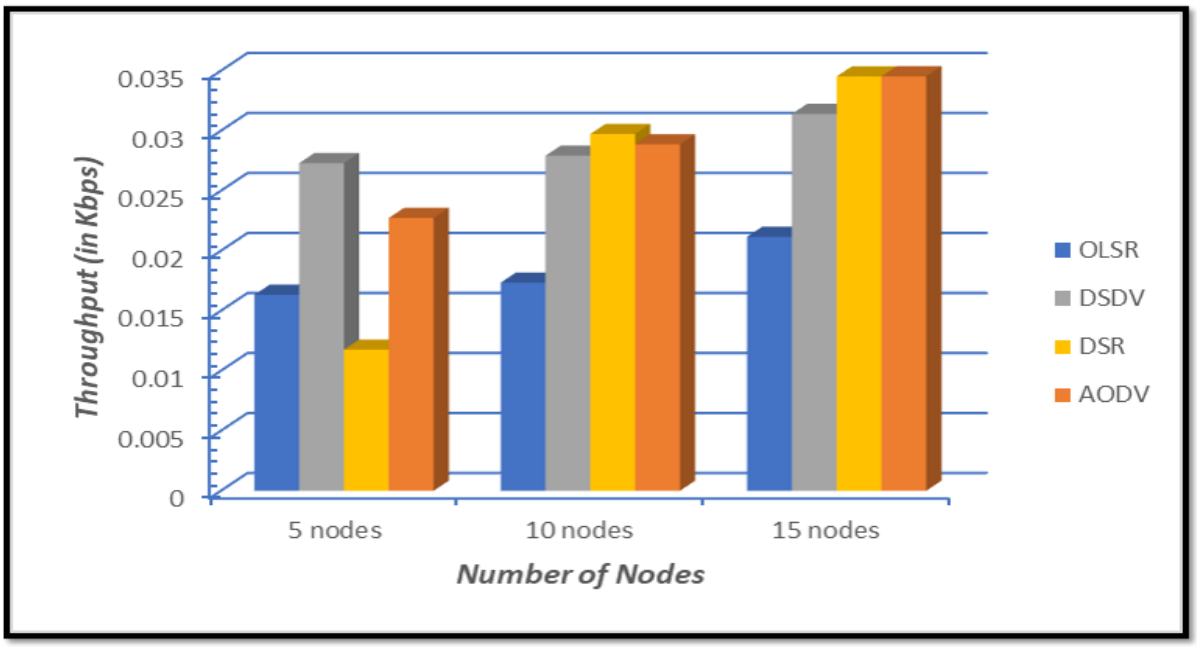

Figure 6: Throughput analysis with varying nodes

The figure 6 illustrates the throughput performance of four routing systems at varying node numbers. AODV has superior throughput relative to OLSR, DSR, and DSDV, signifying its efficacy in managing elevated network demand.

