

# A Comparative Analysis of Channel Switching Latency for OLSR Routing Protocols in Conventional and SDN Multi-Hop Wireless Mesh Networks

Megha Satija<sup>1</sup>, Md. Ejaz Aslam Lodhi<sup>2</sup>

<sup>1</sup>Department of Electronics & Communication, Indira Gandhi Delhi Technical University for Women University, Delhi, India

<sup>2</sup>Assistant Professor, Department of Electronics & Communication, Indira Gandhi Delhi Technical University for Women University, Delhi, India

**Abstract:** *OLSR that uses channel switching systems with multi hop-based and energy-aware routing protocol to establish stable/reliable routes in HMWNs. OLSR combines multi-hop and multi radio with a channel switching-based and energy-aware routing protocol. The channel switching system is important to evaluate the nodes in terms of latency and route discovery in forwarding packets in terms of multi-dimensional data generated values are calculated for each node and developed for two methods as conventional and SDN is used to send the packets through highly channel switched nodes having sufficient energy to minimize the possibility of breaking the route. This protocol is implemented over the Wireless Mesh Networks and simulated using Matlab. Performance evaluated from the parameters such as delay, energy consumed and throughput.*

**Keywords:** Channel switching, OLSR, Route discovery, Latency, SDN-Software Defined Networks, WMN-Wireless Mesh Networks

## 1. Introduction

The Mesh networks rewards the nodes that relay others' packets and charges those that send packets. The channel switching system evaluates the nodes' competence and reliability in relaying packets in terms of multi-dimensional channel switching values. The channel switching values are attached to the nodes' AES key to be used in making routing decisions. We develop a software based networks routing protocol OLSR to direct traffic through those highly-channel switched nodes having sufficient energy to minimize the probability of breaking the route. The proposed routing protocol is based on AODV. But the complexity is high since security parameters carried in RREQ is broadcasted and more energy is consumed. So we will use reactive geographic routing protocol to reduce the complexity and reduce energy consumption[1] WirelessMesh systems have the consequent attributes:

- It comprise of sensor nodes with some level of vitality can keenness their own particular remaining vitality and have the comparative design and One Base Station (BS) without vitality requirement is removed far from the region of sensor nodes.
- All sensor nodes are stationary. They utilize the straight communication or multi-bounce communication to speak with the BS.
- Sensor nodes sense air at a settled rate and at consistent times have information to transmit to the BS.
- Sensor nodes can alter the transmission vitality of wireless transmitter on the premise of the separation.
- The lifespan of WSN is the aggregate sum of time before the primary sensor node comes up short on power. [2]
- To design the channel switching multi hop networks for generate proficient latency
- Main goal is to meet the necessity of stretching out lifetime is to propose energy proficient routing algorithms that incorporate the objective to adjust the heap in the midst of the sensor nodes in the system.
- To enhance the routing protocol OLSR for SDN working under mesh networks than other conventional methods
- To compare the enhanced SDN and conventional with implementing OLSR routing protocol in terms of delay, energy consumed and throughput parameters

With a specific end goal to meet the necessity of stretching out lifetime is to propose vitality proficient routing algorithms that incorporate the objective to adjust the heap in the midst of the sensor nodes in the system. At the point when the workload of a node is the comparable as that of further nodes, then the remaining vitality of every node will decrease at the comparable rate with system capacity. [3]

The transmission reach is controlled by the transmission force and the radio proliferation properties. By expanding the transmission extent, shrouded station issue happens less every now and again however the uncovered station issue turns out to be more vital as the TX reach distinguishes the zone influenced by the single transmission. Notwithstanding the transmission range, additionally the Physical bearer detecting extent and the impedance range must be considered to effectively comprehend the conduct of Mobile systems [4]. Objectives of the thesis are as follows:

## 2. Background of the Problem

OLSR protocol establishes the shortest route that can satisfies the source nodes requirements is trusted enough to act as a relay. In this protocol the source node embeds its requirements in the RREQ packet, and the nodes that can satisfy these requirements broadcast the RREQ packet, the source node broadcasts RREQ packet. The RREQ packet contains the identities of the source and destination nodes, the maximum number of intermediate nodes, hop and energy requirements and the source node's signature and certificate then the source node is trust requirements are verified at each intermediate node can have low sink packet count, then verified at each subsequent intermediate nodes till it reaches at the highly trusted nodes. These verifications are necessary to ensure that the packet is sent and relayed by genuine nodes and the nodes can satisfy the trust requirements because their sink packet count are signed by networks.