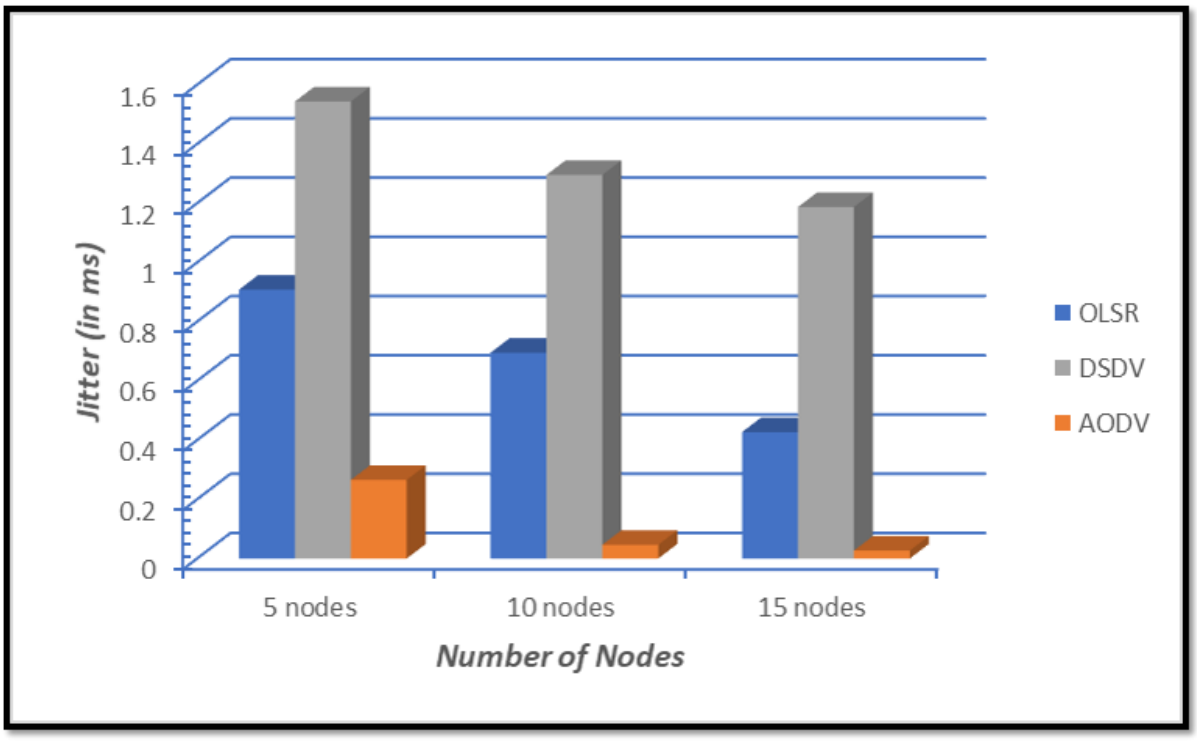

Figure 7: Jitter analysis with varying nodes

The figure 7 above shows a performance analysis of protocols based on jitter levels across different node counts. In all cases, the OLSR protocol has less jitter than the DSDV and AODV protocols.

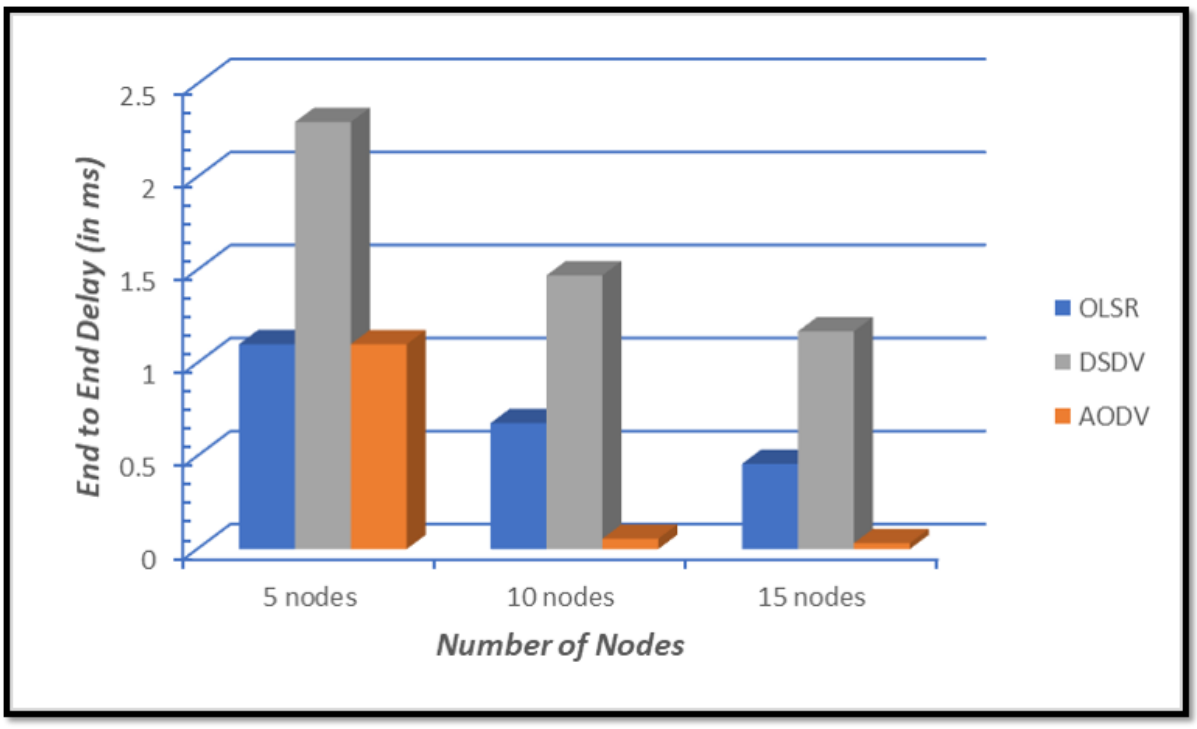

Figure 8: Delay analysis with varying nodes

Figure 8 depicts the end-to-end delay with different node counts. For optimal performance, there should be minimal end-to-end delay. The end-to-end delay for OLSR is consistent regardless of the number of nodes, and is significantly lower than that of other protocols.