The intermediate node signs the packet's signature forming a chain of signatures of the nodes that broadcast the packet. This signature authenticates the intermediate node and proves that the node is the certificate holder and thus the attached sink packet count belongs to the node. The signature also enables the trust system to make sure that the intermediate nodes have indeed participated in the route to hold them responsible for breaking the route. Finally, the intermediate node broadcasts the packet after adding the signature chain and its identity and certificate. If a node receives the same request packet from different nodes, it processes only the first packet and discards the subsequent packets. The destination node composes the RREP packet for the route traversed by the first received RREQ packet, and sends it to the source node. This route is the shortest one that can satisfy the source node's requirements. The source node's requirements cannot be achieved if it does not receive the RREP packet within a time period. It can initiate a second RREQ packet but with more flexible requirements. The source node verifies the hash message and the node's certificates to make sure that the nodes satisfy its trust requirements and the future destination node was reached, then it starts data transmission.

## 3. Related Work

Related studies are as follows:

Reputation-based schemes [8] experience the ill effects of false allegations where some genuine nodes are dishonestly recognized as vindictive. This is on the grounds that the nodes that drop packets briefly, e.g., because of blockage, might be dishonestly distinguished as vindictive by its neighbors. With a specific end goal to decrease the false allegations, the plans ought to utilize tolerant limits to ensure that a node's packet dropping rate can just achieve the edge if the node is malicious.

In [9], payment is utilized to frustrate the balanced packet dropping assaults, where the assailants drop parcels since they don't profit by transferring packets. A notoriety framework is additionally used to recognize the silly parcel dropping assailants once their packet dropping rates surpass a threshold.

For the proxy discovery, Luo et al. [10] proposed two algorithms eager and on-interest proxy disclosure algorithms. When all is said in done, the covetous proxy revelation protocol is proactive and the on-interest proxy disclosure protocol is latent. The ravenous proxy revelation requires an insatiable way to achieve aproxy customer with high HDR downlink channel rate. An insatiable way is built by a mobile customer sending the course ask for message (RTREQ) to its neighbor customer with the best HDR downlink channel rate for every hop. In any case, this avaricious way may not generally find the proxy customer with the best general channel rate for the destination customer.

## 4. Proposed Methodology

### a. Experimental Design

A parallel event driven simulator, MATLAB was utilized for comparing the results of protocols. Simulation experiments were run on computer installed with MATLAB with impacts of speed of simulation and network size on the trial results. Mean end-to-end delay, energy consumed and throughput as measured by the amount of control packets made for routing are the execution lattices that were used to consider the two different approaches i.e. conventional and SDN.

- 1) Mean end-to-end delay: Average time taken for a packet to take off from source to end of the line including course securing delay.
- 2) Energy consumed: Energy consumed for control packets made for routing.
- 3) Throughput: the total number of control packets transmitted by the source node to destination node.

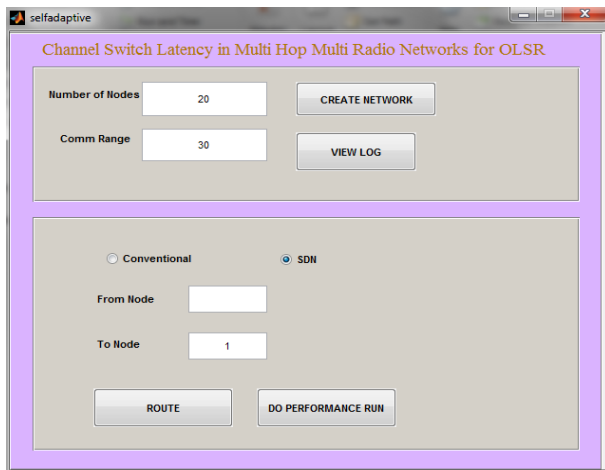
Mean end-to-end delay, energy consumed and throughput were measured for rate of reproduction in analysis 1 and system size were for three unique levels of packet delivery in research 2. Steady bit rate generator was utilized for creating packets of altered size. [52] Three unique sorts of movement load were utilized for simulation experiments, for example,

- 1) Low traffic load – one packet transmitted every 10 seconds.
- 2) Medium traffic load – one packet every second and
- 3) High traffic load – one packet every 0.1 second.

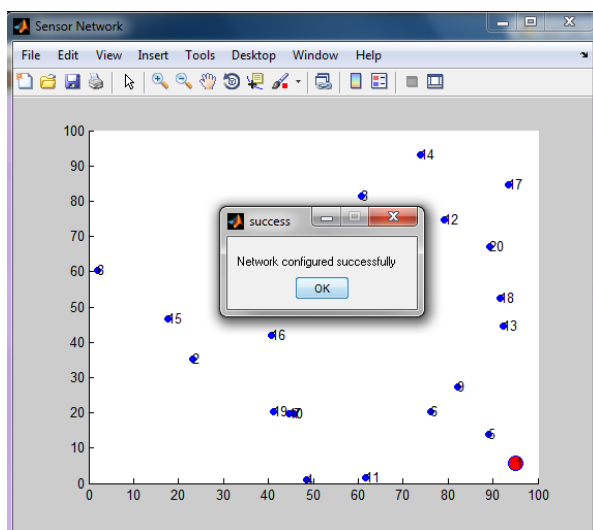
### b. Proposed Implementation

Implementation processes is shown as follows:

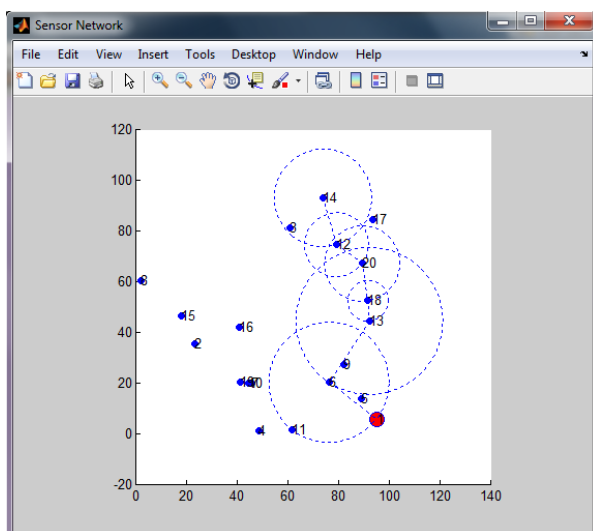
Open project in Matlab and run the project using command selfadaptive. The fig.1 shows the GUI architecture of proposed work i. e. channel switching latency in multi hop multi radio networks for OLSR. Provide the number of nodes as 20 (as per choice) and range of communication of each node as 30 (as per choice) and then press button create network. A wireless mesh network will be created with given number of nodes as shown in fig.2.