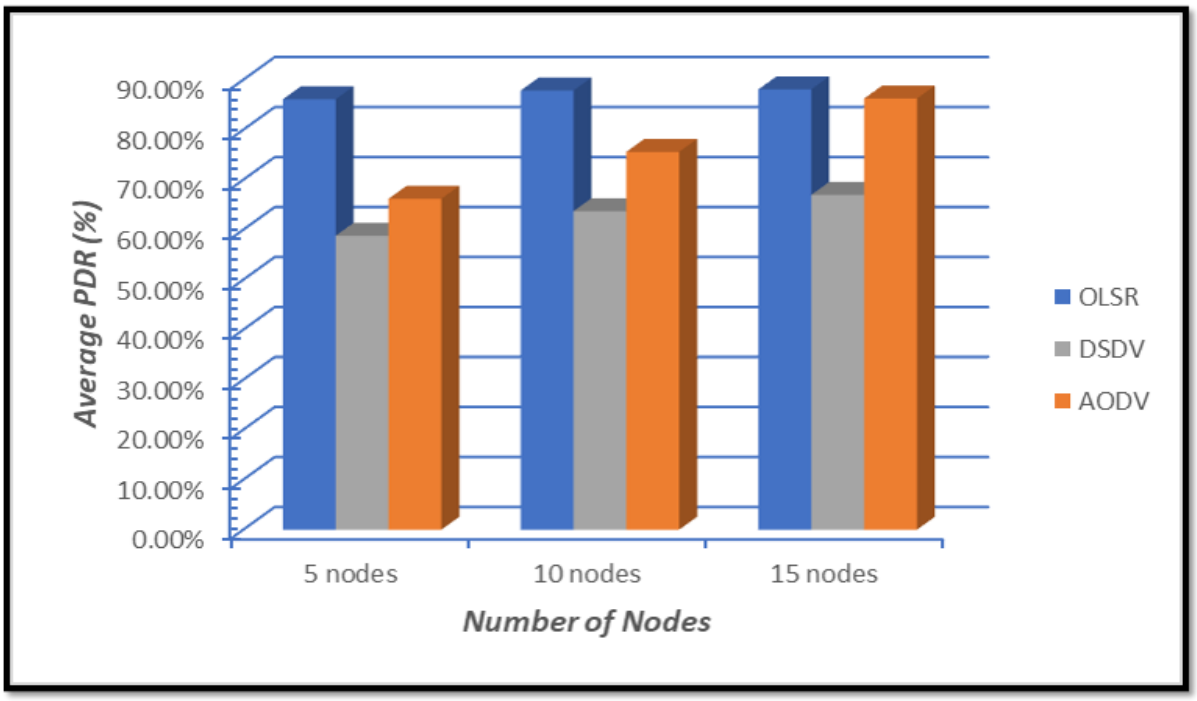

Figure 9: PDR analysis with varying nodes

Figure 9 illustrates how PDR varies with the number of nodes. Increasing the number of nodes leads to higher packet delivery ratios in all cases. OLSR protocol consistently outperforms AODV in terms of packet delivery ratio.

Conclusion:

This paper compares three protocols' performance on parameters such as packet delivery ratio, end-to-end delay, jitter, and throughput. Simulation results show that AODV outperforms competing protocols in terms of throughput for networks with different numbers of nodes. The OLSR protocol outperformed the other two protocols in terms of packet delivery ratio, packet drop rate, jitter, and end-to-end delay.

References:

[1] Saravanan, S., Poovazhaki, R. & Shanker, N.R. Cluster Topology in WSN with SCPS for QoS. *Wireless Pers Commun* 99, 1295–1314 (2018). https://doi.org/10.1007/s11277-017-5185-0

[2] Sheenam and R. Chadha, "A novel approach for channel assignment using optimization technique in wireless networks," in *2024 International Conference on Emerging Smart Computing and Informatics (ESCI)*, 2024, pp. 1–5.

[3] Sheenam and R. Chadha, “Efficient channel allocation for load balancing in wireless mesh networks,” in *2024 International Conference on Integrated Circuits, Communication, and Computing Systems (ICIC3S)*,vol. 1, 2024, pp. 1–4.

[4] Sheenam and R. Chadha, “A novel hybrid routing algorithm for upgrading network efficiency,” in *2023 First International Conference on Advances in Electrical, Electronics and Computational Intelligence (ICAEECI)*, 2023, pp. 1–5.

[5] Sheenam and R. Chadha, “Performance enhancement in data transmission over wireless network,” in *2022 Second International Conference on Computer Science, Engineering and Applications (ICCSEA)*, 2022, pp. 1–5.

[6] Sheenam and R. Chadha, “A hybrid framework for routing and channel assignment in wmn’s,”*Indonesian Journal of Electrical Engineering and Computer Science*, vol. 34, no. 2, pp. 1226–1234, 2024,doi: 10.11591/ijeecs.v34.i2.pp1226-1234.

[7] Feng, Y., Wang, Y., Zhang, B., & Zhou, L. (2025). Deep Reinforcement Learning-Based TCP Congestion Control in UAV-Assisted Wireless Networks. Presented at the 2023 International Conference on Wireless Communications and Signal Processing (WCSP), Hangzhou, China, pp. 862-867. doi: 10.1109/WCSP58612.2023.10404994.

[8] Gupta, A., et al. (2025). Q-Learning-Based Congestion Avoidance in Wireless Mesh Networks. Published in ACM SIGCOMM 2025.

[9] Liu, X., et al. (2024). Federated Learning for Congestion Control in Wireless Networks. IEEE Transactions on Networking.

[10] Li, Y., et al. (2020). Traffic-Aware Load Balancing Algorithm for Wireless Mesh Networks. IEEE Wireless Communications.