**Figure 1:** GUI for proposed work- channel switching latency in multi hop multi radio networks for OLSR



**Figure 2:** Network creation



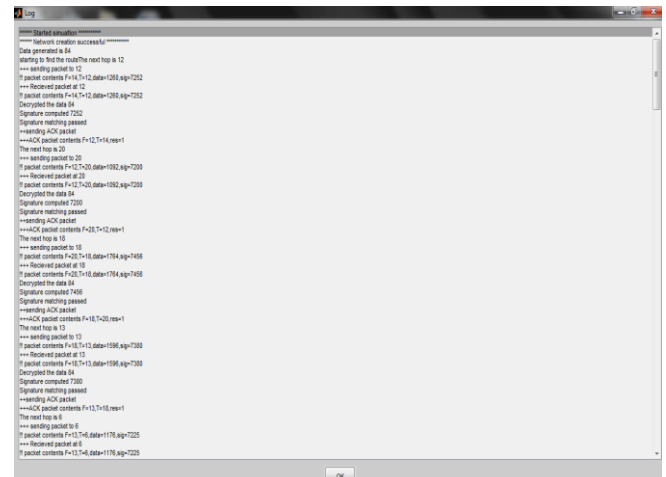
**Figure 3:** Route discovery process

In fig.2 a dialog box is showing with message “Network Configured successfully”. Press OK and a sensor network with 20 scattered nodes and 1 fixed destination node. After network creation we will choose the strategies among conventional and SDN to use routing protocol for route discovery. And after that the source node is provided to GUI as 14 provided here. In fig.3 conventional strategies is used to

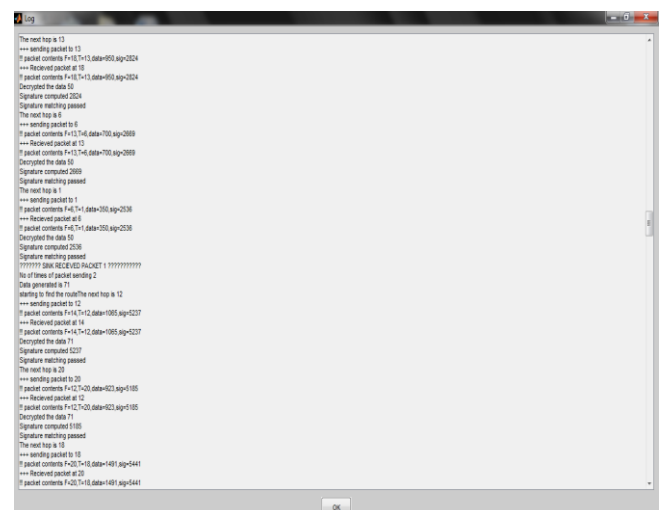
process the route discovery that shows the circle connections between multihop nodes and route from node 14 to node 1.

Route created is 14 – 12 – 20 – 18 – 13 – 6 – 1

The log file for conventional strategies is generated as shown in fig.4 with channel switching and security enhanced with AES procedure.



**Figure 4:** Route discovery logs for conventional strategies



**Figure 5:** Route discovery logs for SDN strategies

After that we will choose the strategies SDN use routing protocol for route discovery as provided source node 14.

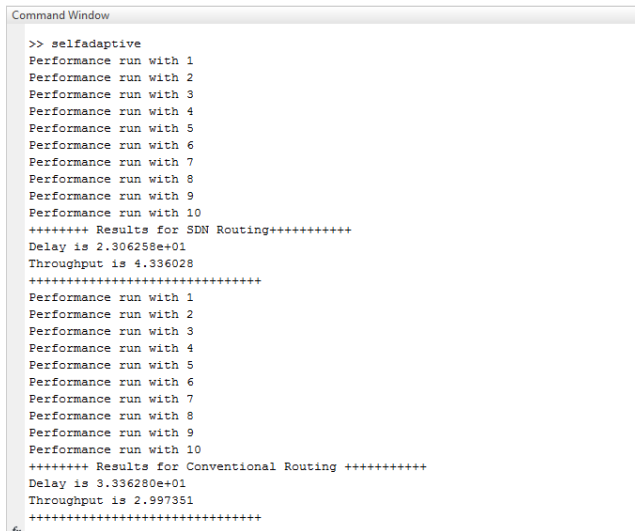
Route created is 14 – 12 – 20 – 18 – 13 – 6 – 1

The log file for SDN strategies is generated as shown in fig.5 with channel switching and security enhanced with AES procedure. In this multiple acknowledgement message will be generated for sink packets.

## 5. Simulation Results

Results of experimental work are shown below:

### Performance evaluation:



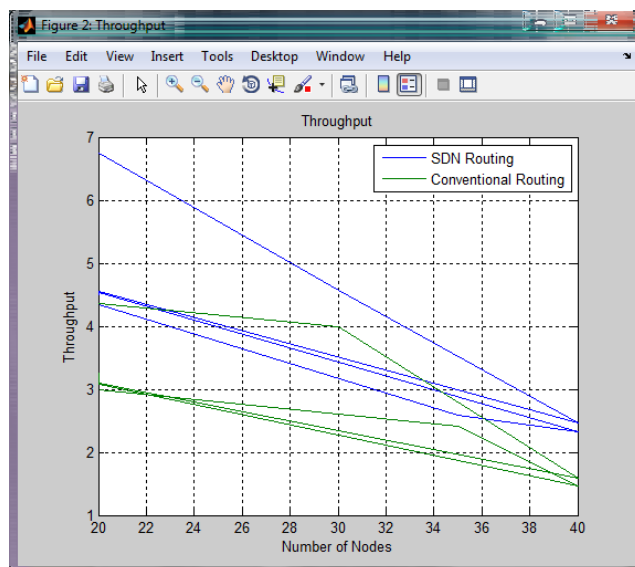
**Figure 6:** Performance evaluation methods for conventional and SDN approaches

In fig.6 performance evaluation methods are shown for both as conventional as well as SDN is described.

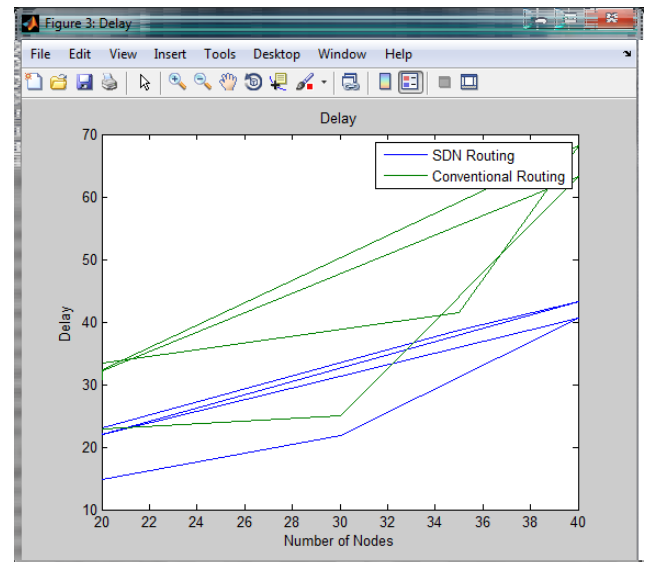
**Table 1:** Comparison results between conventional and SDN approach based on different parameters

Parameters	SDN	Conventional
Delay	2.306	3.336
Energy consumed	425	650
Throughput	4.33	2.997

Fig.7 shows the comparison graph for throughput between conventional and SDN approaches. Results depicts that the throughput value is better in SDN than conventional method.



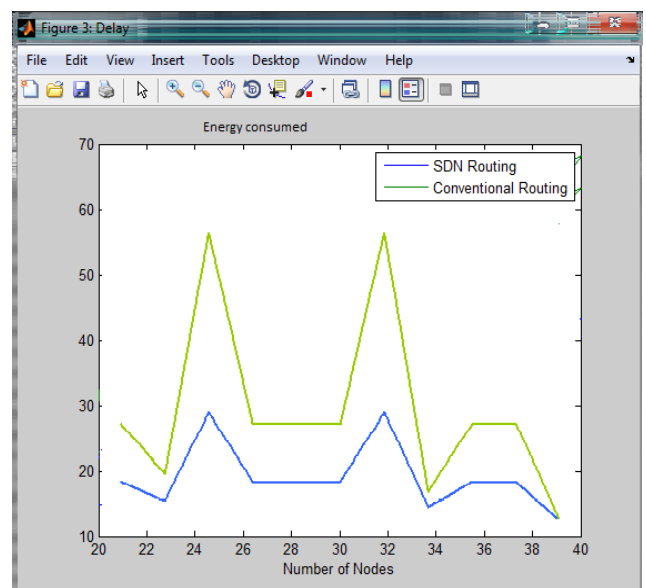
**Figure 7:** Comparison performance results for throughput between conventional and SDN approaches



**Figure 8:** Comparison performance results for delay between conventional and SDN approaches

Fig.8 shows the comparison graph for delay between conventional and SDN approaches. Results depicts that the delay value is less in SDN than conventional method.

Fig.9 shows the comparison graph for energy consumed between conventional and SDN approaches. Results depicts that the energy consumed is less in SDN than conventional method.



**Figure 9:** Comparison performance results for energy consumed between conventional and SDN approaches

## 6. Conclusion

In proposed SDN networks for OLSR protocol is used for establishing the reliable and stable routes for wireless sensor network. It uses the channel switching system with multi hop based and energy aware routing protocol for stable routes. Proposed approach provides the layer of encryption and decryption process to secure the packet while transmitting to destination node and this system uses the multi hop route forwarding algorithm to find the shortest path from source to destination. Proposed protocol with Advanced Encryption



Standard algorithm is a two key encryption process. When compared to the existing system our proposed system provides less energy consumed, better throughput and minimizes the delay of network. In future work give security to every packet, so that the gatecrashers can't ready to get or harm the parcels.

## References

- [1] T. Chen, O. Mehani and R. Boreli, "Trusted routing for VANET," in *Proc. International Conference on Intelligent Transport Systems Telecommunications*, October 20-22, 2009, pp. 647-652.
- [2] B. Yu and B. Xiao, "Detecting selective forwarding attacks in wireless sensor networks," in *Proc. International Symposium and Parallel and Distributed Processing*, April 25-29, 2006.
- [3] R. Shaikh, H. Jameel, and H. Lee, "Group-based trust management scheme for clustered wireless sensor networks," *IEEE transactions on Parallel and Distributed Systems*, vol. 20, no. 11, pp. 1698-1712, 2009.
- [4] M. Deno and T. Sun, "Probabilistic trust management in pervasive computing," in *Proc. International Conference on Embedded and Ubiquitous Computing*, 17-20 December 2008, vol. 2, pp. 610-615.
- [5] T. Raisinghani and S. Iyer, "Cross-layer design optimizations in wireless protocol stacks," *Computer Communications*, vol. 27, no. 4, pp. 213-217, 2006.
- [6] M. Satyanarayanan, "Mobile computing: The next decade," in *Proc. 1st ACM Workshop on Mobile Cloud Computing and Services: Social Networks and Beyond (MCS)*, 2010, pp. 5:1-5:6.
- [7] S. Khan *et al.*, "Cross-layer optimization for wireless video streaming performance and cost," presented at International Conference on Multimedia and Expo, Amsterdam, July 2005.
- [8] T. Zia, "Reputation-based trust management in wireless sensor networks," in *Proc. International Conference on Intelligent Sensors, Sensor Networks and Information Processing*, December 15-18, 2008, pp. 163-166.
- [9] A. Gohari and V. Rodoplu, "Congestion-aware spatial routing in hybrid high-mobility wireless multihop networks," *IEEE Transactions on Mobile Computing*, vol. 12, no. 11, pp. 2247-2260, 2013.
- [10] H. Luo, R. Ramjee, P. Sinha, L.E. Li, S. Lu, 2003 || UCAN: a unified cellular and ad-hoc network architecture —, in: *Proceedings of ACM MOBICOM'03*, San Diego, CA, USA, 14–19 September 2003, pp. 353–367.
- [11] C. Perkins, E. Belding-Royer, and S. Das, "Ad-hoc On-Demand Distance Vector (AODV) routing," *Mobile Adhoc Networking Working Group Internet draft*, vol. 5, no. 2, pp. 32-34, July 2003.
- [12] M. Mahmaudet *al.*, "Secure and reliable routing protocols for heterogeneous multihop wireless networks," *IEEE Transactions on Parallel and Distributed Systems*, pp. 1-11, 2013.
- [13] K. Rana and M. Zaveri, "Techniques for Efficient Routing in Wireless Sensor network," presented at International Conference on Intelligent Systems and Data Processing, 2011.
- [14] A. Abdelaziz, M. Nafaa, and G. Salim, "Survey of routing attacks and countermeasures in mobile Ad Hoc networks," in *Proc. 15<sup>th</sup> International Conference on Computer Modelling and Simulation (UKSim)*, 2013, pp. 693-698.